AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

R A P O R T A N U A L

2019

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

Bucureşti

CUVÂNT ÎNAINTE

Stimate Domnule Preşedinte al Senatului,

Stimaţi Senatori,

Anul 2019 a constituit o perioadă de consolidare a aplicării efective a noilor reglementări 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.

Am remarcat pe parcursul acestui an eforturile operatorilor din mediului public si privat de continuare a punerii în practică a regulilor de utilizare a datelor personale, concretizate în special în asigurarea informării persoanelor fizice, în respectarea efectivă a drepturilor persoanelor fizice (de acces, interventie, opozitie), în luarea măsurilor necesare pentru asigurarea confidențialității și securității prelucrărilor de date personale, inclusiv în mediul on-line.

De asemenea, am constatat respectarea, în cea mai mare parte, de către instituţiile publice şi entităţile private, a obligației de a-şi desemna o persoană responsabilă cu protecţia datelor, în situațiile stabilite expres prin prevederile art. 37 din Regulamentul General privind Protecția Datelor.

Considerăm 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.

Totodată, anul 2019 a reprezentat și perioada de asigurare a efectivității aplicării noilor reglementări naționale adoptate în anul 2018, respectiv a Legii nr. 129/2018, a Legii nr. 190/2018, a Legii nr. 363/2018 și a deciziilor cu caracter normativ adoptate de Autoritatea națională de supraveghere, în scopul sprijinirii operatorilor în respectarea noilor reglementări europene.

În același timp, raportat la obiectivele instituției noastre de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat, precum și de informare a publicului larg, subliniem că, în anul 2019, au continuat acțiunile de control, în condițiile în care s-a înregistrat o creștere cu peste 20% a numărului de plângeri față de anul anterior (5808 de plângeri în anul 2019 față de 4822 plângeri înregistrate în 2018). 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, transmiterea de date la biroul de credit, 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 2019, 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. Astfel, pe lângă organizarea anuală de către instituția noastră a evenimentelor prilejuite de Ziua Europeană a Protecției Datelor (pe 28 Ianuarie), am organizat cu prilejul unui an de la aplicarea Regulamentului European privind Protecția Datelor (24 Mai) și o dezbatere aniversară cu principalele asociații și uniuni profesionale ale operatorilor, ocazie cu care a fost lansat Ghidul privind întrebări și răspunsuri cu privire la aplicarea Regulamentului, pregătit de instituția noastră.

Totodată, în acest an s-a putut observa o creștere cu peste 30% a numărului de solicitări de puncte de vedere, precum și primirea spre avizare a 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.

Cu acest prilej, reliefăm și preocupările asociațiilor sau uniunilor profesionale de pregătire a unor coduri de conduită aplicabile operatorilor dintr-un anumit sector, în aplicarea art. 40 și 41 din Regulamentul General privind Protecția Datelor, pe care instituția noastră le-a analizat și față de care a emis recomandările necesare.

În considerarea acestor aspecte, evidențiem că, în anul 2019, am remarcat o creștere a responsabilității operatorilor în legătură cu prelucrările de date cu caracter personal efectuate, cu impact benefic în activitatea acestora de asigurare a unui nivel adecvat de protecție a datelor personale gestionate.

În același timp, raportat la obiectivele instituției noastre pentru acest an, putem aprecia că acestea 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, inclusiv în mediu digital;
- colaborarea cu toate instituțiile și entitățile, inclusiv cu societatea civilă, în vederea asigurării unei corecte aplicări a Regulamentului General privind Protecția Datelor și a legislației din domeniul protecției datelor.

În final, permiteți-mi să vă mulțumesc pentru sprijinul acordat instituției noastre și să-mi exprim, în același timp, speranța că vom beneficia de încrederea dumneavoastră în continuare, pentru edificarea unei adevărate culturi a protecției datelor cu caracter personal în România, în concordanță cu exigențele europene.

Ancuţa Gianina OPRE,

Preşedinte

CUPRINS

CAPITOLUL I
PREZENTARE GENERALĂ

Raportul de activitate pe anul 2019 al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe cinci capitole, după cum urmează:

Capitolul I reprezintă o prezentare sintetică a raportului pe principalele aspecte.

Capitolul al II-lea cuprinde informații relevante referitoare la activitatea de avizare a proiectelor de acte normative, precum şi la cea de autorizare şi de consiliere, în conformitate cu sarcinile și competențele stabilite de Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor).

Această activitate s-a concretizat în emiterea avizelor asupra unui număr însemnat de proiecte de acte normative şi a unui număr semnificativ de puncte de vedere. În acest sens, capitolul al II-lea sintetizează punctele de vedere relevante emise în activitatea de informare a persoanelor vizate în legătură cu exercitarea drepturilor lor în conformitate cu Regulamentul (UE) 2016/679, de consiliere prealabilă oferită operatorilor în cadrul evaluării de impact asupra protecţiei datelor, precum și cea oferită autorităților sau instituțiilor publice ori altor organisme, de analiză a conformității cu Regulamentul (UE) 2016/679 a proiectelor codurilor de conduită prezentate de diverse asociații profesionale ale operatorilor, dar și din activitatea de cooperare prin cu alte autorităţi de supraveghere pentru a se asigura coerenţa aplicării noilor reglementări europene.

În secţiunea privind reprezentarea în faţa instanţelor de judecată, sunt prezentate cele mai semnificative litigii finalizate pe parcursul anului 2019, în care a fost parte Autoritatea naţională de supraveghere, cu evidenţierea soluţiilor favorabile pronunţate.

Secţiunea privind informarea publică expune sintetic principalele modalităţi de popularizare a Regulamentului (UE) 2016/679, în cursul anului 2019, în limitele resurselor bugetare alocate.

Capitolul al III-lea conține o prezentare a principalelor aspecte din activitatea de monitorizare și control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite.

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

art. 33 alin. (1) din Regulamentul (UE) 2016/679, precum și ca urmare a sesizărilor transmise Autorității naționale de supraveghere.

În ceea ce privește incidentele de securitate, acestea au vizat, în principal, următoarele aspecte: dezvăluirea neautorizată a datelor cu caracter personal; pierderea trimiterilor poștale; indisponibilitatea datelor cu caracter personal; accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV); accesul ilegal la datele personale ale clienților în sistemul bancar.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri semnificative a numărului acestora, în anul 2019 au continuat să fie sesizate, în principal, aspecte referitoare la: dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate, încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/679, transmiterea de date la biroul de credit, 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, respectiv neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor efectuate.

De asemenea, capitolul al III-lea prezintă măsurile corective dispuse în urma investigațiilor, inclusiv sancțiunile cu avertisment și amendă aplicate, dar și o serie de fișe de caz în care au fost prezentate cele mai relevante situații verificate.

În cadrul investigaţiilor efectuate în anul 2019, au fost aplicate sancţiuni contravenţionale constând în avertismente şi amenzi în cuantum total de 2.339.291,75 lei.

Capitolul al IV-lea prezintă activitatea de relaţii externe a Autorităţii naţionale de supraveghere, sintetizând diferitele documente adoptate la nivelul UE, cum ar fi orientări, ghiduri, avize, declarații, dar și informații privind transferul datelor în temeiul regulilor corporatiste obligatorii (BCR).

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

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

CAPITOLUL II

ACTIVITATEA DE AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

Secțiunea 1: Avizarea actelor normative

În anul 2019, Autoritatea naţională de supraveghere a emis avize asupra unui număr de **53 de proiecte de acte normative** elaborate de instituţii şi autorităţi publice care implicau aspecte complexe privind prelucrarea datelor cu caracter personal, în baza atribuțiilor prevăzute de art. 57 alin. (1) lit. c) din Regulamentul (UE) 2016/679.

Astfel, proiectele au fost transmise de către unele ministere, precum Ministerul Afacerilor Interne, Ministerul Muncii și Justiției Sociale, Ministerul Turismului, Ministerul Justiției, dar și de către alte autorități sau instituții publice, cum ar fi Autoritatea Electorală Permanentă, Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor, Agenția Națională a Funcționarilor Publici.

În același timp, Ministerul pentru Relația cu Parlamentul a solicitat punctul de vedere al Autorității naţionale de supraveghere cu privire la diferite propuneri legislative promovate de senatori și deputați.

Pentru majoritatea proiectelor, Autoritatea naţională de supraveghere a apreciat că este necesară completarea/modificarea textelor respective, fiind efectuate o serie de observații și propuneri, ținând cont de necesitatea armonizării unor dispoziții din proiectele respective cu principiile și condițiile de prelucrare a datelor cu caracter personal.

În continuare, evidențiem cele mai importante dintre acestea, astfel:

●**Agenția Națională a Funcționarilor Publici a transmis Autorității naționale de supraveghere, în vederea exprimării unui punct de vedere,** ***proiectul de Hotărâre a Guvernului pentru modificarea și completarea Hotărârii Guvernului nr. 611/2008 pentru aprobarea normelor privind organizarea și dezvoltarea carierei funcționarilor publici, precum și asupra proiectului de Hotărâre a Guvernului pentru modificarea și completarea Hotărârii Guvernului nr. 341/2007 privind intrarea în categoria înalților funcționari publici, managementul carierei și mobilitatea înalților funcționari publici.***

În urma analizării acestor proiecte, a rezultat faptul că sunt necesare o serie de modificări și completări, ținând cont de principiul reducerii la minimum a datelor statuat de art. 5 din Regulamentul (UE) 2016/679, dar și de asigurarea securității acestora, raportat la modalitatea de depunere a unor copii ale documentelor ce conțin date personale, prin mijloace de comunicare electronică.

De asemenea, s-a recomandat reanalizarea mențiunilor referitoare la situațiile în care se solicită consimțământul persoanei în cauză în contextul organizării și desfășurării unui concurs în sectorul public, respectiv dacă consimțământul este temeiul legal adecvat pentru prelucrarea avută în vedere sau trebuie identificat un alt temei legal, cum ar fi, de exemplu, îndeplinirea unei obligații legale.

● **Ministerul Afacerilor Interne a transmis *proiectul de Ordonanță a Guvernului pentru modificarea şi completarea Ordonanţei Guvernului nr. 83/2001 privind înfiinţarea, organizarea şi funcţionarea serviciilor publice comunitare pentru eliberarea şi evidenţa paşapoartelor simple şi serviciilor publice comunitare regim permise de conducere şi înmatriculare a vehiculelor.***

Față de textul acestui proiect, Autoritatea națională de supraveghere a recomandat reanalizarea sa sub aspectul datelor și categoriilor de date prelucrate, precum și în ceea ce privește dezvăluirea acestora către destinatari, prin raportare la principiile statuate de art. 5 din Regulamentul (UE) 2016/679, precum și sub aspectul legalității prelucrării, prin raportare la situațiile stabilite de art. 6 alin. (1) din Regulamentul (UE) 2016/679, acordând atenție faptului că interesul legitim nu se aplică în cazul prelucrării efectuate de autoritățile publice în îndeplinirea atribuţiilor lor.

● **Ministerul pentru Relaţia cu Parlamentul a transmis *propunerea legislativă pentru modificarea și completarea Legii nr. 272/2004 privind protecția și promovarea drepturilor copiilor, republicată - Bp. 524/2019*.**

Având în vedere conținutul propunerii legislative supuse analizei, Autoritatea națională de supraveghere a recomandat stabilirea unei modalități alternative de accesare a informațiilor de către părinții biologici, astfel cum se prevede și în expunerea de motive, ținând cont de asigurarea confidențialității datelor personale și de principiul responsabilității operatorului, stabilite de Regulamentul (UE) 2016/679.

De asemenea, sub aspectul temeiului legal al dezvăluirii datelor persoanei sau ale familiei de plasament către părinții biologici, s-a subliniat faptul că dispozițiile art. 6, 9 și 10 din Regulamentul (UE) 2016/679 stabilesc condițiile în care datele pot fi prelucrate (inclusiv dezvăluite) în funcție de natura acestora (date speciale și cele care nu fac parte din această categorie).

● **Ministerul Muncii și Justiției Sociale a transmis *proiectul Legii pentru modificarea și completarea unor acte normative*.**

Faţă de conținutul textului proiectului sus-menționat, s-a atras atenția asupra dispozițiilor art. 29 din Regulamentul (UE) 2016/679, având în vedere că reprezentantul persoanei cu handicap are calitatea de persoană care acţionează sub autoritatea operatorului, întrucât încheie un contract de muncă cu Consiliul de monitorizare.

De asemenea, reprezentantul persoanei are acces și prelucrează date cu caracter personal, inclusiv din categoria celor speciale, cum sunt datele privind starea de sănătate, motiv pentru care este necesar să se prevadă și obligația reprezentantului personal de a respecta confidențialitatea și securitatea datelor cu caracter personal de care ia cunoștință în exercitarea atribuțiilor sale.

● **Ministerul pentru Relaţia cu Parlamentul a solicitat punctul de vedere al Autorității naționale de supraveghere referitor la *propunerea legislativă privind abrogarea art. 6 și 9 din Legea nr. 190/2018 privind unele măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor)* – Bp. 438/2019.**

Față de această propunere legislativă, raportat la argumentele formulate în Expunerea de motive și textul actului normativ, Autoritatea națională de supraveghere a susținut propunerea, recomandând și analizarea necesității abrogării art. 2 alin. (1) lit. f) din Legea nr. 190/2018, motivat de corelația dintre acest text și cele două articole propuse a fi abrogate.

În ceea ce privește art. 6 din Legea nr. 190/2018, acesta se referă la *date personale şi speciale*, terminologie inadecvată prin raportare la art. 4 pct. 1 din Regulamentul (UE) 2016/679 și instituie doar trei categorii de garanții în condițiile în care se prelucrează date speciale care necesită protecție adecvată și care se prelucrează numai potrivit art. 9 din Regulamentul (UE) 2016/679.

De asemenea, raportat la dispozițiile Regulamentului (UE) 2016/679, ipoteza reglementată la art. 9 din Legea nr. 190/2018 referitoare la prelucrarea unor date cu caracter special de către partidele politice, organizaţiile cetăţenilor aparţinând minorităţilor naţionale și organizaţiile neguvernamentale, fără consimțământul expres al persoanei vizate nu se regăsește în sfera condițiilor de legalitate vizate de art. 6 și 9 din Regulamentul (UE) 2016/679 coroborat cu mențiunile din considerentele (45), (47) și (56) ale aceluiași regulament.

● **Ministerul Afacerilor Interne a solicitat un punct de vedere cu privire la *proiectul de Hotărâre a Guvernului privind stabilirea bazelor de date relevante pentru compararea datelor din registrul cu numele pasagerilor*.**

Având în vedere conținutul proiectului supus analizei, Autoritatea națională de supraveghere a atras atenția asupra completării, în mod corespunzător, a Notei de fundamentare cu argumente privind relevanța și/sau necesitatea accesării de către Unitatea națională de informații privind pasagerii din cadrul IGPF a tuturor bazelor de date enumerate în articolul unic al proiectului.

Totodată, raportat la dispozițiile art. 6 alin. (3) din Directiva (UE) 2016/681 și prevederile art. 20 alin. (2) al Legii nr. 284/2018, precum și în contextul lipsei de motivare din Nota de fundamentare, Autoritatea națională de supraveghere și-a exprimat rezerve față de accesarea bazei de date menționate la lit. g) din proiect și, în special, a celei prevăzute la lit. i) din proiect, respectiv RECOM online, gestionat de Oficiul Național al Registrului Comerțului.

Proiectul a fost retransmis de Ministerul Afacerilor Interne, cu modificări și completări, potrivit recomandărilor Autorității naţionale de supraveghere.

● **Ministerul pentru Relaţia cu Parlamentul a solicitat un punct de vedere cu privire la *propunerea legislativă privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice* (Bp. 363/2019, Plx. 181/2019)** prin care se dorește transpunerea în legislația națională a prevederilor Regulamentului 910/2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.

În scopul asigurării respectării Regulamentului (UE) 2016/679, raportat la conținutul propunerii legislative supuse analizei, s-au formulat mai multe observații, apreciindu-se că propunerea de act normativ trebuie să se supună normelor aplicabile domeniului protecției datelor și să respecte principiile stabilite prin Regulamentul (UE) 2016/679, având în vedere considerentul (11) al Regulamentului nr. 910/2014, în care se prevede că: *”Prezentul regulament ar trebui aplicat în deplină concordanţă cu principiile referitoare la protecţia datelor cu caracter personal prevăzute*

de Directiva 95/46/CE a Parlamentului European şi a Consiliului. În această privinţă, având în vedere principiul recunoaşterii reciproce instituit de prezentul regulament, autentificarea pentru un serviciu online ar trebui să vizeze numai prelucrarea acelor date de identificare care sunt adecvate şi relevante şi care nu sunt excesive în vederea acordării accesului la respectivul serviciu online. Mai mult, cerinţele prevăzute în Directiva 95/46/CE privind confidenţialitatea şi securitatea prelucrării ar trebui să fie respectate de către prestatorii de servicii de încredere şi de către organismele de supraveghere."

Prin urmare, Autoritatea națională de supraveghere a propus inserarea unor prevederi referitoare la faptul că sistemul de evidență care va asigura colectarea, înregistrarea și stocarea datelor personale, în contextul creării unui nou Registru automatizat care va conține și date cu caracter personal, trebuie să fie constituit în concordanță cu principiile stabilite de Regulamentul (UE) 2016/679, să asigure și să respecte standarde de securitate şi de confidenţialitate adecvate pentru protejarea datelor, astfel încât să nu fie afectate drepturile fundamentale ale persoanelor.

● **Autoritatea Aeronautică Civilă Română a solicitat un punct de vedere cu privire la *proiectul Programului Național de Securitate Aeronautică – PNSA*.**

Având în vedere conținutul documentului transmis spre analiză, Autoritatea națională de supraveghere a precizat următoarele:

În contextul dat, s-a subliniat că, prin raportare la prevederile punctului 14.3.2. litera c. - "Cadrul de cooperare" din proiectul Anexei 1 - Capitolul 14 – Securitate Cibernetică – PNSA, pe de o parte Autoritatea națională de supraveghere are, potrivit dispozițiilor art. 57-58 din Regulamentul (UE) 2016/679, atribuții de **monitorizare şi control** al prelucrărilor de date cu caracter personal efectuate de diverse entități publice sau private, în calitatea acestora de operatori de date, iar pe de altă parte, potrivit art. 16 lit. c) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, *CERT-RO se consultă şi cooperează, după caz, cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal în cazul incidentelor care au ca rezultat încălcarea securităţii datelor cu caracter personal, în condiţiile legii."*

Ca atare, raportat la atribuțiile Autorității naționale de supraveghere, s-a propus eliminarea precizărilor de la punctul 14.3.2. litera c) din proiect.

● **Ministerul Afacerilor Interne a solicitat formularea unui punct de vedere cu privire la *proiectul de Ordonanță de Urgență a Guvernului privind măsuri de punere în aplicare a Regulamentului (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieşire (EES) pentru înregistrarea datelor de intrare şi de ieşire şi a datelor referitoare la refuzul intrării ale resortisanţilor ţărilor terţe care trec frontierele externe ale statelor membre, de stabilire a condiţiilor de acces la EES în scopul aplicării legii şi de modificare a Convenţiei de punere în aplicare a Acordului Schengen şi a Regulamentelor (CE) nr. 767/2008 şi (UE) nr. 1077/2011.***

Având în vedere textul proiectului de Ordonanță de Urgență a Guvernului, Autoritatea națională de supraveghere a formulat, în principal, următoarele observații și propuneri:

Cu privire la dispozițiile art. 12 din proiect, s-a subliniat că este necesară notificarea Autorității naționale de supraveghere în cazul unei încălcări a securității datelor, în concordanță cu prevederile art. 33 din Regulamentul (UE) 2016/679, respectiv ale art. 36 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 care transpune în legislația națională Directiva (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, cu respectarea termenului stabilit de aceste acte normative.

S-a apreciat ca necesară reformularea alin. (2) al art. 13 din proiect, raportat la sarcinile și competențele Autorității naționale de supraveghere prevăzute de Regulamentul (UE) 2016/679, Legea nr. 190/2018 și Legea nr. 363/2018 și Regulamentul (UE) 2017/2226.

S-a considerat necesară modificarea alin. (3) al art. 13 din proiect în sensul că Autoritatea națională de supraveghere realizează cel puțin odată la trei ani un audit al operațiunilor de prelucrare a datelor, la nivelul EES, respectiv în infrastructura națională de frontieră, în concordanță cu art. 55 alin. (2) din Regulamentul (UE) 2017/2226.

Raportat la obligațiile statelor membre prevăzute de art. 55 alin. (3) din Regulamentul (UE) 2017/2226, s-a apreciat ca necesară introducerea unui nou articol, care să stabilească faptul că „sumele și resursele necesare pentru realizarea atribuţiilor prevăzute la art. 55 din Regulamentul

(UE) 2017/2226, inclusiv pentru auditarea Sistemului EES, se suportă de la bugetul de stat şi sunt prevăzute anual, cu această destinație, în bugetul Autorității naționale de supraveghere."

În ceea ce privește dispozițiile art. 14 din proiect, s-a subliniat faptul că este necesară modificarea acestui articol cu o trimitere la regimul sancționator, așa cum este acesta prevăzut de Legea nr. 190/2018, care reglementează măsurile corective şi sancţiunile în domeniul protecției datelor în cazul autorităţilor şi organismelor publice**.**

● **Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor a transmis *informarea privind asumarea transpunerii Directivei (UE) 843/2018 a Parlamentului European şi a Consiliului din 30 mai 2018 de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanţării terorismului, precum şi de modificare a Directivelor 2009/138/CE şi 2013/36/UE.***

Autoritatea națională de supraveghere a transmis și în cursul anului 2018 observații și propuneri cu privire la proiectul de *Lege pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative*.

Ca atare, față de acest proiect, s-a recomandat Oficiului Naţional de Prevenire şi Combatere a Spălării Banilor să aibă în vedere recomandările efectuate de Autoritatea națională de supraveghere, în sensul aplicării principiilor de prelucrare a datelor ("legalitate, echitate şi transparenţă", "limitări legate de scop", "reducerea la minimum a datelor", "exactitate", "limitări legate de stocare", precum și "integritate şi confidenţialitate") pe care operatorii de date cu caracter personal, respectiv autoritățile competente, au obligația să le respecte potrivit Regulamentului (UE) 2016/679.

● **Ministerul Afacerilor Interne a supus atenției Autorității naționale de supraveghere proiectul de text al *Acordului între Guvernul României și Guvernul Republicii Populare Chineze privind cooperarea în prevenirea și combaterea terorismului, a criminalității organizate și a altor infracțiuni grave*.**

Faţă de conținutul documentului transmis, s-au precizat, în principal, următoarele:

- necesitatea stabilirii autorităților competente cu aplicarea acordului din partea Guvernului Republicii Populare Chineze, având în vedere că fiecare dintre operatorii de date cu caracter personal desemnați de către Părțile semnatare ca "autorități competente" este responsabil de respectarea prevederilor legale în materia protecției datelor

- necesitatea stabilirii unui mecanism prin care România va aplica dispozițiile Directivei (UE) 2016/680, care instituie interdicția transmiterii de date cu caracter personal către state terțe

dacă datele urmează să fie folosite pentru a se solicita, pronunța sau executa pedeapsa cu moartea sau orice formă de tratament crud sau inuman; s-a considerat că simpla mențiune din acest alineat al proiectului supus atenției cu privire la neefectuarea transferului în ”lipsa unor garanții suficiente” nu răspunde exigențelor dispozițiilor art. 37 și art. 39 din Directiva (UE) 2016/680, raportat la considerentul (71) din aceeași Directivă

- reevaluarea tuturor celorlalte Acorduri cu state terțe, semnate deja de România sau aflate în curs de negociere, raportat la eventualitatea ca datele să fie folosite pentru a se solicita, pronunța sau executa pedeapsa cu moartea sau orice formă de tratament crud sau inuman

- stabilirea, ca regulă, a interzicerii prelucrării unor astfel de date și prelucrarea lor numai în situațiile de excepție menționate.

În contextul celor de mai sus, s-a reiterat, în considerarea dispozițiilor art. 37 și art. 39 din Directiva (UE) 2016/680, raportat la considerentul (71) din același act normativ, necesitatea stabilirii unui mecanism concret prin care România va aplica dispozițiile Directivei, care să instituie interdicția transmiterii de date cu caracter personal către state terțe dacă datele urmează să fie folosite pentru a se solicita, pronunța sau executa pedeapsa cu moartea sau orice formă de tratament crud sau inuman.

●**Ministerul Justiției a solicitat un punct de vedere cu privire la *proiectul de Ordin al ministrului justiției pentru aprobarea Sistemului de evidență a datelor pentru personalul din sistemul administrației penitenciare.***

Față de prevederile proiectului transmis, s-a subliniat că activităţile desfăşurate în legătură cu crearea unui *Sistem de evidență a datelor pentru personalul din sistemul administrației penitenciare* referitor la funcționarii publici cu statut special și personalul civil din sistemul administrației penitenciare, inclusiv ale rudelor până la gradul II, ale rudelor și rudelor prin alianță până la gradul IV ale personalului din sistemul administrației penitenciare, presupun efectuarea a numeroase operațiuni de prelucrare a datelor cu caracter personal (colectarea, înregistrarea, organizarea, stocarea, extragerea, consultarea, utilizarea, dezvăluirea către terţi prin transmitere, diseminare sau în orice alt mod etc.), cu precădere a datelor speciale, realizându-se o prelucrare pe scară largă a acestora.

În acest context, Autoritatea națională de supraveghere a subliniat necesitatea luării în considerare a dispozițiilor art. 5, 6 și 9, coroborate cu art. 24 și 25 din Regulamentul (UE) 2016/679.

În vederea respectării principiului minimizării, Autoritatea națională de supraveghere a propus reanalizarea necesității prelucrării tuturor datelor referitoare la rudele până la gradul II, rudele (inclusiv cele prin alianță) până la gradul IV ale personalului din sistemul administrației penitenciare.

Prin urmare, *Sistemul de evidență a datelor pentru personalul din sistemul administrației penitenciare* care va asigura colectarea, înregistrarea și stocarea datelor personale trebuie să fie constituit încă de la început în concordanță cu principiile stabilite de Regulamentul (UE) 2016/679, să asigure și să respecte standarde de securitate și de confidenţialitate adecvate pentru protejarea datelor astfel încât să nu fie afectate drepturile fundamentale ale persoanelor.

Ca atare, Autoritatea națională de supraveghere a recomandat reanalizarea propunerii de act normativ, sub aspectul observațiilor formulate.

●**Ministerul Agriculturii și Dezvoltării Rurale a solicitat un punct de vedere privind *proiectul de Hotărâre privind registrul agricol pentru perioada 2020-2024.***

Față de textul proiectului, s-au formulat următoarele observații și propuneri:

În contextul gestionării de către Agenţia Naţională de Cadastru şi Publicitate Imobiliară a registrului agricol naţional (RAN), ce cuprinde în format electronic registrele agricole de la nivelul unităţilor administrativ-teritoriale, se remarcă faptul că prelucrarea datelor personale este efectuată de mai multe entități, care pot avea calitatea de operatori de date, operatori asociați sau împuterniciți ai operatorilor.

Autoritatea națională de supraveghere a recomandat, față de cele de mai sus, inserarea în textul proiectului hotărârii, a unui nou articol care să prevadă faptul că toate entitățile implicate în completarea și păstrarea registrelor agricole (cel național, respectiv cele de la nivelul unităţilor administrativ-teritoriale) prelucrează date cu caracter personal cu respectarea prevederilor Regulamentului (UE) 2016/679 și legislației naționale de aplicare a acestuia.

De asemenea, s-a subliniat responsabilitatea operatorului potrivit art. 24 din Regulamentul (UE) 2016/679, precum și prevederile art. 25 din Regulamentul (UE) 2016/679 care stabilesc asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit, respectiv asigurarea principiilor *privacy by design* și *privacy by default*. În acest sens, având în vedere faptul că pentru completarea registrelor menționate se utilizează mijloace automatizate de prelucrare a datelor, respectiv aplicații informatice, iar potrivit art. 1 alin. (7) din Ordonanţa nr. 28/2008 privind registrul agricol, cu modificările și completările ulterioare, începând cu data de 1 ianuarie 2018

registrul agricol se întocmeşte şi se ţine la zi în format electronic, trebuie avută în vedere și respectarea acestor principii.

●**Autoritatea naţională de supraveghere și-a exprimat punctul de vedere cu privire la conținutul *Propunerii legislative pentru modificarea şi completarea Legii educaţiei naţionale nr. 1/2011 - Pl-x nr. 236/2019.***

În contextul aplicării în mod direct, începând din data de 25 mai 2018, a prevederilor Regulamentului (UE) 2016/679, și având în vedere faptul că prin propunerea legislativă menționată se intenționează prelucrarea de date cu caracter personal ale minorilor (imagine, voce) prin introducerea obligatorie de camere de supraveghere video și audio în unități care oferă servicii de educație timpurie și funcționează în regim de creșă, unitate antepreșcolară și preșcolară din mediul privat sau de stat (unități educaționale), Autoritatea națională de supraveghere a subliniat, în principal, următoarele:

Raportat la art. 4 pct. 1 din Regulamentul (UE) 2016/679, în categoria datelor cu caracter personal intră și cele vizate de propunerea legislativă în discuție, respectiv imagine și voce, ce ar urma să fie prelucrate de unitățile educaționale.

Regulamentul (UE) 2016/679 creează un nivel suplimentar de protecție în cazul în care sunt prelucrate datele cu caracter personal ale persoanelor fizice vulnerabile, în special ale copiilor, prin considerentele (38) și (75), întrucât c*opiii au nevoie de o protecţie specifică a datelor lor cu caracter personal, deoarece pot fi mai puţin conştienţi de riscurile, consecinţele, garanţiile în cauză şi drepturile lor în ceea ce priveşte prelucrarea datelor cu caracter personal.*

Prin urmare, **întrucât sistemele de supraveghere video comportă anumite riscuri în privinţa drepturilor şi libertăţilor persoanelor care sunt supravegheate, înainte de instalarea unor astfel de sisteme de supraveghere, s-a subliniat că operatorul trebuie să facă în prealabil o *evaluare a riscurilor la care se supune activitatea sa* pentru a stabili necesitatea implementării lor, în special în cazul minorilor și al angajaților** (cadre didactice și personal auxiliar angajat în unitățile educaționale unde ar urma să fie instalate astfel de sisteme.)

În același context, s-a precizat că a fost adoptată și **Recomandarea (2015)5 a Consiliului Europei referitoare la protecția datelor în contextul angajării**, care conține principiile pe care statele membre ale Uniunii Europene ar trebui să le urmeze în legislaţiile naţionale privind prelucrarea datelor cu caracter personal ale angajaților, de exemplu, în ceea ce privește monitorizarea la locul de muncă.

Această Recomandare prevede că angajatorii ar trebui să evite orice amestec nejustificat și nerezonabil în dreptul angajaţilor la viața privată la locul de muncă, aceasta fiind aplicabilă pentru toate dispozitivele de tehnologie informațională.

Astfel, punctul 15 al Recomandării prevede că *„introducerea și utilizarea sistemelor informatice și tehnologiilor în scopul direct și principal de a monitoriza activitatea și comportamentul angajaților nu ar prebui permisă.”*

De asemenea, Recomandarea se referă la o serie de garanții ce trebuie implementate pentru a se asigura faptul că datele cu caracter personal ale angajaţilor sunt protejate în mod corespunzător.

