# AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

# R A P O R T  A N U A L

## 2017

Raportul de activitate este prezentat Senatului României, în temeiul art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare.

**Bucureşti**

## CUVÂNT ÎNAINTE

***Stimate Domnule Preşedinte al Senatului,***

***Stimaţi Senatori,***

Specificitatea activității instituției noastre în anul 2017 a constat în pregătirea actelor normative naționale de natură să asigure optima aplicare 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 pe data de 27 aprilie 2016, de către Parlamentul European și Consiliul.

Efectul adoptării acestei reglementări europene constă în uniformizarea principiilor și regulilor de prelucrare a datelor personale în toate statele membre ale Uniunii Europene, în condițiile în care, începând cu data de 25 mai 2018, Regulamentul General privind Protecția Datelor dobândește aplicabilitate directă.

În acest context, reliefăm consolidarea adusă drepturilor persoanelor fizice și consacrarea unor noi drepturi, cum sunt dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării. În mod corelativ, este de remarcat importanța deosebită acordată responsabilității operatorilor în legătură cu prelucrările efectuate, care au obligația de a demonstra că respectă Regulamentul General privind Protecția Datelor.

Un aspect de noutate, pe care doresc să-l supun atenţiei dumneavoastră, constă în instituirea obligației instituţiilor publice şi, în anumite situații, a entităţilor private, de a-şi desemna o persoană responsabilă cu protecţia datelor, în funcţie de anumite criterii stabilite expres prin dispozițiile art. 37 din Regulament. Apreciem că aceasta va avea un impact pozitiv în activitatea operatorilor din România și, implicit, efecte benefice în privința respectării drepturilor persoanelor fizice.

Având în vedere că Regulamentul General privind Protecția Datelor conține unele dispoziții care oferă posibilitatea statelor membre de a interveni cu anumite reglementări naționale, s-au realizat în cursul anului 2017, consultări cu ministerele responsabile pentru analizarea și pregătirea cadrului național legislativ adecvat.

Astfel, instituția noastră a pregătit proiectul de lege de modificare și completare a Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Acest proiect este necesar pentru asigurarea concordanței competențelor și sarcinilor de monitorizare și control ale instituției noastre cu prevederile art. 55-59 din Regulamentul General privind Protecția Datelor.

De asemenea, a fost supus consultărilor interministeriale și un proiect de act normativ destinat stabilirii măsurilor necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 9 alin. (4), art. 37-39, art. 42-43, art. 83 alin. (7), art. 85, art. 87-89 din Regulamentul General privind Protecția Datelor.

În același timp, instituția noastră s-a implicat și în consultările interministeriale referitoare la pregătirea reglementării naționale de transpunere a Directivei 680/2016/EC privind protecţia persoanelor fizice faţă de prelucrările efectuate de către autorităţile competente în scopul prevenirii, cercetării, constatării sau urmăririi penale a infracţiunilor ori executării pedepselor penale şi libera circulaţie a acestor date.

Totodată, în anul 2017, s-a continuat activitatea intensă de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat, alături de acțiunile numeroase de informare a acestora și a publicului larg cu privire la noile condiții aplicabile domeniului protecției datelor cu caracter personal. S-a remarcat creșterea semnificativă a numărului de plângeri și sesizări față de anul anterior, în principal referitoare la prelucrarea datelor personale de către birourile de credit, din cadrul sistemelor ce utilizează mijloace de supraveghere video și din sectorul comunicațiilor electronice.

În considerarea acestor aspecte, apreciem că, în anul 2018, acţiunile Autorităţii vor urmări în mod special:

- finalizarea adoptării cadrului normativ național în concordanță cu noile reglementări ale Uniunii Europene, prin implicare alături de instituțiile responsabile;
- asigurarea conștientizării publice cu privire la noile reguli de prelucrare a datelor personale;
- consolidarea capacității administrative interne prin luarea măsurilor necesare destinate aplicării noilor acte normative europene și naționale;
- monitorizarea aplicării Regulamentului General privind Protecția Datelor și a celorlalte reglementări aplicabile în domeniu.

Permiteți-mi să mulțumesc pentru sprijinul pe care l-ați acordat până în prezent instituției noastre și să-mi exprim, în același timp, speranța că vom beneficia de încrederea dumneavoastră pentru asigurarea unei efective respectări a dreptului fundamental la viață privată și la protecția datelor cu caracter personal.

***Ancuţa Gianina OPRE,***

***Preşedinte***

# CUPRINS

## CAPITOLUL IV
## ACTIVITATEA DE CONTROL



## CAPITOLUL V


## CAPITOLUL VI

## ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL



## CAPITOLUL VII

# CAPITOLUL I
# PREZENTARE GENERALĂ

Raportul de activitate pe anul 2017 al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe şapte capitole, după cum urmează:

**Capitolul I** asigură o prezentare sintetică a raportului pe principalele aspecte.

În cuprinsul **Capitolului al II-lea** sunt prezentate aspecte relevante referitoare la pachetul legislativ de reformă în domeniul protecţiei datelor cu caracter personal, adoptat pe data de 27 aprilie 2016 la nivelul Uniunii Europene, în special cu privire la aplicabilitatea Regulamentului General privind Protecția Datelor în toate statele membre începând cu data de 25 mai 2018.

**Capitolul al III-lea** cuprinde informații relevante referitoare la activitatea de avizare a proiectelor de acte normative şi la aceea de consultare referitoare la aplicarea regulilor de protecţie a datelor personale, inclusiv de clarificare a unor chestiuni semnalate de diverşi operatori. Aceasta s-a concretizat în emiterea avizelor asupra unui număr mare de proiecte de acte normative şi a unui număr semnificativ de puncte de vedere.

În contextul intrării în vigoare a Regulamentului General privind Protecția Datelor din 25 mai 2018, atât persoanele fizice cât şi operatorii de date și-au exprimat interesul pentru noile reglementări aduse în materia protecției datelor de acest act normativ și au solicitat, în special, informaţii cu privire la aplicabilitatea Regulamentului.

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

Secţiunea privind informarea publică expune principalele modalităţi de popularizare a Regulamentului General privind Protecția Datelor, utilizate în cursul anului 2017, în limitele resurselor bugetare alocate.

**Capitolul al IV-lea** constă într-o prezentare a activităţii de control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite.

Această activitate constă în verificarea modului de aplicare a dispoziţiilor legale în materie.

Investigaţiile efectuate din oficiu au vizat verificarea modului de respectare a prevederilor Legii nr. 677/2001, modificată și completată, precum şi a dispoziţiilor Legii nr. 506/2004, modificată și completată, în cadrul prelucrării datelor cu caracter personal atât în sistemul public, cât și în cel privat.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri exponențiale a numărului acestora, în anul 2017 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, cu precădere, cele care vizează prelucrarea datelor personale de către birourile de credit, dar și cele din cadrul sistemelor ce utilizează mijloace de supraveghere video sau din sectorul comunicațiilor electronice.

În cadrul investigaţiilor efectuate în anul 2017, au fost aplicate sancţiuni contravenţionale constând în avertismente şi amenzi în cuantum total de 870.500 lei.

**Capitolul al V-lea** prezintă activitatea de relaţii externe a Autorităţii naţionale de supraveghere.

**Capitolul al VI-lea** privind activitatea de supraveghere a prelucrărilor de date cu caracter personal cuprinde principalele concluziile rezultate din analizarea formularelor transmise de operatorii de date, persoane fizice şi juridice, care au avut obligaţia depunerii acestora. Au fost înregistrate un număr total de 6115 notificări privind prelucrări de date realizate atât pe teritoriul României, cât şi în statele membre, ori transferuri în state terţe.

**Capitolul al VII-lea** referitor la resursele materiale şi financiare conţine informaţii privind creditele bugetare puse la dispoziţia Autorităţii naţionale de supraveghere şi sumele cheltuite pe fiecare articol al clasificaţiei bugetare.

## CAPITOLUL II

## NOI ACTE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

**Secţiunea 1 - Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE *(Regulamentul General privind Protecția Datelor)***

Pachetul legislativ adoptat pe data de 27 aprilie 2016 cuprinde două acte normative:

- Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

Adoptarea Regulamentului General privind Protecția Datelor constituie un moment crucial în domeniul protecției datelor personale, cu efecte directe asupra activității operatorilor, în condițiile în care se realizează o consolidare a drepturilor specifice ale persoanelor fizice.

În primul rând, subliniem consacrarea expresă a „dreptului de a fi uitat”, iar pe de altă parte stabilirea dreptului la portabilitatea datelor și a dreptului la restricționarea prelucrării, de natură să ofere persoanelor fizice un control efectiv asupra datelor lor personale.

Alt element de noutate din Regulament constă în obligativitatea instituţiilor publice şi entităţilor private de a-şi desemna un responsabil cu protecţia datelor la nivel intern, în funcţie de anumite criterii, ceea ce va conduce la o schimbare semnificativă în activitatea operatorilor din România.

În același timp, s-a realizat o reglementare mai detaliată a obligaţiilor operatorilor, un accent deosebit fiind pus pe creşterea gradului de responsabilizare a acestora. Consacrarea expresă a principiilor de prelucrare *privacy by design* și *privacy by default* reprezintă un alt element de noutate al acestei reglementări, implicând asigurarea protecției datelor din momentul inițial al stabilirii mijloacelor de prelucrare.

Subliniem că Regulamentul stabilește și un mecanism nou de cooperare între autoritățile naționale de supraveghere care va implica un organism european cu personalitate juridică – Comitetul European pentru Protecția Datelor (European Data Protection Board - EDPB). Acesta va răspunde de medierea pozițiilor între autoritățile naționale de supraveghere, precum și de elaborarea unor ghiduri și recomandări destinate unei aplicări unitare a acestei noi reglementări în spațiul Uniunii Europene.

Mai mult, se prevede o extindere a competențelor și sarcinilor autorităților naționale de supraveghere și, pe cale de consecință, rezultă necesitatea anumitor modificări legislative naționale prin care să se consolideze capacitatea instituţională şi administrativă a Autorităţii naționale de supraveghere, inclusiv prin alocarea și asigurarea unor resurse umane, materiale și financiare corespunzătoare.

Prevederile Regulamentului general privind protecția datelor vor fi aplicabile începând cu data de 25 mai 2018.

**Secțiunea 2 - Directivei (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului**

Această reglementare distinctă urmează a fi transpusă în plan național prin lege, astfel încât să se asigure o previzibilitate necesară a normelo raportat la specificitatea prelucrărilor de date cu caracter personal efectuate scopul prevenirii, detectării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor.

# CAPITOLUL III

# ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

## Secţiunea 1 Elaborarea proiectelor actelor normative de aplicare a RGDP

În considerarea faptului că Regulamentul General privind Protecția Datelor conține unele dispoziții care oferă posibilitatea statelor membre de a interveni cu anumite reglementări naționale, în cursul anului 2017, au avut loc mai multe consultări cu ministerele responsabile pentru analizarea și pregătirea cadrului național legislativ adecvat.

Instituția noastră a pregătit proiectul de lege de modificare și completare a Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Acest proiect este destinat asigurării concordanței competențelor și sarcinilor de monitorizare și control ale instituției noastre cu prevederile art. 55-59 din Regulamentul General privind Protecția Datelor.

Tot în cursul anului 2017 a fost elaborat și supus consultărilor interministeriale și un proiect de act normativ destinat stabilirii măsurilor necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 9 alin. (4), art. 37-39, art. 42-43, art. 83 alin. (7), art. 85, art. 87-89 din Regulamentul General privind Protecția Datelor.

De asemenea, instituția noastră a luat parte activă și în consultările interministeriale referitoare la pregătirea reglementării naționale de transpunere a Directivei 680/2016/EC privind protecţia persoanelor fizice faţă de prelucrările efectuate de către autorităţile competente în scopul prevenirii, cercetării, constatării sau urmăririi penale a infracţiunilor ori executării pedepselor penale şi libera circulaţie a acestor date.

## Secţiunea 2 Avizarea actelor normative

Autoritatea naţională de supraveghere a emis, în temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, avize asupra unui număr de 31 de proiecte de acte normative elaborate de instituţii şi autorităţi publice, care implicau aspecte complexe privind prelucrarea datelor cu caracter personal.

În condițiile diversității situațiilor reglementate prin actele normative transmise în vederea avizării, în cele mai multe cazuri s-a apreciat că este necesară completarea textelor respective, s-au efectuat observații și propuneri, prin raportare la necesitatea respectării principiilor și condițiilor de prelucrare a datelor cu caracter personal.

Asupra majorității proiectelor de acte normative analizate s-au efectuat recomandări pentru reanalizarea acestora și armonizarea lor cu dispozițiile legale privind protecția datelor, inclusiv în contextul aplicării Regulamentului general privind protecția datelor începând cu data de 25 mai 2018.

În continuare prezentăm, pentru exemplificare, unele dintre cele mai relevante proiecte de acte normative avizate:

- **Consiliul Național pentru Combaterea Discriminării a transmis spre avizare *proiectul de "Hotărâre a Guvernului privind aprobarea Strategiei naționale "Egalitate, incluziune, diversitate" pentru perioada 2016-2020 și a Planului operațional privind implementarea Strategiei naționale "Egalitate, incluziune, diversitate" 2016 - 2020"***

Autoritatea națională de supraveghere a formulat următoarele observații și propuneri, în scopul asigurării respectării cerinţelor legislaţiei din domeniul protecţiei datelor cu caracter personal, cu privire la prelucrarea de date cu caracter personal ale persoanelor considerate discriminate pe anumite criterii (gen, vârstă, sex, etnie, stare de sănătate etc.), cu precădere a unor categorii speciale de date (de ex. referitoare la originea rasială sau etnică, date privind starea de sănătate sau viaţa sexuală), și, în mod particular, cu privire la confidențialitatea și securitatea datelor.

Cu privire la conținutul Cap. IV – Obiective specifice, raportat la atribuțiile Autorității naționale de supraveghere, 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 (de ex. Ministerul Educației, Institutul Național de Statistică, unități de învățământ) și la cea potrivit căreia Autoritatea națională de supraveghere poate formula recomandări şi avize asupra oricărei chestiuni legate de protecţia datelor, s-a apreciat ca fiind necesară modificarea unor prevederi referitoare la elaborarea de către CNCD, în parteneriat cu Ministerul Educației și Institutul Național de Statistică, cu avizul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, a unor instrumente (...).

Referitor la colectarea de date cu privire la discriminare și egalitate (genul, etnia, religia, dizabilitatea, situația familială etc.) în instituții de învățământ superior, s-a subliniat faptul că datele cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenenţa sindicală, precum şi datele cu caracter personal privind starea de sănătate sau viaţa sexuală, sunt date cu caracter special, protejate de reguli speciale instituite de Legea nr. 677/2001, iar condiţiile de prelucrare ale acestora sunt prevăzute în art. 7 şi art. 9 din această lege.

Regula instituită de art. 7 alin. (1) din Legea nr. 677/2001 este aceea că astfel de informaţii sunt interzise de la prelucrare. Însă, prelucrarea acestor date este permisă în anumite cazuri de excepţie, expres prevăzute în alin. (2) al art. 7 din Legea nr. 677/2001.

În consecință, prelucrarea datelor sus menționate, inclusiv colectarea acestora, realizată pe scară largă, poate reprezenta o nouă situaţie de risc pentru protecţia datelor cu caracter personal ale persoanelor fizice şi, implicit, pentru respectarea şi garantarea drepturilor fundamentale ale acestora, în special cel la viaţă privată și, ca atare, la prelucrarea acestor date este necesară luarea în considerare a tuturor principiilor de prelucrare a datelor, instituite de art. 4 alin. (1) din Legea nr. 677/2001.

În același timp s-a subliniat că, la alegerea modalităţilor de transmitere a datelor sau a documentelor ce conţin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii au obligaţia de a aplica măsuri tehnice şi 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 reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală, având în vedere prevederile art. 20 din Legea nr. 677/2001.

În contextul Strategiei naționale ”Egalitate, incluziune, diversitate” 2016 - 2020, Autoritatea națională de supraveghere a apreciat că este necesară o evaluare a cadrului juridic și, implicit, a actelor normative referitoare la egalitatea de șanse, incluziune și diversitate, astfel încât acesta să prevadă sau să întărească normele referitoare la protecţia drepturilor şi libertăţilor persoanelor în ceea ce privește prelucrările de date cu caracter personal.

Cu acest prilej, s-a menționat că a intrat în vigoare Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), aplicabil în mod direct în toate statele membre ale Uniunii Europene.

S-a subliniat, totodată, că, potrivit principiului responsabilității din Regulamentul (UE) 2016/679, operatorii de date cu caracter personal (precum cei menționați în Strategie) 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.

Autoritatea națională de supraveghere **a avizat cu observații** proiectul de ”Hotărâre a Guvernului privind aprobarea Strategiei naționale ”Egalitate, incluziune, diversitate” pentru perioada 2016-2020 și a Planului operațional privind implementarea Strategiei naționale ”Egalitate, incluziune, diversitate” 2016 - 2020”.

- **Autoritatea Națională de Reglementare în Domeniul Energiei a solicitat punctul de vedere cu privire la *proiectul de ”Ordin privind implementarea la nivel național a sistemelor de măsurare inteligentă a energiei electrice și stabilirea calendarului de implementare”***

Autoritatea națională de supraveghere a formulat observaţii și propuneri, astfel:

Din analiza textului proiectului a reieșit faptul că, în cadrul activităţilor ce urmează a fi desfăşurate de către operatorii de distribuție a energiei electrice concesionari și furnizorii de energie electrică, în contextul dezvoltării platformei Metering Data Management System în cadrul *Sistemului de măsurare inteligentă a energiei electrice* (SMI), ar urma să fie prelucrate şi

date cu caracter personal ale consumatorilor persoane fizice, în calitatea acestora de beneficiari ai sistemelor de măsurare inteligentă.

În acest context, s-a atras atenția asupra faptului că în proiect nu sunt specificate datele cu caracter personal ce vor fi prelucrate în SMI, fapt pentru care s-a recomandat introducerea unui alineat nou la articolul 11 din proiect, care să clarifice acest aspect.

Totodată, s-a precizat că pentru prelucrarea datelor cu caracter personal din SMI este necesară luarea în consideraţie a principiilor de protecţie a datelor, instituite de art. 4 alin. (1) din Legea nr. 677/2001, în special prin stabilirea garanţiilor adecvate pentru respectarea drepturilor persoanelor vizate şi stabilirea persoanelor autorizate care vor avea acces la date, în scopuri legitime.

Întrucât prelucrările de date cu caracter personal pot fi expuse unor serii de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor, s-a recomandat ca, la alegerea modalităţilor de transmitere a datelor sau a documentelor ce conţin date cu caracter personal, să se aibă în vedere faptul că operatorii au obligaţia de a aplica măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special în contextul în care prelucrarea de date în SMI comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Sub aspectul celor de mai sus, s-a atras atenția asupra faptului că a fost emis, de către Grupul de lucru Art. 29, *Avizul nr. 12/2011 privind contorizarea inteligentă*, care precizează că serviciile și tehnologiile care se bazează pe prelucrarea datelor cu caracter personal ar trebui proiectate din start astfel încât să respecte viața privată. În acest sens, punerea în aplicare a contorizării inteligente ar trebui să respecte din start viața privată, nu doar în ceea ce privește măsurile de securitate, ci și prin reducerea la minimum a cantității de date cu caracter personal prelucrate.

Mai mult, s-a subliniat că operatorilor de distribuție a energiei electrice concesionari și furnizorilor de energie electrică, în calitate de operatori de date cu caracter personal, le revine obligația de respectare a dreptului la informare al persoanelor vizate, prevăzut de art. 12, de respectare a drepturilor persoanelor fizice ale căror date le prelucrează, prevăzute de art. 13 - 18, precum și obligațiile de asigurare a confidenţialităţii şi securităţii prelucrării datelor, așa cum sunt prevăzute de Legea nr. 677/2001.

În sensul celor de mai sus, cu privire la informarea și drepturile persoanelor vizate, s-a recomandat introducerea unui alineat nou la art. 11 din proiect.

Având în vedere aspectele de mai sus, **Autoritatea națională de supraveghere a apreciat că proiectul de ordin necesită reanalizare.**

- **Ministerul Muncii și Justiției Sociale a transmis în vederea formulării unui punct de vedere *proiectul de "Hotărâre pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 76/2002 privind sistemul asigurărilor pentru şomaj şi stimularea ocupării forţei de muncă, aprobate prin Hotărârea Guvernului nr. 174/2002, şi pentru modificarea şi completarea Procedurilor privind accesul la măsurile pentru stimularea ocupării forţei de muncă, modalităţile de finanţare şi instrucţiunile de implementare a acestora, aprobate prin Hotărârea Guvernului nr. 377/2002"***

Autoritatea națională de supraveghere a formulat observaţii și propuneri:

În contextul reglementării sistemului asigurărilor pentru şomaj şi stimulării ocupării forţei de muncă, entități precum Agenţia Naţională pentru Ocuparea Forţei de Muncă și agenţiile pentru ocuparea forţei de muncă judeţeane sau, după caz, a municipiului Bucureşti, desfășoară activități ce presupun efectuarea de operaţiuni de prelucrare de date.

Raportat la conținutul proiectului de act normativ supus analizei, Autoritatea națională de supraveghere a subliniat necesitatea stabilirii de garanţii adecvate pentru respectarea drepturilor persoanelor vizate în ceea ce privește prelucrarea de date cu caracter personal, așa cum se regăsesc acestea în art. 12 – 18 din Legea nr. 677/2001 (dreptul la informare, dreptul de acces la date, dreptul de intervenţie asupra datelor, dreptul de opoziţie, dreptul de a nu fi supus unei decizii individuale, dreptul de a se adresa justiţiei).

Cât privește comunicarea de informații și date între diversele entităţi la care face referire *proiectul de Hotărâre* (de ex. art. I pct. 6 privind introducerea art. $46^3$ alin. (5) ce reglementează faptul că informaţiile privind veniturile nete realizate "se pun la dispoziţia Agenţiei Naţionale pentru Ocuparea Forţei de Muncă, de către Casa Naţională de Pensii Publice, Agenţia Naţională pentru Plăţi şi Inspecţie Socială şi Agenţia Naţională de Administrare Fiscală"

ori art. I pct. 6 privind introducerea art. $46^4$ alin. (5)), s-a subliniat că o comunicare de acest tip se poate expune la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor.

S-a mai precizat că la aceleași riscuri ca cele anterior menționate se expune și comunicarea prin poștă, fax ori e-mail (de ex. art. I pct. 6 privind introducerea art. $46^4$ alin. (2) din proiect), a documentelor conținând date cu caracter personal între solicitanții primei de instalare sau de relocare și agenţiile pentru ocuparea forţei de muncă judeţeane sau, după caz, a municipiului Bucureşti.

În legătură cu transmiterea datelor sau a documentelor (de ex. copii certificate ale actelor de identitate, adeverințe, declarații, formulare etc.) ce conţin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii de date cu caracter personal au obligaţia de a aplica măsuri tehnice şi 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 reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispoziţiile art. 17 alin. (1) din Directiva 95/46/CE a Parlamentului European şi prevederile art. 20 din Legea nr. 677/2001.

În consecință, s-a recomandat ca, în cuprinsul proiectului de Hotărâre, să se includă un articol distinct, eventual în care să facă referire la faptul că prelucrarea datelor cu caracter personal se va realiza în conformitate cu reglementările legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

Autoritatea națională de supraveghere a apreciat că ***proiectul de Hotărâre*** **necesită reanalizare**, sub aspectul observațiilor și propunerilor menționate anterior.

Ulterior, Ministerul Muncii și Justiției Sociale a retransmis Autorităţii naţionale de supraveghere proiectul *de Hotărâre pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 76/2002 privind sistemul asigurărilor pentru şomaj şi stimularea ocupării forţei de muncă, aprobate prin Hotărârea Guvernului nr. 174/2002, şi pentru modificarea şi completarea Procedurilor privind accesul la măsurile pentru stimularea ocupării forţei de muncă, modalităţile de finanţare şi instrucţiunile de implementare a acestora, aprobate prin Hotărârea Guvernului nr. 377/2002*, în vederea avizării.

Întrucât textul proiectului a fost modificat, Autoritatea națională de supraveghere **a avizat favorabil proiectul.**

- **Ministerul Afacerilor Interne a solicitat propuneri și observații cu privire la *proiectul de "Lege pentru modificarea și completarea unor acte normative în domeniul ordinii și siguranței publice"***

Autoritatea națională de supraveghere a prezentat următoarele observații:

În ceea ce privește art. II punctul 7 din proiect, referitor la noile prevederi legale introduse la art. 31 alin. (1) lit. q) s-a subliniat că, în contextul utilizării sintagmei *"organe ale administrației de stat"*, este necesară reanalizarea textului, în sensul clarificării sintagmei prin restrângerea sferei și stabilirea clară a autorităților ale căror baze electronice de date ar putea fi accesate de polițistul învestit cu exerciţiul autorităţii publice, în realizarea atribuţiilor ce îi revin, potrivit legii, cu respectarea principiului proporționalității, prevăzut de art. 4 din Legea nr. 677/2001 și art. 5 din Legea nr. 238/2009, republicată.

S-a atras atenția asupra necesității reformulării textului anterior menționat în contextul în care dispozițiile Constituției României delimitează clar structura administrației publice din România, în administrație publică centrală de specialitate și administraţie publică locală.

În contextul celor de mai sus, a fost evidențiat considerentul (30) din Decizia nr. 440/2014 referitoare la excepţia de neconstituţionalitate a dispoziţiilor Legii nr. 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice şi ale art. 152 din Codul de procedură penală, care precizează: *"S-a mai reţinut că protecția datelor cu caracter personal, care rezultă din obligația explicită prevăzută la art. 8 alin. (1) din Cartă, prezintă o importanță deosebită pentru dreptul la respectarea vieții private, consacrat la art. 7 din aceeaşi Cartă (par. 51), motiv pentru care directiva în cauză ar trebui să cuprindă norme clare și precise cu privire la conținutul și aplicarea măsurii reținerii datelor și să prevadă o serie de limitări, aşa încât persoanele ale căror date au fost păstrate să beneficieze de garanții suficiente care să asigure o protecție eficientă împotriva abuzurilor și a oricărui acces sau utilizări ilicite (par. 54)."*

De asemenea, cu privire la accesarea sistemelor de supraveghere a spațiului public, Autoritatea națională de supraveghere a solicitat reanalizarea necesității acestor prevederi, raportat la respectarea principiului proporționalității prelucrării datelor și implicațiile accesului nediscriminatoriu și în integralitate la aceste sisteme de evidență.

În sensul celor anterioare, a fost supus atenției inițiatorului considerentul (57) din Decizia nr. 440/2014 care precizează: *"(...) legea nu prevede criterii obiective care să limiteze la strictul necesar numărul de persoane care au acces și pot utiliza ulterior datele păstrate, că accesul autorităților naționale la datele stocate nu este condiționat, în toate cazurile, de controlul prealabil efectuat de către o instanță sau de o entitate administrativă independentă, care să limiteze acest acces şi utilizarea lor la ceea ce este strict necesar pentru realizarea obiectivului urmărit. Garanţiile legale privind utilizarea în concret a datelor reţinute nu sunt suficiente şi adecvate pentru a îndepărta teama că drepturile personale, de natură intimă, sunt violate, aşa încât manifestarea acestora să aibă loc într-o manieră acceptabilă."*

Cu privire la reglementarea accesului polițiștilor la bazele electronice de date ale "organelor administrației de stat și la sistemele de supraveghere", în baza "unor documente de cooperare încheiate între deținătorii acestora și unitățile competente ale Poliției Române, care vor cuprinde cel puțin măsurile specifice de protecție a datelor cu caracter personal", s-a recomandat reanalizarea acestei prevederi în considerarea hotărârii date de Curtea de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții (C-201/14).

Prin hotărârea pronunțată, instanța Uniunii Europene a constatat că informațiile transmise între autorități publice, precum și modalitățile de efectuare a transmiterii acestora, au fost stabilite nu prin intermediul unei măsuri legislative, ci prin intermediul unui protocol, care nu a făcut obiectul unei publicări oficiale.

În ceea ce privește art. III punctul 3 din proiect, referitor la prevederile art. $27^2$ alin. (3), s-a subliniat necesitatea precizării bazelor electronice de date în care polițistul de frontieră are acces în vederea verificării identității unei persoane și cărei/căror entități aparțin aceste baze.

Autoritatea națională de supraveghere a recomandat **reanalizarea conținutului *proiectului de Lege pentru modificarea și completarea unor acte normative în domeniul ordinii și siguranței publice*** și prin raportare la prevederile aplicabile domeniului penal ale Directivei (UE) 2016/680 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera

circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului Uniunii Europene.

- **Ministerul Muncii și Justiției Sociale a transmis, în vederea avizării, *proiectul de "Hotărâre privind aprobarea Regulamentului de organizare și funcționare a Inspecției Muncii"***

Faţă de conţinutul acestui proiect, Autoritatea națională de supraveghere a prezentat următoarele observații:

Referitor la prevederile generale ale art. 12 alin. (1) punctul B, litera i) din Capitolul III, privind efectuarea schimbului de date extrase din registrul general de evidență a salariaților, "pe baza protocoalelor încheiate la nivel național cu alte instituții ale statului", s-a recomandat reanalizarea acestuia, în considerarea hotărârii date de Curtea de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții (C-201/14), precum și pentru asigurarea exigențelor de previzibilitate a actelor normative.

Astfel, prin hotărârea pronunțată, CJUE a constatat că informațiile transmise între autorități publice, precum și modalitățile de efectuare a transmiterii acestora au fost stabilite nu prin intermediul unei măsuri legislative, ci prin intermediul unui protocol, care nu a făcut obiectul unei publicări oficiale.

Curtea de Justiție a Uniunii Europene, prin aceeași hotărâre, a statuat faptul că articolele 10, 11 și 13 din Directiva 95/46/CE trebuie interpretate în sensul că se opun unor măsuri naționale, care permit unei autorități a administrației publice a unui stat membru transmiterea de date personale unei alte autorități a administrației publice și prelucrarea ulterioară a datelor, fără ca persoanele vizate să fi fost informate despre această transmitere sau despre această prelucrare.

Așadar, cerința prelucrării corecte a datelor personale prevăzută la art. 12 din Legea nr. 677/2001 (ce implementează art. 6 din Directiva 95/46/CE) obligă o autoritate a administrației publice să informeze persoanele vizate despre transmiterea acestor date unei alte autorități a administrației publice în vederea prelucrării de către aceasta din urmă în calitate de destinatar al datelor menționate.

Autoritatea națională de supraveghere a subliniat faptul că dreptul garantat de art. 12 din Legea nr. 677/2001 trebuie respectat de către toți operatorii de date cu caracter personal,

indiferent de condițiile de legitimitate a prelucrării datelor persoanelor vizate, respectiv în baza consimţământului expres şi liber exprimat al acestora sau în baza unor excepții.

S-a recomandat introducerea unui nou articol, distinct, în cuprinsul Regulamentului, referitor la faptul că prelucrarea tuturor datelor cu caracter personal se va realiza de către Inspecția Muncii în conformitate cu prevederile aplicabile în domeniul protecției datelor.