În plus, în același document se precizează că *”Sistemele informatice și tehnologiile care indirect monitorizează activitatea și comportamentul angajaților ar trebui să fie proiectate în mod special și localizate astfel încât să nu încalce drepturile fundamentale ale acestora. Utilizarea supravegherii video pentru monitorizarea locației în care angajații își desfășoară cea mai mare parte din activitate nu este permisă în nicio situație.”*

De asemenea, Autoritatea națională de supraveghere a recomandat să fie avute în vedere și prevederile art. 6, 27, 28, 37 și 52 din Legea nr. 272/2004 privind protecţia şi promovarea drepturilor copilului, republicată.

Prin urmare, **Autoritatea națională de supraveghere a comunicat Ministerului pentru Relaţia cu Parlamentul că nu susține *propunerea legislativă pentru modificarea şi completarea Legii educaţiei naţionale nr. 1/2011 - Pl-x nr. 236/2019.***

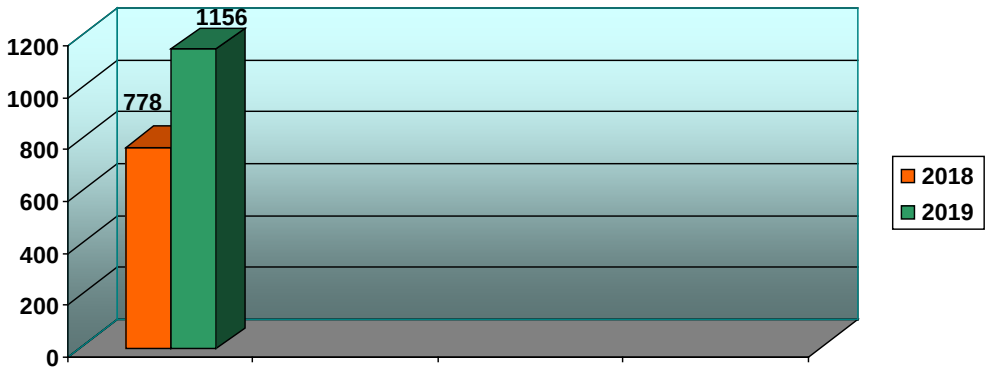
Secțiunea a 2 – a:
Puncte de vedere privind diverse chestiuni de protecţia datelor

Potrivit Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere are competenţe de autorizare şi de consiliere, sens în care emite avize cu privire la conformitatea cu Regulamentul (UE) 2016/679 a proiectelor codurilor de conduită şi le aprobă în cazul în care se constată că acestea oferă garanţii adecvate suficiente, furnizează informaţii oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu Regulamentul (UE) 2016/679, cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă asistenţă reciprocă pentru a asigura coerenţa aplicării şi respectării Regulamentului (UE) 2016/679, oferă consiliere prealabilă operatorului înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor indică

faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului, dar și autorităților sau instituțiilor publice ori altor organisme.

Raportat la aceste competențe, Autoritatea națională de supraveghere a emis în anul 2019 un număr total de **1156 de puncte de vedere**.

Față de anul 2018, când au fost emise 778 de puncte de vedere, în acest an se poate observa o creștere semnificativă a numărului de solicitări (peste 30%), ceea ce relevă interesul crescut al celor operatorilor și împuterniciților în asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 2016/679 și de legislația națională conexă.



<u>Unele dintre cazurile semnificative supuse atenției Autorității naționale de supraveghere sunt prezentate în continuare, astfel</u>:

♦ În mai multe situații, s-a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la prelucrarea codului numeric personal de către unitățile de cazare.

Referitor 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, aceasta se realizează cu consimțământul persoanei vizate sau în condițiile de excepție de la consimțământ, prevăzute de art. 6, art. 9 și art. 10 în funcție de natura datelor și categoriilor de date colectate și prelucrate.

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 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) 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.

(2) Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul general privind protecţia datelor, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă, se efectuează cu instituirea de către operator a următoarelor garanţii:

a) punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul general privind protecţia datelor;

b) numirea unui responsabil pentru protecţia datelor, în conformitate cu prevederile art. 10 din prezenta lege;

c) stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;

d) instruirea periodică cu privire la obligaţiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.”

Astfel, 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 enumerate. În acest sens, în măsura în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau există o obligație legală pentru prelucrarea datelor ori în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, datele pot fi prelucrate fără consimțământul persoanei vizate.

În ceea ce privește existența unei obligații legale, Autoritatea națională de supraveghere a precizat faptul că, potrivit *Normelor din 8 februarie 2001 cu privire la accesul, evidenţa şi protecţia turiştilor în structuri de primire turistice, aprobate prin Hotărârea Guvernului nr. 237/2001, republicată*, completarea fişelor se face de către fiecare turist în momentul sosirii, pe baza actelor de identitate (buletinul/cartea de identitate, paşaportul etc.).

Totodată, potrivit art. 2 alin. (6) din normele sus-menţionate *„fişele de anunţare a sosirii şi plecării, completate şi semnate de turiştii cazaţi, se preiau, împreună cu actele de identitate, de*

către recepţioneri, care sunt obligaţi să confrunte datele din fişe cu cele din actul de identitate, să semneze fişele pentru confirmarea completării corecte a acestora şi să restituie imediat actele de identitate turiştilor."

Sub aspectul informării persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe bază de excepții), 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. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic.

Art. 13 din Regulamentul (UE) 2016/679 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.

Prin urmare, Autoritatea națională de supraveghere a subliniat faptul că, pentru asigurarea principiului transparenței, este necesară realizarea informării persoanelor vizate, în speță, a turiștilor.

De asemenea, Autoritatea națională de supraveghere a precizat faptul că art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor. Printre acestea, se numără cel privind prelucrarea datelor adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (principiul proporționalității), păstrarea datelor într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele (principiul limitării legate de stocare) și prelucrarea datelor într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

Aceleași dispoziții legale sus-menționate prevăd faptul că operatorul este responsabil de respectarea acestor principii şi poate demonstra această respectare (principiul responsabilității).

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

măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar."

Totodată, s-a precizat că, potrivit prevederilor Regulamentului (UE) 2016/679, persoana vizată beneficiază de o serie de drepturi menționate în cadrul art. 12-23 din Regulament.

♦ O persoană fizică a solicitat un punct de vedere cu privire la condițiile în care se pot face dezvăluiri de date din Registrul Național de Evidență a Persoanelor (R.N.E.P.) gestionat de D.E.P.A.B.D.

Autoritatea națională de supraveghere a precizat că Regulamentul (UE) 2016/679 conține în art. 6 reglementări privind legalitatea prelucrărilor de date care nu au un caracter special.

Unele dintre acestea vizează prelucrarea necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului sau prelucrarea necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul.

Dispozițiile art. 11 din O.U.G. nr. 97/2005 privind evidenţa, domiciliul, reşedinţa şi actele de identitate ale cetăţenilor români, republicată, cu modificările și completările ulterioare, stabilesc condițiile de furnizare a datelor, astfel:

"(1) Furnizarea sau verificarea unor date cu caracter personal din R.N.E.P. se face la cererea persoanelor fizice sau a persoanelor juridice, în condiţiile stabilite de lege.

(2) Furnizarea sau verificarea unor date cu caracter personal din R.N.E.P. se face în condiţiile stabilite de lege, în cadrul unor acţiuni de interes public sau în vederea îndeplinirii unor obligaţii legale, cu plata corespunzătoare a taxelor prevăzute de lege, în baza unui contract încheiat între Ministerul Administraţiei şi Internelor, prin D.E.P.A.B.D., şi beneficiar.

(4) În situaţia prevăzută la alin. (3), furnizarea sau verificarea unor date cu caracter personal se face în baza unui protocol încheiat între Ministerul Administraţiei şi Internelor, prin D.E.P.A.B.D., şi persoanele juridice enumerate.

(5) Contractul prevăzut la alin. (2) şi protocolul prevăzut la alin. (4) trebuie să conţină în mod obligatoriu destinaţia datelor, volumul şi structura acestora, suportul pe care se livrează şi măsurile de protecţie şi securitate a datelor prevăzute de lege.

(6) Furnizarea sau verificarea unor date cu caracter personal din R.N.E.P. se realizează de:

a) D.E.P.A.B.D. sau de structurile sale teritoriale, la solicitarea scrisă adresată acestora;

b) serviciile publice comunitare de evidenţă a persoanelor, la solicitarea scrisă adresată acestora de către autorităţile publice locale sau de către persoanele fizice şi juridice în condiţiile prevăzute de lege."

De asemenea, art. 10 din actul normativ menționat anterior prevede că:

"(1) Datele cu caracter personal ale persoanelor fizice sunt protejate de legea specială şi nu pot fi prelucrate decât în condiţiile prevăzute de aceasta.

(2) Beneficiarii datelor cu caracter personal furnizate din R.N.E.P. sunt obligaţi să utilizeze aceste date numai pentru destinaţia stabilită şi să asigure protecţia acestora, în condiţiile legii."

♦ **Mai mulți operatori de date din mediul privat au solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de localizare GPS.**

Autoritatea națională de supraveghere a subliniat că acest tip de prelucrare se supune prevederilor Regulamentului (UE) 2016/679 și că este necesar ca aceste prelucrări să respecte principiile și condițiile de prelucrare stabilite de Regulament, raportat la domeniul de aplicare material al acestuia.

S-au menționat dispozițiile art. 6 alin. (1) lit. a) – f) din Regulamentul (UE) 2016/679 în care se enumeră cazurile în care prelucrarea datelor cu caracter personal este legală, unul dintre acestea fiind cel în care prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Astfel, prelucrarea este legală numai dacă și în masura în care se aplică cel puțin una din condițiile prevăzute de art. 6 alin. (1).

Cu privire la interesul legitim, considerentul (47) din Regulamentul (UE) 2016/679 stabilește următoarele: *„Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terţe părţi, pot constitui un temei juridic pentru prelucrare, cu condiţia să nu prevaleze interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, luând în considerare aşteptările rezonabile ale persoanelor vizate bazate pe relaţia acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relaţie relevantă şi adecvată între persoana vizată şi operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existenţa unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în*

mod rezonabil, în momentul şi în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele şi drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanţe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară."

În sensul celor de mai sus, întrucât dispozitivele de geolocalizare comportă anumite riscuri în privinţa drepturilor şi libertăţilor persoanei care utilizează bunul respectiv (angajatul), 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, precum şi în vederea argumentării și dovedirii unui interes legitim al operatorului care ar trebui să prevaleze față de interesul, drepturile și libertățile persoanei fizice în cauză.**

În același timp, art. 5 din Legea nr. 190/2018 prevede că „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.

De asemenea, Cap. IV din Regulamentul (UE) 2016/679 reglementează obligațiile și responsabilitățile pe care le au operatorul și persoana împuternicită de operator.

Regulamentul (UE) 2016/679 introduce în art. 5 un nou principiu de prelucrare a datelor, cel al responsabilității, potrivit căruia operatorii de date cu caracter personal nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrare a datelor, **dar este necesar ca aceştia să poată demonstra respectarea principiilor menționate.**

Totodată, dispozițiile coroborate ale art. 12, 13 și 14 din Regulamentul (UE) 2016/679 vizează respectarea **principiului transparenței**, **prin asigurarea dreptului la informare a persoanelor vizate**, în funcție de modalitatea de obținere a datelor, respectiv direct de la persoana vizată sau indirect, de la alt operator.

În consecință, Autoritatea națională de supraveghere a subliniat că prelucrarea datelor angajaților prin intermediul sistemului GPS poate fi realizată doar cu îndeplinirea condițiilor prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679 și art. 5 din Legea nr. 190/2018, cu respectarea principiilor de prelucrare a datelor cu caracter personal statuate de același regulament.

Având în vedere faptul că operatorul are obligația respectării și demonstrării respectării condițiilor de legalitate, a principiilor de prelucrare, a măsurilor de confidențialitate și securitate a datelor cu caracter personal pentru a asigura protecția acestora, s-a apreciat că este necesară realizarea unei evaluări de impact raportat la situația concretă a operatorului, inclusiv sub aspectul respectării drepturilor persoanelor vizate, în conformitate cu Regulamentul (UE) 2016/679.

Totodată, în considerarea documentației puse la dispoziția Autorității de către operator, s-a apreciat că este necesară reanalizarea scopului prelucrării, în contextul în care din document nu reieșea cu claritate care este acesta.

♦ Mai multe entități din domeniul privat au solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la transferul datelor cu caracter personal către un stat terț în baza contractelor cu clauze standard.

Cu privire la acest aspect, Autoritatea națională de supraveghere a precizat că art. 46 alin. (1) din Regulamentul (UE) 2016/679 prevede că, în absenţa unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru persoanele vizate.

Garanţiile adecvate menţionate mai sus pot fi furnizate fără să fie nevoie de nicio autorizaţie specifică din partea unei autorităţi de supraveghere, prin:

a) un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;

b) reguli corporatiste obligatorii;

c) clauze standard de protecţie a datelor adoptate de Comisie;

d) clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisie;

e) un cod de conduită, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat în conformitate cu articolul 42, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

În ceea ce privește clauzele standard adoptate de Comisie, Autoritatea națională de supraveghere a menționat că art. 46 alin. (5) din Regulamentul (UE) 2016/679 stabilește faptul că „Deciziile adoptate de Comisie în temeiul articolului 26 alineatul (4) din Directiva 95/46/CE rămân în vigoare până când sunt modificate, înlocuite sau abrogate, dacă este necesar, de o decizie a Comisiei adoptată în conformitate cu alineatul (2) din prezentul articol”.

Astfel, s-a subliniat că Deciziile Comisiei Europene 2001/497/CE și 2004/915/CE reglementează clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe, iar Decizia Comisiei Europene 2010/87/UE reglementează clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului.

Totodată, în plus față de modalitățile principale de transfer mentionate mai sus, art. 46 alin. (3) din Regulamentul (UE) 2016/679 stabilește că pot fi furnizate, de asemenea, garanţii adecvate prin clauze contractuale încheiate între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională sub rezerva autorizării din partea autorităţii de supraveghere competente.

În acest context, considerentul (109) din Regulamentul (UE) 2016/679 subliniază că „Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecţie a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceştia să includă clauzele standard în materie de protecţie a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator şi o altă persoană împuternicită de operator, şi nici să adauge alte clauze sau garanţii suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertăţile fundamentale ale persoanelor vizate.”

♦ **Supravegherea video efectuată în spații publice de către o poliție locală utilizată în scopul monitorizării propriilor angajați.**

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

Astfel, în contextul prelucrării (inclusiv al dezvăluirii) datelor personale, este necesară analizarea temeiului legal al efectuării acesteia, în conformitate cu dispozițiile Regulamentului (UE) 2016/679 mai sus enumerate. Spre exemplu, în măsura în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau există o obligație legală, datele pot fi prelucrate fără consimțământul persoanei vizate. În caz contrar, devin aplicabile condițiile legale privind obținerea consimțământului persoanelor fizice în cauză.

În ceea ce privește datele angajaților, art. 88 din Regulamentul (UE) 2016/679 intitulat ”Prelucrarea în contextul ocupării unui loc de muncă” prevede că:

(1) Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare şi specifice pentru garantarea demnităţii umane, a intereselor legitime şi a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce priveşte transparenţa prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună şi sistemele de monitorizare la locul de muncă.”

În ceea ce privește interesul legitim invocat pentru supravegherea angajaților la locul de muncă prin mijloace de supraveghere video, aceasta se poate efectua în condițiile prevăzute de dispozițiile art. 5 din Legea nr. 190/2018.

Cu toate acestea, în conformitate cu dispozițiile art. 6 lit. f) din Regulamentul (UE) 2016/679, interesul legitim nu se aplică în cazul prelucrării efectuate de autoritățile publice în îndeplinirea atribuțiilor lor, fiind necesară existența unei dispoziții normative în baza căreia se efectuează prelucrarea și care să prevadă garanții adecvate pentru angajații.

Astfel, potrivit art. 6 alin. (2) din Regulamentul (UE) 2016/679, statele membre pot menţine sau introduce dispoziţii mai specifice de adaptare a aplicării normelor regulamentului în ceea ce priveşte prelucrarea în vederea respectării unei obligații legale, prin definirea unor cerinţe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile, inclusiv pentru alte situaţii concrete de prelucrare, astfel cum este prevăzut în capitolul IX al regulamentului (care conține și art. 88 mai sus citat).

În ceea ce privește prelucrarea în scopuri ulterioare, subliniem că art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor, printre care și faptul că datele sunt colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) („limitări legate de scop”).

Sub aspectul informării persoanelor vizate, art. 13 din Regulamentul (UE) 2016/679 stabilește furnizarea unor informații către persoana vizată, în momentul obținerii datelor direct de la aceasta, printre care ”scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării” și ”existența (…) dreptului de a se opune prelucrării”.

De asemenea, alin. (3) și (4) ale art. 13 prevăd că:

”În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2).

(4) Alineatele (1), (2) şi (3) nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.”

Totodată, și în situația în care datele cu caracter personal nu au fost obţinute de la persoana vizată, potrivit art. 14 din Regulamentul (UE) 2016/679, operatorul este obligat la furnizarea unor informații către persoana vizată, printre care scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării și categoriile de date cu caracter personal vizate.

Acest articol stabilește și momentele în care se furnizează informațiile, precum și excepțiile de la obligația de a le furniza, dar și prelucrarea ulterioară a datelor cu caracter personal într-un alt scop.

În ceea ce privește compatibilitatea scopurilor, art. 6 alin. (4) din Regulamentul (UE) 2016/679 este aplicabil.

Prin urmare, monitorizarea prin mijloace video a angajaților poate avea loc numai în condițiile legale mai sus stabilite, iar supravegherea video efectuată în scopul asigurării securității și monitorizării spațiilor publice nu poate fi utilizată și pentru monitorizarea angajaților la locul de muncă, scopurile fiind incompatibile.

♦Prelucrarea datelor în contextul comunicărilor comerciale prin mijloace electronice.

Art. 12 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările și completările ulterioare, prevede condițiile de efectuare a comunicărilor comerciale.

Raportat la prevederile legale de mai sus, rezultă că regula instituită de lege este aceea că astfel de comunicări comerciale prin poșta electronică sunt interzise, excepție făcând situația în care abonatul sau utilizatorul vizat își exprimă în prealabil consimţământul expres (nu prezumat) pentru a le primi.

De asemenea, aceleași dispoziții legale de mai sus stabilesc faptul că, dacă o persoană fizică sau juridică obţine în mod direct adresa de poştă electronică a unui client, cu ocazia vânzării către acesta a unui produs sau serviciu, în conformitate cu prevederile Legii nr. 677/2001 (în prezent, Regulamentul (UE) 2016/679) persoana fizică sau juridică în cauză poate utiliza adresa respectivă, în scopul efectuării de comunicări comerciale referitoare la produse sau servicii similare pe care acea persoană le comercializează.

Astfel, potrivit Regulamentului (UE) 2016/679, act legislativ de directă aplicare și obligatoriu în toate elementele sale, prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează la consimțământul persoanei vizate sau în condițiile de excepție legalitate prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În acest context subliniem că, indiferent de temeiul legal al prelucrării datelor, respectiv la consimțământ sau în situațiile de excepție de la acesta, art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor, cum sunt cele privind faptul că: prelucrarea se face în mod legal, echitabil şi transparent faţă de persoana vizată

(principiul legalității, echității şi transparenţei), datele sunt colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri (principiul limitării legate de scop), prelucrarea de date adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (principiul reducerii la minimum a datelor).

De asemenea, potrivit art. 5 alin. (2) din același regulament, ”operatorul este responsabil de respectarea acestor principii şi poate demonstra această respectare (principiul responsabilității).

Condițiile privind obținerea consimțământului sunt prevăzute în dispozițiile art. 4 pct. 11 coroborate cu art. 7 din Regulamentul (UE) 2016/679. În ceea ce privește interesul legitim, situațiile în care acesta poate fi temei pentru prelucrarea datelor sunt detaliate în documentul emis de Grupul de Lucru Art. 29 (în prezent Comitetul European pentru Protecția Datelor) intitulat ”Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46/CE”.

Sub aspectul informării persoanelor vizate, subliniem că aceasta se face indiferent de temeiul prelucrării, la consimțământ sau pe bază de excepții. 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, raportat la dispozițiile legale mai sus menționate, comunicările comerciale prin poșta electronică pot fi transmise numai cu consimțământul expres al abonatului sau utilizatorului, exprimat anterior primirii unor astfel de comunicări. În caz contrar, astfel de comunicări sunt interzise.

De asemenea, adresa de poştă electronică a unui client, dar care a fost obținută cu ocazia vânzării către acesta a unui produs sau serviciu (iar nu cu ocazia negocierii/încheierii unui contract) se poate utiliza în scopul efectuării de comunicări comerciale referitoare la produse sau servicii similare comercializate de către operator. În plus, legea prevede condiţia de a oferi în mod clar şi expres clienţilor posibilitatea de a se opune printr-un mijloc simplu şi gratuit unei asemenea utilizări, atât la obţinerea adresei de poştă electronică, cât şi cu ocazia fiecărui mesaj, în cazul în care clientul nu s-a opus iniţial.

În plus, documentul emis de fostul Grup de Lucru Art. 29 (în prezent Comitetul European pentru Protecția Datelor), intitulat ”Avizul 4/2007 privind conceptul de date cu caracter personal” recomandă următoarele:

”În cazul în care operatorul de date colectează date privind persoane fizice sau juridice în mod separat şi le include în acelaşi set de date, conceperea mecanismelor de prelucrare a datelor şi sistemul de control pot fi elaborate astfel încât să fie conforme dispoziţiilor privind protecţia datelor. În realitate, poate fi mai uşor pentru operator să aplice dispoziţiile privind protecţia datelor la toate tipurile de informaţii cuprinse în dosarele sale, decât să încerce să separe informaţiile referitoare la persoane fizice de cele referitoare la persoane juridice.”

♦ **Publicarea datelor pe Internet de către autorități și instituții publice.**

În conformitate cu art. 6 din Regulamentul (UE) 2016/679, în măsura în care prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului sau prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, datele pot fi prelucrate fără consimțământul persoanei vizate.

În același timp, în actele normative naționale se pot introduce dispoziții mai specifice de adaptare a aplicării normelor Regulamentului (UE) 2016/679 în ceea ce priveşte prelucrarea prin definirea unor cerinţe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile, cu respectarea principiilor de prelucrare a datelor personale, în conformitate cu art. 6 alin. (4) din Regulamentul (UE) 2016/679.

Aceste dispoziții trebuie să fie în concordanță și cu dispozițiile art. 53 din Constituția României care stabilește condițiile în care poate avea loc restrângerea unor drepturi sau libertăți, inclusiv sub aspectul proporționalității măsurii cu situația care a determinat-o.

Raportat la publicarea pe Internet a unor date cu caracter personal, Autoritatea națională de supraveghere a subliniat în mod constant faptul că diseminarea în spațiul virtual a datelor persoanelor fizice 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, reprezintă o ingerință gravă în drepturile la viață 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 sprijinul acestor argumente amintim jurisprudenţa relevantă a Curții Constituționale (Decizia nr. 440/2014, par. 44 și 45), referitoare la faptul că reglementarea unei obligaţii pozitive care priveşte limitarea în mod necontenit a exerciţiului unui drept fundamental (cum este dreptul la

viaţă privată) face să dispară însăşi esenţa dreptului, prin îndepărtarea garanţiilor privind exercitarea acestuia, persoanele fizice în cauză fiind supuse în permanenţă acestei ingerinţe în exerciţiul drepturilor lor.

De asemenea, în jurisprudența Curţii de Justiţie a Uniunii Europene (Hotărârea din 6 noiembrie 2003, în cauza Bodil Lindqvist) rezultă că referinţele pe o pagină de Internet la diverse persoane şi identificarea lor prin nume sau alte mijloace constituie „prelucrare de date personale efectuată integral sau parţial prin mijloace automate", **iar prin publicarea pe Internet, datele personale devin accesibile unui număr nedefinit de persoane**.

Prin urmare, raportat la dispozițiile legale mai sus menționate, publicarea datelor pe Internet, în condițiile în care aceasta nu este prevăzută de o dispoziție legală care să prevadă garanții pentru persoana vizată, impune din partea operatorului o analiză atentă a condițiilor de legalitate a prelucrării, cu respectarea principiilor și regulilor de prelucrare a datelor personale.

♦ **Prelucrarea datelor personale de către furnizorii de servicii de sănătate.**

Potrivit Regulamentului (UE) 2016/679, prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează la **consimțământul** persoanei vizate sau în condițiile de **excepție** de la consimțământ, prevăzute de art. 6, art. 9 și art. 10 în funcție de natura datelor și categoriilor de date colectate și prelucrate.

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.

(2) Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul general privind protecţia datelor, respectiv al **realizării intereselor legitime** urmărite de operator sau de o parte terţă, se efectuează cu instituirea de către operator a următoarelor **garanţii**:

a) punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul general privind protecţia datelor;

b) numirea unui responsabil pentru protecţia datelor, în conformitate cu prevederile art. 10 din prezenta lege;

c) stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;

d) instruirea periodică cu privire la obligaţiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal."

Astfel, 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 enumerate.

Referitor la **codul numeric personal**, în măsura în care nu există o obligație legală pentru colectarea și prelucrarea acestuia, în anumite cazuri pot deveni aplicabile dispozițiile art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679 coroborate cu cele ale art. 4 alin. (2) din Legea nr. 190/2018 (interesul legitim). În acest sens însă, este necesară, cu prioritate, argumentarea de către operator a interesului legitim care trebuie să prevaleze asupra drepturilor și libertăților persoanei vizate, urmată de instituirea de către operator a garanţiilor prevăzute de lege. În caz contrar, devin aplicabile dispozițiile legale privind consimțământul persoanei în cauză (sau a reprezentantului legal) ori cele referitoare la celelalte condiții de legalitate stabilite prin art. 6 din Regulamentul (UE) 2016/679.

În ceea ce privește responsabilitatea operatorului, art. 24 din Regulamentul (UE) 2016/679 prevede că "Ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar."

Sub aspectul informării persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe bază de excepții), art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul (în speță furnizorul de servicii medicale) 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, este necesară realizarea informării persoanelor vizate, în speță, a pacienților.

În ceea ce privește obținerea consimțământului persoanei vizate, în măsura în care prelucrarea datelor sale are loc pe baza acestuia, trebuie să fie îndeplinite condițiile menționate de Regulamentul (UE) 2016/679. În caz contrar, prelucrarea intră sub incidența celorlalte ipoteze de excepție de la consimțământ, prevăzute de dispozițiile art. 6 și 9 ale Regulamentului (UE) 2016/679, după caz.

Condițiile consimțământului sunt prevăzute de art. 4 pct. 11 coroborat cu art. 7 raportat la considerentele (32), (42) și (43) din Regulamentul (UE) 2016/679.

Art. 7 alin. (4) din Regulamentul (UE) 2016/679 prevede că ”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.”

De asemenea, considerentul (32) din Regulamentul (UE) 2016/679 prevede următoarele: ”Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru toate scopurile prelucrării. (...).”

Totodată, considerentul (42) din Regulamentul (UE) 2016/679 stabilește că: ”Pentru ca acordarea consimţământului să fie în cunoştinţă de cauză, persoana vizată ar trebui să fie la curent cel puţin cu identitatea operatorului şi cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimţământul fără a fi prejudiciată.”

În același timp, considerentul (43) din regulament explică următoarele: ”Pentru a garanta faptul că a fost acordat în mod liber, consimţământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată şi operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimţământului în mod liber în toate circumstanţele aferente respectivei situaţii particulare. Consimţământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimţământul separat pentru diferitele operaţiuni de prelucrare a datelor cu caracter personal, deşi acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este

condiţionată de consimţământ, în ciuda faptului că consimţământul în cauză nu este necesar pentru executarea contractului.”

Referitor la **datele privind sănătatea**, în conformitate cu art. 9 din Regulamentul (UE) 2016/679, prelucrarea datelor speciale este legală dacă:

- persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice;

- prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute la alineatul (3); în acest sens, datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

În cea de-a doua situație de mai sus, datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

♦ **Prelucrarea datelor în contextul asigurării accesului la informațiile de interes public și a libertății de exprimare.**

Art. 2 lit. c) din Legea nr. 544/2001 stabilește că ”prin informaţie cu privire la datele personale se înţelege orice informaţie privind o persoană fizică identificată sau identificabilă.” Această prevedere este în concordanță cu dispozițiile art. 4 pct. 1 din Regulamentul (UE) 2016/679, care definește datele cu caracter personal.

Potrivit art. 14 alin. (1) din Legea nr. 544/2001, informaţiile deţinute de către o autoritate sau instituţie publică cu privire la datele personale ale unui cetăţean pot deveni informaţii de interes public numai în măsura în care afectează capacitatea de exercitare a unei funcţii publice.

Legat de afectarea capacității de exercitare a unei funcţii publice, această analiză se efectuează de către entitatea care deține informațiile și care decide dezvăluirea (sau nu) a acestora, raportat, spre exemplu, la funcția pe care o îndeplinește persoana respectivă, datele care vor fi dezvăluite, în ce măsură acestea afectează capacitatea de exercitare a funcției, scopul solicitării acestora etc.

Prin Decizia Înaltei Curți de Casație și Justiție nr. 37/2015, instanța supremă a statuat următoarele: ”În cazul cererilor de liber acces la informaţii de interes public întemeiate pe dispoziţiile Legii nr. 544/2001, atunci când informaţiile de interes public şi informaţiile cu privire la datele cu caracter personal sunt prezente în cuprinsul aceluiaşi document, indiferent de suportul ori de forma sau de modul de exprimare a informaţiilor, accesul la informaţiile de interes public se realizează prin anonimizarea informaţiilor cu privire la datele cu caracter personal; refuzul de acces la informaţiile de interes public, în condiţiile în care informaţiile cu privire la datele personale sunt anonimizate, este nejustificat.”

În măsura în care situația nu face obiectul art. 14 alin. (1) din Legea nr. 544/2001, devin aplicabile dispozițiile art. 12 alin. (1) lit. d) din aceeași lege, dispoziții care stabilesc faptul că se exceptează de la accesul liber al cetăţenilor informaţiile cu privire la datele personale, potrivit legii.

În acest context, potrivit Regulamentului (UE) 2016/679, prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează la consimțământul persoanei vizate sau în condițiile de excepție de la consimțământ, prevăzute de art. 6, art. 9 și art. 10 în funcție de natura datelor și categoriilor de date colectate și prelucrate.

Astfel, în ceea ce privește îndeplinirea unei obligaţii legale, în măsura în care datele deținute de o autoritate/instituție publică intră sub incidența dispozițiilor art. 14 alin. (1) din Legea nr. 544/2001, modificată şi completată, respectiv afectează capacitatea de exercitare a unei funcţii publice, legea stabilește că acestea pot deveni informaţii de interes public. În caz contrar, devin aplicabile dispozițiile menționate mai sus ale Regulamentului (UE) 2016/679.

În ceea ce privește datele și categoriile de date prelucrate (dezvăluite), art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor.

În măsura în care datele sunt prelucrate în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, art. 85 din Regulamentul (UE) 2016/679 reglementează ”Prelucrarea şi libertatea de exprimare şi de informare”. Aceste dispoziţii au fost puse în aplicare prin 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 privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Art. 7 din legea sus-menționată stabilește o serie de dispoziții derogatorii în ceea ce privește prelucrarea datelor cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, astfel: ”În vederea asigurării unui echilibru între dreptul la protecția datelor cu caracter personal, libertatea de exprimare și dreptul la informație, prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare poate fi efectuată, dacă aceasta privește date cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată**,** prin derogare de la unele capitole din Regulamentul general privind protecția datelor, respectiv:

a) capitolul II - Principii;

b) capitolul III - Drepturile persoanei vizate;

c) capitolul IV - Operatorul și persoana împuternicită de operator;

d) capitolul V - Transferurile de date cu caracter personal către țări terțe sau organizații internaționale;

e) capitolul VI - Autorități de supraveghere independente;

f) capitolul VII - Cooperare și coerență;

g) capitolul IX - Dispoziții referitoare la situații specifice de prelucrare.

Prin urmare, dispozițiile legale sus-menționate devin aplicabile în cazul prelucrării datelor de către entitățile care desfășoară activitate în scop jurnalistic, al exprimării academice, artistice sau literare, iar în măsura în care situația se încadrează în condițiile art. 7 din Legea nr. 190/2018, reglementările derogatorii devin aplicabile.

În concluzie, în măsura în care prelucrarea datelor este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului (cum ar fi respectarea dispozițiilor Legii nr. 544/2001), datele pot fi prelucrate fără consimțământul persoanei vizate.

De asemenea, în condițiile în care informațiile cu privire la datele personale sunt anonimizate, potrivit jurisprudenței ÎCCJ mai sus menționate, este nejustificat refuzul furnizării documentelor solicitate.

În măsura în care situația se circumscrie condițiilor stabilite de art. 7 din Legea nr. 190/2018, mai sus precizate, acestea devin aplicabile.

În situația în care dezvăluirea datelor nu se încadrează în dispozițiile Legii nr. 544/2001 sau ale art. 7 din Legea nr. 190/2018, devin aplicabile condițiile art. 6 din Regulamentul (UE) 2016/679 prezentate anterior.

♦ Stabilirea calității de operator – împuternicit – operatori asociați

În cursul anului 2019, au continuat să fie solicitate Autorității naționale de supraveghere puncte de vedere prin care instituția noastră să stabilescă concret calitățile diferiților actori în contextul unei activități de prelucrare a datelor personale.

Astfel, s-a opinat în mod constant faptul că, la stabilirea calității entităților care prelucrează date cu caracter personal, este necesar a se lua în considerare următoarele dispoziții din Regulamentul (UE) 2016/679:

Art. 4 pct. 7 din Regulamentul (UE) 2016/679 definește „operatorul” ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

De asemenea, art. 26 din același regulament prevede că:

”(1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la articolele 13 și 14, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alineatul (1) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.

(3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori.”

Raportat la prevederile legale sus-menționate, entitățile care prelucrează date cu caracter personal au calitatea de **operatori asociați**, numai în măsura în care aceștia stabilesc în comun scopurile și mijloacele de prelucrare, au încheiat un acord prin care se stabilesc responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului (UE) 2016/679 și indiferent de clauzele acordului, persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori.

În ceea ce privește **calitatea de împuternicit**, **art. 4 pct. 8** din Regulamentul (UE) 2016/679 definește „persoana împuternicită de operator" ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

De asemenea, art. 28 alin.(3) lit. a), g) și h) și alin. (10) din același regulament stabilește că:

"(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un **contract sau alt act juridic** în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

(a) prelucrează datele cu caracter personal **numai pe baza unor instrucțiuni** documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

h) pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

În ceea ce priveşte primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.

(10) Fără a aduce atingere articolelor 82, 83 și 84, **în cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă**."

În consecință, în funcție de activitatea efectiv realizată de entitățile implicate, de modul în care a fost stabilită relația dintre acestea, urmează să se stabilească calitatea în care prelucrează datele, raportat la prevederile legale de mai sus, care conferă un anumit grad de flexibilitate în ceea ce privește stabilirea calităților de operator și împuternicit, respectiv responsabilitățile fiecăruia în ceea ce privește prelucrarea datelor personale.

Astfel, în Avizul nr. 1/2010 emis de Grupul de Lucru Art. 29, în prezent Comitetul european pentru protecția datelor, se precizează că „*primul și cel mai important rol al conceptului de operator este acela de a stabili cine va fi responsabil de respectarea normelor de protecție a datelor și modul în care persoanele vizate își pot exercita drepturile în practică. Cu alte cuvinte: alocarea responsabilității.*"

De asemenea, fiecare dintre aceste entități poate avea, separat, calitatea de operator pentru prelucrările de date pe care le realizează în mod individual, potrivit scopurilor și mijloacelor stabilite de ele însele (sau de un act normativ) și pentru care poartă întreaga răspundere.

În plus, în Avizul nr. 05/2012 privind „cloud computing" emis de Grupul de Lucru Art. 29, în prezent Comitetul european pentru protecția datelor, se precizează faptul că "prezentul aviz se axează pe relația client – furnizor ca relație operator – persoană împuternicită de operator (....); cu toate acestea, pe baza unor circumstanțe concrete, ar putea exista situații în care furnizorul de servicii de cloud computing acționează și în calitate de operator, de exemplu, atunci când furnizorul re-prelucrează unele date cu caracter personal în scopuri proprii. În acest caz, furnizorul este pe deplin (colectiv) responsabil pentru activitatea de prelucrare (...)".

Prin urmare, Autoritatea națională de supraveghere consideră că operatorii și împuterniciții sunt în măsură să își stabilească calitatea, având în vedere cunoașterea în detaliu a activității de prelucrare a datelor în anumite scopuri și folosind anumite mijloace, precum și a drepturilor și obligațiilor fiecărei părți, fără ca aceasta să aducă atingere adoptării măsurilor legale necesare de către Autoritatea națională de supraveghere în îndeplinirea atribuțiilor sale raportat la situații concrete ivite în practică.

♦ **Obligația întocmirii unei evaluări a impactului asupra protecţiei datelor.**

În ceea ce privește realizarea unei evaluări a impactului, aceasta este obligatorie în măsura în care situația se încadrează în ipotezele reglementate de art. 35 din Regulamentul (UE) 2016/679 coroborat cu Decizia nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.

Referitor la prelucrarea pe scară largă, în documentul fostului Grup de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor) intitulat ”**Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679**” se precizează următoarele: ”În orice caz, WP29 recomandă ca în special următorii factori să fie luați în considerare atunci când se stabilește dacă prelucrarea se efectuează pe scară largă:

a. numărul de persoane vizate în cauză, fie ca număr specific sau ca proporție din populația relevantă;

b. volumul de date și/sau gama de diferite elemente de date care sunt prelucrate;

c. durata sau persistența activității de prelucrare a datelor;

d. extinderea geografică a activității de prelucrare.”

De asemenea, în același document, Grupul de Lucru menționează ca exemplu de efectuare a unei evaluări a impactului, situația în care o societate monitorizează sistematic activitățile angajaților săi, inclusiv monitorizarea stațiilor de lucru, a activității pe internet a angajaților săi etc. În acest sens, Grupul de Lucru apreciază că se realizează o monitorizare sistematică, iar datele de referă la persoanele vizate vulnerabile (angajații).

În același timp, în documentul sus-menționat Grupul de Lucru Art. 29 recomandă următoarele: ”În cazurile în care nu este clar dacă este necesară o DPIA, WP29 recomandă efectuarea, cu toate acestea, a unei DPIA, întrucât o DPIA este un instrument util pentru a sprijini operatorii să respecte legislația în materie de protecție a datelor.”

Totodată Grupul de Lucru Art. 29 arată că ”În cele mai multe cazuri, un operator de date poate să considere că o prelucrare care îndeplinește două criterii ar necesita efectuarea unei DPIA. În general, WP29 consideră că, pe măsură ce sunt îndeplinite tot mai multe criterii de prelucrare, aceasta este mai susceptibilă să prezinte un risc ridicat pentru drepturile și libertățile persoanelor vizate și, prin urmare, să necesite o DPIA, indiferent de măsurile pe care operatorul intenționează să le adopte.

Cu toate acestea, în unele cazuri, un operator de date poate considera că o prelucrare care îndeplinește numai unul dintre aceste criterii necesită o DPIA."

În măsura în care operatorul nu efectuează o evaluare a impactului, Grupul de Lucru Art. 29 menționează în documentul său că "În astfel de cazuri, operatorul ar trebui să justifice și să documenteze motivele pentru care nu a efectuat o DPIA și să includă/înregistreze avizele responsabilului cu protecția datelor."

Având în vedere cele de mai sus, revine operatorului obligația de a analiza în ce măsură prelucrarea respectivă reprezintă un risc ridicat pentru drepturile și libertățile persoanelor vizate, precum și cea de a justifica și documenta motivele pentru care nu a efectuat o astfel de evaluare.

♦ **Accesul registratorilor medicali la datele medicale prelucrate de către un furnizor de servicii de sănătate.**

Potrivit Regulamentului (UE) 2016/679, prelucrarea datelor cu caracter personal se realizează la **consimțământul** persoanei vizate sau în condițiile de **excepție** de la consimțământ, prevăzute de art. 6, art. 9 și art. 10 în funcție de natura datelor și categoriilor de date colectate și prelucrate.

Spre exemplu, pentru datele care nu au un caracter special, acestea pot fi prelucrate în temeiul art. 6 din Regulamentul (UE) 2016/679.

Referitor însă la temeiul legal al prelucrării datelor cu caracter special, printre care se numără și datele privind sănătatea, art. 9 din Regulamentul (UE) 2016/679 stabilește condițiile de prelucrare, unele dintre acestea fiind acelea în care:

- persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice;

- prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;

- prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi

serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării unor condiţii şi garanţii. În acest sens, datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

În plus, precizăm că potrivit art. 29 din Regulamentul (UE) 2016/679, orice persoană care acţionează sub autoritatea operatorului (de ex. angajatul), care are acces la date cu caracter personal, nu le prelucrează decât la cererea operatorului.

Prin urmare, având în vedere natura datelor (datele privind sănătatea), acestea pot fi prelucrate cu respectarea principiului proporționalității, respectiv prelucrarea de date adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (în speță, datele necesare îndeplinirii atribuțiilor registratorilor medicali), de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate, precum și cu respectarea principiului securității.

În sensul celor de mai sus, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate care, dacă este necesar, se revizuiesc şi se actualizează, pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul (UE) 2016/679.

De asemenea, în documentul Grupului de Lucru Art. 29 (în prezent, Comitetul european pentru protecția datelor) intitulat ”Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES)” se precizează faptul că ”Datele din sistemele DES sunt constituite din dosare medicale confidenţiale. Astfel, principiul fundamental care guvernează accesul la un DES trebuie să fie acela că – în afară de pacient – doar acele cadre medicale/persoane autorizate de instituţii medicale, care participă activ la tratamentul pacientului pot primi dreptul de acces (...). Protecţia datelor mai poate fi ameliorată cu ajutorul drepturilor de acces modulare, prin formarea de categorii de date medicale într-un sistem DES, cu consecinţa limitării accesului”.

♦ Date biometrice – tehnici de recunoaștere facială.

Art. 4 din Regulamentul (UE) 2016/679 stabilește o serie de definiții, printre care și cea a datelor biometrice.

Astfel, art. 4 pct. 14 din Regulamentul (UE) 2016/679 definește datele biometrice ca fiind ”date cu caracter personal care **rezultă în urma unor tehnici de prelucrare specifice** referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice”.

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

Având în vedere cele de mai sus, datele cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, cum sunt sistemele de recunoaștere facială, reprezintă date biometrice care intră în categoria datelor speciale și se supun condițiilor speciale de prelucrare din Regulamentul (UE) 2016/679.

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

Astfel, sub aspectul proporționalității instituirii unei asemenea măsuri, Grupul de Lucru precizează, în același document menționat anterior, faptul că:

”Utilizarea biometriei ridică problema proporționalității fiecărei categorii de date prelucrate în lumina scopului în care sunt prelucrate acestea. Având în vedere faptul că datele biometrice pot fi utilizate numai dacă sunt adecvate, relevante și neexcesive, trebuie să se evalueze cu exactitate necesitatea și proporționalitatea datelor prelucrate și să se analizeze dacă scopul urmărit ar putea fi atins într-un mod mai puțin intruziv.”

În ceea ce privește temeiul legal al prelucrării datelor biometrice, acesta se subsumează condițiilor art. 9 din Regulamentul (UE) 2016/679 coroborate cu art. 3 din Legea nr. 190/2018.

În acest context, subliniem faptul că dispozițiile art. 3 alin. (1) din Legea nr. 190/2018 devin aplicabile în situația prelucrării datelor biometrice în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri. În caz contrar, se aplică dispozițiile art. 9 din Regulamentul (UE) 2016/679. Astfel, conform art. 9 alin. (2) lit. a) din Regulamentul (UE) 2016/679, datele biometrice pot fi prelucrate dacă persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date pentru unul sau mai multe scopuri specifice.

În ceea ce privește consimțământul persoanei vizate, 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 regulament prevede condițiile de obținere a consimțământului, inclusiv sub aspectul demonstrării, de către operator, a obținerii acestuia.

Corelat cu aspectele de mai sus, Grupul de Lucru Art. 29 precizează în același aviz menționat anterior următoarele:

”… în contextul relației angajat-angajator, consimțământul trebuie să fie pus sub semnul întrebării și justificat în mod corespunzător. În loc să încerce să obțină consimțământul angajaților, angajatorii ar putea să cerceteze dacă este cu adevărat necesar să utilizeze datele biometrice ale angajaților într-un scop legitim și să evalueze această necesitate în raport cu drepturile și libertățile fundamentale ale angajaților. (…) Angajatorul trebuie să caute întotdeauna metoda cea mai puțin intruzivă, prin alegerea unui proces care nu implică prelucrarea datelor biometrice, dacă acest lucru este posibil.”

În ceea ce privește responsabilitatea operatorului, **art. 24** din Regulamentul (UE) 2016/679 prevede că ”Ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare **măsuri tehnice şi organizatorice adecvate** pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. (...)”.

Față de cele de mai sus, în lipsa unui act normativ de nivelul legii, care să prevadă garanţii adecvate pentru protecția datelor și a drepturilor persoanelor vizate, având în vedere natura sensibilă a datelor care necesită protecție, raportat la principiul proporționalității instituit de art. 5 din Regulamentul (UE) 2016/679, la condițiile de obținere a consimțământului prevăzute de art. 7 din același regulament, precum și aplicabilitatea acestora în relația angajat-angajator, **Autoritatea**

națională de supraveghere a considerat că nu se justifică necesitatea și proporționalitatea datelor prelucrate prin raportare la scopul urmărit (accesul angajaților și al vizitatorilor în clădirile unei instituții publice), fiind necesară analizarea atingerii acestuia într-un mod mai puțin intruziv, prin alegerea unui sistem care nu implică prelucrarea datelor biometrice ale persoanelor vizate.

♦ Stabilirea de termene de stocare a datelor în contextul recrutării personalului.

Raportat la Regulamentul (UE) 2016/679, precizăm faptul că art. 5 alin. (1) lit. e) din acest regulament prevede următoarele în ceea ce privește termenele de stocare a datelor pe care operatorii trebuie să le respecte, astfel:

(1) Datele cu caracter personal sunt: (...)

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);”

În același timp, art. 89 alin. (1) din Regulamentul (UE) 2016/679 stabilește că: ”Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivele garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivele măsuri pot include pseudonimizarea, cu condiția ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.”

Prin urmare, Regulamentul (UE) 2016/679 stabilește păstrarea datelor într-o formă care permite identificarea persoanelor vizate **pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele,** precum și faptul că datele cu caracter personal **pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu instituirea unor garanții.**

Astfel, operatorului i se conferă posibilitatea de a avea diferite termene de stocare a datelor, în funcție de scopul/scopurile prelucrării și pe durata necesară realizării scopului/scopurilor, prin stabilirea din proprie inițiativă a unei durate maxime de păstrare raportat la **necesitatea argumentată a stocării datelor**, cu respectarea principiului **proporționalității scopului și a reducerii la minimum a datelor** și cu punerea în aplicare a măsurilor de ordin tehnic și organizatoric adecvate, astfel încât să se asigure conformitatea cu Regulamentul (UE) 2016/679.

De asemenea, termenele de stocare pot fi prevăzute și în diferite acte normative specifice unor domenii de activitate, pe care operatorul trebuie să le respecte.

În ceea ce privește stocarea datelor referitoare la candidații respinși, aceasta nu intră sub incidența dispozițiilor privind arhivarea în interes public, iar termenul de stocare se stabilește, în măsura în care nu există norme legale specifice, pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele, respectiv finalizarea procesului de selecție.

Păstrarea datelor pe o perioadă ce depășește acest termen se poate efectua pe baza interesului legitim al operatorului (art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679), cu informarea prealabilă a candidatului și oferirea posibilității de a-și exercita drepturile de care beneficiază.

Totodată, în măsura în care persoana vizată în cauză își exercită și dreptul la ștergere, aceasta are dreptul ca, în temeiul art. 17 din Regulamentul (UE) 2016/679 să obțină din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate, unele dintre motive fiind următoarele:

”a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b) persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), şi nu există niciun alt temei juridic pentru prelucrare;

c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);”.

De asemenea, art. 17 din Regulamentul (UE) 2016/679 nu face distincție între datele și categoriile de date pe care operatorul are obligaţia de a le şterge, textul de lege referindu-se la datele cu caracter personal care privesc persoana vizată în cauză și, în același timp, la excepțiile de la acest drept care ar justifica păstrarea datelor.

În acest context, prelucrarea datelor în contextul relațiilor de muncă este analizată în documentul Grupului de Lucru Art. 29 (în prezent, Comitetul european pentru protecția datelor) intitulat ”**Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă**” în care se precizează faptul că: ”Datele colectate în timpul procesului de recrutare ar trebui să fie, în general, șterse de îndată ce devine evident faptul că nu va fi înaintată o ofertă de muncă sau că aceasta nu este acceptată de către persoana în cauză. De asemenea, persoana trebuie să fie corect informată cu privire la orice astfel de prelucrare înainte de a se angaja în procesul de recrutare.”

Referitor la datele și categoriile de date colectate în contextul recrutării, precizăm faptul că art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor. Printre acestea, se numără, așa cum s-a menționat anterior și cel privind prelucrarea datelor adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

Legat de cele de mai sus, același document al Grupului de Lucru Art. 29 menționat anterior, explică faptul că ”angajatorii nu ar trebui să presupună că, doar datorită faptului că profilul unei persoane de pe platformele de comunicare socială este public, aceștia sunt autorizați să prelucreze respectivele date în scopuri proprii. Este nevoie de un temei juridic pentru o astfel de prelucrare, cum ar fi interesul legitim. În acest context, înainte de verificarea unui profil de pe platformele de comunicare socială, angajatorul trebuie să aibă în vedere dacă profilul candidatului de pe respectivele platforme este legat de un context profesional sau personal, deoarece acest lucru poate fi un element important care indică admisibilitatea juridică a inspecției datelor. În plus, angajatorii sunt autorizați să colecteze și să prelucreze datele cu caracter personal referitoare la candidații la un post doar în măsura în care colectarea acestor date este necesară și relevantă pentru îndeplinirea atribuțiilor postului pentru care aceștia s-au înscris.”

♦ **Consimțământul persoanei vizate în contextul furnizării serviciilor de sănătate.**

Referitor la legitimitatea prelucrării datelor, consimțământul este unul dintre cele șase temeiuri de legalitate în ceea ce privește prelucrarea datelor personale care nu au caracter special, enumerate de art. 6 alin (1) din Regulamentul (UE) 2016/679 și unul dintre cele zece temeiuri de legalitate privind prelucrarea datelor personale speciale, enumerate de art. 9 alin. (2) din Regulamentul (UE) 2016/679.

Astfel, în cadrul activităților ce presupun prelucrarea de date cu caracter personal, în speță cu caracter special, operatorul trebuie să analizeze dacă consimțământul este temeiul legal adecvat pentru prelucrarea avută în vedere sau trebuie identificat un alt temei legal.

În acest context, precizăm 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) 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 niciun 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 Regulamentul (UE) 2016/679, 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 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.”

Astfel, în ceea ce privește prelucrarea bazată pe consimțământul persoanei vizate, aceasta trebuie să respecte condițiile consimțământului prevăzute de art. 4 pct. 11 coroborat cu art. 7 raportat la considerentul (32), (42) și (43) din Regulamentul (UE) 2016/679.

Art. 7 alin. (4) din Regulamentul (UE) 2016/679 prevede că ”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.”

De asemenea, considerentul (32) din Regulamentul (UE) 2016/679 prevede următoarele: ”Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru toate scopurile prelucrării. (...).”

Totodată, considerentul (42) din Regulamentul (UE) 2016/679 stabilește că: ”Pentru ca acordarea consimţământului să fie în cunoştinţă de cauză, persoana vizată ar trebui să fie la curent cel puţin cu identitatea operatorului şi cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimţământul fără a fi prejudiciată.”

În același timp, considerentul (43) din regulament explică următoarele: ”Pentru a garanta faptul că a fost acordat în mod liber, consimţământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată şi operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimţământului în mod liber în toate circumstanţele aferente respectivei situaţii particulare. Consimţământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimţământul separat pentru diferitele operaţiuni de prelucrare a datelor cu caracter personal, deşi acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiţionată de consimţământ, în ciuda faptului că consimţământul în cauză nu este necesar pentru executarea contractului.”

Legat de cele de mai sus, precizăm că în conformitate cu art. 9 alin. (2) lit. a) din Regulamentul (UE) 2016/679 prelucrarea datelor speciale este legală dacă persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice.

Ca atare, obținerea consimțământului persoanei vizate, în măsura în care prelucrarea datelor sale are loc pe baza acestuia, trebuie să îndeplinească condițiile mai sus menționate din Regulamentul (UE) 2016/679. În caz contrar, prelucrarea intră sub incidența celorlalte ipoteze de excepție de la consimțământ, prevăzute de dispozițiile art. 6 și 9 ale Regulamentului (UE) 2016/679, după caz.

În plus, potrivit art. 9 alin. (3) din Regulamentul (UE) 2016/679, ”Datele cu caracter personal menţionate la alineatul (1) pot fi prelucrate în scopurile menţionate la alineatul (2) litera (h), în cazul în care datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană

supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente."

Aplicabilitatea temeiului consimțământului în prelucrarea datelor privind sănătatea a fost analizată în documentul Grupului de Lucru Art. 29 (în prezent, Comitetul european pentru protecția datelor) intitulat "Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES)" în care se precizează faptul că "orice consimţământ dat ca urmare a ameninţării întreruperii tratamentului sau a tratamentului de calitate inferioară într-o circumstanţă medicală nu poate fi considerat „de bună voie".

În același document se mai menționează faptul că "în cazul în care un cadru medical trebuie să prelucreze date cu caracter personal în sistemul DES ca o urmare necesară şi inevitabilă a actului medical, justificarea acestei prelucrări prin primirea acordului este falsă. Utilitatea acordului trebuie limitată la cazurile în care subiectul individual al datelor beneficiază de mai multe opţiuni reale şi poate ulterior să-şi retragă acordul fără a suferi neajunsuri."

Totodată, Grupul de Lucru precizează că "Consimţământul dat de către o persoană vizată căreia nu i s-a oferit şansa unei opţiuni autentice sau care a fost pusă în faţa faptului împlinit nu poate fi considerat ca fiind valabil."

În acest context, subliniem faptul că, în funcție de scopul prelucrării datelor, pot deveni aplicabile, după caz, și prevederile Legii nr. 46/2003 sau ale Legii nr. 95/2006 sub aspectul informării și obținerii acordului pacientului pentru situațiile specifice reglementate de aceste acte normative.

Prin urmare, raportat la cele mai sus menționate, prelucrarea datelor personale ale pacienților se poate efectua, fie pe baza consimțământului în măsura în care sunt întrunite cerințele acestuia, fie în celelalte condiții prevăzute de art. 6 și 9 din Regulamentul (UE) 2016/679, după caz, potrivit naturii datelor prelucrate și scopurilor vizate, cu informarea prealabilă a persoanelor vizate.

■Puncte de vedere solicitate în contextul cooperării prin Sistemul IMI

În contextul cooperării cu alte autorități de supraveghere în vederea asigurării asistenței reciproce, au fost gestionate circa **30 de solicitări** cu privire la Regulamentul (UE) 2016/679. Dintre acestea, unele s-au referit la modalitatea de interpretare și aplicare a unor dispoziții din Regulamentul (UE) 2016/679.

Astfel, prin sistemul IMI, s-au trimis o serie de solicitări de opinii adresate instituției noastre din partea autorităților de supraveghere din Cipru, Cehia, Islanda, Luxembourg, Polonia și Slovenia.

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

În anul 2019, au fost transmise mai multe puncte de vedere ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în cauze pendinte în fața Curții de Justiție a Uniunii Europene, referitoare la interpretarea anumitor articole din Directiva 95/46/CE, Directiva 2002/58/CE, dar și din Regulamentul (UE) 2016/679, respectiv:

■ **Cauza C-746/18**, în cadrul căreia cererea a fost adresată de o instanță din Estonia, raportat la întrebările adresate Curții referitoare la interpretarea **art. 15 alin. (1) din Directiva 2002/58/CE**.

■ **Cauza C-645/19**, în cadrul căreia cererea a fost adresată de o instanță din Belgia, raportat la întrebările adresate Curții referitoare la interpretarea **art. 55 alin. (1) art. 56-58 și 60-66 din Regulamentul (UE) 2016/679.**

■ **Cauza C-470/19**, în cadrul căreia cererea a fost adresată de o instanță din Irlanda, raportat la întrebările adresate Curții referitoare la interpretarea **art. 2 punctul 2 din Directiva 2003/4/CE din 28 ianuarie 2003 privind accesul publicului la informaţiile despre mediu şi de abrogare a Directivei 90/313/CEE a Consiliului.**

■ **C-272/19 – Landul Hessa**, în cadrul căreia cererea a fost adresată de către o instanţă de trimitere din Germania (Verwaltungsgericht Wiesbaden), referitoare la interpretarea dată **art. 15 raportat la art. 4 pct. 7 din Regulamentul (UE) 2016/679 și imparțialitatea și independența instanței de trimitere raportat la art. 267 TFUE coroborat cu art. 47 par. 2 din Carta drepturilor fundamentale a Uniunii Europene.**

■ **C-439/19 – Latvijas Republikas Saeima**, în cadrul căreia cererea a fost adresată de către o instanţă de trimitere din **Letonia**, (Satversmes tiesa - Curtea Constituțională din Letonia), referitoare la interpretarea **Regulamentului (UE) 2016/679 și a Directivei 2003/98 cu scopul de a se stabili dacă acestea interzic statelor membre să prevadă în legislația lor că informațiile referitoare la punctele atribuite conducătorilor auto pentru încălcarea normelor de circulație rutieră sunt accesibile publicului, permițând astfel o prelucrare a datelor cu caracter personal în cauză prin comunicarea și transmiterea acestora în scopul reutilizării lor.**

■ **Cauza C-597/19 – Mircom**, în cadrul căreia cererea a fost adresată de către o instanţă de trimitere din Belgia (Ondernemingsrechtbank Antwerpen, afdeling Antwerpen), referitoare la ”interpretarea noțiunii „comunicare publică” de la **articolul 3 alineatul (1) din Directiva 2001/29; interpretarea capitolului II din Directiva 2004/48 și a noțiunii „prejudiciu” menționate la articolul 13 din aceasta; relevanța circumstanțelor concrete pentru aprecierea proporționalității atunci când se evaluează comparativ respectarea drepturilor de proprietate intelectuală și drepturile și libertățile garantate de Cartă; justificarea înregistrării sistematice a adreselor IP în temeiul articolului 6 alineatul (1) litera (f) din Regulamentul (UE) 2016/679**.

■ **C-620/19 – J & S Service**, în cadrul căreia cererea a fost adresată de către o instanţă de trimitere din Germania (Bundesverwaltungsgericht), referitoare la interpretarea **articolului 23 alineatul (1) litera (j) și (e) din Regulamentul (UE) 2016/679**.

■ **Cauza C-708/18 - Asociaţia de Proprietari bloc M5A-Scara A** în cadrul căreia cererea a fost adresată de către o instanţă de trimitere din România (Tribunalul Bucureşti – România) în legătură cu interpretarea **art. 8 și 52 din Carta drepturilor fundamentale a Uniunii Europene și art. 7 lit. f) din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.**

■ **<u>Puncte de vedere exprimate în contextul analizării codurilor de conduită</u>**

În ceea ce privește **codurile de conduită**, după punerea în aplicare a Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a primit și analizat un număr de **11 proiecte de coduri de conduită**, care au vizat, în principal, următoarele domenii de activitate: bănci, asigurări și reasigurări, birou de credit, pensii administrate privat, executori judecătorești, notari, detectivi particulari, jocuri de noroc.

Asupra tuturor proiectelor de coduri au fost efectuate observații și propuneri, fiind necesară punerea în acord a acestora cu Regulamentul (UE) 2016/679 și Orientările nr. 1/2019 privind codurile de conduită și organismele de monitorizare prevăzute în Regulamentul (UE) 2016/679 emise de Comitetul european pentru protecția datelor, inclusiv sub aspectul organismului de monitorizare.

Având în vedere că cerințele de acreditare a organismelor de monitorizare urmează să fie elaborate, fiind necesară îndeplinirea procedurii de consultare a Comitetului european pentru protecția datelor, Autoritatea națională de supraveghere aprobă codurile de conduită care respectă

prevederile art. 40 și 41 din Regulamentul (UE) 2016/679 și Ghidul nr. 1/2019 al Comitetului european pentru protecția datelor.

În anul 2019 nu au fost aprobate de către Autoritatea națională de supraveghere coduri de conduită ale asociațiilor profesionale.

■ Puncte de vedere exprimate în contextul analizării evaluărilor de impact

În anul 2019 au fost supuse analizei Autorității naționale de supraveghere unele documentații privind evaluări de impact întocmite de către operatori (4).

În ceea ce privește evaluarea impactului asupra protecţiei datelor, precizăm că aceasta se supune condițiilor stabilite de dispozițiile art. 35 din Regulamentul (UE) 2016/679 **coroborate cu cele ale Deciziei Autorității naționale de supraveghere nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal**.

Cu toate acestea, art. 35 alin. (3) din Regulamentul (UE) 2016/679 lasă libertatea operatorului de a recurge la o astfel de evaluare, în măsura în care apreciază ca fiind necesară și în alte situații.

În plus, fostul Grup de Lucru Art. 29, în prezent Comitetul european pentru protecția datelor, a adoptat ”Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului (UE) 2016/679”. În conținutul acestuia se găsesc informații privind o serie de exemple ce ilustrează modul în care criteriile trebuie folosite pentru a analiza dacă o anumită operațiune de prelucrare necesită o evaluare de impact.

Acest ghid, poate fi găsit pe site-ul Autorității naționale de supraveghere, inclusiv în limba română (traducere neoficială a instituției noastre, pentru a veni în sprijinul celor interesați), la adresa http://www.dataprotection.ro/?page=Comunicat_ghid_final_DPIA&lang=ro.