Corelat cu acest aspect, s-a menționat că nu este suficientă prevederea introdusă la Capitolul III, art. 12 alin. (1) punctul B, litera h) din proiect întrucât, raportat la atribuțiile Inspecției Muncii, aceasta efectuează și alte prelucrări de date cu caracter personal, nu doar cele referitoare la gestionarea bazei de date organizate la nivel național ce conține registrele generale de evidență a salariaților.

Astfel, în contextul celor anterioare, cu titlu de exemplu, s-a menționat că, potrivit lit. e) din același art. 12 alin. (1) pct. B din proiect, Inspecția Muncii *"realizează fotografii și înregistrări audio-video"* care pot conține și date cu caracter personal (imagine și voce) ale angajaților sau reprezentanților legali ai entităților controlate.

Autoritatea națională de supraveghere **a avizat cu observațiile** sus menționate *proiectul de Hotărâre privind aprobarea Regulamentului de organizare și funcționare a Inspecției Muncii.*

Ulterior, **Ministerul Muncii și Justiției Sociale a retransmis proiectul de act normativ modificat conform recomandărilor Autorității naționale de supraveghere, acesta fiind avizat favorabil.**

- **Ministerul pentru Relaţia cu Parlamentul a solicitat punctul de vedere cu privire la *propunerea legislativă privind "Codul Administrativ al României"* (BP. 649/2017)**

Faţă de textul propunerii legislative, Autoritatea naţională de supraveghere a formulat următoarele observaţii:

În argumentele cuprinse la punctul E din Expunerea de motive a propunerii legislative nu se regăsește o mențiune cu privire la calitatea de operator a Agenției Naționale a Funcționarilor Publici, în privința Sistemului electronic naţional de evidenţă a ocupării în sectorul public, în

concordanță cu atribuțiile acestei instituții, ținând cont de definiția dată de art. 3 lit. e) din Legea nr. 677/2001.

Faţă de modul de redactare a dispoziţiilor art. 421 alin. (2) din acest proiect, s-a apreciat ca fiind necesară reformularea acestuia, în sensul utilizării sintagmei ”datele necesare colectate”, prin raportare la principiul proporționalității datelor instituit de art. 4 alin. (1) din Legea nr. 677/2001.

Totodată, faţă de forma actuală a dispoziţiilor art. 421 alin. (2) și (5) din propunerea legislativă transmisă, s-a solicitat reanalizarea prevederilor referitoare la încheierea unui protocol de colaborare între Agenţia Naţională a Funcţionarilor Publici și Inspecţia Muncii, având în vedere că din textul proiectului nu reiese că protocolul ar urma să fie publicat în Monitorul Oficial al României sau că ar urma să fie adus la cunostința publicului larg, astfel încât să fie respectate exigențele Curții de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții.

Prin urmare, raportat la exigenţele informării persoanelor vizate cu privire la schimbul de informaţii, ţinând cont de cele stabilite prin Hotărârea Curții de Justiţie a Uniunii Europene sus menționată, propunem ca modalitatea de colaborare să se stabilească prin ordin comun al celor două entități.

Autoritatea naţională de supraveghere a recomandat ca textul propunerii legislative **să se completeze în concordanţă cu observaţiile şi propunerile** formulate.

- **Ministerul Muncii și Justiției Sociale a solicitat un punct de vedere cu privire la *proiectul de ”Hotărâre pentru aprobarea normelor metodologice privind detașarea salariaților în cadrul prestării de servicii transnaționale pe teritoriul României”***

Față de proiectul Hotărârii de Guvern transmis, s-au formulat următoarele observații și propuneri:

În contextul reglementării cooperării administrative și a schimbului de informații cu privire la detașarea transnațională a salariaților pe teritoriul României (inclusiv date cu caracter personal ale salariaților), instituțiile naționale desemnate ca autorități competente (Inspecția Muncii, inspectorate teritoriale de muncă, Casa Națională de Pensii Publice) în calitate de operatori, desfășoară activități ce presupun efectuarea de operaţiuni de prelucrare de date, ce pot avea implicaţii directe asupra drepturilor fundamentale ale persoanelor fizice şi pot conduce

la grave atingeri aduse dreptului la viaţă privată al cetăţenilor, în ceea ce priveşte protecţia datelor lor cu caracter personal.

Autoritatea națională de supraveghere recomandă introducerea unui nou articol, distinct, în cuprinsul proiectului de Hotărâre, referitor la faptul că prelucrarea datelor cu caracter personal de către instituțiile naționale desemnate ca autorități competente se va realiza în conformitate cu reglementările legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

S-a subliniat că, în legătură cu transmiterea datelor sau a documentelor (de ex. declarații privind detașarea salariaților) ce conţin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii de date cu caracter personal au obligaţia de a aplica măsuri tehnice şi 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 reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispoziţiile art. 17 alin. (1) din Directiva 95/46/CE a Parlamentului European și a Consiliului şi prevederile art. 20 din Legea nr. 677/2001.

De asemenea, s-a propus introducerea în textul proiectului de Hotărâre a unui articol distinct referitor la respectarea drepturilor persoanelor vizate în ceea ce privește prelucrarea de date cu caracter personal (dreptul de informare, de acces, intervenţie, de opoziţie, de a nu fi supus unei decizii individuale) prevăzute de art. 12 – 18 din Legea nr. 677/2001.

Prin urmare, Autoritatea națională de supraveghere **propus reformularea proiectului**.

- **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul *proiectului de "Lege privind cooperarea autorităţilor publice române cu Agenţia Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL)"***

Autoritatea națională de supraveghere a formulat următoarele observații:

S-a propus înlocuirea referirilor la Legea nr. 677/2001 cu sintagma „se exercită potrivit reglementărilor aplicabile în domeniul protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date", prin raportare la Regulamentul General privind Protecţia Datelor aplicabil din 25 mai 2018 şi la Directiva (UE) 2016/680.

La art. 28 alin. (2) din proiect, s-a recomandat modificarea acestuia, în sensul înlocuirii referirii la art. 38 alin. (8) sau (9) cu art. 37 alin. (8) sau (9) din Regulamentul (UE) 2016/794 al Parlamentului European şi al Consiliului, secţiunea „Dreptul la rectificare, ştergere şi restricţionare".

În contextul menționat, s-a recomandat desemnarea unui responsabil cu protecția datelor în cadrul Unității Naționale Europol din cadrul Inspectoratului General al Poliției Române – Centrul de cooperare polițienească internațională, precum şi în cadrul celorlalte autorităţi din domeniu, raportat la dispozițiile Directivei (UE) 2016/680.

Ulterior, Ministerul Afacerilor Interne a transmis spre avizare proiectul modificat al actului normativ.

Autoritatea națională de supraveghere **a avizat favorabil** *proiectul de "Lege privind cooperarea autorităţilor publice române cu Agenţia Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL)"*.

- **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul *proiectului de Lege pentru modificarea și completarea unor acte normative care cuprind dispoziții privind evidența persoanelor și actele de identitate ale cetățenilor români***

Autoritatea națională de supraveghere a formulat următoarele observații:

În ceea ce privește modificările propuse textului O.U.G. nr. 97/2005, referitoare la propunerea de completare a art. 9 alin. (4) lit. c), s-a apreciat că argumentele prezentate în Expunerea de motive nu includ și menționarea unor garanții privind modalitatea de respectare a drepturilor persoanelor vizate (în special cel de intervenție).

Referitor la propunerea vizată de art. $12^1$, respectiv la posibilitatea eliberării opţionale a cărţii de identitate electronice sub vârsta de 14 ani, întrucât aceasta poate să conțină și datele biometrice ale titularilor (imaginea facială și, de la 12 ani, impresiunile papilare), Autoritatea națională de supraveghere și-a menținut aprecierea potrivit căreia aceste prevederi sunt de natură să afecteze dreptul la viaţă privată al minorilor lipsiţi de capacitate de exerciţiu, raportat la colectarea şi stocarea datelor biometrice ale acestora.

În acest context, raportat la toate argumentele prezentate în corespondența anterioară, Autoritatea națională de supraveghere și-a menținut rezervele cu privire la propunerea de

emitere a cărții electronice de identitate care conține datele biometrice, pentru minorii aflați sub vârsta de 14 ani.

Totodată, instituția noastră și-a menținut rezervele și în ceea ce privește argumentele referitoare la necesitatea colectării și prelucrării datelor biometrice ale minorilor cu vârsta între 0 și 14 ani și de emitere chiar și a unei cărți de identitate simple pentru minorii între 0 și 14 ani, în lipsa unui act normativ al Uniunii Europene care să oblige la luarea unei astfel de măsuri, a respectării principiului proporționalității și a dispozițiilor constituționale ale art. 49 (Protecția copiilor și a tinerilor) coroborat cu art. 26 (Dreptul la viață intimă, familială și privată).

De asemenea, referitor la propunerea de la art. $12^1$, sub aspectul sintagmei ”la solicitarea unuia dintre părinți”, Autoritatea națională de supraveghere și-a menținut observația potrivit căreia propunerea se impune a fi reanalizată și prin raportare la dispozițiile Legii nr. 272/2004 privind protecţia şi promovarea drepturilor copilului, republicată, care stabilește obligaţia ambilor părinți de a-şi exercita drepturile şi de a-şi îndeplini obligaţiile faţă de copil ţinând seama cu prioritate de interesul superior al acestuia.

La art. 13 alin (3) din proiect, s-a apreciat că sintagma ”sisteme informatice ale altor instituții publice sau private” se impune a fi completată cu mențiuni adecvate, în vederea unei identificări mai clare a acestora. În acest sens, este necesar a se avea în vedere și coroborarea dispozițiilor art. 13 alin (3) cu cele ale art. $17^1$ alin. ($1^1$) din proiect.

În ceea ce privește modificările propuse la art. 338 alin. (4) și (5) din Legea nr. 95/2006, instituția noastră și-a menținut aprecierile privind faptul că se impun a fi efectuate precizări privind modalitatea de stabilire a autentificării și în sistemul informatic al asigurărilor sociale de sănătate, în vederea instituirii unor garanții privind asigurarea dreptului la viață privată și protecția datelor cu caracter personal, cu atât mai mult cu cât autentificarea se efectuează pentru accesul la un sistem de evidență privind starea de sănătate a titularului cărții de identitate, respectiv date cu caracter sensibil ale acestuia.

Totodată, Autoritatea națională de supraveghere și-a menținut și recomandarea referitoare la propunerea de la alin. (5) al art. 338 privind necesitatea stabilirii unor dispoziții tranzitorii care să reglementeze trecerea de la cardul de sănătate la cartea electronică de identitate, cu atât mai mult cu cât aceasta din urmă se eliberează în mod eșalonat.

Autoritatea națională de supraveghere **a avizat cu observații** proiectul de act normativ supus avizării.

- **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul *proiectului de "Lege privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, investigarea şi urmărirea penală a infracţiunilor de terorism şi a infracţiunilor grave, precum și pentru prevenirea şi înlăturarea ameninţărilor la adresa securităţii naţionale***

Autoritatea națională de supraveghere a menținut următoarele observaţii şi propuneri, în contextul în care acestea fuseseră comunicate anterior.

S-au menținut aprecierile, în acord cu opinia Grupului de Lucru Articolul 29, exprimate pe parcursul întregii corespondențe anterioare cu privire la această inițiativă legislativă, raportat la colectarea şi prelucrarea datelor cu caracter personal pe scară largă și la necesitatea, legitimitatea şi proporţionalitatea acestui sistem de evidență.

Așa cum se mai precizase, măsura transmiterii de date poate reprezenta o nouă situaţie de risc pentru respectarea şi garantarea drepturilor fundamentale ale persoanelor fizice, precum și a principiilor statuate în Carta drepturilor fundamentale ale UE, în special în art. 7 privind dreptul la viaţă privată şi familială şi art. 8 privind protecţia datelor personale, precum şi în art. 8 din Convenţia pentru apărarea drepturilor şi libertăţilor fundamentale.

Raportat la dispozițiile Directivei (UE) 2016/681, Autoritatea națională de supraveghere și-a exprimat opinia în sensul că scopul proiectului de lege referitor la "prevenirea și înlăturarea amenințărilor la adresa securității naționale" nu se regăsește în sfera de reglementare a acestei Directive.

Potrivit art. 1 alin. (2) din Directiva (UE) 2016/681, *„datele PNR pot fi colectate doar în scopul prevenirii, investigării şi urmăririi penale a infracţiunilor de terorism şi a infracţiunilor grave, astfel cum este prevăzut la art. 6 alin. 2 lit. a), b) şi c)*". În aceste dispoziții nu se regăsește sintagma „înlăturarea ameninţărilor la adresa securităţii naţionale", ele referindu-se la prelucrarea datelor PNR exclusiv în vederea prevenirii activităţilor teroriste sau a unor infracţiuni grave.

De asemenea, directiva sus-menționată face vorbire despre faptul că domeniul său de aplicare este cât se poate de limitat, iar în conformitate cu principiul proporționalității, directiva nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.

Totodată, Directiva (UE) 2016/681 prevede că aplicarea acesteia ”ar trebui să asigure respectarea deplină a drepturilor fundamentale, a dreptului la viață privată și a principiului proporționalității”.

În același timp, Autoritatea națională de supraveghere și-a exprimat opinia în sensul menținerii observațiilor anterioare, referitoare la faptul că raportat la dispozițiile din proiectul de lege ce stabilesc competențele UNIP, scopul sus-menționat vine în contradicție și cu acestea, lăsând să se interpreteze că UNIP îndeplinește ambele scopuri prevăzute de art. 18 (deci inclusiv cel prevăzut de Legea nr. 51/1991), deși este organizat în cadrul IGPF și are calitatea de operator de date cu caracter personal, intrând sub incidența Legii nr. 677/2001, precum și a legii de transpunere a Directivei (UE) 2016/680.

În sensul celor de mai sus, s-a reiterat faptul că este necesară punerea în acord a scopului acestui proiect de lege cu cel stabilit de Directiva (UE) 2016/681, precum și cu dispozițiile acesteia, prin eliminarea din titlul actului normativ a sintagmei „prevenirea și înlăturarea amenințărilor la adresa securității naționale”.

Legat de argumentele de mai sus, s-a reiterat necesitatea faptului că se impune și eliminarea pct. 1 din Anexa proiectului de lege care stabileşte lista infracţiunilor, referitor la „infracţiuni contra securităţii naţionale”, punct care nu se regăseşte în Anexa II a Directivei, care cuprinde limitativ lista infracţiunilor grave.

În acest context, raportat la aspectele invocate în expunerea de motive, s-a precizat că, la considerentul 12 din Directiva (UE) 2016/681, se precizează următoarele: „Definiția infracțiunilor grave ar trebui să cuprindă categoriile de infracțiuni enumerate în anexa II la prezenta directivă.”

De asemenea, raportat la aplicabilitatea legii inclusiv la zborurile intra-UE, prevăzută la art. 1 alin. (1) lit. a), s-a subliniat faptul că aceasta este o măsură excepțională, care poate fi luată numai cu respectarea condițiilor art. 2 din Directiva (UE) 2016/681, fiind de natură să afecteze respectarea principiului proporționalității și necesității, menționate anterior, cu efecte negative asupra respectării dreptului la viață privată al cetățenilor Uniunii Europene. Totodată, această măsură se impune a fi analizată prin coordonare cu măsurile pe care le preconizează și celelalte state membre, cu prezentarea corespunzătoare a situației din aceste state.

Referitor la prevederile art. 17 din proiect, raportat la faptul că Directiva (UE) 2016/681 prevede că statele membre sunt obligate să asigure că o autoritate de supraveghere națională independentă este responsabilă de consilierea și de monitorizarea privind modul de prelucrare a

datelor PNR, instituția noastră și-a menținut observația potrivit căreia acestea se impun a fi eliminate, întrucât competențele de monitorizare ale UNIP contravin art. 15 din Directivă, reprezentând o suprapunere cu atribuțiile de investigare ale Autorității naționale de supraveghere, o ingerință gravă în competențele acesteia și, implicit, o implementare necorespunzătoare a Directivei (UE) 2016/681.