Totodată, potrivit opiniei exprimate în ghidul sus-menționat, în situațiile în care nu este clar dacă o evaluare de impact (DPIA) este obligatorie, se recomandă, totuși, ”efectuarea unei DPIA ca un instrument util pentru a ajuta operatorii de date să respecte legea privind protecția datelor”.

Prin urmare, în măsura în care prelucrarea datelor se realizează în special în cazurile stabilite de decizia sus-menționată, este obligatorie realizarea unei evaluări de impact.

Subliniem că, potrivit art. 36 din Regulamentul (UE) 2016/679, **operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor prevăzută la articolul 35 indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.**

Asupra tuturor evaluărilor de impact transmise, au fost efectuate numeroase observații de instituția noastră, fiind necesară punerea în acord a acestora cu Regulamentul (UE) 2016/679, ținând seama de ”Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentul (UE) 2016/679” adoptat de Comitetul european pentru protecția datelor.

■ **Activitatea de analiză şi soluţionare a plângerilor prealabile**

În anul 2019 au fost depuse la Autoritatea națională de supraveghere un număr de **51 de plângeri prealabile.**

În acest context, precizăm faptul că, 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.

Așadar, dintre plângerile prealabile formulate în condițiile legii, urmare a reanalizării susținerilor și dovezilor transmise de către petenți, **au fost admise un număr de 15 plângeri**, raportat la aspectele semnalate de către persoanele vizate în cauză.

Secțiunea a 3 – a:

Activitatea de reprezentare în fața instanţelor de judecată

În ceea ce privește activitatea de reprezentare în instanță, Autoritatea națională de supraveghere a gestionat în anul 2019 un număr de **207 dosare** aflate pe rolul instanţelor de judecată în diferite stadii procesuale.

Dintre acestea, pe parcursul anului 2019 au fost înregistrate un număr de **31** de cereri noi de chemare în judecată, întemeiate pe Regulamentul (UE) 2016/679 și Legea nr. 506/2004,

în contextul efectelor modificării cadrului normativ, dar și datorită perioadei de timp în care Autoritatea națională de supraveghere a aplicat preponderent avertismente în baza noilor reglementări europene și naționale, lăsând operatorilor o marjă de timp pentru asimilarea noilor dispoziții legale complexe și punerea în practică a acestora.

Și în anul 2019 au fost finalizate mai multe acțiuni în mod favorabil pentru instituția noastră, sub incidența vechii legislații privind protecția datelor (Legea nr. 677/2001), sens în care prezentăm mai jos câteva cazuri relevante:

1. Hotărâri definitive în litigii referitoare la supravegherea video a angajaților

Potrivit unei investigații efectuate de către Autoritatea națională de supraveghere, ca urmare a unor plângeri prin care se sesizau încălcări ale prelucrării datelor prin utilizarea de către un operator a unui sistem de supraveghere video prin care acesta își monitoriza angajații la locul de muncă, inclusiv în birouri, 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 notificat prelucrarea datelor înainte de începerea prelucrării, potrivit legislației în vigoare la data respectivă, a prelucrat în mod nelegal datele, deoarece nu a realizat informarea completă a persoanelor vizate și a prelucrat în mod excesiv datele personale (imaginea) ale angajaţilor săi prin intermediul camerelor video instalate în birouri.

De asemenea, operatorul a fost sancționat pentru neîndeplinirea obligaţiilor privind confidenţialitatea şi aplicarea măsurilor de securitate, întrucât nu a adoptat suficiente măsuri de confidenţialitate şi securitate a datelor prelucrate (imaginilor), sub aspectul elaborării unei politici de securitate, a stabilirii unor instrucţiuni precise pentru persoana care are acces la datele personale, a securizării spaţiului unde se află echipamentele de stocare şi acces la datele prelucrate prin intermediul sistemului de supraveghere video.

Operatorul a contestat în instanță, în cadrul unor **litigii distincte**, **procesul-verbal de constatare/sancţionare**, precum și **decizia** prin care Autoritatea dispunea, în temeiul art. 21 alin. (3) lit. d) din Legea nr. 677/2001, ca operatorul să ia măsuri pentru încetarea prelucrării datelor cu caracter personal efectuate prin intermediul camerelor de supraveghere video montate în birourile angajaţilor și ștergerea acestor înregistrări.

De asemenea, operatorul a solicitat instanței, **într-un alt litigiu**, anularea parțială a **Deciziei nr. 52/2012** privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, publicată în Monitorul Oficial nr. 389/2012, în sensul anulării art. 8 alin. (3) din acest act normativ care prevedea că *"Nu este permisă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, cu excepţia situaţiilor prevăzute expres de lege sau a avizului Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal."*

Instanțele judecătorești au menținut, prin decizii definitive, atât sancțiunea aplicată prin procesul-verbal de constatare-sancționare, cât și decizia prin care Autoritatea națională de supraveghere dispunea măsurile pentru încetarea prelucrării datelor cu caracter personal efectuate prin intermediul camerelor de supraveghere video montate în birourile angajaţilor și ștergerea acestor înregistrări.

Totodată, prin **decizia definitivă** a Curții de Apel Brașov, reconfirmată de Înalta Curte de Casație și Justiție, **s-a constatat că dispozițiile art. 8 alin. (3) din Decizia nr. 52/2012 sunt în acord cu dispozițiile naționale și europene în materie.**

Instanța a reținut că supravegherea angajaților prin mijloace de supraveghere video în interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă ar da angajatorilor puterea de a aplica măsuri discreționare și intruzive asupra propriilor angajați, prin supravegherea constantă a acestora.

Mai mult, instanța a constatat că legiuitorul național a prevăzut în norma contestată anumite situații de strictă interpretare, excepționale sau a instituit avizul Autorității naționale de supraveghere pentru aprobarea prelucrării datelor cu caracter personal ale angajaților pentru a acoperi situațiile ce se pot ivi în practică, în cazul existenței unor scopuri legitime, fără a se afecta dreptul la viață privată al angajaților.

2. Hotărâre definitivă într-un litigu referitor la prelucrarea datelor fără consimțământ

Autoritatea națională de supraveghere a efectuat o investigatie la un operator, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, în contextul primirii unei plângeri de la o persoană vizată ale cărei date cu caracter personal, inclusiv imagini, au fost prelucrate fără consimțământ de către deținătorul unui site de dating.

Persoana vizată a susținut că i-au fost prelucrate datele în legătură cu un cont creat pe un site de dating, deși nu ea crease acest cont și că deținătorul acestuia nu a dat curs solicitării de ștergere a datelor personale și a contului de pe site.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat săvârșirea faptei de „prelucrare nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 5 din aceeaşi lege, întrucât operatorul nu a făcut dovada că a obținut consimțământul expres și neechivoc al persoanei vizate pentru prelucrarea datelor sale cu caracter personal prin intermediul site-ului deținut de acesta.

Pentru faptele constatate operatorul a fost sancţionat contravenţional, procesul-verbal de constatare/sancţionare contravenţională fiind contestat la instanţa competentă.

Instanţa, analizând probatoriul administrat în cauză, a constatat că ”(...) a fost raportat faptul că profilul în discuție nu a fost realizat de titularul adresei de e-mail ....@yahoo.com - care s-a dovedit a fi semnatara petiției prin care a solicitat ștergerea acestuia; a arătat că primește mesaje deranjante, numele și pozele sunt reale, luate în mod abuziv de pe contul de facebook, iar restul informațiilor sunt greșite, unele clar cu tentă vindicativă”.

Tribunalul a reținut că numele și fotografiile în discuție constituie date cu caracter personal care aparțin persoanei vizate și care au fost prelucrate de deținătoarea site-ului.

Tribunalul nu a identificat vreo ipoteză care să atragă încadrarea în vreuna din situațiile de excepție care să permită prelucrarea datelor cu caracter personal fără consimțământ.

Totodată, Tribunalul notează că reclamanta a avut suficiente date care să o determine să efectueze cercetări în cauză, faptele semnalate fiind suficient de grave, afectând nu numai drepturile individului în procesul de prelucrare a datelor cu caracter personal, dar chiar demnitatea persoanei.

Astfel, Tribunalul a reținut că, potrivit art. 20 alin. 1 din Legea nr. 677/2001, operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Tribunalul notează că Legea nr. 677/2001 protejează persoana împotriva prelucrării nelegale a datelor, pe când termenii și condițiile invocate de petentă tind să opereze un transfer de responsabilitate utilizatorilor, deși petenta are calitatea de operator de date cu caracter personal pe platforma care îi aparține. Cu alte cuvinte, chiar dacă există un regulament al site-ului în care o persoană vizată trebuie să își probeze pretențiile, aceasta nu exonerează reclamanta de obligația de a preîntâmpina prelucrările nelegale de date cu caracter personal.

În materie de prelucrare și protecție a datelor cu caracter personal, principiul este dat de art. 5 alin. 1 din Legea nr. 677/2001. Așadar, principiul constă în necesitatea acordării consimțământului persoanei la orice prelucrare a datelor ce o vizează. Însă pentru a determina dacă o persoană are

calitatea de persoană ale cărei date sunt prelucrate, implicit, trebuie stabilită identitatea persoanei care furnizează datele la momentul creării contului; aceasta întrucât orice individ, la un moment dat, poate furniza date personale care nu îi aparțin, iar scopul protecției instituite de Legea nr. 677/2001 să fie înfrânt. Tribunalul consideră că o astfel de obligație se impune reclamantei pentru a evita pe viitor situații cum sunt cele ale conturilor false; eventuala reținere a petentei de a face aplicarea acestei practici poate fi înlăturată în considerarea argumentului că petenta oricum prelucrează date cu caracter personal ale utilizatorilor, fiind vorba de un aspect cantitativ al datelor.

Tribunalul notează că reclamanta a rămas indiferentă la sesizarea unui terț, care s-a dovedit a fi chiar persoana reprezentată în contul de pe platforma.ro, în contextul în care contul creat conținea fotografiile acesteia, iar detaliile personale cuprindeau date cu privire la orientarea sexuală și constituția corpului, că a ignorat cu ușurință o serie de obligații cu privire la colectarea și prelucrarea datelor cu caracter personal, care au avut ca efect atât înfrângerea dreptului asupra manipulării acestora, cât și lezarea demnității individului, că nu și-a dat seama de valorile lezate prin fapta sa."

Prin urmare, instanța de fond a reținut că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit, astfel că au fost menţinute sancţiunile contravenţionale aplicate.

Hotărârea a rămas definitivă în favoarea Autorității naționale de supraveghere, prin respingerea apelului formulat de operatorul sancționat.

3. Hotărâre definitivă într-un litigiu privind dezvăluiri de date

Autoritatea națională de supraveghere a efectuat o investigatie, raportat la prevederile Legii nr. 677/2001, ca urmare a faptului că o persoană fizică a sesizat că au fost publicate în anul 2017 mai multe articole în edițiile on-line ale unui cotidian, în cuprinsul cărora au fost dezvăluite datele cu caracter personal ale persoanei vizate și ale copilului minor, în speță: nume, prenume, locul de muncă al persoanei vizate, instituția de învățământ frecventată de copilul minor.

Petentul a precizat că s-a adresat operatorului care deține cotidianul, atât prin e-mail, cât și prin poștă, solicitând în anul 2017 "ștergerea datelor a căror prelucrare nu este conformă cu legea", respectiv numele și prenumele copilului său minor, însă nu a primit răspuns.

Autoritatea națională de supraveghere și-a exercitat atribuțiile de control, a demarat la începutul anului 2018 o investigație în scris, pentru clarificarea aspectelor semnalate de petent, însă investigația a continuat și după 25 mai 2018, dată de la care a început aplicarea Regulamentului(UE) 2016/679.

Ca urmare a analizării documentelor și informațiilor comunicate de operator, ulterior aplicării Regulamentului (UE) 2016/679, Autoritatea a solicitat operatorului să șteargă orice informație care să ducă la identificarea minorului în articolele menționate și să comunice măsurile adoptate.

Autoritatea a constatat faptul că operatorul nu a respectat dispozițiile legale privind dreptul de intervenție exercitat de petent cu privire la datele fiului minor, prevăzut de art. 14 din Legea nr. 677/2001 (contravenție în baza art. 32 din Legea nr. 677/2001), respectiv de art. 17 și 12 din Regulamentul (UE) 2016/679, întrucât nu a prezentat dovezi că, până la data încheierii procesului-verbal de constatare/sancționare, a transmis un răspuns către petent, cu referire la ștergerea datelor minorului (...), (respectiv nume, prenume, instituția de învățământ frecventată de minor) dezvăluite în edițiile on-line ale cotidianului și în ediția scrisă a acestuia.

Ca urmare a investigației efectuate la operator, Autoritatea națională de supraveghere a dispus prin procesul-verbal de constatare/sancţionare, în temeiul art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, precum și la art. 12 din Legea nr. 190/2018, măsuri corective împotriva acestuia, precum și obligația ca în termen de 45 de zile de la data comunicării procesului-verbal să transmită Autorității dovezi cu privire la respectarea măsurilor corective dispuse.

Operatorul a contestat în instanță măsurile corective dispuse.

Instanța, analizând probatoriul administrat în cauză, faptele săvârșite de operator în anul 2017, dată la care erau vigoare dispozițiile Legii nr. 677/2001, precum și dispozițiile aplicabile la data încheierii procesului-verbal de constatare/sancționare, respectiv Regulamentul (UE) 2016/679 și Legea nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare efectuate în baza Legii nr. 129/2018, care a abrogat Legea nr. 677/2001, a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit.

Hotărârea judecătorească a rămas definitivă în favoarea Autorității naționale de supraveghere.

4. Hotărâri pronunțate în litigii privind modalitatea de prelucrare a datelor cu caracter personal în sistemul Biroului de Credit

► Prin decizia **Curții de Apel București**, **definitivă**, instanța a statuat următoarele: ”Curtea observă că prin Procesul verbal de sancționare contravențională Autoritatea de Supraveghere a reținut că Banca intimată a prelucrat date cu nesocotirea drepturile prevăzute de art. 14 raportat la

art. 12 și art. 4 alin. (1) lit. a) din Legea nr.677/2001, constând în faptul de a nu da curs cererilor d-nului (....), prin care acesta și-a exercitat dreptul de intervenție în sensul de a fi adoptate măsuri de ștergere a datelor negative transmise la Biroul de Credit, având în vedere că banca nu a făcut dovada că a realizat informarea prealabilă a persoanei vizate înainte de transmiterea datelor negative pentru informațiile transmise (...).

Altfel spus, prelucrarea datelor cu caracter personal s-a realizat atât prin încălcarea drepturilor persoanei vizate, respectiv ale d-nului XY, constând în neștergerea de către operator - în urma cererilor expres formulate (...) a datelor a căror prelucrare nu este conformă cu legea, în sensul că, mai înainte de a fi fost transmise la Biroul de Credit, persoana menționată trebuia informată în prealabil, cu 15 zile înainte de transmiterea datelor, cât și prin încălcarea dreptului constând în nefurnizarea persoanei vizate a informațiilor prevăzute la art. 12."

În ceea ce privește modalitatea de săvârșire a faptelor Curtea de Apel apreciază că respectarea dreptului de informare nu se realizează la momentul încheierii contractului prin înștiințarea persoanei cu privire la riscul raportării datelor negative în caz de neplată a ratelor, ci se realizează în concret la momentul conturării datei negative, când raportarea este iminentă.

Pe cale de consecință, refuzul băncii de a da curs cererilor de intervenție formulate de persoanele sus menționate este nelegal, neexistând nici o justificare pentru care ar putea fi reținut de către prezenta instanță ca legal, astfel că faptele contravenționale au fost corect reținute de Autoritatea apelantă prin procesul verbal de contravenție contestat în cauză.

Împrejurarea că respectivul client ar fi cunoscut faptul că înregistrează rate restante, că a fost somat în nenumărate rânduri pentru a plăti ori în sensul că are cunoștință de posibilitatea comunicării respectivelor informații negative către Biroul de Credit încă de la momentul semnării contractului de credit - constituie o apărare ce nu poate fi primită deoarece obligațiile legale ale băncii sunt neechivoce, nesusceptibile de vreo interpretare, statuând în mod clar obligația de comunicare a datelor numai după înștiințarea realizată cu cel puțin 15 zile calendaristice înainte de data transmiterii, obligații neîndeplinite, astfel cum corect s-a reținut prin procesul verbal de contravenție, fapt dovedit de documentația ce a stat la baza emiterii, depusă la dosarul de fond. Este adevărat că petentul a fost somat/notificat în mai multe rânduri, însă în niciuna dintre notificări nu există informații cu privire la transmiterea datelor negative la Biroul de Credit.

Pentru nerespectarea acestui drept la informare, Curtea apreciază că nu are nicio justificare refuzul Băncii intimate de a soluționa favorabil cererile adresate de petent în sensul ștergerii datelor transmise în mod nelegal.

În ceea ce privește mențiunea ,.Cont cumpărat de un alt creditor", înscrisă la Biroul de Credit SA, instanța a statuat că aceasta face parte tot din categoria datelor negative, cum corect a arătat Autoritatea națională de supraveghere, întrucât, coroborată cu informațiile înscrise la ,;Valoarea lunară programată" și „Suma plătită", cât și cu informațiile din notificările cesiunii de creanță, reprezintă o informație referitoare la neplata obligațiilor decurgând din relația de creditare.

►Cu **privire la obligativitatea de a da curs cererii de ștergere a datelor**, într-o speță similară, prin hotărârea pronunțată de **Tribunalul București**, instanța a reținut că "**petenta avea obligația legală**, potrivit prevederilor art. 14 alin. (1) din Legea nr. 677/2001, **de a da curs cererilor acestuia, în sensul ștergerii datelor transmise fară informarea sa prealabilă**. **Solicitantul era îndreptățit să i se șteargă datele negative** transmise la Biroul de Credit, întrucât acestea au fost transmise nelegal, **fără informarea sa prealabilă**, astfel cum este prevăzut la art. 8 alin. (2) al Deciziei ANSPDCP nr. 105/2007 coroborat cu ari. 9 din această Decizie."

Aceeași instanță, cu privire informarea prealabilă a arătat că "**nu se poate considera că prin notificările trimise de bancă clientului cu privire la îndeplinirea obligațiilor contractuale, petenta și-ar fi îndeplinit obligația de informare prealabilă** și ar "fi oferit informațiile prevăzute de art. 9 din Decizia nr. 105/2007. Este de subliniat că petenta **nu a prezentat** nici la data controlului și nici ulterior **dovezi** privind informarea prealabilă a clientului cu cel puțin 15 zile calendaristice înainte de data transmiterii datelor. în vreuna dintre modalitățile prevăzute de art. 8 alin. (2) din Decizia ANSPDCP nr. 105/2007, pentru această raportare.

Notificările trimise de bancă către XY **cu privire la îndeplinirea obligațiilor contractuale nu reprezintă înștiințarea prealabilă prevăzută la art. 8 alin. 2 coroborat cu art. 9 din Decizia nr. 105/2007 raportat la art. 12 din Legea nr. 677/2001.**

În acest sens, tribunalul reține că în mod corect s-a ajuns, în urma verificărilor efectuate de către organele de control ale *Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal,* la concluzia săvârșirii faptei contravenționale de către petentă. Pentru respectarea dispozițiilor art. 8 alin. (2) din Decizia nr. 105/2007 **se impunea informarea persoanelor vizate <u>înainte de fiecare raportare de date negative Ia Biroul de Credit</u>**, fie că acestea erau acumulate din aceeași restanță sau una nouă".

Aceeași instanță a arătat că "fiind vorba de date negative care se schimbă de la o perioada la alta de raportare, este obligatoriu ca fiecare transmitere către sistemele dc evidență de tipul birourilor de credit să aibă loc numai după înștiințarea prealabilă în scris, telefonic, prin SMS sau e-mail, a

persoanei vizate cu privire la întârzierea la plată și transmiterea datelor, realizată cu cel puțin 15 zile calendaristice înainte de data fiecărei transmiteri." "(...) **Informațiile negative raportate la SC Biroul de Credit SA pot fi folosite în detrimentul persoanei în cauză, iar datele sunt disponibile instituțiilor financiare și de credit, cu ocazia analizării gradului de risc și solvabilitate.** Perioada de stocare a datelor referitoare la întârzierile la plată (date negative) este de 4 ani de la data achitării ultimei rate restante sau de la data ultimei actualizări transmise, în cazul neachitării restanțelor până la data respectivă.(...) Date fiind și aceste considerente, concluzia evidentă este aceea că în cauză se impunea informarea persoanei vizate înainte de fiecare raportare cu date negative la Biroul de Credit, fie că acestea erau acumulate din aceeași restanță sau din una nouă."

Hotărârea instanței favorabilă Autorității naționale de supraveghere a rămas definitivă.

5. Hotărâri pronunțate în litigii privind nerespectarea dreptului de acces prevăzut de art. 13 din Legea nr. 677/2001

► Autoritatea națională de supraveghere a efectuat o investigaţie la o instituție bancară centrală, ca urmare a unei plângeri prin care se sesiza nerespectarea drepturilor unei persoane vizate privind prelucrarea datelor la Centrala Riscului de Credit.

Prin documentele anexate petiţiei, persoana vizată a făcut dovada că s-a adresat la instituția bancară în scris, prin intermediul poştei electronice, de la adresa personală de e-mail, cu o cerere în care a invocat dreptul de acces prevăzut de art. 13 din Legea nr. 677/2001, solicitând să i se confirme dacă datele sale cu caracter personal sunt prelucrate în sistemul de evidență al Centralei Riscului de Credit și al Centralei Incidentelor de Plată și să i se elibereze un extras din care să rezulte operatorii care au transmis datele către acest sistem. Persoana vizată a susținut faptul că nu a primit un răspuns la această cerere, conform solicitărilor sale.

Analizând probatoriul administrat în cauză, Tribunalul București a respins, ca neîntemeiată, plângerea contravențională formulată de instituția bancară împotriva procesului-verbal de constatare și sancționare a contravenției, prin care fusese sancționată cu avertisment.

Pentru a dispune astfel, cu privire la **modalitatea de transmitere a cererii persoanei vizate către bancă, Tribunalul București a arătat că aceasta "nu este obligată să soluționeze conform Legii nr. 677/2001 numai cererile primite prin poștă, această interpetare fiind în mod evident contrară legii.**

Cererea trebuie să fie întocmită în formă scrisă, datată și semnată, condiții îndeplinite (...), chiar dacă aceasta a fost trimisă prin e-mail. De asemenea, instanța constată că chiar art. 13 alin. 2 din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor

cu caracter personal și libera circulație a acestor date prevede că solicitantul poate arăta în cerere dacă dorește ca informațiile să îi fie comunicate la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.

De asemenea, instanța a mai stabilit că **”este mai mult decât evident că de vreme ce răspunsul poate fi comunicat la o anumită adresă, care poate fi și de poștă electronică și cererea poate fi formulată prin poștă electronică, răspunsul petentei care este în fapt unul negativ fiind nelegal și abuziv.**

(....) **Prin urmare, instanța apreciază că petenta nu a reușit să răstoarne prezumția de legalitate și temeinicie a procesului-verbal de contravenție contestat, în condițiile în care probele administrate de instanță sunt apte să convingă instanța în privința existenței faptei contravenționale și a vinovăției petentei, în afara oricărui dubiu rezonabil.”**

În ceea ce privește **individualizarea sancțiunii contravenționale principale aplicate,** respectiv avertismentul, **instanța constată legalitatea și temeinicia acesteia, pe care o consideră blândă, având în vedere consecințele faptei contravenționale săvârșite de petentă.**

Instanța apreciază că faptele de acest gen, nelegale și abuzive, sancționate de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date face absolut necesară sancționarea cu amendă contravențională.”

Hotărârea instanței favorabilă Autorității naționale de supraveghere a rămas definitivă.

► **Tribunalul București a respins, ca neîntemeiată, plângerea contravențională formulată de operator** împotriva procesului-verbal de constatare și sancționare a contravenției, prin care operatorul fusese sancționat cu amendă, întrucât **nu a respectat dreptul de acces al persoanei vizate prevăzut de art. 13 din Legea nr. 677/2001.** Prin cererea sa, aceasta solicita informații cu privire la: scopul prelucrării datelor sale cu caracter personal, destinatarii/categoriile de destinatari ai datelor, datele care fac obiectul prelucrării, orice informații disponibile cu privire la originea datelor, activitatea desfășurată, durata activității, veniturile realizate, salariul brut, încadrarea în grupe de muncă, vechime în muncă și în specialitate conform contractului individual de muncă pe perioada în care acesta a fost angajat al operatorului.

Pentru a dispune astfel, instanța a arătat că: ”prin răspunsul adresat solicitantului (...) reclamanta a menționat că pune la dispoziție solicitantului, prin poștă, copia integrală a dosarului personal pe suport de hârtie.

Punerea la dispoziția solicitantului, prin poștă, a copiei dosarului personal pe suport de hârtie, nu echivalează cu comunicare informațiilor solicitate prin cererea formulată (...) în temeiul art. 13 din Legea nr. 677/2001.

În ceea ce privește individualizarea sancțiunii, în concret, Tribunalul a apreciat că ”**fapta comisă de reclamantă prezintă un grad de pericol social care justifică aplicarea amenzii**, în cuantumul stabilit de instituția pârâtă, dat fiind pericolul social al faptei săvârșite, aplicarea sancțiunii contravenționale fiind în concordanță cu dispozițiile art. 21 alin. 3 din OG nr. 2/2001 și în limitele prevăzute de Legea nr. 677/2001.

(...) Mai mult, se are în vedere **atitudinea reclamantei** care **nu a recunoscut săvârșirea faptei contravenționale**, astfel că, în măsura în care aceasta nu s-a manifestat în sensul înțelegerii faptei săvârșite, a recunoașterii acesteia, **instanța apreciază că periculozitatea acesteia este ridicată**”.

Hotărârea instanței favorabilă Autorității naționale de supraveghere a rămas definitivă.

6. Hotărâre pronunțată într-un litigiu privind transmiterea de mesaje comerciale nesolicitate.

Instanțele de judecată au confirmat măsurile dispuse de Autoritatea națională de supraveghere în cazul transmiterii de mesaje comerciale nesolicitate.

► Autoritatea națională de supraveghere a efectuat o investigaţie la un operator, ca urmare a unei plângeri prin care se sesiza o încălcare a legislației privind prelucrarea datelor cu ocazia transmiterii de mesaje comerciale, respectiv fără acordul prealabil al persoanei vizate, reclamându-se totodată lipsa unui răspuns al operatorului la cererea de ștergere.

Analizând probatoriul administrat în cauză, Tribunalul București a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit.

Cu privire la temeinicia procesului-verbal de contravenție, instanța a reținut că ”din actele depuse la dosar petenta nu a dovedit altă stare de fapt decât cea menționata în procesul verbal de contravenție atacat.

Apărarea petentei în sensul că a mai fost sancționată pentru aceeași fapta printr-un alt proces verbal de contravenție pentru refuzul de comunicare a informațiilor a fost considerată neîntemeiată de tribunal care a constat că se referă la o altă perioadă de timp, astfel încât ”**nu există astfel o dubla sancționare (...)” .**

În ceea ce privește individualizarea sancțiunii, în raport cu pericolul social al faptei și criteriile generale de individualizare prevăzute de art. 21 alin. (3) din O.G. nr. 2/2001, instanța în mod corect a constatat ”că sancțiunea aplicată petentului de către agentul constatator a fost corect individualizată.”

Hotărârea instanței favorabilă Autorității naționale de supraveghere a rămas definitivă.

Secțiunea a 4 -a
Informare publică

În cursul anului 2019, Autoritatea naţională de supraveghere a continuat activităţile de comunicare destinate informării publicului larg, cu privire la regulile specifice de prelucrare a datelor cu caracter personal, în contextul Regulamentului (UE) 2016/679, cele mai relevante fiind prezentate în continuare.

♦ Ziua Europeană a Protecţiei Datelor – 28 Ianuarie 2019

Pentru sărbătorirea Zilei Europene a Protecţiei Datelor, Autoritatea naţională de supraveghere a organizat Conferința cu tema **„Asigurarea respectării Regulamentului european privind protecția datelor și a reglementărilor naționale aplicabile”**, la Palatul Parlamentului, pe data de **28 Ianuarie 2019**.

Evenimentul 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 privind unele măsuri de punere în aplicare a Regulamentului General privind protecția datelor, raportat și la competențele Autorității.

Pentru marcarea acestui eveniment, Autoritatea națională de supraveghere a pregătit și pus la dispoziția publicului unele materialele informative (broșuri, pliante) dedicate Zilei Europene a Protecţiei Datelor.

♦ Dezbaterea aniversară ”Un an de la aplicarea Regulamentului (UE) 2016/679” – 24 Mai 2019

De asemenea, cu prilejul sărbătoririi unui **an de la aplicarea Regulamentului (UE) 2016/679**, Autoritatea naţională de supraveghere a organizat, în luna mai 2019, o serie de manifestări în vederea creșterii gradului de informare a publicului larg asupra noilor reguli de asigurare a protecției datelor cu caracter personal și a drepturilor specifice de care beneficiază persoanele fizice.

În acest sens, a fost organizată pe 24 mai 2019 o dezbatere aniversară – 1 an de GDPR, la sediul instituției, la care au participat reprezentanți ai asociațiilor și uniunilor profesionale (Asociația Română de Marketing Direct – ARMAD, Uniunea Colegiilor Consilierilor Jurdici din România - UCCJR, Asociația Română a Băncilor - ARB, Asociaţia de Management al Creanţelor Comerciale – AMCC, Biroul Român de Audit Transmedia - BRAT, Asociația Operatorilor Mobili din România - AOMR, Uniunea Națională a Societăților de Asigurare-Reasigurare din România - UNSAR, Asociația pentru Bune Practici GDPR, Asociația Comunelor.

În cadrul discuțiilor au fost abordate aspecte de aplicabilitate practică referitoare, în special, la responsabilul cu protecția datelor, asigurarea drepturilor persoanelor vizate, evaluarea impactului asupra protecției datelor, codurile de conduită și notificarea încălcării securității datelor cu caracter personal.

De asemenea, pentru marcarea acestui eveniment, Autoritatea națională de supraveghere a lansat și un **Ghid privind întrebări și răspunsuri cu privire la aplicarea Regulamentului (UE) 2016/679**.

În plus, cu sprijinul Societății de Transport București - STB SA, pentru aceste evenimente s-a difuzat în mijloacele de transport în comun **un mesaj de interes public referitor la principalele aspecte reglementate de Regulamentul (UE) 2016/679**, iar la sediul Autorității a fost organizată **”Ziua Porților Deschise”**.

Același mesaj a fost difuzat și prin intermediul sistemului de televiziune disponibil în incintele metroului și în Aeroportul Internațional Henri Coandă.

♦ Conferințe, simpozioane, seminarii, reuniuni

Pe tot parcursul anului 2019, instituţia noastră a participat activ la cele mai **importante evenimente** cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private, inclusiv de organizații neguvernamentale.

La aceste reuniuni, reprezentanții Autorității naționale de supraveghere au clarificat anumite aspecte privind condițiile utilizării datelor, respectarea drepturilor persoanelor vizate şi asigurarea confidenţialităţii prelucrărilor de date cu caracter personal, ceea ce reflectă continuitatea deschiderii Autorității către societatea civilă.