În ceea ce privește autoritățile competente stabilite la art. 11 alin. (1), astfel cum s-a menționat și în corespondența anterioară, pentru claritatea normei, previzibilitatea și predictibilitatea acesteia, s-a apreciat faptul că este necesară precizarea denumirii exacte a celor de la lit. a)-d), inclusiv cu menționarea autorității publice în cadrul căreia sunt organizate direcțiile/departamentele în cauză.

În acest context, s-a apreciat că este necesară menționarea expresă a structurii competente a Poliției Române (lit. a), raportat la art. 5 din Legea nr. 218/2002, republicată, care se referă inclusiv la instituţii de învăţământ pentru formarea şi pregătirea continuă a personalului, precum și la alte unități necesare pentru îndeplinirea atribuţiilor specifice poliţiei, înfiinţate potrivit legii.

Aceleași solicitări au fost reiterate și cu privire la Poliția de Frontieră Română (lit. b), raportat la art. 6 din Ordonanța de urgență nr. 104/2001, modificată și completată, care face vorbire și de unităţi sau instituţii de învăţământ, centre de formare profesională, centre, birouri şi puncte de contact, precum și alte unităţi.

În privința art. 42 din proiect referitor la regimul sancționator, au fost menținute observațiile anterioare cu privire la faptul că acesta vine în contradicție cu art. 41, care stabilește competențele exclusive ale Autorității naționale de supraveghere în ceea ce privește monitorizarea prelucrării datelor în sistemul PNR, dar și cu art. 15 din Directiva (UE) 2016/681 (Autoritatea națională de supraveghere) raportat la art. 4-6 (referitoare la unitatea de informații despre pasageri - UIP) din Directiva (UE) 2016/681.

S-a precizat, ca și în corespondența anterioară avută cu Ministerul Afacerilor Interne, faptul că prevederile art. 42 alin. (1) lit. a)-c) se referă la obligații pe care transportatorii aerieni (operatorii de date) trebuie să le respecte, aspecte ce intră în sfera de competență exclusivă a Autorității naționale de supraveghere. În acest sens, s-a solicitat reanalizarea și modificarea art. 42 alin. (4), în concordanță cu prevederile Directivei (UE) 2016/681, astfel încât constatarea și aplicarea sancțiunilor să revină în competența exclusivă a Autorității naționale de supraveghere.

Față de cele de mai sus, ținând cont de necesitatea respectării principiilor de previzibilitate și predictibilitate ale actelor normative, precum și pentru stabilirea garanțiilor necesare pe care statul trebuie să le asigure în exercitarea drepturilor fundamentale ale cetățenilor, raportat la textul proiectului de lege în forma prezentată, Autoritatea națională de supraveghere **a avizat cu observații și propuneri** acest proiect.

## Secţiunea a 2-a Puncte de vedere privind diverse chestiuni de protecţia datelor

În anul 2017, au fost emise **409 de puncte de vedere**, ca urmare a solicitărilor primite de la persoane fizice, persoane juridice de drept privat și de drept public, referitoare la aplicarea dispozițiilor reglementărilor naționale incidente.

### a) Cu privire la prelucrarea datelor în alt scop decât cel pentru care au fost inițial colectate

**1.** O instituție publică a solicitat punctul de vedere al Autorității naționale de supraveghere în ceea ce privește posibilitatea prelucrării datelor personale ale locatarilor dintr-un cartier rezidențial în alt scop decât cel pentru care au fost inițial colectate.

Faţă de conţinutul acesteia, s-au precizat următoarele:

Regula instituită de Legea nr. 677/2001, modificată şi completată, este aceea că prelucrarea datelor personale ale unei persoane fizice (inclusiv dezvăluirea acestora) de către o altă persoană fizică sau juridică, în calitatea sa de operator, se efectuează numai cu consimţământul persoanei în cauză, dat în mod expres şi neechivoc.

Cazurile de excepţie de la obligativitatea obţinerii consimţământului sunt reglementate expres de art. 5 alin. (2), astfel:

a) când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;

b) când prelucrarea este necesară în vederea protejării vieţii, integrităţii fizice sau sănătăţii persoanei vizate ori a unei alte persoane ameninţate;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale a operatorului;

d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele;

e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate;

f) când prelucrarea priveşte date obţinute din documente accesibile publicului, conform legii;

g) când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică, iar datele rămân anonime pe toată durata prelucrării.

Faţă de textele legale sus menţionate, raportat la conţinutul adresei transmise din care reieșea că instituția publică dorea să utilizeze numerele de telefon aparținând locatarilor din cartierul rezidențial în scopul transmiterii unor informații administrative către aceștia, Autoritatea națională de supraveghere a subliniat că această operațiune de prelucrare se poate realiza doar cu obținerea, în prealabil, a consimțământului expres și neechivoc al locatarilor, strict pentru scopul sus menționat (”transmiterea de informații administrative privind întrețineri și chirii restanțe la plată cât și a altor informații administrative ce vin în sprijinul locatarilor vizați”).

S-a mai precizat că prelucrarea datelor cu caracter personal realizată cu încălcarea dispozițiilor art. 5 din Legea nr. 677/2001 intră sub incidența dispozițiilor art. 32 din aceeași lege privind ”prelucrarea nelegală a datelor cu caracter personal”.

**2.** O instituție de învățământ a solicitat acordarea avizului pentru prelucrarea datelor cu caracter personal, efectuată prin mijloace de supraveghere video în sălile de clasă, în afara perioadei examenelor naționale.

Legat de această solicitare, așa cum în mod constant Autoritatea națională de supraveghere a subliniat că, dreptul la viață privată al elevilor, precum și cel al profesorilor și al altor persoane care lucrează în școală, dar și libertatea esențială a actului didactic (libertatea elevilor de a învăța și de a vorbi, libertatea de predare) ar trebui să fie considerate prioritare necesității de supraveghere permanentă prin camere video.

Prin urmare, ţinând cont de necesitatea asigurării unei protecţii eficiente a dreptului la viaţă privată al persoanelor supravegheate prin utilizarea mijloacelor de supraveghere video, raportat la caracterul determinat, explicit şi legitim al scopului şi la proporţionalitatea prelucrării datelor lor cu caracter personal, Autoritatea naţională de supraveghere a apreciat că extinderea supravegherii video în afara desfăşurării examenelor naţionale în sălile de clasă, spații în care își desfășoară activitatea cadrele didactice și elevii, este excesivă raportat la scopul prezentat.

**b) Cu privire la prelucrarea de date cu caracter personal având funcție de identificare de către Facebook**

O persoană fizică a cerut Autorității naționale de supraveghere informații cu privire la faptul că Facebook i-a solicitat copie după un act de identitate atunci când a încercat să își recupereze parola și contul de pe această rețea de socializare.

Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, modificată şi completată, stabileşte condiţiile în care datele cu caracter personal pot fi prelucrate.

Actul normativ sus menționat se aplică, în principal, prelucrărilor de date cu caracter personal efectuate în cadrul activităţilor desfăşurate de operatori stabiliţi în România.

Potrivit dispoziţiilor art. 5 alin. (1) al legii anterior menţionate, principiul de bază ce guvernează prelucrarea datelor personale este consimţământul persoanei vizate, dat în mod expres şi neechivoc.

În mod excepţional însă, datele cu caracter personal pot fi prelucrate de către un operator, fără consimţământul persoanei vizate, în mai multe situaţii de excepţie, de strictă interpretare şi aplicare, reglementate de art. 5 alin. (2) din Legea nr. 677/2001.

Potrivit art. 8 din Legea nr. 677/2001, prelucrarea datelor cu caracter personal având funcţie de identificare, respectiv prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală poate fi efectuată numai dacă persoana vizată şi-a dat în mod expres consimţământul sau prelucrarea este prevăzută în mod expres de o dispoziţie legală, ori, în alte cazuri, cu avizul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal şi numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.

În contextul celor de mai sus, s-a precizat că Facebook este un operator de date cu sediul în afara României (Statele Unite ale Americii, respectiv Irlanda pentru prelucrări de date efectuate în statele membre ale Uniunii Europene).

S-a mai menționat că Facebook pune la dispoziţie proceduri diverse ce pot fi parcurse de către persoanele interesate (de pildă, pentru schimbarea parolei, raportare de abuzuri etc.), însă parcurgerea acestor proceduri poate presupune furnizarea de informaţii suplimentare, cerute de Facebook tocmai pentru a putea identifica cu exactitate persoana sau problema la care se face referire.

**c) Condiții legale pentru cesionarea unei baze de date**

O societate comercială cu activitate principală de selecție și plasare personal a solicitat un punct de vedere, în contextul în care intenționa să preia de la o altă societate o bază de date cu date ale persoanelor fizice, excluzându-le pe cele cu caracter special.

Faţă de aspectele prezentate, s-au formulat următoarele precizări:

Potrivit art. 4 din Legea nr. 677/2001, modificată şi completată, datele cu caracter personal trebuie colectate în scopuri determinate, explicite şi legitime.

Deşi condiţia obţinerii consimţământului persoanei vizate este regula instituită de Legea nr. 677/2001, modificată şi completată, aceasta stabileşte în mod expres şi anumite situaţii de excepţie de la obligativitatea obţinerii consimţământului în cazul prelucrării datelor personale şi, implicit, al dezvăluirii lor prin transmitere, diseminare sau în orice alt mod. Aceste cazuri de excepţie, de strictă interpretare, sunt menţionate în mod expres la art. 5 alin. (2) din Legea nr. 677/2001 – pentru datele obişnuite – precum şi la art. 7, 8, 9 şi 10 din aceeaşi lege, pentru datele cu caracter special.

De asemenea, art. 6 alin. (1) lit. b) din Legea nr. 677/2001, modificată şi completată, stabileşte faptul că la încheierea operaţiunilor de prelucrare a datelor, dacă persoana vizată nu şi-a dat în mod expres şi neechivoc consimţământul pentru o altă destinaţie sau pentru o prelucrare ulterioară, operatorul poate transfera datele unui alt operator. Condiţia este ca operatorul iniţial (cel care transmite datele) să garanteze, prin intermediul unui act juridic (contract), faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea iniţială.

Totodată, în situaţia în care operatorul obţine în mod indirect datele personale ale unei persoane fizice, art. 12 din Legea nr. 677/2001, modificată şi completată, stabileşte obligaţia

acestuia de a furniza anumite informaţii, printre care identitatea sa, scopul colectării datelor, destinatarii acestora etc. şi, dacă este necesar, sursa obţinerii datelor. Aceste informaţii se furnizează la momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu până în momentul primei dezvăluiri.

În consecinţă, datele personale pot fi transmise unui terţ (persoana căreia i se cedează baza de date), fie la consimţământul persoanei vizate, fie în anumite situaţii de excepţie, expres stabilite de lege, de strictă interpretare.

De asemenea, operatorul iniţial care a colectat datele, cât şi cel care le obţine ulterior, sunt obligaţi să efectueze informarea persoanelor vizate, după cum datele sunt obţinute în mod direct sau indirect de la acestea, în conformitate cu Legea nr. 677/2001, modificată şi completată.

Obligaţiile de mai sus stabilite de lege în sarcina celui care transmite datele şi a celui care le primeşte vor fi stipulate şi în contractul (actul) încheiat între cele două entităţi.

În ceea ce priveşte aplicarea art. 6 alin. (1) din Legea nr. 677/2001, modificată şi completată, aceasta se realizează în momentul încheierii activităţii societăţii respective, dacă se bazează pe prelucrări de date cu caracter personal sau la finalizarea unui segment din activitate, cum ar fi vânzarea unei baze de date către o altă persoană, fără ca baza de date să mai fie utilizată de deţinătorul iniţial care va proceda la ştergerea sau distrugerea datelor, după caz.

**d) Stocarea imaginilor pentru o perioadă mai mare de 30 de zile**

O societate comercială a solicitat emiterea unui punct de vedere privind condițiile de ”stocare a datelor video pe o durată mai mare de 30 de zile”.

Autoritatea națională de supraveghere a precizat următoarele:

Potrivit art. 14 alin. (1) din Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, modificată și completată, ”Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video trebuie să fie proporţională cu scopul pentru care se prelucrează datele, *dar nu mai mare de 30 de zile*, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.”

În contextul prevederilor normative sus-menţionate, s-a precizat că stocarea datelor (imagini) obţinute prin intermediul sistemului de supraveghere video, utilizat şi notificat de operator pentru o perioadă mai mare de 30 de zile, nu se poate realiza decât dacă situația

expusă (monitorizarea zilnică a debitului afluent și a debitului de servitute/salubru aval de captare ori a debitelor asigurate în aval de priza și a prizelor hidrometrice montate la prizele MHC-urilor) este expres reglementată de lege ori operatorul justifică temeinic necesitatea unei astfel de stocări.

S-a menţionat că, potrivit dispoziţiilor art. 4 alin. (1) din Legea nr. 677/2001, modificată și completată, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, colectate în scopuri determinate, explicite şi legitime, să fie adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate, să fie exacte şi, dacă este cazul actualizate, să fie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate. Așadar, o stocare a imaginilor pe o perioadă mai mare de 30 de zile trebuie să fie proporţională cu scopul prelucrării datelor.

În contextul prelucrării menționate anterior, s-a comunicat faptul că este necesară luarea în considerare a faptului că vor fi prelucrate și date ale angajaților, așa cum reieșea din notificarea deja înregistrată în registrul de evidență a prelucrărilor de date cu caracter personal de către operator.

S-a precizat că art. 8 din Decizia nr. 52/2012 stabileşte situaţiile în care prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video este permisă, şi anume: pentru îndeplinirea unor obligaţii legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

De asemenea, în afara situaţiilor de mai sus, prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video se poate efectua pe baza consimţământului expres şi liber exprimat al acestora, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

Ca atare, Autoritatea națională de supraveghere a precizat că este necesară depunerea unei documentații care să ateste incidența unui caz temeinic justificat, raportat la situația prezentată, în măsura în care nu există o prevedere legală expresă.

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

În anul 2017 au fost transmise puncte de vedere ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în mai multe cauze pendinte în fața Curții de Justiție a Uniunii Europene, referitoare la interpretarea anumitor articole din Directiva 95/46/CE, astfel:

**- Cauza C-25/17** privind interpretarea art. 2 lit. b), c), d) și e), 3, 8, 10, 16 și 17 alin. (1) din Directiva 95/46/CE privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;

**- Cauza C - 40/17 – Fashion ID** privind interpretarea art. 2 lit. d) și h), 7 lit. a) și f), 10, 22, 23 și 24 din Directiva 95/46/CE;

**- C - 345/17 – Buivids** privind interpretarea art. 2, 3 și 9 din Directiva 95/46/CE;

**- Cauza C - 507/17 – Google** privind interpretarea art. 7 lit. e) și f), 12, 14 raportat la Hotărârea Google Spain SL, Google Inc. împotriva Agencia Española de Protección de Datos (AEPD), Mario Costeja González a Curții de Justiție, pronunțată în cauza C - 131/12 (în special, prin raportare la punctele 53-56 din aceasta);

**- Cauza C - 573/17** privind interpretarea art. 8 alin. (2) și (5), 14, în contextul Hotărârii pronunțate de Curtea de Justiție în cauza C - 131/12;

**- Cauza C - 623/17** privind impactul Hotărârii Curții de Justiție a Uniunii Europene din 21 decembrie 2016, în cauzele conexate **C-203/15 și C-698/15** (Hotărârea Watson), cu precădere prin raportare la punctele 119-125, în cazul activităților legate de securitatea națională, desfășurate de agențiile de securitate și de informații ale unui stat membru.

## Secţiunea a 3-a Aspecte relevante referitoare la aplicarea Regulamentului General privind Protecția Datelor

### a) Măsuri naționale destinate asigurării aplicării Regulamentului

O persoană fizică a solicitat informații privind măsurile de aplicare a Regulamentului (UE) 2016/679.