În acest context, menționăm că, în anul 2019, Autoritatea națională de supraveghere a participat gratuit, ca în fiecare an, la o serie de **conferințe, simpozioane și seminarii, în București și în țară**, cum ar fi:

- la Cluj-Napoca, Iași, Constanța și Timișoara, la reuniuni organizate de către Asociația Expert Forum, pentru susținerea de prelegeri referitoare la prelucrarea datelor de către ONG-uri;
- la Instituția Prefectului Județului Timiș și Instituția Prefectului Județului Mehedinți, pentru susținerea seminariilor cu tema ”Protecția datelor în administrația publică locală”;
- în județul Brașov, pentru participarea la conferința ”Program de pregătire pentru organizațiile minorităților naționale – asistență financiară și utilizarea sumelor de la bugetul de stat";
- în București, la Camera de Comerț și Industrie București, pentru susținerea unei prelegeri la conferința ”Data Protection - Solutions and Responsabilities”;
- în București, la Uniunea Națională a Notarilor Publici (UNNP) pentru susținerea unei prelegeri privind protecția datelor în cadrul Colocviului organizat de acest for profesional;
- în București, la Institutul European din România (IER) pentru susținerea unei prelegeri intitulate ”Protecția datelor cu caracter personal în cadrul raporturilor de muncă”;
- în București, la conferința intitulată ”GDPR Talks”, pentru susținerea unei prelegeri, precum și la alte conferințe organizate de instituții publice sau private;
- în București, la o conferința dedicată GDPR, organizată de o firmă de avocatură, pentru susținerea unei prelegeri.

Pe de altă parte, subliniem că **s-a acordat consiliere zilnică telefonic și la sediu** mai multor operatori din mediul public și privat, 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.

Astfel, 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.

Prin urmare, s-au derulat întâlniri cu **autorități și instituții publice**, atât la sediul acestora, cât și la sediul Autorității naționale de supraveghere, precum: Autoritatea Națională pentru Protecția Consumatorilor, Inspectoratul pentru Situații de Urgență, Ministerul Justiției, Consiliul Superior al Magistraturii, Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, Ministerul Sănătății, Oficiul Național de Prevenire și Combatere a Spălării Banilor, Casa Națională de Asigurări de Sănătate, Autoritatea Electorală Permanentă, Ministerul Afacerilor Externe, inclusiv Agentul Guvernamental pentru CJUE, Consiliul Naţional pentru Studierea Arhivelor Securităţii.

Totodată, **reprezentanții Autorității naționale de supraveghere au participat și la comisiile parlamentare de specialitate** în vederea susținerii unor propuneri sau proiecte de legi ce vizau aspecte de protecția datelor personale.

În ceea ce privește **operatorii din sectorul privat**, au fost realizate întâlniri de lucru la sediul Autorității naționale de supraveghere, în cadrul cărora au fost purtate discuții pe aspecte privind condițiile legale de prelucrare a datelor în diferite domenii de activitate, precum și referitoare la redactarea codurilor de conduită de către unele asociații ale operatorilor.

Astfel, au fost efectuate **întâlniri** cu Asociația Română a Băncilor (ARB), SC Biroul de Credit SA, Biroul Român de Audit Transmedia (BRAT), Vodafone România SA, Telekom, Asociația Operatorilor Mobili din România (AOMR), Camera de Comerț Româno-Americană (AmCham), Consiliul Investitorilor Străini (FIC), Uniunea Națională a Societăților de Asigurare-Reasigurare din România (UNSAR), Raiffeisen Bank, precum și societăți de avocatură reprezentanți ai operatorilor, Asociația de Acreditare din România - RENAR, Asociația Specialiștilor în Confidențialitate și Protecția Datelor (ASCPD), Asociația Expert Forum.

Având în vedere întrebările frecvente adresate Autorității naționale de supraveghere cu privire la chestiuni punctuale privind aplicarea Regulamentului (UE) 2016/679, pentru a veni în sprijinul celor interesați, **instituția noastră a elaborat și dat publicității, în anul 2019, ”Ghidul «Întrebări și Răspunsuri» cu privire la aplicarea Regulamentului (UE) 2016/679”.**

♦ Site-ul Autorității naționale de supraveghere

O informare promptă şi eficientă a persoanelor fizice, dar și a operatorilor, s-a realizat și prin intermediul site-ului Autorității, atât prin prisma celor **48 de comunicate de presă** postate la secțiunea ”Știri”, cât și a informațiilor de la **secțiunea specială dedicată Regulamentului General privind Protecția Datelor**, actualizată pe măsura adoptării de către Comitetul pentru Protecția

Datelor a diferitelor opinii și ghiduri, precum și a altor documente de interes în domeniul protecției datelor.

De asemenea, o nouă abordare din punct de vedere a informațiilor de interes public a reprezentat-o publicarea de către instituția noastră a sancțiunilor și măsurilor corective dispuse în anul 2019, în baza Regulamentului (UE) 2016/679.

Pe parcursul anului 2019, operatorii au continuat să declare **responsabilii cu protecția datelor**, înregistrându-se la Autoritatea națională de supraveghere un număr de **4318** responsabili numiți de către operatorii din sectorul public și privat. Declararea acestora se realizează în sistem on-line, prin completarea formularului dedicat în acest sens, pus la dispoziție pe site-ul www.dataprotection.ro în anul 2019.

De asemenea, în anul 2019, pe site-ul Autorității naționale de supraveghere au fost puse la dispoziție și alte formulare, instituția noastră oferind posibilitatea completării ON-LINE a acestora, astfel:

- *Formularul de Plângere potrivit Regulamentului (UE) 2016/679*
- *Formularul de Notificare de încălcare a securității datelor cu caracter personal pentru operatorii de date cu caracter personal, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)*
- *Formularul de Notificare de încălcare a securității datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicările electronice.*

CAPITOLUL IIII

ACTIVITATEA DE MONITORIZARE ȘI CONTROL

Secțiunea 1. Prezentare generală

Și în anul 2019, 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 2019, s-a continuat activitatea de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat. Astfel, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea prevederilor Regulamentului (UE) 2016/679, dar și ale Legii nr. 506/2004.

Investigaţiile efectuate din oficiu au avut ca obiect verificarea respectării prevederilor legale ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, potrivit art. 33 alin. (1) din Regulamentul (UE) 2016/679, precum și ca urmare a sesizărilor transmise Autorității de către diverse entități.

Astfel, în ceea ce privește incidentele de securitate, acestea au vizat, în principal, următoarele aspecte: dezvăluirea neautorizată a datelor cu caracter personal; pierderea trimiterilor poștale; indisponibilitatea datelor cu caracter personal; accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV); accesul ilegal la datele personale ale clienților în sistemul bancar.

Totodată, sesizările privind posibile neconformități cu dispozițiile Regulamentului (UE) 2016/679 au avut ca obiect aspecte precum: lipsa măsurilor de securitate a prelucrărilor de date; prezența camerelor de supraveghere video; publicarea datelor cu caracter personal în mediul online.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul menținerii numărului semnificativ al acestora (5808), în anul 2019 au continuat să fie sesizate, în principal, aspecte referitoare la:

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

•instalarea de sisteme de supraveghere video la nivelul diverselor entități;

•primirea de mesaje comerciale nesolicitate;

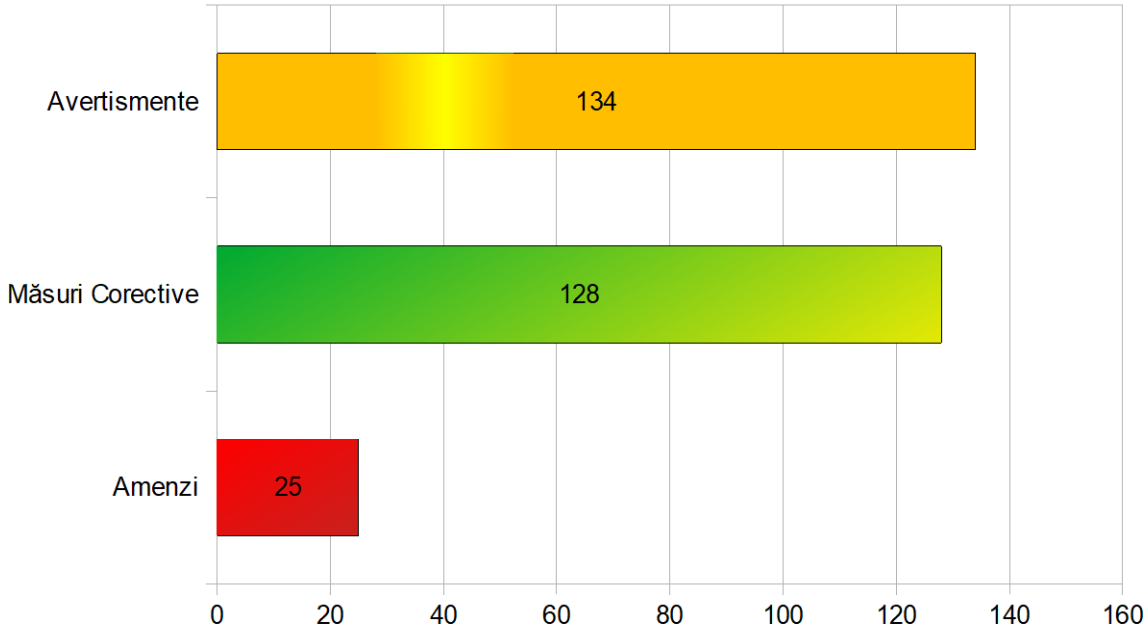
•încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale, respectiv, neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor;

•nerespectarea condițiilor privind consimțământul în mediul online.

În anul 2019, Autoritatea națională de supraveghere a primit un **număr total de 6193 de plângeri, sesizări și notificări privind incidente de securitate**, pe baza cărora au fost deschise **912 investigații.**

Ca urmare a investigațiilor efectuate, au fost aplicate **28 de amenzi în cuantum total de 2.339.291,75 lei.**

De asemenea, au mai fost aplicate **134 de avertismente** și au fost dispuse **128 de măsuri corective.**



Secțiunea a 2 – a: Investigații din oficiu

1. Prezentare generală

Începând din data de 25 mai 2018, dată la care a fost pus în aplicare și în România Regulamentul (UE) 2016/679, investigațiile din oficiu au avut ca obiect verificarea respectării prevederilor legale ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, potrivit art. 33 alin. (1) din Regulamentul (UE) 2016/679, precum și ca urmare a sesizărilor transmise Autorității naționale de supraveghere.

În anul 2019, s-a continuat activitatea de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat.

Astfel, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea prevederilor Regulamentului (UE) 2016/679.

În ceea ce privește incidentele de securitate, în anul 2019, operatorii de date au transmis un număr de **233 de notificări**, atât în temeiul Regulamentului (UE) 2016/679, cât și al Legii nr. 506/2004 și au vizat, în principal, următoarele aspecte: dezvăluirea neautorizată a datelor cu caracter personal; pierderea trimiterilor poștale; indisponibilitatea datelor cu caracter personal; accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV); accesul ilegal la datele personale ale clienților în sistemul bancar.

Totodată, **sesizările** privind posibile neconformități cu dispozițiile Regulamentului (UE) 2016/679 s-au ridicat la un număr de **152** și au avut ca obiect aspecte precum: lipsa măsurilor de securitate a prelucrărilor de date; prezența camerelor de supraveghere video; publicarea datelor cu caracter personal în mediul online.

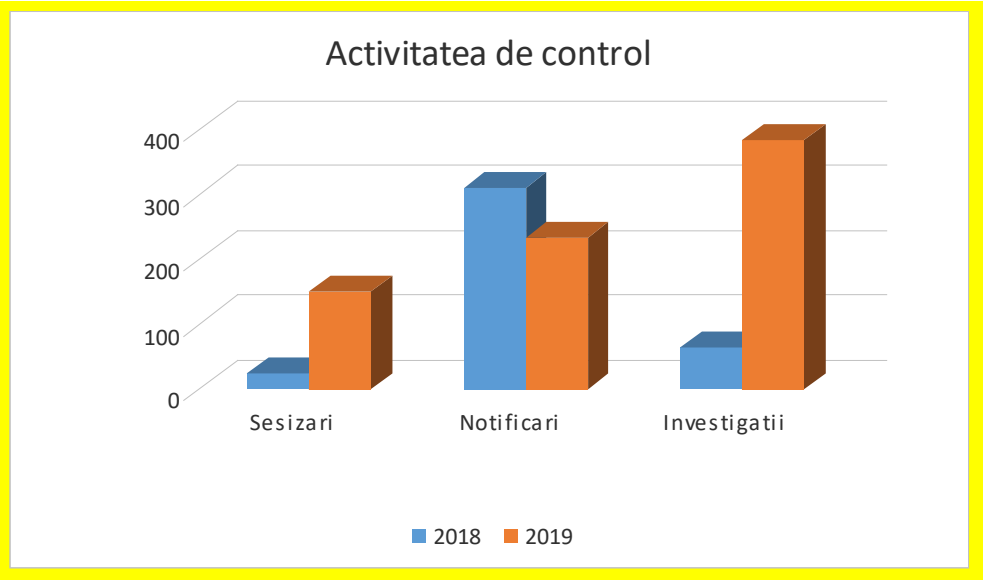
Ca urmare a sesizărilor primite și încălcărilor de securitate notificate de către operatorii de date cu caracter personal, pe parcursul anului 2019, la nivelul Autorității naționale de supraveghere a fost deschis un număr de **385 de investigații din oficiu**.

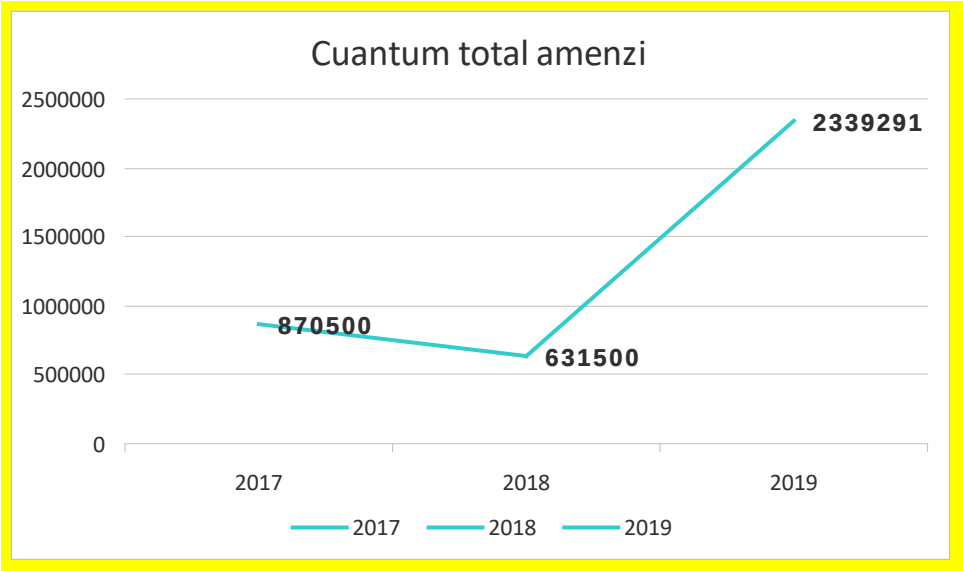
Urmare a investigațiilor efectuate din oficiu, în anul 2019 au fost aplicate **11 amenzi** în cuantum total de **2.099.124,95 lei (445.000 Euro)**, **14** avertismente și **13** măsuri corective.

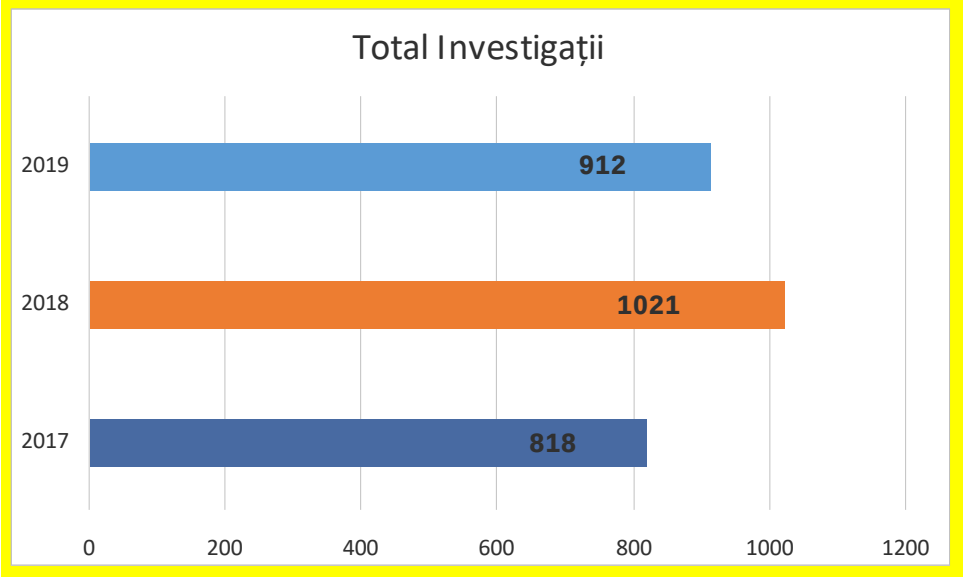
Măsurile corective dispuse în urma investigațiilor din oficiu au vizat, în special, următoarele:

- Revizuirea și actualizarea măsurilor tehnice și organizatorice implementate, inclusiv ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor

- Revizuirea și actualizarea procedurilor de lucru referitoare la protecția datelor cu caracter personal
- Realizarea informării persoanelor vizate potrivit art. 12 din RGPD, prin combinarea cu 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, în vederea menținerii securității și a prevenirii prelucrărilor care încalcă Regulamentul (UE) 2016/679, 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.







A. Investigații referitoare la prelucrarea datelor cu caracter personal în domeniul financiar-bancar

După intrarea în vigoare a Regulamentului (UE) 2016/679, 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, ca de exemplu instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

1. FIȘĂ DE CAZ – Divulgare neautorizată de date cu caracter personal prin intermediul extraselor de cont/detaliilor tranzacțiilor

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, prin intermediul formularelor de extras de cont/detalii tranzacție emise de către o instituție bancară clienților săi, ca urmare a unei tranzacții on-line, la rubrica „Plătitor” sunt dezvăluite către beneficiarul tranzacției și date privind CNP-ul și adresa persoanei care a efectuat plata.

Ca urmare a informațiilor solicitate de către Autoritatea națională de supraveghere, în cadrul investigației desfășurate, instituția bancară a comunicat faptul că avea cunoștință de situația semnalată și a solicitat modificarea funcționalităților sistemelor informatice utilizate pentru emiterea și comunicarea extraselor de cont/a documentelor electronice ce cuprind detaliile tranzacțiilor online, în sensul filtrării informațiilor ce sunt dezvăluite în cadrul acestor documente, astfel încât informațiile legate de CNP și adresa plătitorului să nu mai fie afișate în extrasele de cont eliberate clienților, luând în considerare toate canalele vizate.

Totodată, instituția bancară a declarat că eliminarea *CNP* și *adresa plătitor* din listele de tranzacții ale beneficiarilor, clienți ai Băncii, a fost una dintre măsurile de conformare identificate în cadrul analizei de impact a prevederilor Regulamentului (UE) 2016/679, cu scopul minimizării datelor și al evitării unei prelucrări excesive a acestora, nefiind identificat un moment anume în care datele au devenit vizibile în extrasele de cont.

De asemenea, anterior demarării investigației Autorității naționale de supraveghere, au fost puse în producție anumite update-uri ale funcționalităților IT pentru canalul online banking, urmând să fie realizate și update-uri în vederea conformării cu prevederile Regulamentului (UE) 2016/679.

În ceea ce privește numărul de tranzacții efectuate prin canalul online banking, în perioada investigată, clienții operatorului (persoane fizice și juridice) au realizat prin intermediul canalului online banking 28.743.554 tranzacții (plăti, transferuri, schimburi valutare, în lei și în valută) atât către conturi deschise la Bancă, cât și către conturi deschise la alte instituții de credit. Din numărul total de 28.743.554 de tranzacții indicat mai sus, adresa plătitorului a fost postată în cazul a 1.884.604 de tranzacții.

Din investigația efectuată în acest caz, a rezultat că instituția bancară, în documentele ce conțin detaliile tranzacțiilor și care sunt puse online la dispoziția clienților beneficiari ai plăților (vizualizate prin intermediul aplicației online banking), a dezvăluit către beneficiarii tranzacțiilor date cu caracter personal, astfel:

- date privind CNP-ul și adresa persoanei care a efectuat plata (plătitorului), pentru situațiile în care plătitorul efectua tranzacția dintr-un cont deschis la o alta instituție de credit – (tranzacții externe și depuneri la casierie);
- date privind adresa plătitorului, pentru situațiile în care plătitorul efectua tranzacția dintr-un cont deschis la instituția bancară respectivă – (tranzacții interne).

De asemenea, s-a constatat că operatorul a încălcat prevederile art. 25 din Regulamentul (UE) 2016/679, deoarece nu a pus în aplicare măsuri tehnice şi organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât şi în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum și reducerea la minimum a datelor, şi să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele Regulamentului (UE) 2016/679 şi a proteja drepturile persoanelor vizate. Aceasta a condus la dezvăluirea, în documentele ce conţin detaliile tranzacţiilor şi care sunt puse online la dispoziţia clienţilor beneficiari ai plăţilor, a datelor privind CNP-ul și adresa plătitorului (pentru situaţiile în care plătitorul efectua tranzacţia dintr-un cont deschis la o altă instituţie de credit - tranzacţii externe şi depuneri la casierie), respectiv a datelor privind adresa plătitorului (pentru situaţiile în care plătitorul efectua tranzacţia dintr-un cont deschis la instituția bancară respectivă - tranzacţii interne), pentru un număr de 337.042 persoane vizate, în perioada 25 mai 2018 – 10 decembrie 2018.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 613.912 lei (echivalentul a 130.000 EURO), pentru încălcarea prevederilor art. 25 alin. (1) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ – Acces neautorizat la datele cu caracter personal prelucrate prin aplicația informatică utilizată de către o instituție bancară în activitatea de creditare și divulgarea neautorizată a datelor cu caracter personal.

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 două dintre angajatele sale, utilizând datele din documentele de identitate ale unor persoane fizice, transmise de către angajați ai unei societăți de brokeraj, prin intermediul aplicației mobile WhatsApp, precum și date fictive, au efectuat interogări ale sistemului Biroului de Credit, pentru a obține datele necesare în vederea determinării eligibilității la creditare a respectivelor persoane fizice, printr-o simulare de prescoring (1194 de simulări de prescoring, cu privire la 1177 de persoane fizice). De asemenea, pentru 124 de persoane fizice s-a efectuat și consultarea bazei de date a Agenției Nationale de Administrare Fiscală (ANAF).

Simulările de prescoring menționate mai sus au fost efectuate prin intermediul aplicației informatice utilizate de către instituția bancară respectivă în activitatea de creditare, pe baza datelor obținute din sistemul Biroului de Credit și din baza de date ANAF, a datelor din documentele de identificare și a unor date fictive cu privire la starea civilă, studii, poziția ocupată și situația domiciliară a persoanelor vizate, introduse de către cele două angajate în aplicația specifică, cu încălcarea procedurilor interne.

În urma simulărilor de prescoring menționate, decizia negativă de creditare a fost comunicată de angajatele instituției bancare către angajații societății de brokeraj.

Acest incident a vizat următoarele date cu caracter personal: a) fotocopii ale cărților de identitate; b) date financiare (datele din sistemul Biroului de Credit, datele din sistemul de evidenţă administrat de ANAF); c) simularea deciziei de creditare pe care ar fi adoptat-o instituția bancară pe baza datelor menționate, precum şi pe baza unor date fictive simulate, introduse de angajatele instituției bancare în sistemul de prescoring pentru a putea finaliza simularea de prescoring (date fictive privind starea civilă, studii, poziţia ocupată şi situaţia domiciliară a persoanelor vizate).

Investigația demarată de Autoritatea națională de supraveghere a vizat atât prelucrările de date cu caracter personal efectuate de instituția bancară, cât și prelucrările de date efectuate de societatea de brokeraj.

În urma investigaţiei efectuate la instituția bancară, s-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 distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Aceasta a condus la accesul neautorizat la datele cu caracter personal prelucrate prin aplicația informatică utilizată de instituția bancară în activitatea de creditare și la divulgarea neautorizată a datelor cu caracter personal.

Autoritatea națională de supraveghere a sancționat instituția bancară cu amendă în cuantum de 712.680 lei (echivalentul a 150.000 EURO), pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Totodată, ca urmare a investigaţiei efectuate la societatea de brokeraj, s-a constatat că aceasta 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 distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Aceasta a condus la divulgarea neautorizată a datelor cu caracter personal a 1177 de persoane fizice/clienți ai societății de brokeraj (nume, prenume, adresă domiciliu, Seria/Nr. CI/BI, data eliberării și emitent CI/BI, data valabilitate CI/BI, CNP), prin transmiterea de fotocopii ale actelor de identitate ale acestora, către persoane neautorizate să prelucreze aceste date, respectiv angajați ai instituției bancare.

De asemenea, s-a constatat că, până la finalizarea investigației, societatea de brokeraj nu a notificat autorității de supraveghere încălcarea securității datelor cu caracter personal, fără întârzieri nejustificate, deși constatase producerea acestui incident încă din luna decembrie 2018.

Autoritatea națională de supraveghere a sancționat societatea de brokeraj cu amendă în cuantum total de 95.024 lei (echivalentul a 20.000 EURO), pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, precum și ale art. 33 alin. (1) din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ - neimplementarea unui proces pentru testarea, evaluarea şi aprecierea periodice ale eficacității măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării

Autoritatea națională de supraveghere a fost sesizată cu privire la prelucrarea datelor cu caracter personal, de către o instituție bancară, în contextul tranzacțiilor efectuate de clienții băncii într-o anumită perioadă din luna octombrie 2018.

Având în vedere cele sesizate, Autoritatea națională de supraveghere a solicitat Autorității Naționale pentru Protecția Consumatorilor (ANPC) informații cu privire la constatările efectuate ca urmare a controlului demarat de către aceasta, în contextul incidentului operațional referitor la dublarea tranzacțiilor de către instituţia bancară în cauză.

ANPC ne-a informat că situaţia semnalată s-a datorat unui incident operațional la nivelul instituției bancare, care a constat în dublarea unor tranzacții efectuate de către consumatori. Totodată, s-a precizat că, urmare a acestui incident au fost afectate interesele economice ale unui număr de 225.525 consumatori, dintre care, aproximativ 7.000 de clienți au fost direct afectaţi, în sensul în care tranzacțiile acestora au fost respinse pe motiv de fonduri insuficiente, în mod eronat.

În cadrul investigației efectuate, Autoritatea națională de supraveghere a constatat că incidentul operațional care a cauzat dublarea tranzacțiilor cu cardul, efectuate de către clienții băncii, s-a datorat unei erori umane/tehnice, prin procesarea de două ori a fișierului de plăți, care conţine şi date cu caracter personal. Acest incident a fost posibil deoarece restricțiile tehnice nu au fost suficiente pentru a preîntâmpina incidentul, respectiv nu au fost de natură să asigure o protecție adecvată împotriva prelucrării neautorizate asupra datelor cu caracter personal, ceea ce a condus la deteriorarea accidentală a datelor.

Totodată, deficiențele care au permis materializarea incidentului operațional au fost legate de procesul IT Monitoring, care nu includea toate restricțiile de sistem necesare, funcții multiple ce trebuie rulate în cadrul pasului intermediar manual care au generat erori operaționale, respectiv prelucrări neautorizate care au dus la deteriorarea accidentală a datelor.

De asemenea, s-a constatat că au fost afectați de incidentul operațional 225.525 de clienți, pentru un număr de 445.000 de tranzacții cu cardul dublate, aproximativ 7000 dintre acești clienți neputând realiza alte operațiuni de plată din cauza soldului insuficient (ca urmare a intervenirii incidentului, tranzacțiile acestora au fost respinse pe motiv de fonduri insuficiente).

Autoritatea națională de supraveghere a constatat că persoanele fizice afectate de incidentul operațional au postat în spațiul public, pe o rețea de socializare, prejudiciile create, astfel: sold/balanță negativ/ă per client; sumele retrase depășeau cuantumul sumei/sumelor privind operațiunile inițiate de către clienți; situații de fonduri insuficiente; lipsă fonduri pentru persoanele vizate aflate în afara țării (turiști); fonduri insuficiente pentru plată cumpărături; fonduri insuficiente intervenții medicale; retragere de bani care nu aparțineau unei persoane vizate.

La finalizarea investigației, s-a constatat că operatorul nu a asigurat respectarea principiului protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor (privacy by design și privacy by default), întrucât nu a procedat la adoptarea de măsuri tehnice și organizatorice corespunzătoare, privind integrarea de garanții adecvate în sistemul automatizat de prelucrare a datelor în cadrul procesului de decontare a tranzacțiilor cu cardul, fiind afectat un număr de 225.525 de clienți ale căror operațiuni de plată au fost dublate în perioada 8-10.10.2018, raportat și la prevederile art. 32 alin. (1) lit. d) din Regulamentul (UE) 2016/679.

În urma investigației efectuate, operatorul a fost sancționat cu amendă în cuantum de 380.400 lei (echivalentul a 80.000 EURO), pentru încălcarea art. 25 alin. (1) coroborat cu art. 5 alin. 1 lit. f) din Regulamentul (UE) 2016/679.

4. FIȘĂ DE CAZ – Divulgare neautorizată de date cu caracter personal 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.

Incidentul de securitate notificat a constat în faptul că, urmare a unei erori tehnice a aplicației utilizate de instituția bancară pentru comunicarea automată către clienții proprii a formularului de definire și actualizare date personale – persoane fizice, în procesul de înrolare/actualizare au fost transmise către un număr de 56 de adrese de e-mail eronate formulare de definire și actualizare date personale – persoane fizice, care conțineau următoarele date cu caracter personal: nume, prenume, data nașterii, codul numeric personal, numărul și seria actului de identitate, data nașterii, locul nașterii, profesie, loc de muncă, număr de telefon, adresa de e-mail, adresa de domiciliu, situație familială, date privind bunurile deținute, salariu.

Ca urmare a producerii incidentului de securitate, instituţia bancară a contactat telefonic persoanele care au recepționat în mod eronat corespondența transmisă din partea băncii, 30 de persoane confirmând distrugerea/ștergerea corespondenței recepționate în mod eronat. Pentru alte 27 de persoane, comunicarea solicitării de ștergere/distrugere de îndată a informațiilor transmise eronat a fost comunicată pe adresa de e-mail pe care a fost transmis inițial, în mod eronat, documentul menționat, persoanele afectate de incidentul de securitate, care nu au confirmat ștergerea/distrugerea corespondenței recepționate eronat, urmând să fie notificate cu privire la incidentul produs.

În urma investigaţiei efectuate la instituția bancară, Autoritatea națională de supraveghere a constatat că instituţia bancară nu a implementat măsuri tehnice și organizatorice adecvate, în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, prin transmiterea formularelor pentru definire și actualizare date personale – persoane fizice (clienți) către adrese de e-mail eronate, din cauza unei erori tehnice a aplicației, fiind afectate de incident un număr de 56 de persoane fizice vizate. Aceasta a condus la încălcarea confidențialității datelor cu caracter personal (nume, prenume, data nașterii, codul numeric personal, numărul și seria actului de identitate, data nașterii, locul nașterii, profesie, loc de muncă, număr de telefon, adresa de e-mail, adresa de domiciliu, situație familială, date privind bunurile deținute, salariu), deși instituţia bancară avea aceste obligații, inclusiv potrivit prevederilor art. 5 lit. f), „integritate și confidențialitate” din Regulamentul (UE) 2016/679.

În acest caz, Autoritatea națională de supraveghere a constatat că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) din Regulamentul (UE) 2016/679și a dispus operatorului o măsură corectivă, 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, respectiv instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

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

În anul 2019, au fost efectuate 6 investigații la furnizori de servicii medicale, demarate ca urmare a notificărilor de încălcare a securității datelor cu caracter personal, precum și a sesizărilor transmise Autorității naționale de supraveghere.

Toate notificările încălcărilor de securitate în domeniul sănătății au fost transmise de către entități din sectorul public și au avut ca obiect divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal ale persoanelor vizate.

În urma investigațiilor efectuate, au fost aplicate sancțiuni contravenționale constând în avertisment, dar și o serie de măsuri corective 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, republicată, astfel:

- ștergerea de pe rețelele de socializare a filmărilor în care sunt dezvăluite date cu caracter personal/imagini captate electronic;

- instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale;

- 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;

- revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal;

- luarea unor măsuri suplimentare astfel încât, pe viitor, să fie evitate situații de prelucrare a datelor cu caracter personal fără un consimțământ explicit și informat al persoanelor vizate și fără informarea acestora în condițiile art. 13 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ – divulgare neautorizată a datelor pacienților

Prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, un furnizor de servicii medicale a notificat Autoritatea națională de supraveghere cu privire la faptul că un medic primar, angajat în cadrul Clinicii, a filmat cu telefonul propriu, în timpul programului de lucru, activitatea curentă din blocul operator, din saloane și din sala de tratament, și a postat, ulterior, filmările respective pe rețelele de socializare.

În înregistrările video/audio postate pe rețelele de socializare apăreau atât angajați, cât și pacienți ai furnizorului de servicii medicale, fiind dezvăluite date cu caracter personal referitoare la imagine, domiciliu, nume, prenume și diagnostic.

Investigația demarată de Autoritatea națională de supraveghere a vizat atât prelucrările de date cu caracter personal **efectuate de furnizorul de servicii medicale**, cât și prelucrările de date efectuate de medicul care a filmat și dezvăluit imaginile respective.

În urma investigației efectuate la furnizorul de servicii medicale, s-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 și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Aceasta a condus la publicarea, pe o rețea de socializare, a mai multor înregistrări video/audio realizate de către un medic în timpul programului de lucru, în care sunt dezvăluite imagini captate electronic, în blocul operator, în saloane și în sala de tratament, inclusiv date referitoare la nume, prenume, funcție, date referitoare la viața privată a medicilor, asistentelor, personalului de conducere din cadrul spitalului, personalului de pază, precum și date privind numele, prenumele, diagnosticele și procedurile medicale la care au fost supuși diverși pacienți.

Referitor la cele constatate ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că **operatorul investigat (furnizor de servicii medicale)** a încălcat prevederile art. 32 alin. (4) raportat la art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679și a dispus furnizorului de servicii de sănătate, 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, 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 și scopurile prelucrării; și

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

Totodată, medicul, angajat al furnizorului de servicii medicale, a fost sancționat cu avertisment pentru încălcarea prevederilor art. 5 alin. 1 lit. a) din Regulamentul (UE) 2016/679și art. 6 din Regulamentul (UE) 2016/679, deoarece a prelucrat date cu caracter personal prin înregistrarea, publicarea pe rețeaua de socializare, divulgarea prin transmitere, diseminarea sau punerea la

dispoziție în orice mod, a înregistrărilor video/audio realizate cu telefonul propriu, în timpul programului de lucru, în blocul operator, în saloane și în sala de tratament, fără consimțământul persoanelor vizate sau în temeiul unui alt motiv legitim, prevăzut de lege, și nu a furnizat persoanelor vizate informațiile prevăzute de art. 12 și art. 13 din Regulamentul (UE) 2016/679 pentru a asigura o prelucrare echitabilă şi transparentă.

De asemenea, Autoritatea națională de supraveghere a dispus medicului în cauză și măsura corectivă de a întreprinde demersuri pentru ștergerea de pe rețelele de socializare a filmărilor în care sunt dezvăluite date cu caracter personal.

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

Investigațiile efectuate de Autoritatea națională de supraveghere în domeniul comunicațiilor electronice au fost demarate ca urmare a depunerii de către furnizorii de servicii de comunicații electronice a unor notificări privind încălcarea securității datelor cu caracter personal, prin completarea formularului prevăzut de Decizia nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicațiile electronice, precum și prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.

Astfel, neimplementarea unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător a condus la accesarea și divulgarea neautorizată a unor date cu caracter personal ale clienților proprii.

1. FIȘĂ DE CAZ - Încălcarea securității datelor cu caracter personal de către o societate de telefonie mobilă – transmitere eronată a facturilor prin e-mail

O societate de telefonie mobilă a notificat Autoritatea națională de supraveghere cu privire la o încălcare a securității datelor cu caracter personal, care a constat în faptul că, în decursul unei luni

calendaristice, în funcție de ciclul de facturare, societatea a transmis, din eroare, unui număr de 4424 de clienți, e-mail-uri conținând link-urile aferente facturilor altor clienți decât titularii.

Facturile nu erau atașate e-mail-urilor transmise eronat, ci se puteau accesa numai prin deschiderea unui link. Eroarea care s-a produs a constat în corelarea greșită a adreselor de e-mail furnizate de clienți și codurile de facturare ale acestora, din bazele de date ale societății comerciale. Datele care au fost dezvăluite prin transmiterea eronată a facturilor au fost: nume și prenume, adresă, număr de telefon, cod de client, cod de facturare.

Ca urmare a analizei interne, desfășurate după primirea unui număr de sesizări prin Call-Center, din partea clienților, operatorul a precizat că operațiunea s-a realizat manual, fiind vorba despre o eroare umană.

În urma investigaţiei efectuate, societatea a fost sancționată cu avertisment pentru săvârșirea contravenției prevăzute de art. 13 alin. (1) lit. a) din Legea nr. 506/2004, deoarece nu a luat măsuri tehnice și organizatorice adecvate în vederea asigurării securității prelucrării datelor cu caracter personal, ceea ce a condus la transmiterea eronată a unor e-mail-uri, conținând link-urile aferente facturilor unor clienți, către alți clienți decât titularii facturilor, precum și la accesarea și divulgarea ilicită a unor date cu caracter personal ale clienților proprii.

2. FIȘĂ DE CAZ - Încălcarea securității datelor cu caracter personal de către o societate de telefonie mobilă – accesare neautorizată a bazei de date

O societate de telefonie mobilă a notificat Autoritatea națională de supraveghere cu privire la o încălcare a securității datelor cu caracter personal, care a constat în faptul că un angajat a accesat neautorizat o aplicație care stochează datele de cont și datele de trafic ale utilizatorilor serviciilor pre-plătite, printre care: nume, prenume, adresă, numărul de telefon apelat și durata convorbirii, numărul de telefon către care s-au transmis sau de la care s-au primit SMS-uri cât și sesiuni de date.

Urmare a unei reclamații, societatea a declanșat o investigație internă privind modalitatea de accesare a aplicației care stochează datele de cont și datele de trafic ale utilizatorilor serviciilor pre-plătite și a constatat faptul că angajatul respectiv avea drept de acces în aplicație, însă a realizat, în mod individual, o serie de accesări în scop personal, vizualizând datele de cont aferente unui număr de telefon, pe un anumit interval de timp, precum și apelurile efectuate de la și către acest număr. Totodată, datele de cont ale titularului și apelurile efectuate în perioada indicată, salvate sub formă de capturi de ecran, au fost transmise de către angajatul societății unei terțe persoane, fără consimțământul titularului.

În urma investigaţiei efectuate, societatea a fost sancționată cu avertisment pentru săvârșirea contravenției prevăzute de art. 13 alin. (1) lit. a) din Legea nr. 506/2004, deoarece nu a luat măsuri tehnice și organizatorice adecvate în vederea asigurării securității prelucrării datelor cu caracter personal, de natură să protejeze datele cu caracter personal stocate sau transmise împotriva distrugerii accidentale ori ilicite, împotriva pierderii sau deteriorării accidentale și împotriva stocării, prelucrării, accesării ori divulgării ilicite, ceea ce a condus la accesul neautorizat la contul unei persoane vizate, în aplicația utilizată pentru stocarea datelor de cont și de trafic ale utilizatorilor serviciilor pre-plătite, precum și la divulgarea ilicită a datelor cu caracter personal ale persoanei vizate referitoare la nume, prenume, oraș, lista apelurilor telefonice efectuate/primite și durata convorbirilor efectuate, numărul de telefon către care s-au transmis/primit SMS-uri, date care aparțineau titularului cu numărul de telefon interogat de către angajatul societății.

3. FIȘĂ DE CAZ - Încălcarea securității datelor cu caracter personal de către o societate de telefonie mobilă – accesare neautorizată a bazei de date

O societate de telefonie mobilă a notificat Autoritatea națională de supraveghere cu privire la o încălcare a securității datelor cu caracter personal, care a constat în faptul că 8 dintre angajații săi au accesat neautorizat, în mod individual, aplicația care stochează datele de trafic existente pe factura detaliată a abonaților, în scop personal, cu depășirea atribuțiilor din fișa postului. Datele cu caracter personal accesate neautorizat au fost doar vizualizate de către respectivii angajați, acestea neputând fi tipărite, copiate, exportate sau descărcate din aplicație.

În urma investigaţiei efectuate de Autoritatea națională de supraveghere, societatea de telefonie mobilă a fost sancționată cu avertisment pentru săvârșirea contravenției prevăzute de art. 13 alin. (1) lit. a) din Legea nr. 506/2004, deoarece nu a luat suficiente măsuri tehnice şi organizatorice adecvate în vederea garantării că datele cu caracter personal pot fi accesate numai de persoane autorizate, în scopurile autorizate de lege, ceea ce a condus la faptul că datele cu caracter personal cuprinse în facturile detaliate ale unui număr de 12 abonați ai societății, persoane fizice, au fost vizualizate de 8 angajați cu drept de accesare în aplicația respectivă, în scop neautorizat, în mod individual și în scop personal, cu depășirea atribuțiilor din fișa postului.

4. FIȘĂ DE CAZ - Încălcarea securității datelor cu caracter personal de către o societate de telefonie mobilă – divulgare neautorizată de date pe Internet

O societate de telefonie mobilă a notificat Autoritatea națională de supraveghere cu privire la o încălcare a securității datelor cu caracter personal, care a constat în faptul că o listă de CV-uri depuse pe website-ul societății, la secțiunea „Cariere", a putut fi vizualizată pe Internet, prin accesarea unui link asociat acestui website.

În cadrul analizei interne, efectuate ca urmare a sesizării unei persoane vizate, societatea a concluzionat faptul că, dintr-o eroare tehnică, website-ul societății nu a fost securizat în mod corespunzător nici la momentul realizării, nici ulterior, când a fost copiat în mod identic pe serverul din România, astfel încât anumite informații, care în mod uzual pot fi vizualizate doar de deținătorul website-ului și/sau de persoana care îl gestionează, au putut fi accesibile și unor terți, în situația efectuării unor căutări precise, prin utilizarea de criterii precum denumirea societății și numele persoanelor care au aplicat pe website.

În urma investigaţiei efectuate de Autoritatea națională de supraveghere, societatea a fost sancționată cu avertisment pentru săvârșirea contravenției prevăzute de art. 25 și art. 32 alin. (1) 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, deși avea această obligație potrivit art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679, ceea ce a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale persoanelor care și-au depus CV-urile pe website-ul societății.

D. Investigații referitoare la prelucrarea datelor cu caracter personal în domeniul serviciilor poștale

În cursul anului 2019, Autoritatea națională de supraveghere a efectuat investigații ca urmare a înregistrării notificărilor de încălcare a securității datelor cu caracter personal în domeniul serviciilor poștale.

În toate cazurile înregistrate, prin formularele de notificare transmise de societăți care activează în domeniul serviciilor poștale, cât și de cele care au calitatea de împuternicit al acestora pentru prelucrarea datelor cu caracter personal, a fost notificată pierderea trimiterilor poștale sau a anumitor documente (tichete de masă personalizate, carduri și documente bancare), în timpul transportului.

Datele cu caracter personal afectate de incidentele de securitate notificate au fost:

- pentru documentele bancare pierdute: nume, prenume, număr card, cod siguranță card (cvv), adresă titular card, cod numeric personal, serie și număr card identitate (fără copia documentului), număr cont IBAN, limită credit aprobată; pentru tichetele de masă personalizate: nume, prenume, cod numeric personal, angajator, date de identificare și date de contact angajator, valoarea și durata de valabilitate a tichetelor de masă/cadou/vacanță emise;

- pentru alte trimiteri poștale: nume, prenume, adresă și date contractuale.

Din investigațiile efectuate ca urmare a notificării incidentelor de securitate, de către operatori din domeniul serviciilor poștale, a rezultat că aceștia nu au implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, ceea ce a condus la pierderea datelor cu caracter personal și la divulgarea/accesarea către beneficiari care nu sunt autorizați să primească/acceseze datele cu caracter personal sau la oricare altă formă de prelucrare care încalcă Regulamentul (UE) 2016/679, prin pierdere, sustragere/furt în timpul transportului.

Pentru faptele constatate ca urmare a investigațiilor efectuate în anul 2019 la operatori din domeniul serviciilor poștale, prin procesele-verbale de sancționare/constatare au fost aplicate atât amenzi, cât și măsuri corective, în temeiul art. 58 alin. (2), raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, republicată.

1. FIȘĂ DE CAZ – Pierderea unor documente în timpul transportului de către o societate care prestează servicii poștale

Autoritatea națională de supraveghere a fost notificată cu privire la încălcarea securității datelor cu caracter personal de mai multe societăți comerciale, precum și de societatea împuternicită de acestea pentru prestarea serviciilor poștale.

În toate cazurile, prin formularele de notificare transmise, a fost notificată pierderea anumitor documente (tichete de masă personalizate, carduri și documente bancare), în timpul transportului, de către societatea împuternicită de operatori pentru prestarea serviciilor poștale.

Ulterior producerii incidentelor de securitate, societatea împuternicită pentru prestarea serviciilor poștale a sesizat IGPR și a implementat măsuri tehnice și organizatorice privind metode de securitate suplimentară a transporturilor (de ex. montarea unui suport pentru a doua bară de

siguranță pentru blocarea ușilor pe interior, montarea de senzori de deschidere a ușilor pe semiremorci, cu monitorizare în aplicația GPS, instalarea pe fiecare mașină a unui sistem de avertizare sonoră dotat cu sirenă foarte puternică ce se declanșează la deschiderea ușilor, instalarea pe fiecare mașină în partea din spate a unei camere de filmat, pentru a surprinde imagini cu infractorii și mașinile acestora, transmise în timp real în cabina șoferului).

Totodată, persoanele vizate afectate de incidentele de securitate au fost despăgubite, după caz.

În urma investigaţiei efectuate de Autoritatea națională de supraveghere, s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, ceea ce a condus la pierderea datelor cu caracter personal și la divulgarea/accesarea datelor cu caracter personal către beneficiari care nu sunt autorizați să primească/acceseze datele cu caracter personal sau la oricare altă formă de prelucrare care încalcă Regulamentul (UE) 2016/679, prin sustragere/furt în timpul transportului.

Operatorul investigat a fost sancționat cu amendă în cuantum de 52.325,9 lei (echivalentul a 11.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

E. Investigații în alte cazuri

1. FIȘĂ DE CAZ – Obținerea consimțământul persoanelor vizate pentru prelucrarea datelor cu caracter personal la crearea unui cont pe website

Autoritatea naţională de supraveghere a fost sesizată de o persoană fizică cu privire la faptul că, pentru crearea unui cont pe website-ul unei societăți de consultanță, nu se solicită/obține consimțământul persoanei vizate, abonarea realizându-se automat, dacă utilizatorul nu bifează opțiunea Nu vreau să primesc Personal update". Ulterior, pentru acești utilizatori, societatea transmitea zilnic o informare prin e-mail.

Ca urmare a verificărilor efectuate, Autoritatea națională de supraveghere a constatat faptul că operatorul investigat a apreciat și implementat, într-un mod total eronat, faptul că o inacțiune a utilizatorului (nebifarea unei căsuțe) poate constitui un consimțământ valabil exprimat pentru prelucrarea datelor cu caracter personal, deși consimțământul trebuia să fie granular pentru fiecare dintre scopurile avute în vedere. Astfel, societatea a transmis prin e-mail ”Personal Update”, pentru

un număr de 4357 de utilizatori, a colectat date personale într-un mod nelegal și netransparent față de persoana vizată, le-a prelucrat ulterior într-un mod incompatibil cu scopul în care au fost colectate inițial, respectiv executarea contractului, și nu a putut face dovada obținerii consimțământului granular pentru fiecare dintre scopurile avute în vedere, exprimat printr-o acțiune neechivocă, care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, prin bifarea căsuței/opțiunii pentru această prelucrare.

Față de cele constatate în cadrul investigației, operatorul a fost sancţionat cu amendă în cuantum de 42.714 lei (echivalentul sumei de 9000 EURO), pentru încălcarea prevederilor art. 5. alin. (1) lit. a) și lit. b), art. 6 alin. (1) lit. a) și art. 7 din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ – Dezvăluirea listei de pasageri în mediul online

Prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, o companie de transport aerian a notificat Autoritatea națională de supraveghere cu privire la faptul că o listă de pasageri a fost fotografiată de un angajat al companiei, în urma accesării serviciului de rezervări, ceea ce a condus la dezvăluirea în mediul online a datelor cu caracter personal ale unor clienți/pasageri ai companiei, prin publicarea unor articole în presa online.

În urma investigației efectuate, s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al unui drept intern și în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Aceasta a condus la accesarea neautorizată, de către un angajat propriu, a datelor unor pasageri/clienți ai companiei de transport aerian și la divulgarea neautorizată în mediul online a acestei liste, fapt ce poate duce în special la prejudicii fizice, materiale sau morale aduse persoanelor fizice afectate, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau pierderea confidențialității datelor cu caracter personal protejate prin

secret profesional sau alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Compania de transport aerian a fost sancționată cu amendă, în cuantum de 95.194 lei, (echivalentul sumei de 20.000 EURO) pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Totodată, 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 dispus și măsura corectivă de revizuire și actualizare a măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal și instruirea personalului propriu, precum și măsura corectivă de a solicita deținătorilor resurselor publice de internet, ștergerea/anonimizarea datelor cu caracter personal din lista de pasageri fotografiată din sistemul de rezervări.

3. FIȘĂ DE CAZ – Dezvăluire de date pe website-ul unei societăți

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că un set de fișiere cu privire la detaliile tranzacțiilor recepționate pe website-ul unei societăți de consultanță privind Regulamentul (UE) 2016/679, care conțineau nume, prenume, adresa de corespondență, email, telefon, loc de muncă și detalii tranzacții efectuate, erau accesibile public prin intermediul motorului de căutare Google.

În urma investigației efectuate, 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 (nume, prenume, adresa de corespondență, email, telefon, loc de muncă, detalii tranzacții efectuate) ale persoanelor care au efectuat tranzacții recepționate de website-ul societății, documente accesibile public prin intermediul motorului de căutare Google.

Operatorul investigat a fost sancționat cu amendă în cuantum de 14.173 lei (echivalentul sumei de 3.000 EURO) pentru încălcarea prevederilor art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

4. FIȘĂ DE CAZ – Dezvăluirea datelor cu caracter personal ale clienților unei unități hoteliere în mediul online

Prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, o unitate hotelieră a notificat Autoritatea națională de supraveghere cu privire la faptul că o listă tipărită pe suport de hârtie, utilizată pentru verificarea clienților care servesc micul dejun, ce conținea date cu caracter personal ale unor clienți cazați la unitatea hotelieră, a fost fotografiată de persoane neautorizate din afara societății, ceea ce a condus la dezvăluirea în mediul online a datelor cu caracter personal ale clienților, prin publicarea unui articol de presă.

Autoritatea națională de supraveghere a constatat că neimplementarea unor măsuri tehnice și organizatorice adecvate, în vederea asigurării unui nivel de securitate corespunzător, a condus la pierderea confidențialității datelor cu caracter personal prin fotografierea listei printate pe suport de hârtie, din aplicația hotelieră în care sunt stocate datele clienților, de către persoane neautorizate din afara societății, și la dezvăluirea în mediul online a datelor cu caracter personal ale unor clienți, prin publicarea unui articol de presă, ceea ce poate conduce la prejudicii morale aduse persoanelor fizice afectate, cum ar fi compromiterea reputației sau alt dezavantaj semnificativ de natură economică sau socială.

Ca urmare a investigației efectuate, operatorul a fost sancționat cu amendă în cuantum de 71.028 lei (echivalentul sumei de 15.000 EURO) pentru încălcarea prevederilor art. 32 alin. (4) raportat la art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Totodată, 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 dispus operatorului și măsura corectivă de a revizui și actualiza măsurile tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal.

Secţiunea a 3 -a: Activitatea de soluţionare a plângerilor

I. Prezentare generală

În exercitarea atribuţiilor sale legale, în cursul anului 2019, 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.

Regulamentul (UE) 2016/679 prevede la art. 77 că ”orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.”

Prevederile de mai sus au fost implementate prin art. 20-21 din Legea nr. 102/2005, republicată, și puse în aplicare prin Procedura de primire și soluționare a plângerilor, aprobată prin Decizia președintelui Autorității naționale de supraveghere nr. 133/2018.

Plângerile pot fi adresate de orice persoană vizată identificată, care consideră că prelucrarea datelor sale cu caracter personal încalcă prevederile legale în vigoare, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României.

Totodată, plângerile pot fi transmise prin reprezentant, cu anexarea împuternicirii emise în condiţiile legii de un avocat sau a procurii notariale, după caz. Plângerile pot fi înaintate şi de către mandatarul persoanei vizate care este soţ sau rudă până la gradul al doilea inclusiv, cu anexarea unei declaraţii pe propria răspundere semnată de petiţionar, respectiv a unei procuri notariale, după caz. În cazul în care plângerea este depusă prin intermediul unui organism, al unei organizaţii, al unei asociaţii sau fundaţii fără scop patrimonial, acestea trebuie să dovedească faptul că au fost constituite legal, cu un statut ce prevede obiective de interes public, şi că sunt active în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal.

Persoanele care doresc să adreseze o plângere autorității de supraveghere au la dispoziție mai multe modalități de transmitere, și anume: depunere la registratura generală de la sediul ANSPDCP, transmitere prin poştă, inclusiv cea electronică, ori prin utilizarea formularului electronic, disponibil pe pagina de internet a autorității, www.dataprotection.ro, din anul 2019 fiind disponibilă inclusiv o variantă de depunere online. Pentru primirea şi înregistrarea valabilă a plângerilor, petiționarii trebuie să furnizeze datele de identificare (nume, prenume, adresă poştală de domiciliu sau de reşedinţă, adresa de poştă electronică, după caz), datele de identificare ale operatorului reclamat sau ale persoanei împuternicite reclamate, sau cel puţin informațiile disponibile deţinute de petiţionar, în vederea identificării acestora, să precizeze în detaliu obiectul plângerilor, demersurile întreprinse la nivelul operatorului reclamat sau al persoanei împuternicite reclamate, după caz, informațiile disponibile pentru susţinerea afirmaţiilor, precum şi să anexeze dovezi concludente, în măsura în care le deţin.

Principalele motive pentru care, în 2019, o serie de plângeri nu au putut fi considerate admisibile și, pe cale de consecință, nu au format obiectul unor demersuri de investigare, au fost, ca și în anul precedent, următoarele: lipsa furnizării datelor de identificare ale petenților, lipsa dovezilor în susţinerea aspectelor reclamate, solicitarea exercitării unor drepturi în numele petenților de către instituția noastră (de ex. ștergerea datelor în lipsa unei cereri de exercitare a dreptului transmisă de petent operatorului), sesizarea unor aspecte care nu intră în competența legală materială a autorității 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.

De asemenea, 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).

De asemenea, în anul 2019, au fost primite plângeri care au avut ca obiect solicitarea de ștergere a datelor negative din sistemul de evidență al Biroului de Credit, pe motivul nerealizării informării prealabile cu 15 zile. Acestea au fost respinse, întrucât Regulamentul (UE) 2016/679 nu prevede în sarcina operatorilor astfel de obligații care erau anterior stabilite prin Legea nr. 677/2001 și Decizia nr. 105/2007, acte care și-au încetat aplicabilitatea din 25 mai 2018, odată cu punerea în aplicare a Regulamentului (UE) 2016/679. În ceea ce privește prelucrarea datelor de către Biroul de Credit, o serie de plângeri au vizat modalitățile de exercitare a drepturilor prin intermediul portalului acestui operator.

În anul 2019, au fost primite **5808 plângeri (față de 4822 plângeri înregistrate în 2018)**, care au vizat, în principal, următoarele aspecte:

•dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;

•încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/679;

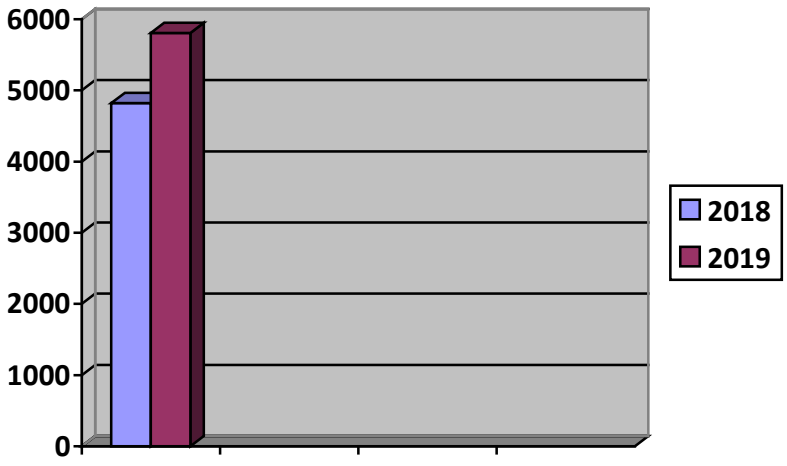
•transmiterea de date la Biroul de Credit;

•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, respectiv, neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor;

•nerespectarea condițiilor privind consimțământul în mediul online.



Pentru soluţionarea plângerilor primite, considerate admisibile, în anul 2019, au fost demarate **527 de investigații**.

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

•**17 amenzi**, dintre care **14** în baza Regulamentului (UE) 2016/679, reprezentând un cuantum total de **210.166,8 lei** (echivalentul sumei de 44.000 Euro, prin raportare la cursul de schimb valutar oficial al BNR de la data aplicării sancțiunii) și **3 amenzi** în baza Legii nr. 506/2004, în cuantum total de **30.000 lei;**

•**120 de avertismente**.

De asemenea, au fost dispuse **115 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679, care au vizat, în principal, următoarele:

•respectarea dreptului la informare a persoanelor vizate și efectuarea unei informări complete;

•comunicarea de răspunsuri complete și în termen legal, fără întârzieri nejustificate, la cererile persoanelor vizate privind exercitarea dreptului de acces;

•respectarea principiilor de prelucrare a datelor, în special cele privind legalitatea, transparența și proporționalitatea;

•respectarea condițiilor de validitate a consimțământului persoanelor vizate/tutorilor legali ai persoanelor vizate minori;

•anonimizarea datelor cu caracter personal ale minorilor dezvăluite pe Internet;

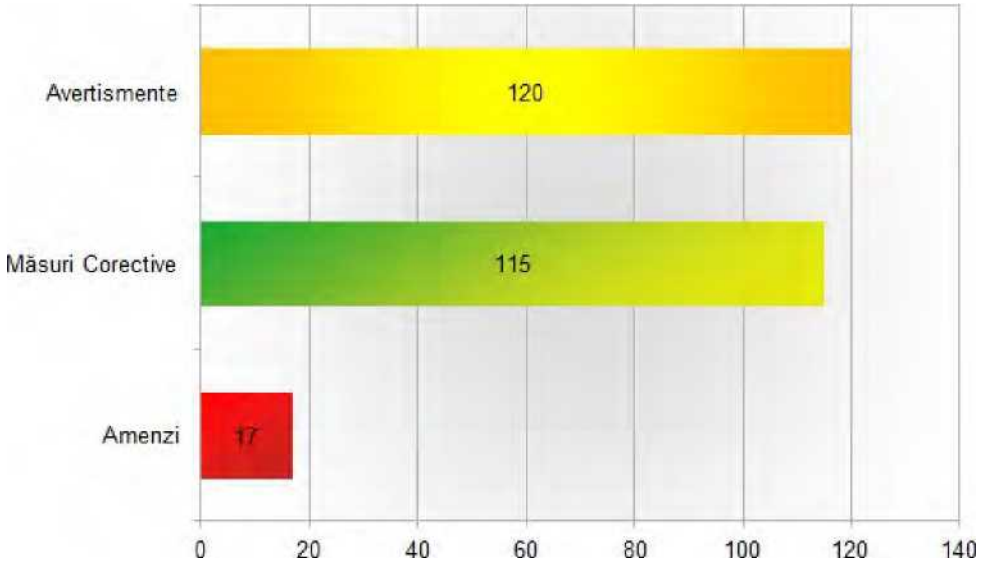
•luarea măsurilor necesare astfel încât prelucrarea (inclusiv dezvăluirea) datelor cu caracter personal ale persoanelor vizate să se realizeze cu respectarea condițiilor de legitimitate;

•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;

•ștergerea datelor cu caracter personal după împlinirea termenului de stocare stabilit, prin raportare la scopul în care au fost colectate.



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.

II. Principalele constatări rezultate din activitatea de soluționare a plângerilor

Prezentăm în secțiunile următoare câteva **fișe de caz** relevante pentru principalele domenii de activitate, tipuri de prelucrări de date personale și categorii de încălcări ale legislației în vigoare, în legătură cu care au fost finalizate **investigații în anul 2019, în baza plângerilor** adresate Autorității naționale de supraveghere.

1. Investigaţii referitoare la prelucrarea datelor cu caracter personal ale angajaților

Prelucrarea datelor cu caracter personal ale unor categorii de persoane vulnerabile, precum angajații, impune asigurarea unei protecţii eficiente a drepturilor acestor persoane, în special în cazul anumitor operaţiuni de prelucrare a datelor cu caracter personal care prezintă riscuri pentru drepturile şi libertăţile persoanelor.

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 persoanei, 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. 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.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că fostul angajator supraveghează prin mijloace audio/video birourile angajaților, vestiarele, sala de mese și că în anumite locații accesul se realizează pe bază de amprentă. Totodată, petentul a susținut că angajatorul s-a folosit de identitatea sa în transmiterea unor e-mail-uri în interes de serviciu.