Autoritatea națională de supraveghere a precizat că, întrucât Ministerul Afacerilor Interne a condus negocierile în cadrul Reuniunii Comitetului pentru protecţia datelor şi schimbul de informaţii – DAPIX de la Consiliul European, cu privire la pachetul legislativ din domeniul protecției datelor personale, acesta a inițiat Memorandumul cu tema: Transpunerea în legislaţia naţională a Directivei (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016, precum şi crearea cadrului legal pentru aplicarea Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016.

Prin acest Memorandum, s-a propus constituirea Grupului Interministerial de Lucru pentru asigurarea luării măsurilor privind aplicarea directă a dispozițiilor Regulamentului (UE) 2016/679 și pentru transpunerea Directivei (UE) 2016/680, coordonat de către Ministerul Afacerilor Interne.

În contextul lucrărilor desfășurate în cadrul Grupului, Autoritatea națională de supraveghere a pregătit proiectul de Lege pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, dar și a Expunerii de motive. Acest proiect de lege vizează punerea în aplicare a unor dispoziții ale regulamentului, respectiv a prevederilor art. 51-55, 57-59, 62, 77, 79, 80 și 82-84.

Prin urmare, la data primirii solicitării, s-a comunicat că proiectul de lege sus-menționat se afla în procedurile de avizare prevăzute de Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării, adoptat prin Hotărârea Guvernului nr. 561/2009.

S-a mai precizat că, în cadrul Grupului Interministerial de Lucru, se află în analiză și un alt proiect de Lege privind unele măsuri de punere în aplicare a Regulamentului (UE) 2016/679.

**b) Responsabilul cu protecția datelor - DPO**

Mai multe persoane fizice și juridice au solicitat puncte de vedere referitoare la responsabilul cu protecția datelor.

Autoritatea națională de supraveghere a comunicat următoarele:

Referitor la responsabilul cu protecția datelor cu caracter personal menționăm că, potrivit art. 37 alin. (5) din Regulamentul UE 2016/679, acesta trebuie să fie ”desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39.”

Responsabilul cu protecția datelor poate fi angajat al operatorului/persoanei împuternicite de operator sau poate să-și îndeplinească sarcinile pe baza unui contract de prestări servicii. S-a menționat că Regulamentul nu impune o formă de organizare sub care poate funcționa responsabilul pentru protecția datelor.

Prin prisma Regulamentului, s-a apreciat că responsabilul cu protecția datelor poate îndeplini și altă funcție în cadrul operatorului sau al unei persoane împuternicite de operator și îi pot fi încredințate și alte sarcini și atribuții, cu condiția ca acestea să nu dea naștere unor conflicte de interese (de ex: nu poate fi, de pildă, director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane ori șeful departamentului IT).

De asemenea, s-a precizat că, în contextul prevederilor din Regulament referitoare la responsabilul cu protecția datelor și al dispozițiilor art. 10 și art. 11 din Legea nr. 514/2003 privind organizarea și exercitarea profesiei de consilier juridic, care stabilesc, în mod expres, atât incompatibilitățile, cât și compatibilitățile cu privire la exercitarea profesiei de consilier juridic, Uniunea Colegiilor Consilierilor Juridici din România a considerat că nu există impedimente sau restricții legale, deontologice sau procedurale pentru exercițiul simultan al profesiei de consilier juridic și al ocupației de responsabil cu protecția datelor în cadrul aceluiași operator sau distinct la operatori diferiți.

Cu toate acestea, responsabilul trebuie să aibă capacitatea de a îndeplini sarcinile, fiind necesare anumite calități personale (ex: integritate și etică profesională), cunoștințe, dar și o anumită poziție în cadrul organizației.

De asemenea, responsabilul trebuie să aibă anumite calități profesionale, precum: experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere adecvată a RGPD; nivelul necesar de cunoștințe în domeniul protecției datelor în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție necesar pentru datele cu caracter personal prelucrate; să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor prelucrate de operator; în cazul unei autorități sau instituții publice, responsabilul cu protecția datelor trebuie să dețină, de asemenea, cunoștințe privind reglementările legale referitoare la organizarea și funcționarea acestora, precum și a procedurilor interne administrative ce vizează desfășurarea activității.

S-a subliniat, totodată, faptul că, potrivit art. 37 alin. (7) din Regulament, operatorul sau persoana împuternicită de operator are obligația de a comunica autorităţii de supraveghere doar datele de contact ale responsabilului cu protecţia datelor.

Prin Ordinul nr. 1786/2017 privind modificarea şi completarea Clasificării ocupaţiilor din România - nivel de ocupaţie (şase caractere), aprobată prin Ordinul ministrului muncii, familiei şi protecţiei sociale şi al preşedintelui Institutului Naţional de Statistică nr. 1.832/856/2011, a fost introdusă în COR această nouă ocupație sub denumirea ”responsabil cu protecţia datelor cu caracter personal” - cod COR 242231.

Pentru mai multe informații Autoritatea națională de supraveghere a recomandat consultarea *Ghidului privind Responsabilul cu protecția datelor (DPO)*, emis de Grupul de Lucru Art. 29, care este format din reprezentanții tuturor autorităților de supraveghere din statele membre ale Uniunii Europene și care, printre altele, elaborează o serie de opinii/ghiduri, privind aplicarea coerentă și unitară a dispozițiilor regulamentului.

**c) Consimțământ în mediul on-line**

În ceea ce privește forma consimțământului, prevederile art. 5 din Legea nr. 677/2001 impun regula potrivit căreia orice prelucrare de date cu caracter personal poate fi efectuată

numai dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru acea prelucrare.

Prin urmare, acesta trebuie obținut într-o modalitate care să dovedească acordarea sa de către persoana vizată sau de către reprezentantul legal al acesteia, cu sublinierea că acordul trebuie obținut în mod expres pentru fiecare dintre scopurile prelucrării (de ex. dacă se intenționează a se realiza și activitatea de reclamă, marketing și publicitate, alături de scopul principal) care trebuie precizate în mod explicit.

Această cerință este în acord și cu art. 7 din Regulamentul (UE) 2016/679, care abrogă Directiva 95/46/CE și, implicit, Legea nr. 677/2001, Regulament ce va fi pus în aplicare începând cu data de 25 mai 2018.

Astfel, potrivit dispozițiilor legale sus-menționate, ”În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.”

Considerentul 32 din regulamentul sus-menționat stabilește următoarele: ”Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.”

În măsura în care serviciile operatorului se adresează și minorilor, art. 8 din Regulamentul (UE) 2016/679, intitulat ”Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale” stabilește faptul că: ”Operatorul

depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile."

În acest context, este de precizat faptul că, până la 25 mai 2018, potrivit art. 1 alin. (1) lit. h) din Decizia nr. 200/2015 a Preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (publicată în Monitorul Oficial al României, Partea I, nr. 969 din 28 decembrie 2015), notificarea autorităţii de supraveghere este necesară când prelucrarea datelor cu caracter personal ale minorilor este efectuată prin intermediul internetului sau al mesageriei electronice.

Astfel, în măsura în care un operator prelucrează datele minorilor prin intermediul internetului sau al mesageriei electronice, se impune fie depunerea unei notificări, fie completarea unei notificări existente.

În ceea ce privește tipul de date care trebuie prelucrate, Legea nr. 677/2001, modificată și completată, stabilește, la art. 4 alin. (1) lit. c), faptul că acestea trebuie să fie "adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate", cu alte cuvinte, cele strict necesare îndeplinirii scopului.

În același timp, este de subliniat faptul că prelucrările de date efectuate vor fi precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 12 din Legea nr. 677/2001, care obligă operatorul să furnizeze persoanei vizate o serie de informații.

În acest context, este de precizat faptul că art. 25 din Regulamentul (UE) 2016/679 stabilește, ca obligații generale ale operatorului, următoarele:

"(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și 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, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date

colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane."

În cadrul prelucrărilor menționate operatorii vor avea în vedere și prevederile Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

**d) Incidente de securitate și notificare**

O persoană fizică a solicitat un punct de vedere referitor la notificarea prelucrărilor de date cu caracter personal efectuate după 25 mai 2018.

Autoritatea națională de supraveghere a precizat următoarele:

De la data aplicării Regulamentului (UE) 2016/679, își va înceta aplicabilitatea Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Ca atare, după data de 25 mai 2018, operatorii nu vor mai avea obligația de notificare a prelucrărilor de date, obligație instituită de prevederile art. 22 din Legea nr. 677/2001. De asemenea, operatorii nu vor mai avea nici obligația obținerii numărului de operator.

Pe de altă parte, art. 33 din Regulamentul (UE) 2016/679 prevede că operatorul are obligația de a *notifica autoritatea de supraveghere în situația în care are loc o încălcare a securității datelor cu caracter personal.* Alin. (3) al acestui articol stabilește ce trebuie să vizeze notificarea autorității de supraveghere.

Referitor la stabilirea unui formular de notificare, în prezent există stabilit un astfel de formular, pentru îndeplinirea obligației operatorilor - furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, potrivit Deciziei Autorității nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice (a se vedea informațiile postate pe pagina http://www.dataprotection.ro/servlet/ViewDocument?id=1100).

Prin urmare, Autoritatea națională de supraveghere va avea în vedere punerea la dispoziția operatorilor a posibilității de îndeplinire a obligației de notificare a autorității, în temeiul art. 33 din Regulamentul (UE) 2016/679.

**Secţiunea a 4-a Activitatea de reprezentare în faţa instanţelor de judecată**

În anul 2017, s-a înregistrat o **creștere semnificativă a acțiunilor prin care s-au contestat actele Autorității naționale de supraveghere care au ajuns la 221**, spre deosebire de anul 2016 când s-au primit 112 cereri de chemare în judecată.

Având în vedere finalizarea în mod favorabil pentru instituția noastră a multor acțiuni în instanță, pe parcursul anului 2017, prezentăm mai jos câteva cazuri relevante:

- **Hotârâre pronunţată într-un litigiu privind neîndeplinirea obligațiilor privind informarea persoanelor vizate**

În exercitarea atribuţiilor de control, Autoritatea națională de supraveghere a efectuat o investigaţie din oficiu la un operator de date cu caracter personal, instituție publică centrală.

Investigația sus-menționată a avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, a măsurilor de securitate, precum şi a dispoziţiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

Prin procesul-verbal de constatare/sancţionare s-a constatat săvârşirea următoarei fapte:

”Prelucrarea nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, prin încălcarea art. 12 din această lege, întrucât instituția publică în cauză nu a realizat informarea persoanelor vizate ale căror date personale au fost prelucrate ca urmare a protocoalelor încheiate având ca obiect schimbul de informații în niciuna din modalitățile prevăzute de lege, conform constatărilor din acest proces-verbal. Pentru această faptă s-a acordat sancțiunea amenzii în cuantum de 6000 lei.

Din investigație a rezultat faptul că instituția publică realizează schimbul de informații referitoare la prelucrarea de date cu caracter personal atât cu instituții publice, cât și cu alte entități din domeniul privat, în baza unor protocoale încheiate cu acestea. Prin aceste

protocoale sunt stabilite, printre altele, obiectul protocolului, obligațiile părților și modalitatea de realizare a schimbului de informații.

În ceea ce privește informarea persoanelor vizate ale căror date cu caracter personal sunt prelucrate și dezvăluite de către instituția publică, la data efectuării controlului, aceasta nu a prezentat dovada informării persoanelor vizate, individual sau în altă modalitate, în concordanță cu art. 12 din Legea nr. 677/2001, pentru nicio situație în care a realizat schimburi de informații referitoare la date cu caracter personal.

Pe site-ul instituției publice respective era postată o notă de informare a persoanelor vizate cu privire la prelucrarea datelor cu caracter personal realizată de instituție conform atribuțiilor legale, dar care nu cuprindea mențiuni cu privire la prelucrarea datelor personale și dezvăluirea acestora în scopul realizării schimburilor de informații în baza protocoalelor respective și nu respecta pe deplin cerințele art. 12 din Legea nr. 677/2001.

Fiind vorba de o prelucrare nouă, specifică, efectuată în baza unor protocoale al căror conținut nu era cunoscut de persoanele fizice în cauză, prin mijloace electronice, prin intermediul unei aplicații care viza un număr mare de persoane fizice, instituția publică avea obligația informării persoanei vizate așa cum stabilesc dispozițiile art. 12 alin. (1) din Legea nr. 677/2001, cu atât mai mult cu cât colecta datele direct de la persoana fizică.

Chiar și dispozițiile legale care reglementează activitatea acestei instituții fac trimitere la respectarea Legii nr. 677/2001, deci implicit și la art. 12 din lege.

Prin urmare, instituția publică are obligația să asigure informarea persoanei vizate într-un mod clar și exact, astfel încât aceasta să cunoască detaliile prelucrării datelor sale, precum și drepturile de care beneficiază.

Astfel, în măsura în care, ulterior momentului colectării datelor de la persoanele fizice, în relația cu instituția publică, apar scopuri noi (atribuții noi ale operatorului, în speță instituția publică) pentru care se prelucrează datele, precum și destinatari noi, necunoscuți la momentul obținerii datelor personale (în speță, încheierea protocoalelor cu entitățile respective și dezvăluirea datelor către acestea), informațiile vizate de art. 12 din Legea nr. 677/2001 trebuie completate cu toate elementele nou-apărute, pentru a se asigura prelucrarea datelor cu bună-credință și în conformitate cu legea (principiul statuat de art. 4 alin. 1 lit. a) din Legea nr. 677/2001).

Prin urmare, conținutul informării sumare identificate pe site-ul instituției publice, la data efectuării controlului, nu respecta exigențele acestor principii, respectiv al caracteristicilor

”determinat” și ”explicit” ale scopului, precum și al prelucrării datelor cu bună-credință și în conformitate cu legea.

În acest context, Autoritatea națională de supraveghere a apreciat că nu se poate admite faptul că persoana vizată ar cunoaște toate aceste informații, încă de la începutul raporturilor sale cu instituția publică, astfel încât să nu mai fie necesară informarea sa pe întreg parcursul acestei relații, în cadrul activității de prelucrare a datelor personale.

Curtea de Apel București a menținut procesul-verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere, ca legal și temeinic.

Pentru a hotărî astfel, instanța de apel a reținut că legiuitorul a permis ca informarea să se realizeze în funcție de circumstanțele prelucrării, pentru a acoperi toate ipotezele care s-ar ivi în practică. Prin urmare, instituția publică a nesocotit dispozițiile art. 32 din Legea nr. 677/2001, întrucât nu a luat o minimă măsură de informare colectivă, informare care putea fi expusă pe site-ul propriu, adresată tuturor persoanelor fizice aflate în relație cu instituția publică, iar nu în mod obligatoriu individual.

Totodată, Curtea de Apel București a reamintit că, prin hotărârea preliminară pronunțată în Cauza C-201/14 Bara și alții împotriva Președintelui Casei Naționale de Asigurări de Sănătate, Casei Naționale de Asigurări de Sănătate și Agenției Naționale de Administrare Fiscală, CJUE a statuat faptul că ”articolele 10, 11 și 13 din Directiva 95/46/CE trebuie interpretate în sensul că se opun unor măsuri naționale precum cele în discuție în litigiul principal, care permit unei autorități a administrației publice a unui stat membru să transmită date personale unei alte autorități a administrației publice și prelucrarea lor ulterioară, fără ca persoanele vizate să fi fost informate despre această transmitere sau despre această prelucrare”.

De asemenea, instanța de apel a subliniat aspectele reținute de Curtea de Justiție a Uniunii Europene, potrivit cărora ”această cerință a informării persoanelor vizate de prelucrarea datelor lor cu caracter personal este cu atât mai importantă cu cât este o condiție necesară exercitării de către aceste persoane a dreptului lor de acces și de rectificare a datelor prelucrate, definit la articolul 12 din Directiva 95/46/CE, și a dreptului de opoziție al acestora față de prelucrarea datelor respective, vizat la articolul 14 din această directivă.”

În concluzie, Autoritatea națională de supraveghere subliniază că obstrucționarea sau negarea dreptului de informare este o practică inacceptabilă care aduce atingere principiului transparenței prelucrărilor de date efectuate de către instituțiile publice care, cu atât mai mult, au obligația legală pozitivă de a asigura respectarea drepturilor și libertăților fundamentale ale

cetăţenilor aflați pe o poziție de inegalitate, întrucât prelucrarea nu se efectuează pe baza consimțământului lor, iar nu doar o obligaţie negativă de a nu aduce atingere acestora.

Hotărârea pronunțată de instanță în favoarea instituției noastre a rămas definitivă.

- **Hotârâre pronunţată într-un litigiu privind nerespectarea dreptului de acces al persoanei vizate**

O persoană fizică s-a adresat Autorității naționale de supraveghere și a reclamat faptul că o societate din domeniul privat care furnizează servicii de comunicații electronice nu i-a furnizat toate informaţiile solicitate în urma exercitării dreptului de acces prevăzut de art. 13 alin. (1) din Legea nr. 677/2001, informații pe care le-a solicitat, de la acest operator, în scris, în mai multe rânduri.

În plus, petentul reclama şi faptul că trei dintre răspunsurile societății i-au fost trimise prin intermediul poştei electronice, cu toate că solicitase în mod expres ca răspunsurile să-i fie comunicate prin intermediul Poştei Române, indicând adresa la care să-i fie transmise.

Urmare a investigației efectuate de Autoritatea națională de supraveghere s-a constatat săvârşirea faptei de ”Prelucrare nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 13 din Legea nr. 677/2001, întrucât operatorul nu a comunicat persoanei fizice vizate toate informațiile solicitate de către aceasta prin cererile sale și nici nu i-a transmis răspunsurile la adresa indicată în cereri. Operatorului i s-a aplicat amendă în cuantum de 1500 lei, iar acesta a contestat în instanță sancțiunea aplicată.

Așa cum s-a putut constata din investigație, răspunsurile operatorului au fost formulate generic, fără furnizarea tuturor informațiilor pe care Legea nr. 677/2001 le stabilește în art. 13, deși persoana fizică în cauză are dreptul la comunicarea informațiilor privind scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele, precum și la comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării.

De asemenea, s-a constatat că operatorul nu desfășura efectiv activitățile prevăzute la art. 2 alin. (5) din Legea nr. 677/2001, respectiv dintre cele din domeniul ordinii publice sau al dreptului penal, nefiind o autoritate publică ce face aplicarea excepțiilor art. 16 din Legea nr. 677/2001.

Totodată, în timpul investigației, operatorul nu a făcut dovada faptului că ar fi fost o solicitare din partea autorităților publice de acces la datele petentului înregistrate în evidențele sale, pentru a justifica faptul că nu avea posibilitatea de a asigura exercitarea dreptului de acces al acestuia, la data formulării cererilor petentului.

În consecință, nefiind îndeplinite prevederile art. 16 din Legea nr. 677/2001 coroborate cu art. $3^1$ din Legea nr. 506/2004, dreptul de acces la date, astfel cum este prevăzut de art. 13 din Legea nr. 677/2001, trebuia asigurat de către operator petentului.

Art. $3^1$ intitulat "Proceduri de accesare" din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, modificată și completată, stabilește faptul că: "Furnizorii au obligaţia de a stabili proceduri interne pentru a răspunde solicitărilor de accesare a datelor cu caracter personal ale utilizatorilor. La cerere, aceştia oferă Autorității naționale de supraveghere informaţii despre procedurile respective, numărul de solicitări primite, justificarea legală invocată în solicitare şi răspunsul oferit solicitanţilor."

Prin urmare, operatorul nu poate stabili, în mod arbitrar și subiectiv, o altă procedură de asigurare a exercitării drepturilor persoanelor vizate, care excede dispozițiilor art. 13 din Legea nr. 677/2001.

Instanța de fond a respins acțiunea operatorului și a menținut procesul-verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere, ca temeinic și legal.

Prin hotărârea sa, instanța de fond a reținut că:

*"...reclamanta nu a comunicat petiționarului niciuna din informațiile solicitate și nici nu a uzat de calea indicată pentru transmiterea acestora. Mai mult, reclamanta a recunoscut faptul că în procesul de verificare nu a putut identifica cu certitudine dezvăluiri către terți ale datelor personale ale petentului.*

*Răspunsurile reclamantei au fost generice, emise într-un vădit dezinteres față de drepturile subiective ale petiționarului.*

*Situația de excepție invocată de reclamantă, de la furnizarea datelor solicitate de petent nu o poate exonera de răspundere întrucât nu s-a făcut dovada incidenței sale, respectiv a premisei reglementate de art. 2 alin. (5) din Legea nr. 677/2001. Reclamanta nu a făcut dovada faptului că ar fi existat o solicitare din partea autorităților publice cu competență în urmărirea activității infracționale, cu privire la datele personale ale petentului, pentru a justifica abordarea sa în relația cu acesta.*

*Reclamanta nu a furnizat niciun motiv care ar fi împiedicat-o să respecte modalitatea concretă de transmitere a informațiilor, respectiv calea poștei clasice și nu cea electronică."*

De asemenea, instanța a reținut în mod corect faptul că *"...față de atitudinea reclamantei Tribunalul consideră că în speță nu se impune înlocuirea sancțiunii amenzii cu avertisment, gradul de pericol social al faptei comise fiind unul ridicat, omisiunea reclamantei creând un sentiment de insecuritate și arbitrar petentului ale cărui drepturi era obligată să le respecte."* Totodată, instanța a mai reținut și faptul că *"reclamanta se face vinovată de o dublă încălcare a drepturilor petentului, respectiv atât de necomunicarea informațiilor solicitate cât și de ignorarea modalității de comunicare a acestora."*

Hotărârea instanței a rămas definitivă.

- **Hotârâre pronunţată într-un litigiu privind neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate**

Autoritatea națională de supraveghere a demarat o investigație din oficiu la o societate care are ca domeniu de activitate servicii de transport în regim taxi, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi a măsurilor de securitate și a Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

În urma investigaţiei efectuate, s-a constatat săvârşirea de către entitatea controlată a următoarelor fapte contravenţionale:

**I.** *Omisiunea de a notifica şi notificarea cu rea-credinţă*, contravenție prevăzută de art. 31 din Legea nr. 677/2001, sub forma omisiunii de a efectua notificarea în condiţiile art. 22 din Legea nr. 677/2001, întrucât societatea nu a notificat prelucrarea datelor cu caracter personal pe care o efectuează prin intermediul aplicației utilizate în scopul preluării/plasării comenzilor de taxi, pentru care s-a aplicat *amendă în cuantum de 1000 lei.*

**II.** Neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, prevăzută de art. 33 din Legea nr. 677/2001, întrucât societatea, până la data procesului-verbal de constatare/sancționare nu a adoptat măsuri de confidențialitate și securitate a datelor cu caracter personal prelucrate, conform art. 19 și 20 din Legea nr. 677/2001, sub aspectul elaborării/implementării unei politici de securitate, a stabilirii unor

instrucțiuni precise pentru persoana care are acces la datele personale sau instrucțiuni pentru persoanele împuternicite, pentru care s-a aplicat amendă în cuantum de 3000 de lei.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat, acesta solicitând anularea procesului-verbal.

Instanța a respins plângerea, apreciind că *"petenta nu a invocat critici concrete de nelegalitate și netemeinicie a procesului-verbal de contravenție, susținând că individualizarea sancțiunilor aplicate a fost realizată cu nerespectarea dispozițiilor art. 5 alin. 5 din Ordonanța Guvernului nr. 2/2001."*

Împotriva sentinţei instanței de fond societatea a declarat apel, iar instanța superioară a respins apelul formulat, soluţia fiind definitivă în favoarea instituției noastre.

Decizia definitivă a instanței a confirmat abordarea Autorității naționale de supraveghere de respectare a condițiilor de legitimitate a prelucrării datelor cu caracter personal, așa cum sunt acestea prevăzute de Legea nr. 677/2001 și Legea nr. 506/2004.

În contextul dat, atragem atenția asupra faptului că prelucrarea de date cu caracter personal, în cadrul activității derulate de societățile care au ca domeniu de activitate servicii de transport în regim taxi, intră sub incidenţa legislaţiei privind protecţia datelor personale, astfel de societăți fiind ţinute, în calitate de operatori de date, de respectarea tuturor obligaţiilor stabilite de lege în sarcina acestora.

- ***Hotârâre pronunţată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal, de către o casă de asigurări de sănătate***

Autoritatea națională de supraveghere a demarat o investigație din oficiu la o casă de asigurări de sănătate, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum şi a dispoziţiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

Investigația s-a declanșat ca urmare a unei sesizări a mass-media privind publicarea pe Internet, pe pagina proprie a casei de asigurări de sănătate, a unei liste conținând un număr total de 18.607 persoane fizice (nume, prenume, adresă completă). Astfel, din verificările efectuate, s-a constatat că această listă denumită "Situația cardurilor returnate la sediul instituției de către Poșta Română" era publicată pe internet.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a constatat săvârşirea de către casa de asigurări de sănătate a faptei contravenţionale de prelucrarea nelegală a datelor cu caracter personal, contravenţie prevăzută de art. 32 din Legea nr. 677/2001, prin încălcarea art. 4 alin. (1) lit. a) şi art. 5 alin. (1) din aceeaşi lege, întrucât începând cu perioada iulie-august 2015, casa de asigurări de sănătate a publicat pe Internet, pe pagina proprie, o listă accesibilă oricărei persoane care accesează pagina de Internet în cauză, conţinând datele personale a 18.607 persoane fizice (nume, prenume, adresă completă) privind situația cardurilor returnate la sediul instituției, pentru care s-a aplicat sancţiunea amenzii în cuantum de 8000 lei.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat, acesta solicitând anularea procesului-verbal.

Instanța a analizat actul contestat de reclamantă, respectiv procesul-verbal de contravenţie, acesta fiind verificat din perspectiva legalităţii şi a temeiniciei, inclusiv sub aspectul motivelor invocate de ambele părţi din dosar.

Astfel, în mod corect instanța a constatat că *„Situația de fapt reținută de agentul constatator nu este contestată de reclamantă”.*

În consecință, instanța a reținut că respectiva casă de asigurări de sănătate, în calitate de operator, a prelucrat și dezvăluit pe Internet date cu caracter personal a 18.607 asigurați.

*Împotriva sentinţei instanței de fond casa de asigurări de sănătate a declarat apel, dar instanța superioară a respins apelul formulat, soluţia rămânând definitivă în favoarea instituției noastre.*

- **Hotârâre pronunţată într-un litigiu privind securitatea datelor și supravegherea angajaților**

Autoritatea națională de supraveghere a efectuat o investigaţie la un operator, ca urmare a unei plângeri prin care se sesiza faptul că au fost găsite pe stradă documente aparținând operatorului, care conțineau date personale ale angajaților operatorului și ale proprietarilor apartamentelor din imobilul administrat de acesta.

De asemenea, a mai fost sesizat aspectul că operatorul are montate camere de supraveghere în birouri şi nu a adoptat măsurile legale ce se impun pentru securitatea și protecția datelor personale.

Ca urmare a controlului efectuat, Autoritatea națională de supraveghere a constatat că operatorul deținea un sistem de supraveghere video, începând cu luna august 2015, alcătuit din 8 camere de supraveghere video, montate atât în exteriorul clădirii, cât și în interiorul acesteia (în birouri). Operatorul nu a putut face dovada notificării prelucrării datelor prin sistemul de supraveghere video şi nici a informării persoanelor vizate cu privire la acest sistem.

De asemenea, operatorul nu a putut face dovada obţinerii consimţământului expres şi neechivoc al salariaţilor, a acordului sindicatului anterior montării camerelor sau a unui aviz din partea Autorităţii naționale de supraveghere consultate în acest sens.

S-a mai constatat că operatorul nu a făcut dovada existenţei măsurilor de securitate a prelucrărilor datelor personale.

Faptele săvârşite de operator au fost sancţionate contravenţional, atât cu avertisment cât şi cu amendă, iar procesul-verbal de constatare/sancţionare a fost contestat în instanţă.

*Instanţa, analizând probatoriul administrat în cauză, a constatat 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 fost contestată de operator, însă soluția instanței care a judecat calea de atac a fost aceeași, prin respingerea recursului declarat de operator.*

- **Hotârâre pronunţată într-un litigiu privind transmiterea 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 prelucrării datelor prin transmiterea de mesaje comerciale nesolicitate, respectiv fără acordul prealabil al persoanei vizate.

La momentul controlului, operatorul a declarat că adresele de e-mail folosite pentru trimiterea de newslettere provin din mai multe surse: importarea listei din CSV, abonare la newsletter pe site-ul operatorului, completare de pliante denumite ”Fișe impresii” de către clienții societății, din pagina de facebook a societății, din completarea formularului de ”Cerere ofertă” de pe site-ul societății.

În cadrul investigației s-au efectuat mai multe teste privind modalitatea de abonare și dezabonare, constatându-se astfel că la acel moment funcționa mecanismul de abonare ”dublu opt-in”, implementat odată cu utilizarea unei aplicații.

De asemenea, operatorul a mai declarat că în anul 2016 a derulat și o campanie de trimitere de mesaje către utilizatorii adreselor de e-mail din baza de date, cu solicitarea de a confirma expres dacă se dorește sau nu primirea în continuare de newsletter. Dintre utilizatorii contactaţi astfel au răspuns 1071, dintre care 142 au declarat că nu doresc să mai primească newsletter.

Din verificarea site-ului operatorului în timpul controlulului a rezultat că nu exista o informare completă privind prelucrarea datelor personale, conform art. 12 din Legea nr. 677/2001, în special sub aspectul drepturilor persoanelor vizate și al condițiilor de exercitare a acestora. De asemenea, pe ”Fișele de impresii” nu era inclus un acord expres al persoanelor cu privire la utilizarea adresei de e-mail sau a numărului de telefon în scopul trimiterii de comunicări comerciale prin mijloace de comunicații electronice, așa cum prevede art. 12 alin. (1) din Legea nr. 506/2004.

S-a constatat că operatorul nu a putut face dovada privind obținerea în prealabil a consimțământului expres al petentului care a sesizat posibila încălcare a prelucrării datelor cu caracter personal.

Faptele săvârşite de operator au fost sancţionate contravenţional atât cu avertisment cât şi cu amendă, iar procesul-verbal de constatare/sancţionare a fost contestat în instanţă.

Analizând probatoriul administrat în cauză, *instanţa a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit*, astfel fiind menţinute sancţiunile contravenţionale aplicate.

Hotărârea instanței a rămas definitivă.

- **Hotârâre pronunţată într-un litigiu privind prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit**

Autoritatea națională de supraveghere a efectuat o investigatie, din oficiu, la un operator, având ca obiect prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit.

În acest sens, Autoritatea națională de supraveghere a solicitat operatorului printr-o adresă rapoartele de credit, precizarea datei scadenței (ziua) privind obligația de plată pentru zece clienţi precizaţi, notificările (informările) clienţilor cu privire la faptul că aceştia urmează să fie raportaţi la Biroul de Credit cu debite restante, conform Deciziei nr. 105/2007, dar nu mai vechi de 6 luni, precum şi dovada notificărilor transmise către clienţi.

Operatorul a răspuns adresei Autorităţii naționale de supraveghere transmiţând documentele pe care le deţinea raportat la solicitarea autorităţii.