În cadrul investigației, s-a constatat că operatorul nu a făcut dovada unui interes legitim justificat în ceea ce privește prelucrarea datelor personale rezultată din utilizarea sistemului de supraveghere video instalat la sediul său, care să prevaleze asupra intereselor sau drepturilor și libertăților fundamentale ale persoanelor vizate și nu a făcut dovada consultării sindicatului sau, după caz, a reprezentanților angajaților înainte de introducerea sistemului de monitorizare.

Totodată, s-a constatat că monitorizarea video a birourilor anumitor persoane cu funcție de conducere excede scopului declarat de operator, și anume protejarea bunurilor societății, descurajarea furtului și a actelor de vandalism asupra autovehiculelor societății, fiind o măsură intruzivă în viața privată a angajaților.

De asemenea, s-a constatat că imaginile prelucrate prin intermediul camerelor video instalate în birouri și spații cu destinația de vestiare nu sunt colectate în scopuri adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (”reducerea la minimum a datelor”), scopul declarat de operator - descurajarea furtului - putându-se realiza prin mijloace mai puțin intruzive pentru viața privată a angajaților.

În ceea ce privește informarea persoanelor vizate, s-a constatat că operatorul nu a făcut dovada respectării acestei obligații raportat la toate persoanele vizate, în conformitate cu prevederile art. 13 din Regulamentul (UE) 2016/679, în condițiile în care în această categorie se încadrează și vizitatorii, nu numai angajații societății.

Referitor la temeiul legal pentru prelucrarea imaginilor captate prin intermediul camerelor de supraveghere instalate la sediul operatorului, s-a considerat că acesta nu poate fi consimțământul, întrucât nu sunt respectate prevederile art. 4 pct. 11 și ale art. 7 din Regulamentul (UE) 2016/679, în special sub condiția de a fi liber exprimat.

În ceea ce privește sistemul de control acces cu tehnologie biometrică, s-a constatat că datele biometrice (amprentele) nu sunt colectate în scopuri adecvate, relevante și limitate la ceea ce este

necesar în raport cu scopurile în care sunt prelucrate (”reducerea la minimum a datelor”), scopul declarat de operator - acces în zone restricționate - putându-se realiza prin mijloace mai puțin intruzive pentru viața privată a angajaților, cum ar fi utilizarea cartelelor de acces.

În ceea ce privește securitatea prelucrării imaginilor prin intermediul sistemului de supraveghere video, precum și a datelor biometrice (amprente) ale angajaților, operatorul nu a făcut dovada existenței unor politici adecvate de protecție a datelor și a implementării unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc.

Astfel, accesarea la distanță (prin internet) a imaginilor prelucrate prin intermediul camerelor de supraveghere video, de către administratorul societății, pe lângă faptul că nu se justifică pentru scopul declarat de operator, prezintă un risc pentru drepturile și libertățile persoanelor fizice, în sensul posibilității de interceptare a informațiilor (imaginilor) transmise prin intermediul unei rețele de comunicații, în lipsa implementării unor măsuri de securitate adecvate, în conformitate cu art. 32 din Regulamentul (UE) 2016/679.

De asemenea, s-a constatat că au fost încălcate prevederile art. 6 din Regulamentul (UE) 2016/679, întrucât, după încetarea raporturilor juridice dintre operator și petent, societatea nu mai avea temei legal pentru prelucrarea adresei de e-mail a acestuia, coroborat cu numele și prenumele său.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul, cu 2 avertismente și amendă în cuantum total de 47786 lei (echivalentul a 10000 EURO), pentru încălcarea dispozițiilor art. 12, art. 13, art. 5 alin. (1) lit. c), art. 6, art. 7, art. 9, art. 5 alin. (1) lit. a), b) și e) din Regulamentul (UE) 2016/679 și a aplicat măsuri corective, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679.

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

Una dintre principalele obligații ale operatorilor de date personale și ale persoanelor împuternicite prevăzute de Regulamentul (UE) 2016/679 se referă la adoptarea măsurilor tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate a prelucrărilor și de respectare a regulilor de confidențialitate.

În acest sens, datele cu caracter personal trebuie prelucrate astfel încât să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

În anul 2019, Autoritatea națională de supraveghere a înregistrat o serie de plângeri care au avut ca obiect fie dezvăluirea datelor personale către terțe persoane, fie accesarea neautorizată a datelor personale (inclusiv de către angajații proprii), ca urmare a faptului că operatorii în cauză nu au implementat proceduri interne eficiente, de ordin tehnic sau organizatoric, care să conducă la prevenirea unor astfel de probleme.

FIȘĂ DE CAZ

O instituție financiară nebancară a colectat o adresă de e-mail eronată, ce nu aparținea persoanei care a solicitat obținerea unui credit la distanță, fără să aplice măsuri de verificare a exactității datelor astfel colectate și a transmis ulterior către adresa respectivă de e-mail, de mai multe ori, documente care conțineau date personale ale debitorului, fără nicio măsură de securizare. Cu toate că titularul real al adresei de e-mail (petentul, în acest caz) a atras atenția în mod repetat societății în cauză cu privire la faptul că i-au fost dezvăluite documente ale altei persoane, operatorul nu a luat nicio măsură de remediere a respectivei situații.

Față de constatările rezultate din investigația întreprinsă în acest caz, s-au aplicat următoarele amenzi:

- amendă în cuantum de 14336,1 lei (echivalentul a 3000 euro), pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. a) din Regulamentul (UE) 2016/679, pentru încălcarea principiilor de prelucrare a datelor personale prevăzute de art. 5 alin. (1) lit. d) și f), art. 5 alin. (2) din Regulamentul (UE) 2016/679;
- amendă în cuantum de 47787 lei (echivalentul a 10.000 euro), pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (4) lit. a) din Regulamentul (UE) 2016/679, pentru încălcarea măsurilor de securitate prevăzute la art. 25 și 32 din Regulamentul (UE) 2016/679;
- amendă în cuantum de 4778,7 lei (echivalentul a 1000 euro), pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (4) lit. a) din Regulamentul (UE) 2016/679 (raportat la art. 33 alin. (1) din Regulamentul (UE)

2016/679), pentru încălcarea art. 33 din Regulamentul (UE) 2016/679, privind obligația de notificare a încălcării de securitate la autoritatea de supraveghere.

De asemenea, s-au aplicat următoarele măsuri corective:

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale în scopul încheierii și executării contractelor de împrumut, în special, sub aspectul verificării datelor personale colectate, precum adresa de poștă electronică, ce permit comunicarea la distanță a datelor personale, prin implementarea unor metode eficiente de validare a exactității datelor;

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale în scopul încheierii și executării contractelor de împrumut, în vederea respectării secretului profesional și a confidențialității datelor personale ale clienților săi, în special, în cazul transmiterii unor documente și mesaje ce conțin date personale la distanță, prin implementarea unor măsuri adecvate și eficiente de securitate, atât din punct de vedere tehnic, cât și din punct de vedere organizatoric, prin instruirea persoanelor ce prelucrează date sub autoritatea sa, în vederea identificării și limitării imediate a riscurilor ce pot afecta persoanele vizate;

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale în scopul implementării unei politici interne adecvate pentru identificarea riscurilor, analiza acestora și notificarea către autoritate în cazul producerii unei încălcări a securității, în condițiile prevăzute de art. 33 alin. (1) din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că primește la adresa sa de domiciliu facturi adresate unei alte persoane, client al operatorului, precum și faptul că a semnalat operatorului această situație, dar nu a primit răspuns.

În urma investigației efectuate, s-a constatat că operatorul nu a putut face dovada exactității datelor prelucrate, fapt ce a condus la încălcarea principiului de bază pentru prelucrarea datelor prevăzut de art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679.

De asemenea, s-a constatat că operatorul nu a luat măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor cu caracter personal, fapt care a condus la dezvăluirea datelor cu caracter personal ale unui client al operatorului prin expedierea pe adresa petentului a unor facturi emise pe numele clientului respectiv.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul, cu avertisment și amendă în cuantum de 9544,4 lei (echivalentul a 2000 EURO), pentru

încălcarea dispozițiilor art. 32 alin. (1) lit. b), art. 32 alin. (2) și ale art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679.

3. Investigații referitoare la prelucrarea datelor cu caracter personal de către asociații de proprietari

În anul 2019, 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

O asociație de proprietari, prin unii dintre reprezentanții săi, a accesat sistemul de supraveghere video instalat la nivelul condominiului pentru protecția bunurilor și a persoanelor din imobil, de unde a extras imagini ale petentului și le-a difuzat pe grupul de whatsapp al proprietarilor care locuiau la una din scările blocului. Scopul invocat a fost acela de a identifica persoana care ar fi aruncat deșeuri la intrarea în imobil și de a remedia situația creată; nu s-a menționat dacă, ulterior acestui incident, imaginile respective au fost șterse de pe respectivul grup de whatsapp și cum a fost ”remediată situația” care a determinat accesarea imaginilor.

Prin urmare, 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.

Față de aceste constatări, asociația de proprietari a fost sancționată cu amendă în cuantum de 2389,05 lei (echivalentul a 500 euro) pentru contravenția constatată potrivit art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. a) din Regulamentul (UE) 2016/679, pentru încălcarea principiilor de prelucrare a datelor personale prevăzute de art. 5 alin. (1) lit. a), b) și c), art. 5 alin. (2) din Regulamentul (UE) 2016/679, precum și prin raportare la condițiile de legalitate a prelucrării stabilite de art. 6 alin. (1) din Regulamentul (UE) 2016/679, cu recomandarea de a elimina imaginile de pe grupul de whatsapp.

De asemenea, s-au mai aplicat două avertismente în baza art. 12 din Legea nr. 190/2018, prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. b) și la art. 83 alin. (4) lit. a) din Regulamentul (UE) 2016/679 și au fost dispuse următoarele măsuri corective:

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare efectuate prin intermediul sistemului de supraveghere video în sensul informării persoanelor vizate conform art. 12 și 13 din Regulamentul (UE) 2016/679, inclusiv prin postarea unor avertizări și note de informare în apropierea locurilor unde sunt montate camerele video;

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare prin adoptarea unor măsuri de securitate, tehnice și organizatorice, adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, inclusiv sub aspectul integrării principiilor de protecție a datelor (cum ar fi cel al stocării limitate a înregistrărilor), al stabilirii 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.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a Regulamentului (UE) 2016/679 de către o asociație de proprietari care a afișat la avizierul condominiului petiția sa adresată asociației, transmisă prin poștă cu confirmare de primire, petiție care conținea datele sale cu caracter personal, inclusiv codul numeric personal.

În cursul investigației, operatorul a declarat că a postat reclamația petentului, deoarece a considerat că aceasta era modalitatea prin care trebuia adusă la cunoștința locatarilor de la scara respectivă, întrucât efectuarea de reparații impune acordul majorității. Totodată, operatorul a sugerat că datele petentului au fost dezvăluite din culpa acestuia, deoarece și le-a menționat de bunăvoie în petiția adresată asociației.

Autoritatea națională de supraveghere a apreciat că aspectele sesizate asociației de proprietari de către petent puteau fi aduse la cunoștința tuturor membrilor în cadrul adunării generale. și nu prin afișare.

De asemenea, în lipsa consimțământului petentului, datele personale ale acestuia puteau fi dezvăluite doar în condițiile în care devenea incident un alt temei legal reglementat la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

În plus, Regulamentul (UE) 2016/679 a introdus la art. 5 un nou principiu de prelucrare a datelor, cel al responsabilității, potrivit căruia operatorii de date cu caracter personal nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrare a datelor (”legalitate, echitate şi transparenţă”, ”limitări legate de scop”, ”reducerea la minimum a datelor”, ”exactitate”, ”limitări legate de stocare”, precum și ”integritate şi confidenţialitate”), dar este necesar ca aceștia să poată demonstra respectarea principiilor menționate.

Întrucat asociația de proprietari nu a dovedit respectarea prevederilor susmenționate, a rezultat că a dezvăluit datele personale ale petentului, respectiv numele, prenumele, adresa și codul numeric personal, fără consimțământul acestuia și fără existența unei alte situații în care consimțământul nu este necesar, prin afișarea cererii petentului la avizierul condominiului. În consecință, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea dispozițiilor art. 5 și 6 din Regulamentul (UE) 2016/679, coroborate cu cele ale art. 4 alin. (1) din Legea nr. 190/2018.

Totodată, operatorului i s-a stabilit obligația de a implementa o serie de măsuri corective, astfel încât, pe viitor, datele cu caracter personal ale membrilor asociației să nu fie utilizate și dezvăluite cu încălcarea condițiilor de legalitate prevăzute la art. 6 din Regulamentul (UE) 2016/679, precum și de a adopta măsuri pentru asigurarea securității și confidențialității datelor cu caracter personal ale membrilor asociației, potrivit art. 32 din Regulamentul (UE) 2016/679.

4. <u>Nerespectarea măsurilor dispuse de Autoritatea națională de supraveghere</u>

Potrivit prevederilor Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere are și competența de a da dispoziții operatorului şi persoanei împuternicite de operator să furnizeze orice informaţii pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale precum și de a obţine, din partea operatorului şi a persoanei împuternicite de operator, accesul la toate datele cu caracter personal şi la toate informaţiile necesare pentru îndeplinirea sarcinilor sale.

Cu toate că, în majoritatea cazurilor, operatorii de date cu caracter personal au dat curs solicitărilor Autorității naționale de supraveghere, au fost și situații în care aceștia nu au furnizat autorității informațiile solicitate în îndeplinirea atribuțiilor de investigare.

FIȘĂ DE CAZ

Autoritatea naţională de supraveghere a fost sesizată de către o secție de poliție pentru a verifica respectarea prevederilor Regulamentului (UE) 2016/679 de un operator de date cu caracter personal.

Poliția Orașului Y a semnalat faptul că în urma verificărilor efectuate, ca urmare a unei sesizări primite de la o persoană fizică, a constatat că persoana respectivă a fost contactată de un bărbat care s-a recomandat a fi angajat al unei agenții care se ocupă de recrutarea de copii pentru a participa la ședințe foto de prezentare articole sportive, propunându-i încheierea unei convenții și achitarea unei taxe în acest sens. La pct. 7 al convenției, petenta a fost informată cu privire la prelucrarea datelor cu caracter personal conform Legii nr. 677/2001, lege abrogată de Legea nr. 129/2018.

În urma verificărilor efectuate de Poliția Orașului Y la punctul de lucru al operatorului respectiv, au fost prezentate spre verificare mai multe contracte de prestări servicii încheiate cu diverse persoane fizice, fără a exista indicii că sunt respectate prevederile Regulamentului (UE) 2016/679.

Autoritatea națională de supraveghere a efectuat demersuri în vederea soluționării aspectelor semnalate, dar operatorul de date nu a dat curs solicitărilor instituției noastre, fapt pentru care a fost sancționat contravențional cu avertisment și s-a dispus măsura corectivă de a transmite răspuns complet la adresele autorității, în termen de 5 zile lucrătoare de la comunicarea procesului-verbal.

În continuarea investigației, s-a încheiat un alt proces-verbal de constatare/sancționare, deoarece s-a constatat că societatea nu a adus la îndeplinire măsura corectivă dispusă prin procesul-verbal anterior, respectiv de a transmite Autorității naționale de supraveghere răspuns la adresele prin care s-au solicitat mai multe informații cu privire la aspectele reclamate, în termen de 5 zile lucrătoare de la comunicarea procesului-verbal, încălcându-se astfel prevederile art. 58 alin. (1) lit. a) și lit. e) din Regulamentul (UE) 2016/679.

Față de aceste constatări, operatorul a fost sancționat cu amendă în cuantum de 9551,800 lei (echivalentul sumei de 2000 euro), pentru fapta prevăzută de art. 83 alin. (5) lit. e) din Regulamentul (UE) 2016/679, raportat la art. 58 alin. (1) lit. a) și lit. e) din Regulamentul (UE) 2016/679, coroborat cu art. 8 din OG nr. 2/2001.

De asemenea, s-a aplicat măsura corectivă de aducere la îndeplinire a măsurii corective dispuse prin procesul-verbal anterior, respectiv de a transmite Autorității naționale de supraveghere răspuns la adresele ANSPDCP.

5. <u>Investigaţi referitoare la nerespectarea drepturilor persoanelor vizate</u>

Respectarea drepturilor persoanelor vizate reglementate de Regulamentul (UE) 2016/679 reprezintă o obligație esențială a operatorilor de date.

Cu toate acestea, nerespectarea acestor drepturi a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere și în anul 2019.

Astfel, ca urmare a investigaţiilor efectuate, s-a constatat faptul că operatorii de date cu caracter personal nu soluţionează cererile adresate de persoanele vizate în exercitarea drepturilor lor sau nu respectă 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

Printr-o petiţie înregistrată la Autoritatea naţională de supraveghere un petent ne-a sesizat cu privire la faptul că deținătorul unui site i-a încălcat dreptul de acces.

Astfel, petentul a solicitat să i se confirme dacă îi sunt prelucrate datele cu caracter personal, care sunt categoriile de date prelucrate, informații cu privire la destinatarii datelor sale, precum și copii de pe informațiile existente sau o metodă de a le accesa. Din informațiile transmise de petent, a reieșit faptul că nu a primit un răspuns la cererea sa.

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 alin. (3) și art. 15 din Regulamentul (UE) 2016/679, întrucât nu a facut dovada că a transmis, până la data procesului-verbal de constatare/sancționare, un răspuns complet la cererea petentului prin care acesta și-a exercitat dreptul de acces.

Față de constatări, operatorul a fost sancționat contravențional cu avertisment și s-au dispus următoarele măsuri corective:

- să transmită un răspuns complet petentului la cererea prin care și-a exercitat dreptul de acces, prevăzut de art. 15 din Regulamentul (UE) 2016/679;

- să ia măsuri astfel încât să fie respectate, în toate cazurile, prevederile art. 12 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

O petiționară a sesizat o posibilă încălcare a legislației privind protecția datelor personale de către o instituție financiară nebancară, care nu a răspuns în termenul legal la cererile sale de ștergere a datelor transmise prin sistemul online al Biroului de Credit.

Operatorul a comunicat, în cursul investigației, că a răspuns cu întârziere la cererea petentei, prin depășirea termenului reglementat la 12 alin. (3) din Regulamentul (UE) 2016/679, din cauza unor probleme de natură organizatorică.

Conform art. 12 alin. (3) din Regulamentul (UE) 2016/679, „Operatorul furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.”

Ca urmare, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea art. 12 alin. (3) din Regulamentul (UE) 2016/679.

Totodată, operatorului i s-a aplicat măsura corectivă de a adopta măsuri, la nivelul societății, cu privire la soluționarea cererilor persoanelor vizate întemeiate pe prevederile Regulamentului (UE) 2016/679, astfel încât să fie respectate, în toate cazurile, prevederile art. 12 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Prin petiţia adresată Autorității naționale de supraveghere, un petent a semnalat că o instituție financiară nebancară nu a răspuns în termenul legal la cererea sa transmisă prin sistemul online pus la dispoziție de Biroul de Credit.

În cadrul investigației, a reieșit că petentul s-a adresat operatorului prin intermediul portalului *biroului de credit*, solicitând ștergerea datelor sale prelucrate nelegal.

Prin adresa transmisă de către operator petentului la adresa de e-mail precizată în contract, acesta a fost informat în termenul legal de 30 de zile că, în temeiul art. 12 alin. (3) din Regulamentul (UE) 2016/679, termenul de răspuns se va prelungi cu maximum 60 zile. Ulterior, operatorul a depășit termenul suplimentar prevăzut la acest articol (respectiv în cel mult o lună de la primirea

cererii, perioadă care poate fi prelungită cu două luni atunci când este necesar), răspunsul către petent fiind transmis prin curier, la adresa de domiciliu precizată în contract, după aproximativ 4 luni de la data depunerii cererii sale la operatorul de date. De altfel, răspunsul operatorului a fost comunicat petentului după ce acesta a transmis plângerea la Autoritatea națională de supraveghere.

Prin urmare, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea art. 12 alin. (3) din Regulamentul (UE) 2016/679, fiindu-i aplicată și măsura corectivă de a adopta măsuri la nivelul societății, cu privire la soluționarea cererilor clienților întemeiate pe prevederile Regulamentului (UE) 2016/679, astfel încât să fie respectate, în toate cazurile, prevederile acestui articol.

FIȘĂ DE CAZ

Prin petiţia înregistrată la Autoritatea naţională de supraveghere, un petent a sesizat faptul că deținătorul unui site i-a încălcat dreptul de opoziție garantat de art. 21 din Regulamentul (UE) 2016/679.

În fapt, petentul a solicitat societății care deținea site-ul respectiv să fie dezactivată din baza de date opțiunea de trimitere către adresa sa de e-mail a unor mesaje tip chestionare, dar solicitarea sa nu a fost luată în considerare. Astfel, deși i s-a confirmat dezabonarea de la comunicările comerciale trimise de societate, ulterior petentul a primit un alt mesaj conținând un chestionar de evaluare a ultimei sale comenzi.

Ca urmare a investigației efectuate, s-a constatat că operatorul a încălcat dispozițiile art. 21 alin. (1) – (3) din Regulamentul (UE) 2016/679, întrucât nu a luat în considerare opțiunea petentului de a-i fi dezactivată din baza de date opțiunea exprimată, de a nu mai primi pe adresa sa de e-mail mesaje de tipul chestionarelor de satisfacție, fapt care a condus la transmiterea unui nou mesaj de acest gen.

Față de constatări, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea prevederilor art. 21 din Regulamentul (UE) 2016/679. De asemenea, s-au dispus următoarele măsuri corective:

- să ia în considerare solicitarea petentului de a fi dezactivată din baza de date opțiunea privind transmiterea pe adresa sa de e-mail a mesajelor referitoare la chestionarele de satisfacție;

- să ia măsuri astfel încât să fie respectate, în toate cazurile, prevederile art. 21 din Regulamentul (UE) 2016/679.

6. Investigații referitoare la transmiterea de comunicări comerciale prin mijloace de comunicație electronică

Autoritatea națională de supraveghere a înregistrat și în anul 2019 un număr semnificativ de plângeri având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (SMS) sau prin poşta electronică.

Ca urmare a investigaţiilor efectuate, s-a constatat faptul în unele cazuri expeditorii mesajelor comerciale nu au respectat prevederile legale sub aspectul obţinerii consimțământului prealabil şi al respectării opţiunii persoanelor vizate de a nu mai primi mesaje comerciale nesolicitate.

FIȘĂ DE CAZ

Prin petiţiile înregistrate la Autoritatea naţională de supraveghere un petent ne-a sesizat cu privire la faptul că un furnizor de telefonie i-a încălcat dreptul de opoziție.

Astfel, petentul a solicitat societății să nu mai primească mesaje referitoare la promoții, concursuri și orice alte mesaje în afara celor care privesc costurile și securitatea convorbirilor. Astfel, deși inițial i s-a confirmat dezabonarea de la comunicările comerciale trimise de operator, ulterior a primit un alt mesaj nesolicitat.

În urma demersurilor efectuate, operatorul a fost sancționat cu amendă în cuantum de 10.000 lei pentru contravenția prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004.

De asemenea, s-au recomandat societății următoarele:

- să respecte solicitarea petentului de a nu mai primi mesaje referitoare la promoții, concursuri și orice alte mesaje în afara celor care privesc costurile și securitatea convorbirilor;

- să adopte măsurile necesare pentru asigurarea respectării prevederilor art. 12 din Legea nr. 506/2004, în vederea transmiterii de mesaje comerciale prin mijloace de comunicare electronică numai cu consimţământul expres prealabil al destinatarilor.

FIȘĂ DE CAZ

Un petent a reclamat o posibilă încălcare a prevederilor legale privind prelucrarea datelor sale cu caracter personal de către deținătorul unui website, prin faptul că a primit mesaje comerciale, în ciuda faptului că s-a dezabonat, atât prin intermediul formularului existent pe site-ul operatorului reclamat, cât și prin utilizarea link-urilor de dezabonare din cadrul mesajelor de tip newsletter primite.

În urma investigației efectuate, operatorul nu a putut face dovada obținerii consimțământului prealabil expres și neechivoc al petentului pentru transmiterea de mesaje comerciale pe adresa sa de e-mail.

Pentru faptele constatate, operatorul a fost sancționat cu amendă în cuantum de 10.000 de lei pentru contravenția prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004, cu recomandarea de a se lua măsurile necesare respectării prevederilor art. 12 din Legea nr. 506/2004, în vederea transmiterii de mesaje comerciale prin mijloace de comunicare electronică numai cu consimţământul expres prealabil al destinatarilor.

7. Investigații referitoare la prelucrarea datelor cu caracter personal de către autoritățile publice

Potrivit art. 2 alin. (1) lit. a) din Legea nr. 190/2018, autoritățile și organismele publice sunt: Camera Deputaților și Senatul, Administrația Prezidențială, Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale, autoritățile și instituțiile publice autonome, autoritățile administrației publice locale și de la nivel județean, alte autorități publice, precum și instituțiile din subordinea/coordonarea acestora; de asemenea, sunt asimilate autorităților/organismelor publice și unitățile de cult și asociațiile și fundațiile de utilitate publică.

În măsura în care entitatea în cauză, potrivit actelor normative de înființare, organizare și funcționare, se înscrie stricto-sensu în definiția dată de textul de lege, dispozițiile specifice din Legea nr. 190/2018, inclusiv sub aspectul sancțiunilor, devin aplicabile.

În acest context, în anul 2019, 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

Un petent a sesizat faptul că au fost făcute fotografii cu toți angajații care au participat la un eveniment organizat de angajatorul său, fără a fi informați în ce scop vor fi utilizate ulterior. Petentul precizează că a considerat că fotografiile vor fi utilizate la întocmirea raportului de activitate, în circuitul intern al instituției, dar la revenirea la serviciu a aflat că acestea au fost postate pe pagina de Facebook a instituției, fără consimțământul său.

Din investigația efectuată, a rezultat că publicarea pe pagina de Facebook a respectivei instituții publice a unor fotografii cu angajații acesteia, cu ocazia organizării unui eveniment de promovare, a fost un ”demers privat”, după cum a declarat operatorul. O astfel de prelucrare nu se încadrează în niciuna dintre situațiile menționate în nota de informare prezentată, excedând scopurilor și categoriilor de destinatari precizate, astfel încât pentru o astfel de prelucrare operatorul avea obligația de a obține consimțământul expres și informat al persoanelor vizate (angajați) în condițiile prevăzute de art. 7 și 13 din Regulamentul (UE) 2016/679; un ”acord verbal”, așa cum a declarat operatorul, nu putea fi demonstrat în această speță, cu atât mai mult în contextul celor declarate de petent care a menționat că a fost de acord cu efectuarea fotografiilor, considerând că vor fi folosite în ”circuitul intern al instituției”, însă nu a fost de acord și nu a fost informat în prealabil în legătură cu postarea respectivelor fotografii pe pagina de Facebook a instituției, spațiu public.

Față de constatări, au fost aplicate două avertismente în baza art. 12-14 din Legea nr. 190/2018, pentru nerespectarea condițiilor prevăzute de art. 6 alin. (1) lit. a) și 7 din Regulamentul (UE) 2016/679, respectiv, pentru nerespectarea tuturor condițiilor prevăzute de art. 13 din Regulamentul (UE) 2016/679.

Totodată, avertismentele au fost însoțite de un plan de remediere prin care s-au dispus următoarele măsuri:

-respectarea condițiilor de prelucrare a imaginii angajaților prin raportare la dispozițiile art. 6 și 7 din Regulamentul (UE) 2016/679, prin analizarea situațiilor existente și remedierea deficiențelor constatate;

-realizarea informării complete a persoanelor vizate, potrivit cerințelor art. 13 și după caz, art. 14 din Regulamentul (UE) 2016/679, prin raportare la toate scopurile în care sunt prelucrate datele cu caracter personal.

FIȘĂ DE CAZ

Un petiționar a sesizat Autoritatea națională de supraveghere cu privire la o posibilă încălcare a prevederilor legale privind prelucrarea datelor cu caracter personal de către o primărie, prin faptul că imagini captate prin intermediul unui sistem de supraveghere audio/video al acestui operator au fost dezvăluite unor terți și postate pe internet.

În cadrul investigației efectuate, operatorul a declarat că reprezentantul legal al primăriei a pus la dispoziţia unor ziariști locali o filmare de câteva secunde, surprinsă pe domeniul public, în care petentul amenința şi aducea injurii primăriei, însă a considerat că acest demers nu fost în măsură

să contravină prevederilor Regulamentului (UE) 2016/679, mai ales că petentul nu a făcut solicitări în acest sens, respectiv nu a cerut ştergerea imaginii sale, fiind aplicabile, în opinia operatorului, prevederile art. 17 alin. (3) lit. a) din Regulamentul (UE) 2016/679.

Întrucât s-a constatat că primăria nu a respectat dispozițiile legale privind prelucrarea datelor cu caracter personal, astfel încât a fost dezvăluită imaginea petentului, captată de sistemul de supraveghere video al instituției fără consimțământul său sau alt temei legal, unui ziar local, s-a aplicat sancțiunea avertismentului în baza art. 12-14 din Legea nr. 190/2018, pentru nerespectarea condițiilor prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Totodată, avertismentul a fost însoțit de un plan de remediere.

8. Dezvăluirea datelor cu caracter personal către diverse entităţi

În anul 2019, o pondere însemnată în numărul plângerilor adresate Autorităţii naționale de supraveghere a fost reprezentată de petițiile prin care s-au semnalat situații diverse de încălcare a dispozițiilor legale privind condiţiile în care date personale au fost dezvăluite publicului larg, către terțe persoane neautorizate sau către diverse entităţi de drept public şi privat, fără să fi fost obţinut în prealabil acordul persoanelor vizate, fără să existe un alt temei legal sau fără informarea acestora.

FIŞĂ DE CAZ

Prin petiţia adresată Autorității naționale de supraveghere, un petent a reclamat dezvăluirea datelor sale (ex. nume și prenume, adresă, date autoturism) pe site-ul unei societăți comerciale care își desfășoară activitatea în domeniul asigurărilor, fără consimțământul său, situație în care datele sale au putut fi obținute de către o altă persoană fizică care le-a postat ulterior pe pagina sa de Facebook.

Petentul a mai susținut că sistemul de evidență deținut de acest operator poate fi accesat pe internet.

În urma investigației efectuate, a reieșit că datele cu caracter personal ale petentului au fost furnizate de către acesta în momentul emiterii unei polițe CASCO. Ulterior, aceste date au fost dezvăluite neautorizat pe Facebook de către angajata unei alte societăți care avea calitatea de persoană împuternicită a operatorului.

Operatorul a declarat că dezvăluirea datelor petentului a fost remediată după constatarea acesteia, prin ștergerea datelor de pe Facebook, iar persoana care a dezvăluit aceste date a suportat consecințele unei măsuri disciplinare.

Totodată, a reieșit că site-ul în cauză nu este un site cu informații accesibile tuturor, ci este o interfață pentru accesarea unei aplicații de emitere oferte/produse de asigurare care aparține operatorului, iar personalul propriu și asistenții de brokeraj ai operatorului, avizați de către Autoritatea de Supraveghere Financiară (ASF), se pot loga la această aplicație doar pe bază de credențiale (user și parolă individuală) conform condițiilor/restricțiilor de securitate prevăzute de Norma 6/2015 emisă de ASF.