Din documentele puse la dispoziţie, s-a constatat, pentru unii dintre clienți, că operatorul nu a realizat o înştiinţare prealabilă a persoanei vizate la fiecare obligaţie de plată (în scris), aşa cum prevede art. 8 alin. (2) din Decizia nr. 105/2007. În cazul altor clienţi, deşi a transmis o înştiinţare prealabilă cu 15 zile înainte de raportare, operatorul nu a furnizat acestora informaţiile prevăzute de art. 9 din Decizia nr. 105/2007.

De asemenea, din documentele puse la dispoziţie de operator și din situaţia de transmitere de date la Biroul de Credit, a reieşit că, pentru anumiţi clienţi, operatorul a transmis date negative la Biroul de Credit înainte de împlinirea termenului de 30 de zile de la data scadenței, contrar prevederilor art. 5 alin. (1) din Decizia nr. 105/2007.

Totodată, s-a constatat că operatorul prelucrează date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit în mod neunitar la nivel naţional, astfel că în majoritatea situațiilor nu respectă prevederile Deciziei nr. 105/2007.

Operatorul investigat nu a putut pune la dispoziţia Autorităţii naționale de supraveghere documente și dovezi privind informarea prealabilă transmisă persoanelor vizate cu 15 zile înainte de a raporta datele negative la Biroul de Credit, în conformitate cu art. 8 alin. (2) şi art. 9 alin. (1) din Decizia nr. 105/2007 coroborat cu art. 12 din Legea nr. 677/2001, astfel că raportarea nu a respectat termenul de 30 de zile de la scadenţă.

În consecință, operatorul a fost sancţionat cu amendă la cuantumul maxim prevăzut de lege, iar procesul-verbal de constatare/sancţionare a fost contestat la instanţă.

*Instanţa, analizând probatoriul administrat în cauză, a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit, fapt pentru care au fost menţinute sancţiunile contravenţionale aplicate.*

Hotărârea a devenit definitivă prin respingerea apelului declarat de operator.

**Secţiunea a 5-a Informare publică**

În cursul anului 2017, Autoritatea naţională de supraveghere a continuat activităţile şi modalităţile de comunicare destinate informării publicului larg, cu privire la regulile specifice de prelucrare a datelor cu caracter personal, cu precădere în contextul Regulamentului (UE) 2016/679.

Astfel, a fost organizată Ziua Europeană a Protecţiei Datelor, ca în fiecare an, eveniment de prestigiu ce a fost onorat de prezența unor reprezentanți de marcă ai autorităților publice centrale, ai societății civile și ai mediului privat.

Un rol important în activitatea de popularizare a domeniului protecției datelor l-a avut și difuzarea pe postul public de televiziune a unui clip de informare privind datele personale.

Pe tot parcursul anului, 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. 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.

Dintre evenimentele semnificative în care instituţia noastră a fost implicată, reliefăm:

- **Ziua Europeană a Protecţiei Datelor**

Pe data de 28 ianuarie 2017, s-a aniversat Ziua Europeană a Protecţiei Datelor, care a marcat împlinirea a 36 de ani de la semnarea la Strasbourg, în anul 1981, a Convenţiei 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal - primul instrument legal adoptat în domeniul protecţiei datelor.

Scopul celebrării acestei zile este creșterea gradului de informare a publicului larg asupra importanţei protecţiei datelor cu caracter personal şi a drepturilor specifice pe care cetățenii le pot exercita.

Cu această ocazie, autorităţile naţionale independente pentru protecţia datelor din statele europene organizează evenimente specifice.

În cinstea Zilei Europene a Protecţiei Datelor, pe data de 27 ianuarie 2017, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal a organizat Simpozionul

cu tema „Noul Regulament General privind Protecția Datelor – implicații și efecte”, la Palatul Parlamentului.

În aceeași zi aniversară, Autoritatea națională de supraveghere a organizat evenimentul *”Ziua porților deschise”* , prilej cu care persoanele interesate de domeniul protecţiei datelor cu caracter personal au fost invitate la sediul instituţiei noastre și au avut posibilitatea de a vizita zonele deschise publicului şi de a primi informaţii generale privind activitatea specifică a Autorităţii naţionale de supraveghere.

- **Masa Rotundă cu tema *Aplicarea Noului Regulament General privind Protecția Datelor în sectorul public – obligații și responsabilități***

Instituția noastră a organizat, pe data de 22 septembrie 2017, Masa Rotundă intitulată “Aplicarea Noului Regulament General privind Protecția Datelor în sectorul public – obligații și responsabilități”, în considerarea adoptării Regulamentului (UE) 2016/679, aplicabil direct în toate statele membre ale Uniunii Europene începând cu data de 25 mai 2018,.

Evenimentul menționat s-a adresat autorităților și instituțiilor publice centrale din România, cu ocazia acestuia fiind reliefate noile obligații ce revin operatorilor din sectorul public pentru respectarea regulilor de prelucrare stabilite de Noul Regulament.

În acest context, au fost abordate interactiv, în cadrul panelurilor, aspecte privind:

- *Responsabilul pentru protecția datelor*
- *Cartografierea și evaluarea de impact*
- *Respectarea drepturilor persoanelor vizate*
- *Asigurarea securității datelor /Notificarea încălcarilor de securitate*

Cu acest prilej, s-a subliniat că fiecare instituție publică are obligația de a-și desemna un responsabil cu protecția datelor personale, având în vedere prevederile art. 37-39 din Regulamentul General privind Protecția Datelor.

Evenimentul s-a bucurat de larga prezență a reprezentanților ministerelor, instituțiilor din subordinea acestora, a agențiilor și autorităților publice autonome, reprezentanților Parlamentului, instituțiilor judecătorești și a altor operatori.

- **Conferințe și evenimente privind aplicarea Regulamentului General privind Protecția Datelor**

**1.** Pe data de 10 aprilie 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la **un eveniment** dedicat regulilor actuale de prelucrare a datelor personale și noutăților aduse de Regulamentul General privind Protecția Datelor, în organizarea unei societăți de avocatură.

Invitaților prezenți, în special din domeniile bancar și IT, li s-au prezentat principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018.

Manifestarea interactivă a reliefat interesul deosebit al sectorului privat pentru respectarea regulilor stabilite de Noul Regulament.

Acest eveniment a fost precedat de Conferința ”Noua Ordine europeană în domeniul protecției datelor”, desfășurată pe data de 16 martie 2017, care a beneficiat de o largă prezență a reprezentanților societăților din diverse sectoare de activitate.

În deschiderea acestei conferințe, reprezentanții Autorității naționale de supraveghere au adus în atenția participanților impactul noii reglementări europene și implicațiile respectării drepturilor persoanelor vizate.

Participările constante ale reprezentanților instituției noastre la aceste evenimente se circumscriu campaniei de informare derulate de Autoritatea națională de supraveghere în scopul popularizării noilor reguli de prelucrare a datelor personale atât în rândul operatorilor, cât și al publicului larg.

**2.** Pe data de 4 mai 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la **a doua ediție a Conferinței ”Noua Ordine europeană în domeniul protecției datelor”**, dedicată sectorului financiar-bancar și sectorului public.

Aceștia au adus în atenția participanților principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018, precum și impactul noii reglementări europene asupra respectării drepturilor persoanelor vizate.

Cu această ocazie a fost subliniată obligativitatea autorităților și organismelor publice (cu excepția instanțelor judecătorești) de a-și desemna un responsabil cu protecția datelor, în concordanță cu prevederile art. 37-39 din Regulamentul (UE) 2016/679, precum și sarcinile acestuia.

De asemenea, s-au prezentat și situațiile în care operatorii sau împuterniciții lor din mediul privat au obligația stabilirii unui responsabil cu protecția datelor până la data de 25 mai 2018, respectiv în cazurile în care se efectuează monitorizări periodice și sistematice pe scară largă ale persoanelor vizate sau în care se prelucrează, tot pe scară largă, date sensibile, cum sunt cele privind originea rasială, etnică, opinii politice, convingeri religioase, filozofice, apartenența sindicală, date genetice sau date biometrice.

Acest eveniment interactiv a reliefat preocuparea deosebită a sectorului privat și public pentru respectarea regulilor de prelucrare stabilite de Noul Regulament.

Cu acest prilej mesajul instituției noastre a fost difuzat către publicul larg de postul public național Radio România Actualități. Astfel, și această participare a reprezentanților instituției noastre se înscrie în cadrul campaniei de informare derulate de Autoritatea națională de supraveghere, în scopul popularizării noilor reguli de prelucrare a datelor personale.

**3.** Pe data de 25 mai 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la reuniunea **"Aspecte practice referitoare la implementarea Regulamentului general privind protecția datelor"** dedicată dezbaterii principalelor implicații ale Regulamentului General privind Protecția Datelor, organizată de Camera de Comerț Româno-Americană.

Au fost reliefate elementele de noutate aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018, precum și impactul noii reglementări europene asupra respectării drepturilor persoanelor vizate.

Cu această ocazie a fost subliniată obligativitatea entităților private de a-și desemna, în anumite situații, un responsabil cu protecția datelor, până la data de 25 mai 2018, în concordanță cu prevederile art. 37-39 din Regulament.

Au fost discutate situații cu implicații asupra informării persoanelor vizate, referitoare la condițiile de legitimitate ale prelucrărilor efectuate, obligația anumitor categorii de operatori de a păstra o evidență a activităților de prelucrare conform art. 30 din Regulamentul General

privind Protecția Datelor, notificarea încălcărilor de securitate în condițiile art. 33 din Regulament și evaluarea de impact în conformitate cu art. 35 din același act normativ.

Prezența numeroasă a reprezentanților mediului privat la acest eveniment interactiv a ilustrat, încă o dată, interesul în creștere al sectorului privat pentru aplicarea corespunzătoare a regulilor de prelucrare stabilite de Noul Regulament.

**4.** Pe data de 17 octombrie 2017 reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la un **eveniment** dedicat noilor reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor, în organizarea unei societăți de avocatură.

Invitaților prezenți, în special operatori de date din domeniile financiar-bancar, IT și marketing, li s-au prezentat principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018.

Acest eveniment a fost precedat de o **conferință**, desfășurată pe data de 11 octombrie 2017, dedicată întregului mediu de afaceri interesat de aplicarea Regulamentului General privind Protecția Datelor.

La cele două evenimente, reprezentanții Autorității naționale de supraveghere au adus în atenția participanților obligațiile ce revin operatorilor și împuterniciților acestora în ceea ce privește respectarea regulilor de prelucrare stabilite de Noul Regulament, fiind abordate, de asemenea, implicațiile respectării drepturilor persoanelor vizate, precum și aspecte legate de numirea unui responsabil cu protecția datelor, asigurarea securității datelor și notificarea încălcărilor de securitate.

Manifestarea interactivă a participanților în cadrul evenimentelor a reliefat interesul deosebit al sectorului privat de conformare cu noile reguli de prelucrare a datelor personale.

Cele două evenimente derulate cu participarea Autorității naționale de supraveghere au fost reflectate în mass-media.

**5.** Pe data de 2 noiembrie 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la evenimentul "**ZF Insurance Summit: Calea către o creștere sănătoasă a pieței asigurărilor"**, organizat de Ziarul Financiar. În cadrul uneia dintre secțiunile evenimentului au fost puse în discuție noile reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor.

**6.** În 17 noiembrie 2017, Asociația de Management al Creanțelor Comerciale - AMCC a organizat un **workshop** în cadul căruia invitaților prezenți, operatori de date ce activează în domeniul financiar nebancar, le-au fost prezentate de reprezentanții Autorității naționale de supraveghere principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018. De asemenea, au fost discutate implicațiile aplicării acestei reglementări în domeniul recuperărilor de creanțe.

**7.** Evenimentul anterior a fost urmat, pe 21 noiembrie 2017, de dezbaterea "Securitate în sănătate. Protecţia datelor personale: proceduri și responsabilităţi" în organizarea New Strategy Center, dedicată operatorilor de date din domeniul sănătății interesați de aplicarea Regulamentului General privind Protecția Datelor, la care au fost prezentate principalele implicații ale noii reglementări asupra activității acestora.

**8.** În organizarea Uniunii Agențiilor de Publicitate din România a avut loc în 22 noiembrie 2017 **workshopul** pe tema protecției datelor cu caracter personal în publicitate, la care au participat reprezentanți ai mai multor agenții de specialitate.

**9.** La finalul lunii, în 28 noiembrie 2017, a avut loc un alt **eveniment** pe tema protecției datelor și a implementării Regulamentului (UE) 2016/679, în sectorul hotelier și turistic, sub patronajul Federației Industriei Hoteliere din România – FHIR.

La toate evenimentele menționate au participat reprezentanți ai Autorității naționale de supraveghere care au adus în atenția participanților obligațiile ce le revin, raportat la calitatea acestora de operatori și împuterniciți, în ceea ce privește respectarea regulilor de prelucrare a datelor așa cum au fost stabilite de noul cadru legislativ european.

Au fost abordate, totodată, chestiuni legate de respectarea tuturor drepturilor persoanelor vizate, așa cum sunt reglementate de Noul Regulament, precum și aspecte legate de numirea unui responsabil cu protecția datelor, asigurarea securității datelor și notificarea încălcărilor de securitate.

Evenimentele, reflectate și în mass-media, au fost marcate de discuții interactive, fapt ce a demonstrat interesul participanților de conformare cu noile reguli de prelucrare a datelor personale.

➢ **Reuniuni de informare în judeţele Timiș, Caraș-Severin, Iași și Neamț**

În continuarea **campaniei de informare la nivel național în sectorul public** s-au desfăşurat pe data de 4 iulie 2017, în municipiul Timișoara şi 5 iulie 2017, în municipiul Reșița, reuniunile cu tema ”Protecția datelor personale în administraţia publică locală”, evenimente realizate cu sprijinul Instituției Prefectului Județului Timiș şi al Instituției Prefectului Județului Caraș-Severin.

La aceste reuniuni au fost invitați reprezentanţii autorităţilor publice locale şi ai serviciilor deconcentrate ale ministerelor, precum şi ai celorlalte organe ale administraţiei publice.

Cu acest prilej s-au abordat subiecte de actualitate referitoare la asigurarea protecţiei datelor cu caracter personal de către operatorii din sectorul public.

Astfel, referitor la obligația notificării, s-a precizat că, în prezent, autorităţile publice locale şi cele de la nivel judeţean sunt scutite de obligaţia de notificare pentru prelucrările prevăzute de lege în sarcina acestora (raportat la obiectul de activitate), conform Deciziei Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea. Cu toate acestea, subzistă obligația de notificare a prelucrărilor efectuate prin utilizarea sistemelor de supraveghere video, în concordanţă cu prevederile art. 14 din Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video.

Totodată, s-a evidențiat că, în toate situaţiile, autorităţile publice locale şi cele de la nivel judeţean au obligaţia respectării prevederilor Legii nr. 677//2001, atât sub aspectul condiţiilor de prelucrare, al confidenţialităţii şi securităţii prelucrărilor, cât şi sub aspectul asigurării exercitării drepturilor persoanelor vizate (drepturile de informare, acces, intervenţie, opoziţie).

În acest context, s-a precizat că autorităţile publice locale şi cele de la nivel judeţean sunt obligate să aplice măsurile tehnice şi organizatorice adecvate pentru protejarea datelor personale împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum şi împotriva oricărei alte forme de prelucrare ilegală.

O altă temă de actualitate abordată în cadrul acestor reuniuni a fost cea privind Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția

persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, ce va fi aplicabil din 25 mai 2018.

În cadrul reuniunilor, s-a subliniat faptul că Regulamentul (UE) 2016/679 înlocuiește Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, fiind direct aplicabil în toate statele membre ale UE fără a fi necesară transpunerea în legislația națională.

În acest context, s-au evidențiat elementele de noutate impuse de noul regulament, în special responsabilizarea operatorului care, deși va fi scutit de la depunerea notificării, va fi ținut de respectarea drepturilor persoanelor vizate, efectuarea unui studiu de impact asupra protecției datelor al operațiunilor de prelucrare a datelor cu caracter personal în anumite cazuri, precum și numirea unui responsabil cu protecția datelor.