Astfel, față de informațiile și documentele transmise în cadrul investigației, s-a constatat că operatorul nu a respectat prevederile legale referitoare la prelucrarea datelor prin intermediul unei persoane împuternicite, întrucât nu a elaborat instrucțiuni documentate în sarcina împuternicitului său, conform prevederilor art. 28 din Regulamentul (UE) 2016/679.

De asemenea, s-a apreciat că operatorul nu a asigurat suficiente măsuri tehnice și organizatorice prevăzute de art. 32 din Regulamentul (UE) 2016/679, respectiv, nu a luat în calcul riscurile prezentate de prelucrare, generate, în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal prelucrate.

Prin urmare, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea art. 28 alin. (1) și (3) și art. 32 din Regulamentul (UE) 2016/679 și au fost aplicate măsuri corective prin care operatorul a fost obligat să întreprindă demersurile necesare pentru asigurarea conformității cu aceste prevederi.

CAPITOLUL IV

ACTIVITATEA ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

În anul 2019, activitatea Autorității naţionale de supraveghere a fost marcată și de participarea la activitatea la nivel european, dominată de aspecte complexe și tehnice. Autoritatea naţională de supraveghere, reprezentată de unul sau mai mulți dintre membrii săi, a participat în 2019 la diferite grupuri de lucru la nivel european, conferinţe, seminarii şi 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 Europol şi Organismul comun de control în domeniul Vamal,
- Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II şi Grupul de coordonare comună Eurodac.

■ Comitetul european pentru protecția datelor

În anul 2019, Comitetul european pentru protecția datelor a adoptat un număr de 8 avize pe marginea proiectelor de liste de operațiuni pentru care este necesară realizarea evaluării impactului asupra protecției datelor, în conformitate cu art. 35 (4) din Regulamentul (UE) 2016/679, 2 avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii, 2 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, 1 aviz pe marginea clauzelor contractuale standard înaintate în temeiul art. 28 alin. (8) 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, declarații, note de informare, după cum urmează:

- orientări privind codurile de conduită și organismele de monitorizare prevăzute în Regulamentul (UE) 2016/679 – codurile de conduită pot funcționa ca mecanism prin care să se demonstreze respectarea Regulamentului General privind Protecția Datelor. Documentul adoptat are

drept obiectiv oferirea de îndrumări practice în ceea ce privește aplicarea art. 40 și 41 din Regulamentul (UE) 2016/679. Acestea sunt menite să contribuie la clarificarea procedurilor și a normelor implicate în transmiterea, aprobarea și publicarea codurilor de conduită, atât la nivel național, cât și la nivel european. Totodată, prin acest ghid s-a intenționat să se stabilească cerințele pentru monitorizarea eficace a respectării unui cod de conduită;

- orientări privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din Regulamentul (UE) 2016/679 în contextul furnizării de servicii online persoanelor vizate – documentul se referă la aplicabilitatea art. 6 alin. (1) litera (b) cu privire la prelucrarea datelor cu caracter personal în contextul contractelor pentru servicii online, indiferent de modul de finanțare a serviciilor. Ghidul prezintă elementele prelucrării legale în temeiul art. 6 alin. (1) din Regulamentul (UE) 2016/679 și ia în considerare conceptul de „necesitate” în sensul aplicat sintagmei „necesar pentru executarea unui contract”;
- orientări privind prelucrarea datelor cu caracter personal prin dispozitive video - utilizarea intensivă a dispozitivelor video are impact asupra comportamentului cetățenilor. Implementarea semnificativă a unor astfel de instrumente în multe domenii ale vieții persoanelor va pune o presiune suplimentară asupra persoanei fizice pentru a preveni detectarea a ceea ce ar putea fi perceput ca anomalii. Ghidul vizează oferirea de îndrumări cu privire la modul de aplicare a Regulamentului (UE) 2016/679 în legătură cu prelucrarea datelor cu caracter personal prin dispozitive video. Exemplele oferite în document nu sunt exhaustive, raționamentul general putând fi aplicat tuturor domeniilor de utilizare posibile;
- aviz privind Întrebările și Răspunsurile referitoare la interacțiunea dintre Regulamentul privind studiile clinice (CTR) și Regulamentul (UE) 2016/679 [art. 70 alin. (1) litera (b)] – întrebările și răspunsurile Comisiei Europene abordează o serie de subiecte care vor deveni mai relevante atunci când Regulamentul privind studiile clinice devine aplicabil. Printre aceste subiecte se numără: temeiul juridic adecvat, consimțământul informat și retragerea sa, informarea persoanelor vizate, transferurile și utilizările secundare. Cu toate că Regulamentul privind studiile clinice nu este încă aplicabil, informațiile furnizate în cadrul acestor întrebări frecvente constituie o bază bună pentru un studiu clinic care respectă Regulamentul (UE) 2016/679. Opinia Comitetului european pentru protecția datelor se concentrează asupra chestiunii temeiului juridic adecvat pentru prelucrarea datelor cu caracter personal în contextul studiilor clinice (utilizare primară) și al utilizării secundare a datelor rezultate în urma studiilor clinice în alte scopuri de cercetare științifică;

- declarație cu privire la Regulamentul privind viața privată și comunicațiile electronice – Comitetul european pentru protecția datelor a solicitat legiuitorilor UE să-și intensifice eforturile în vederea adoptării unui regulament privind viața privată și comunicațiile electronice, care este necesar pentru a completa cadrul UE pentru protecția datelor și confidențialitatea comunicațiilor. De asemenea, a subliniat faptul că Regulamentul privind viața privată și comunicațiile electronice nu trebuie în niciun caz să reducă nivelul de protecție oferit de actuala Directivă 2002/58/CE privind confidențialitatea și comunicațiile electronice și trebuie să completeze Regulamentul (UE) 2016/679 prin furnizarea de garanții solide suplimentare pentru toate tipurile de comunicații electronice;
- declarație privind utilizarea datelor cu caracter personal în cadrul campaniilor politice – prin documentul adoptat, Comitetul european pentru protecția datelor a subliniat o serie de aspecte esențiale care trebuie respectate atunci când partidele politice prelucrează date cu caracter personal în cadrul activităților electorale, și anume: prelucrarea datelor cu caracter personal care dezvăluie opinii politice, ca principiu general, este interzisă și face obiectul unei serii de condiții strict interpretate, cum ar fi consimțământul explicit, specific, pe deplin informat și liber exprimat al persoanelor fizice; datele cu caracter personal care au fost făcute publice sau care au fost comunicate în alt mod de votanții persoane fizice, chiar dacă nu sunt date care dezvăluie opinii politice, fac în continuare obiectul protecției oferite de legislația UE privind protecția datelor; chiar și în cazul în care prelucrarea este legală, organizațiile trebuie să își respecte celelalte îndatoriri în temeiul Regulamentului (UE) 2016/679, inclusiv obligația de a fi transparenți și de a oferi informații suficiente persoanelor care sunt analizate și ale căror date cu caracter personal sunt prelucrate, indiferent dacă datele au fost obținute direct sau indirect; în cazul în care, din punct de vedere juridic sau similar, decizia afectează în mod semnificativ persoana care face obiectul deciziei, este restricționat doar procesul decizional automatizat, inclusiv crearea de profiluri; în caz de direcționare, ar trebui furnizate informații adecvate alegătorilor care să explice de ce primesc un anumit mesaj, cine este responsabil pentru acesta și modul în care își pot exercita drepturile în calitate de persoane vizate. Respectarea normelor de protecție a datelor, inclusiv în contextul activităților electorale și al campaniilor politice, este esențială pentru protejarea democrației;
- notă de informare privind transferurile de date efectuate în conformitate cu Regulamentul (UE) 2016/679 în cazul unui Brexit fără acord – în lipsa unui acord între SEE și Regatul Unit (Brexit fără acord), Regatul Unit va deveni o țară terță. Acest lucru înseamnă că transferurile datelor cu caracter personal către Regatul Unit trebuie efectuate în conformitate cu unul dintre următoarele instrumente: clauze standard sau ad-hoc de protecție a datelor; reguli corporatiste obligatorii; coduri de conduită și mecanisme de certificare; derogări. Documentul adoptat de Comitetul european pentru

protecția datelor furnizează informații organizațiilor comerciale și publice cu privire la aceste instrumente de transfer prevăzute în Regulamentul (UE) 2016/679 pentru transferul datelor cu caracter personal către Regatul Unit în cazul unui Brexit fără acord;

- notă de informare cu privire la regulile corporatiste obligatorii (BCRs) pentru întreprinderile a căror autoritate de supraveghere principală pentru BCRs este Oficiul Comisarului pentru Informații (ICO) – documentul abordează situatia în care nu se ajunge la un acord privind Brexitul, iar ICO nu mai are un rol în comunitatea BCRs. Astfel, pentru *grupurile cu sediul în Regatul Unit care doresc să aplice pentru BCRs*, acestea trebuie să identifice cea mai adecvată autoritate de supraveghere principală pentru BCRs dintr-un stat membru al UE. Referitor la *grupurile ale căror BCRs sunt în stadiu de examinare de către ICO*, acestea trebuie să identifice o nouă autoritate de supraveghere principală BCRs, iar noua autoritate de supraveghere principală pentru BCRs va prelua cererea și va iniția oficial o nouă procedură, la momentul unui Brexit fără acord. Cât privește *proiectul de BCR-uri depuse la Comitetul european pentru protecția datelor*, dacă proiectul de decizie ICO de aprobare a BCRs este în așteptare la Comitetul european pentru protecția datelor la momentul unui Brexit fără acord, grupul trebuie să identifice o nouă autoritate de supraveghere principală pentru BCRs, iar noua autoritate de supraveghere principală pentru BCRs va prelua și va depune din nou la Comitetul european pentru protecția datelor proiectul de decizie pentru aprobarea BCRs. În ceea ce priveste grupurile deținătoare de BCRs autorizate, acestea trebuie să identifice noua autoritate de supraveghere principală pentru BCRs.

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

- orientări privind asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit – documentul oferă îndrumări generale privind obligația asigurării protecţiei datelor începând cu momentul conceperii şi în mod implicit prevăzută la art. 25 din Regulamentul (UE) 2016/679, unde obligația principală este implementarea efectivă a principiilor de protecție a datelor, precum și a drepturilor și libertăților persoanelor fizice atât la momentul conceperii, cât și în mod implicit. Acest lucru înseamnă că operatorii trebuie să implementeze măsuri tehnice și organizatorice adecvate, precum și garanții necesare, concepute pentru a implementa principiile de protecție a datelor într-un mod eficient și pentru a proteja drepturile și libertățile persoanelor vizate. Totodată, operatorii trebuie să poată demonstra eficacitatea măsurilor implementate. Ghidul acoperă elemente de care operatorii trebuie să țină seama atunci cand stabilesc mijloacele de prelucrare. Criteriile „de ultimă generație” impun operatorilor să fie la curent cu progresul tehnologic pentru a asigura

implementarea eficientă continuă a principiilor de protecție a datelor. „Costul implementării" impune operatorului să țină seama de costurile și resursele necesare pentru implementarea eficientă și menținerea continuă a tuturor principiilor de protecție a datelor pe parcursul operațiunii de prelucrare. Alte elemente de care operatorii trebuie să țină seama sunt natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea;

- orientări privind criteriile dreptului de a fi uitat în cazul motoarelor de căutare – acest document își propune să interpreteze dreptul de a fi uitat în cazul motoarelor de căutare ținând cont de dispozițiile art. 17 din Regulamentul (UE) 2016/679. Într-adevăr, dreptul de a fi uitat a fost adoptat, în special în temeiul art. 17 din Regulamentul (UE) 2016/679, pentru a ține cont de dreptul de a solicita delistarea, stabilit în hotărârea Costeja. Trebuie ținut cont de faptul că, în timp ce art. 17 din Regulamentul (UE) 2016/679 este aplicabil tuturor operatorilor, acest document se concentrează numai pe prelucrarea efectuată de furnizorii de motoare de căutare și cererile de delistare transmise de persoanele vizate.

■ Comitetul Consultativ al Convenţiei 108 al Consiliului Europei

La nivel european, Convenţia 108 acoperă toate domeniile de prelucrare a datelor cu caracter personal, iar dispoziţiile acesteia au scopul de a reglementa prelucrarea datelor cu caracter personal la nivel general.

Obiectivul Convenției 108 este de a proteja orice persoană, indiferent de naționalitatea sau reședința acesteia, în ceea ce privește prelucrarea datelor cu caracter personal, contribuind astfel la respectarea drepturilor și libertăților fundamentale ale omului și, în special, a dreptului la viață privată.

Dreptul la protecția datelor cu caracter personal trebuie luat în considerare ținând cont de rolul său în societate și trebuie reconciliat cu alte drepturi și libertăți fundamentale ale omului, inclusiv cu libertatea de exprimare.

Modernizarea normelor la nivelul Consiliului Europei a coincis cu reforma legislaţiei în domeniul protecţiei datelor cu caracter personal la nivelul Uniunii Europene. Procesul de revizuire a urmărit cele două mari obiective, respectiv să răspundă provocărilor la adresa vieţii private ca rezultat al utilizării noilor tehnologii în domeniul comunicaţiilor şi să sublinieze importanţa mecanismului de follow-up cu privire la implementarea principiilor stabilite prin Convenţia 108.

Astfel, în anul 2019, Ministerul Afacerilor Externe a coinițiat împreună cu Autoritatea națională de supraveghere Memorandumul cu tema „Aprobarea semnării Protocolului de amendare a

Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal", 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.

În ceea ce privește aderarea la Convenția CoE pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal adoptată la Strasbourg la 28 ianuarie 1981, începând cu data de 1 iunie 2019, Convenția 108 și Protocolul privind autoritățile de supraveghere și fluxurile transfrontaliere de date vor deveni aplicabile și în Argentina, iar, începând cu data de 1 septembrie 2019, vor deveni aplicabile și în Maroc.

■ Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II, Grupul de coordonare comună Eurodac, Comitetul de Cooperare Europol si Grupul de coordonare comună Vămi

Grupul de coordonare comună VIS a decis să abordeze un nou subiect aflat în programul său de lucru și anume oferirea de instruire privind protecția datelor membrilor personalului autorităților cu acces la VIS, prin adoptarea unui chestionar și transmiterea acestuia, spre completare, autorităților naționale competente să aibă acces la datele introduse în VIS.

În urma analizării contribuțiilor primite de la statele membre, s-a concluzionat faptul că majoritatea statelor membre au instituit proceduri pentru a se asigura că membrii personalului cu acces direct la VIS au primit o instruire adecvată privind normele de protecție a datelor cu caracter personal. În ceea ce privește persoana responsabilă cu instruirea, mai multe state membre au atribuit această sarcină responsabilului cu protecția datelor. În legatură cu o posibilă îmbunătățire a instruirii, există posibilități de e-training, instruiri orientate pe diverse tematici.

În același timp, merită mentionat faptul că autoritățile de supraveghere au fost implicate în oferirea de instruire cu privire la regulile și principiile de protecție a datelor cu caracter personal. Totodată, autoritățile de supraveghere verifică respectarea acestei obligații a operatorului de a oferi instruire corespunzătoare personalului autorităților care au drept de acces la VIS, verificarea realizându-se prin inspecții și audituri.

Grupul de coordonare comună VIS încurajează toate statele membre să se asigure că astfel de instruiri se realizează pentru tot personalul care are acces direct sau indirect la VIS.

Referitor la activitatea autorităților de supraveghere în ceea ce privește Eurodac, Grupul de coordonare comună Eurodac a colaborat cu Agenția pentru Drepturi Fundamentale (FRA) în legătură cu un nou instrument de informare a persoanelor vizate cu privire la drepturile lor. Ca urmare a acestei colaborări, a fost redactat și adoptat pliantul „Dreptul la informare – Ghid pentru autorități atunci când colectează amprentele digitale pentru EURODAC".

Acest pliant ajută ofițerii și autoritățile în realizarea obligației de informare a solicitanților de azil și imigranților, într-un mod inteligibil și accesibil, cu privire la prelucrarea amprentelor lor în sistemul Eurodac.

În același timp, referitor la chestionarul privind drepturile persoanelor vizate, ca urmare a răspunsurilor primite de la statele membre, a reieșit faptul că mai multe state membre oferă informații persoanelor vizate cu privire la colectarea de date despre acestea și accesul autorităților de aplicare a legii, într-o manieră completă și cuprinzătoare, acordând o atenție specială minorilor. De asemenea, s-a evidențiat faptul că toate statele membre respondente au proceduri specifice cu privire la asigurarea dreptului de acces.

În ceea ce privește activitatea în domeniul Europol, în anul 2019 Comitetul de Cooperare Europol a adoptat proiectul de adresă referitoare la revizuirea acordurilor de cooperare încheiate cu state terțe în temeiul art. 25 (1) din Regulamentul (UE) 2016/794 care, ulterior, a fost transmisă Comisiei Europene.

Respectivul document face trimitere la posibilitatea Europol de a transfera date cu caracter personal unei autorități dintr-un stat terț în baza unei decizii privind nivelul de protecție adecvat recunoscut prin Decizia Comisiei Europene, a unui acord internațional sau a unui acord de cooperare care permite schimbul de date cu caracter personal, încheiat între Europol și statul terț anterior intrării în vigoare a Regulamentului (UE) 2016/794.

În același timp, alin. (4) al aceluiași articol din Regulamentul (UE) 2016/794 prevede că, până la 14 iunie 2021, Comisia Europeană ar trebui să evalueze dispozițiile cuprinse în acordurile de cooperare încheiate în trecut. Aceste examinări trebuie realizate ținând cont de prevederile Directivei (UE) 2016/680.

Astfel, prin adresa transmisă, Comitetul de Cooperare Europol a încurajat Comisia Europeană să realizeze respectivele revizuiri cât mai curând posibil pentru a permite continuarea schimbului de date cu statele terțe după termenul prevăzut de Regulamentul (UE) 2016/794 – 14 iunie 2021, în conformitate cu cadrul legal al protecției datelor UE.

Referitor la activitatea de promovare și facilitarea exercitării drepturilor persoanelor vizate, s-a stabilit necesitatea elaborării unui ghid de acces în legătură cu activitățile Europol, întrucat astfel de îndrumări pot oferi o imagine de ansamblu a autorității competente din fiecare stat membru și informațiile de contact ale autoritatilor de supraveghere la care poate fi trimisă o plângere.

Autoritatea națională de supraveghere, în calitate de raportor pe acest subiect, a înaintat un prim proiect al acestui ghid menit să explice persoanelor vizate cum să-și exercite drepturile în domeniul protecției datelor în legătură cu activitățile Europol.

În domeniul Vămilor, având în vedere faptul că pagina web reprezintă un instrument util în ceea ce priveste informarea persoanelor vizate, autoritățile pentru protecția datelor din Grecia, Polonia și România, împreună cu secretariatul Grupului de coordonare comună Vămi vor revizui și actualiza conținutul paginii web al grupului de coordonare.

■ **A 41-a Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private**

În anul 2019, cea de-a 41 - a Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private a fost organizată de Autoritatea pentru protecţia datelor din Albania. În cadrul conferinței au fost adoptate următoarele rezoluții și declarații:

- rezoluție privind direcția strategică a conferinței
- rezoluție privind viața privată ca drept fundamental al omului și condiție prealabilă pentru exercitarea altor drepturi fundamentale
- rezoluție privind promovarea instrumentelor practice noi și pe termen lung și eforturile legale continue pentru cooperarea eficientă în aplicarea transfrontalieră
- rezoluție privind privind social media și conținutul extremist violent în mediul online
- rezoluție pentru a sprijini și a facilita cooperarea de reglementare între autoritățile pentru protecția datelor și autoritățile pentru protecția consumatorilor și concurență pentru a atinge standarde clare și în mod constant ridicate de protecție a datelor în economia digitală
- rezoluție pentru a aborda rolul erorii umane în cadrul încălcărilor de securitate a datelor cu caracter personal.

■ Conferința de primăvară a autorităţilor europene pentru protecţia datelor

În anul 2019, Conferința de primăvară a autorităților europene pentru protecția datelor cu caracter personal a fost organizată de Autoritatea pentru protecția datelor din Georgia. Subiectele dezbătute au vizat următoarele aspecte:

- 1 an de aplicare a Regulamentului (UE) 2016/679
- Convenția 108 modernizată
- protecția datelor cu caracter personal ale minorilor
- protecția datelor cu caracter personal și organizațiile internaționale.

În cadrul conferinței de primăvară a autorităților europene pentru protecția datelor a fost adoptată rezoluția privind acreditarea Autorității pentru protecția datelor din Turcia.

■ Misiuni de evaluare Schengen

O parte din activitatea Autorității naționale de supraveghere în plan extern în anul 2019 se referă la participarea instituției noastre la misiunile de evaluare Schengen în domeniul protecţiei datelor din Cehia și Cipru.

Misiunile Schengen se referă la evaluarea și monitorizarea aplicării *acquis-ului* Schengen, respectiv analizarea modului de implementare a regulilor de protecție a datelor cu caracter personal, asigurându-se astfel că statele membre aplică reglementările Schengen în mod eficient și în conformitate cu principiile și normele fundamentale. La finalul fiecarei misiuni de evaluare se întocmește un raport pe baza răspunsurilor transmise de statul evaluat la chestionarul standard[1] și a informațiilor furnizate de autoritățile statului respectiv pe durata vizitei de evaluare. Respectivul document conține, printre altele, constatări și evaluări cu privire la legislație, autoritatea pentru protecția datelor, drepturile persoanelor vizate, cooperarea internațională.

■ 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.

[1] Art. 9 din Regulamentul (UE) NR. 1053/2013 al Consiliului din 7 octombrie 2013 de instituire a unui mecanism de evaluare și monitorizare în vederea verificării aplicării acquis-ului Schengen și de abrogare a Deciziei Comitetului executiv din 16 septembrie 1998 de instituire a Comitetului permanent pentru evaluarea și punerea în aplicare a Acordului Schengen

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

În anul 2019, Autoritatea națională de supraveghere a primit și a analizat cereri de aprobare a BCRs transmise de 53 de companii multinaționale. De asemenea, Autoritatea națională de supraveghere 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.

Procedura de aprobare a BCRs s-a schimbat de la un sistem de recunoaștere reciprocă în conformitate cu Directiva 95/46/CE la sistemul actual în care toate BCRs trebuie să fie prezentate Comitetului european pentru protecția datelor în vederea obținerii unui aviz în temeiul art. 64 din Regulamentul (UE) 2016/679.

Această procedură presupune că toate autoritățile de supraveghere au posibilitatea de a transmite observații pe marginea cererilor BCRs, ceea ce duce la o procedură de cooperare ceva mai lungă. Procedura va ajuta Comitetul european pentru protecția datelor la redactarea avizului său dacă toate chestiunile problematice sunt soluționate înainte de demararea procedurii prevăzute la art. 64 din Regulamentul (UE) 2016/679. În anul 2019, Comitetul european pentru protecția datelor a emis opinii în temeiul art. 64 din Regulamentul (UE) 2016/679 cu privire la 2 cereri BCRs depuse prin autoritățile de supraveghere din Regatul Unit și din Belgia.

■ 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 cca **18 solicitări** cu privire la aplicarea și respectarea Regulamentul (UE) 2016/679. Solicitările venite din partea autorităților de supraveghere din Cehia, Estonia, Italia, Letonia, Luxembourg, Malta, Norvegia, Polonia, Slovacia, Ungaria au vizat aspecte referitoare la temeiul legal pentru prelucrarea datelor cu caracter personal din cazierul judiciar, stocarea datelor cu caracter personal în temeiul interesului legitim, condiții privind desemnarea responsabilului cu protecția datelor și răspunderea acestuia, interacțiunea dintre termenele prevăzute de Regulamentul (UE) 2016/679 și legislația națională.

■ **Contribuții pe marginea documentelor din perspectiva protecției datelor cu caracter personal**

În cursul anului 2019, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

➢ studiile de impact lansate de Comisia Europeană având ca temă echipamente radio conectate la Internet și echipamente radio portabile și sistem radio reconfigurabile – Autoritatea națională de supraveghere a subliniat faptul că, în situația în care, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal, potrivit art. 35 din Regulamentul (UE) 2016/679 și art. 1 lit. e) și f) din Decizia nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal adoptată de Autoritatea națională de supraveghere. În același timp, au fost evidențiate prevederile art. 35 alin. (10) din Regulamentul (UE) 2016/679 ale și art. 1 alin. (2) din Decizia nr. 174/2018;

➢ raportul anual 2018 și planul de lucru 2020 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;

➢ raportul de țară privind situația drepturilor omului pentru anul 2018, întocmit de Departamentul de Stat al Statelor Unite ale Americii – în urma consultării raportului referitor la România, Autoritatea națională de supraveghere a transmis o serie de observații pe marginea Secțiunii 2. Respect for Civil Liberties, care au vizat competențele de control ale Autorității naționale de supraveghere, autonomia și independența acesteia în îndeplinirea sarcinilor și exercitarea competenţelor sale, potrivit art. 52 din Regulamentul (UE) 2016/679, prelucrarea datelor în scop jurnalistic. Cu această ocazie, Autoritatea națională de supraveghere a evidențiat faptul că a luat și va lua și în continuare în considerare întreaga jurisprudență CEDO în domeniul protecției datelor, ținând cont de circumstanțele particulare ale fiecărui caz în parte. Totodată, a fost subliniat încă o dată faptul că Autoritatea națională de supraveghere, în considerarea rolului său de garant al dreptului la viață privată și a dreptului la protecția datelor personale, s-a exprimat și a acționat în

mod constant, încă de la înființare, în sensul asigurării unui echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare;

- întrebările formulate de Consiliul Uniunii Europene pentru reuniunile DAPIX – Autoritatea națională de supraveghere a menționat faptul că nu s-a confruntat cu situații în care au fost folosite deciziile privind caracterul adecvat al nivelului de protecție pentru a transfera date cu caracter personal către o țară terță sau o organizație internațională. De asemenea, au fost facute referiri la procedura de numire a președintelui și de reînnoire a mandatului de președinte, la bugetul Autorității naționale de supraveghere, aspecte care denotă independența autorității. Cât privește mecanismul de cooperare și coerență, a fost precizat că Autoritatea națională de supraveghere cooperează cu celelalte autorități de supraveghere folosind platfoma IMI (Sistemul de informare al pieței interne) pusă la dispoziție de Comisia Europeană, cele mai frecvent utilizate solicitări de cooperare fiind cererile întemeiate pe art. 56 și pe art. 61 din Regulamentul (UE) 2016/679;
- proiectul de Protocol de amendare a Convenției PCC SEE – Autoritatea națională de supraveghere a formulat o serie de recomandări de completare a dispozițiilor protocolului, recomandări care au vizat evidențierea modernizării Convenției 108, prezentarea tuturor situațiilor referitoare la formatul de păstrare a datelor cu caracter personal (pe hârtie/electronic), asigurarea unei modalități eficiente de ștergere și/sau distrugere a datelor cu caracter personal;
- documente referitoare la propunerea de regulament ePrivacy cu implicații asupra reținerii datelor – Autoritatea națională de supraveghere a transmis o serie de mențiuni referitoare la aspecte care țin de stocarea și stergerea datelor cu caracter personal;
- acordurile de securitate socială aflate în negociere între România și state terțe – au fost înaintate o serie de propuneri de reformulare care au vizat:

- i) menționarea dreptului la informare cu trimiterea expresă la prevederile art. 13 și 14 din Regulamentul (UE) 2016/679,
- ii) eliminarea sintagmei „dreptul de a retrage consimțământul”, având în vedere faptul că temeiul legal al prelucrării este reprezentant de Acordul de securitate socială, și nu de consimțământul persoanei vizate,
- iii) completarea dispoziției privind dreptul de a depune o plângere în fața unei autorități de supraveghere, prin menționarea expresă a autorității pentru protecția datelor din România,
- iv) eliminarea sintagmelor „dreptul la informații privind scopul secundar de prelucrare dacă este diferit de cel inițial de colectare” și „dreptul la informații cu privire la garanțiile adecvate referitoare la transfer, în cazul în care datele cu caracter personal sunt transferate

către celălalt stat contractant", întrucât acestea sunt subsumate dreptului la informare, potrivit art. 13 și art. 14 din Regulamentul (UE) 2016/679;

- videoconferință referitoare la evaluarea legislației naționale de implementare a Regulamentului (UE) 2016/679 și a Directivei de aplicare a legii – reprezentanții Autorității naționale de supraveghere, împreună cu cei ai Ministerului Afacerilor Interne, ai Ministerului de Justiție și ai Ministerului Afacerilor Externe au participat la videoconferința organizată cu reprezentanții Comisiei Europene. Subiectele dezbătute în cadrul videoconferinței au vizat, în principal, independența Autorității naționale de supraveghere, spre ex. procedura de numire a președintelui și a vicepreședintelui Autorității naționale de supraveghere, procedura pentru reînnoirea mandatului de președinte sau vicepreședinte al Autorităţii naţionale de supraveghere, atribuțiile președintelui Autorității naționale de supraveghere, procedura pentru stabilirea bugetului Autorității naționale de supraveghere, sancțiunile aplicate operatorilor, procedura de soluționare a plângerilor. În ceea ce privește Directiva de aplicare a legii, discuțiile s-au axat pe transpunerea Directivei (EU) 2016/680 în legislația națională, respectiv domeniul de aplicare, drepturile persoanelor vizate, răspundere și sancțiuni.

CAPITOLUL V

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activităţii, Autorității naționale de supraveghere i s-a alocat prin Legea nr. 50/2019 a bugetului de stat pe anul 2019 un buget în sumă de 5.820.000 lei, modificat în conformitate cu prevederile Ordonanţei Guvernului nr. 12/2019 și ale Ordonanţei de Urgență a Guvernului nr. 71/2019 cu privire la rectificarea bugetului de stat pe anul 2019. Având în vedere aceste aspecte și în urma anulărilor de credite realizate în luna decembrie 2019, conform reglementărilor Legii nr. 500/2002 privind finanţele publice, rezultă următoarea sinteză:

Denumire indicator	Cod	Buget iniţial 2019 - mii lei -	Buget actualizat la 31.12.2019 - mii lei -	Execuție bugetară la 31.12.2019 - mii lei -	Execuţie bugetară la 31.12.2019 (%)
Total cheltuieli	51.01	5.820	5.147	5.097	99,03
Titlul I Cheltuieli de personal	10	5.000	4.247	4.241	99,86
Titlul II Bunuri şi servicii	20	800	880	837	95,11
Cheltuieli de capital Titlul XIII Active nefinanciare	71	20	20	19	95,00

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.

Creditele definitive aprobate au asigurat realizarea obiectivelor propuse, ținându-se cont atât de solicitările permanente privind eficiența utilizării fondurilor publice, cât și de restricțiile privind creditele de angajament și creditele bugetare.

În ceea ce privește modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorității naționale de supraveghere a constituit un procent de 82,5% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 4.240.516 lei (prin ocuparea unor posturi temporar, prin detașare), înregistrându-se în continuare un deficit major de personal (48 posturi neocupate și 9 posturi ocupate temporar prin detașare, reprezentând 67% din numărul total de 85 de posturi – exclusiv demnitarii – prevăzute de Legea nr. 102/2005, republicată). 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 2019 au avut o pondere de 17% 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. 38% bunuri și servicii pentru întreținere și funcționare (servicii de actualizare informatică, 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.)

În anul 2019, cheltuielile cu bunuri și servicii au crescut cu 9,6% față de anul 2018.

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 2019, 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.

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 instituţia noastră.