De asemenea, în cadrul acestor reuniuni s-a abordat și obiectul de reglementare al Directivei (UE) 2016/680 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

Potrivit acestei directive, statele membre vor adopta și publica, până la 6 mai 2018, actele cu putere de lege și actele administrative necesare pentru a se conforma acestei directive.

- **Abordări ale Regulamentului General privind Protecția Datelor în cadrul Colocviului „Aplicarea noilor cerințe europene de protecție a datelor personale și aspecte juridice privind creditarea consumatorilor”**

Reprezentanții Autorității Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat, pe data de 23 octombrie 2017, la colocviul găzduit de Facultatea de Drept din cadrul Universității ”Alexandru Ioan Cuza” din Iași, ce a avut ca principale teme identificarea și clarificarea unor probleme cheie care rezultă din aplicarea Reegulamentului la nivelul instituțiilor financiar-bancare, precum și de creditare a consumatorului.

Evenimentul menționat s-a adresat operatorilor de date din domeniul financiar-bancar, avocaților, dar și studenților Facultății de Drept.

Cu această ocazie au fost reliefate noile obligații ce revin operatorilor din sectorul privat pentru respectarea regulilor de prelucrare stabilite de Noul Regulament, dar și noile drepturi ale persoanelor vizate.

În acest context, reprezentantul Autorității naționale de supraveghere a adus în atenția participanților, în cadrul panelului specific, aspecte privind responsabilul cu protecția datelor, cartografierea și evaluarea de impact asupra protecției datelor, respectarea drepturilor persoanelor vizate, notificarea încălcărilor de securitate și asigurarea securității datelor.

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

Dincolo de aceste evenimente, **pagina de internet a Autorității naționale de supraveghere** a reprezentat unul dintre cele mai utile și complete mijloace de informare, atât a operatorilor cât și a publicului larg, cu privire la evoluțiile din domeniu și la activitatea specifică.

La începutul anului 2017, a fost creată o **secțiune specială pe pagina de internet a Autorității naționale de supraveghere, dedicată Noului Regulament General de Protecția Datelor**, în cadrul căreia au fost puse la dispoziția celor interesați o serie de materiale informative, inclusiv documente emise de Grupul de Lucru Art. 29 care, printre altele, elaborează o serie de opinii/ghiduri privind aplicarea coerentă și unitară a dispozițiilor regulamentului.

Grupul de Lucru Art. 29 a adoptat și dat publicității o serie de ghiduri, precum *Ghidul privind evaluarea de impact*, *Ghidul privind Responsabilul cu protecția datelor*, *Ghidul privind consimțământul*.

Aceste ghiduri, în limba engleză, cât și traducerea lor neoficială în limba română, efectuată prin eforturile Autorității naționale de supraveghere, se regăsesc în secțiunea specială dedicată Noului Regulament General de Protecția Datelor, alături de Ghidul orientativ destinat operatorilor, elaborat de autoritate.

În scopul popularizării activităţii instituţiei şi a reglementărilor specifice în materie, au fost publicate comunicate de presă prin care au fost prezentate aspecte semnificative din activitatea de comunicare ori cu referire la multiplele manifestări în care a fost implicată Autoritatea naţională de supraveghere. De asemenea, prin informaţiile furnizate telefonic şi în

cadrul audienţelor acordate la sediul Autorităţii naţionale de supraveghere, s-a realizat informarea rapidă şi eficientă a cetăţenilor şi a operatorilor, în sensul că au fost oferite, într-o manieră directă, informaţii utile privind drepturile persoanelor vizate şi obligaţiile specifice operatorilor, lămuriri referitoare la condiţiile prelucrării datelor şi dezvăluirii acestora către terţi.

Articolele de presă publicate şi reportajele difuzate la principalele posturi de televiziune au reflectat interesul manifestat de mass-media faţă de domeniul protecţiei datelor cu caracter personal.

# CAPITOLUL IV

# ACTIVITATEA DE CONTROL

## Secțiunea 1 - Prezentare generală

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

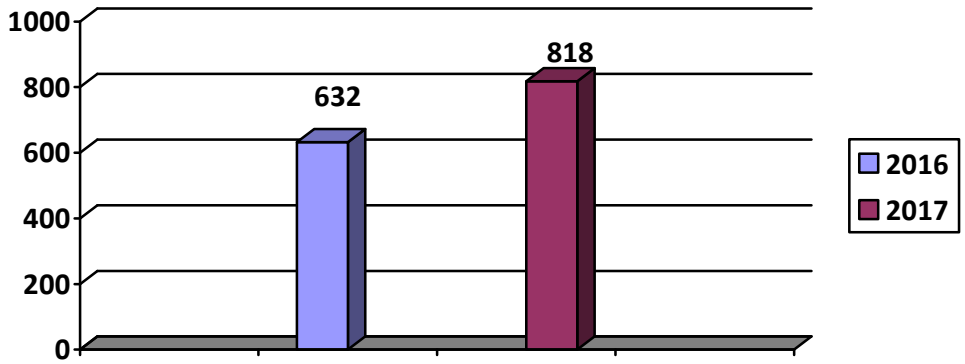
În anul 2017, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile în cadrul prelucrării datelor cu caracter personal atât în sistemul public, cât și în cel privat.

Investigațiile efectuate au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum şi a dispoziţiilor Legii nr. 506/2004.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri exponențiale a numărului acestora (**3543 plângeri și 191 sesizări**), în anul 2017 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, cu precădere, cele care vizează prelucrarea datelor personale de către birourile de credit, dar și cele din cadrul sistemelor ce utilizează mijloace de supraveghere video sau din sectorul comunicațiilor electronice.

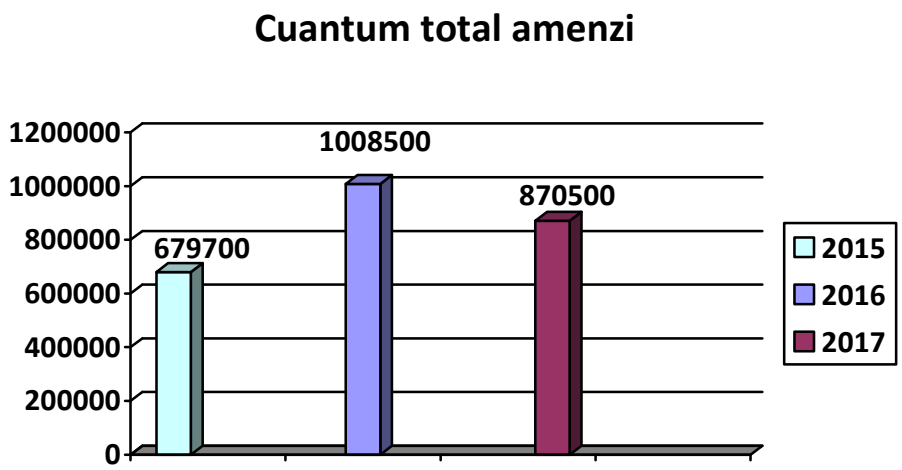
**Numărul total de investigații** efectuate de Autoritatea națională de supraveghere în 2017 este de **818**, în creștere față de anul anterior.

**Investigații**



În urma investigațiilor efectuate, au fost aplicate sancțiuni contravenționale constând în **128 amenzi și** respectiv, **217 avertismente**.

**Cuantumul total al amenzilor** aplicate în 2017 a fost de **870.500 lei.**




**Secțiunea a 2-a – Investigații din oficiu**

**1. Prelucrarea datelor cu caracter personal la nivelul sectorului public - oficii de cadastru şi publicitate imobiliară**

În anul 2017, la nivelul sectorului public au fost efectuate 4 acţiuni de control în cadrul oficiilor de cadastru și publicitate imobiliară, pentru verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum şi a dispoziţiilor Legii nr. 506/2004.

Oficiile de cadastru și publicitate imobiliară sunt instituţii publice cu personalitate juridică, subordonate Agenţiei Naţionale de Cadastru şi Publicitate Imobiliară.

Investigaţiile efectuate au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, a măsurilor de securitate, precum şi a dispoziţiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

Ca urmare a acestor acțiuni de control, au fost aplicate un avertisment şi o amendă în cuantum de 2000 lei.

Obiectivele avute în vedere au fost următoarele:

- îndeplinirea obligaţiei de notificare cu privire la prelucrările efectuate prin mijloace de supraveghere video;

- modalităţile de prelucrare a datelor cu caracter personal, în temeiul Legii nr. 677/2001;

- asigurarea drepturilor persoanelor vizate;

- îndeplinirea obligaţiei de confidenţialitate şi securitate a prelucrărilor.

Prezentăm mai jos, principalele constatări rezultate din investigaţiile efectuate:

- documentele de colectare/dezvăluire/stocare a datelor cu caracter personal utilizate de către oficiile de cadastru și publicitate imobiliară sunt tipizate şi au fost stabilite prin Ordinul nr. 700/2014 al Directorului General al ANCPI publicat în Monitorul Oficial nr. 571 bis/31.VII 2014;

- oficiile de cadastru și publicitate imobiliară controlează și îndrumă toate activităţile privind cadastrul, cartea funciară, geodezia/topografia și cartografia;

- în baza Legii nr. 7/1996 a cadastrului şi a publicităţii imobiliare, republicată, a fost înfiinţat sistemul integrat de cadastru şi carte funciară, care cuprinde evidenţa tehnică, economică şi juridică a imobilelor din aceeaşi unitate administrativ-teritorială: comună, oraş sau municipiu;

- sistemul informatic integrat este utilizat la nivel naţional de către Agenția Națională de Cadastru și Publicitate Imobiliară şi instituţiile sale subordonate, ca mediu de lucru unic. Oficiile de cadastru și publicitate imobiliară prelucrează date cu caracter personal prin intermediul acestui sistem şi colectează/arhivează documentele pe format de hârtie;

- oficiile de cadastru și publicitate imobiliară au acces la sistemul integrat de cadastru și carte funciară (e-Terra 3) ca utilizator, prin alocarea de nume de utilizator și parolă pentru angajații care au acces, potrivit atribuțiilor de serviciu. Alocarea numelui de utilizator și a parolei se face de către Agenția Națională de Cadastru și Publicitate Imobiliară;

- prin sistemul integrat de cadastru şi carte funciară se realizează:

a) identificarea, descrierea şi înregistrarea în documentele cadastrale a imobilelor prin natura lor, măsurarea şi reprezentarea acestora pe hărţi şi planuri cadastrale, precum şi stocarea datelor pe suporturi informatice;

b) identificarea şi înregistrarea proprietarilor, a altor deţinători legali de imobile şi a posesorilor;

c) furnizarea datelor necesare sistemului de impozite şi taxe pentru stabilirea corectă a obligaţiilor fiscale ale contribuabililor, solicitate de instituţiile abilitate;

d) publicitatea imobiliară, care asigură opozabilitatea drepturilor reale imobiliare, a drepturilor personale, a actelor şi faptelor juridice, precum şi a oricăror raporturi juridice supuse publicităţii, referitoare la imobile.

- autorităţile şi instituţiile publice centrale şi locale au obligaţia de a pune la dispoziţia Agenţiei Naţionale de Cadastru și Publicitate Imobiliară, gratuit, datele, informaţiile şi copiile certificate ale documentelor referitoare la sistemele informaţionale specifice domeniilor proprii de activitate, pentru lucrările sistematice de cadastru în vederea înscrierii în cartea funciară;

- la nivelul oficiilor de cadastru și publicitate imobiliară, există proceduri referitoare la circuitul și manipularea documentelor pe format de hârtie și administrarea infrastructurii de comunicații;

- s-au stabilit proceduri referitoare la asigurarea confidențialității și securității datelor cu caracter personal;

- informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001 se realizează prin afișare la sediu/pe site-ul web al oficiului;

- s-a constatat instalarea la sediu a unui sistem de supraveghere video.

În funcție de constatările rezultate pe teren, pentru operatorii investigați au fost emise recomandări privind:

- completarea politicii privind măsurile minime de securitate și confidențialitate a prelucrărilor de date cu caracter personal efectuate în cadrul activității specifice;

- adoptarea măsurilor tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal;

- notificarea prelucrării datelor cu caracter personal în scopul monitorizării/securității persoanelor, spaţiilor şi/sau bunurilor publice/private, prin sistemul de supraveghere video;

- completarea informării persoanelor vizate cu mențiuni referitoare la toate scopurile în care sunt prelucrate date cu caracter personal, conform art. 12 din Legea nr. 677/2001 și în condițiile art. 11 din Decizia Președintelui ANSPDCP nr. 52/2012.

**2. Respectarea prevederilor Legii nr. 677/2001 și ale Legii nr. 506/2004, referitor la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit (instituții financiare bancare/nebancare)**

În anul 2017, Autoritatea națională de supraveghere a desfășurat în continuare investigații din oficiu la instituțiile financiare bancare și nebancare participante la sistemul de

evidență al biroului de credit cu privire la prelucrările de date cu caracter personal în sisteme de evidență de tipul birourilor de credit. Au fost supuse controlului un număr de **17 entități** care prelucrează date cu caracter personal în sisteme de evidenţă de tipul birourilor de credit, iar cuantumul total al sancțiunilor aplicate a fost de **220.000 lei**.

Controalele efectuate au vizat verificarea respectării prevederilor Legii nr. 677/2001 și ale Deciziei Președintelui ANSPDCP nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit, în special în ceea ce privește respectarea drepturilor persoanelor vizate.

În cadrul controalelor efectuate au fost solicitate informații referitoare la rapoartele de credit ale clienților care au fost raportați la biroul de credit cu debite restante, notificările (informările) transmise clienţilor cu privire la faptul că aceştia urmează să fie raportaţi, conform Deciziei Președintelui ANSPDCP nr. 105/2007, precum și dovada transmiterii acestor notificări.

Ca urmare a investigațiilor desfășurate, s-a constatat că majoritatea instituțiilor financiare bancare/nebancare supuse controlului realizau raportări la biroul de credit fără respectarea dispozițiilor legale, fiind sancționate 11 entități din cele 17 controlate.

Principalele deficiențe constatate în activitatea de prelucrare a datelor cu caracter personal realizată de instituțiile financiare bancare/nebancare în sistemele de evidență de tipul birourilor de credit au fost următoarele:

- transmiterea de date negative cu încălcarea dispozițiilor art. 5 alin. (1) din Decizia Președintelui ANSPDCP nr. 105/2007, care prevede că datele negative se transmit către sistemele de evidență de tipul birourilor de credit după 30 de zile de la data scadenței;

- transmiterea de date negative cu încălcarea dispozițiilor art. 8 alin. (2) din Decizia Președintelui ANSPDCP nr. 105/2007, care prevede că datele negative se transmit către sistemele de evidență de tipul birourilor de credit numai după înștiințarea prealabilă a persoanei vizate, realizată de către participanți cu cel puțin 15 zile calendaristice înainte de data transmiterii;

- transmiterea către clienţi a notificărilor (informărilor) cu privire la faptul că aceştia urmează să fie raportaţi cu debite restante fără respectarea prevederilor art. 9 alin. (1) din Decizia Președintelui ANSPDCP nr. 105/2007.

Față de aspectele constatate în urma controalelor efectuate, s-au recomandat instituțiilor financiare bancare și nebancare verificate următoarele:

- să adopte măsuri necesare în vederea respectării tuturor prevederilor Deciziei Președintelui ANSPDCP nr. 105/2007 pentru prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit;

- să întreprindă măsurile necesare pentru ştergerea informațiilor transmise ca date negative la biroul de credit, fără realizarea informării prealabile potrivit art. 8 alin. (2) din Decizia Președintelui ANSPDCP nr. 105/2007.

**3. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de operatorii care au ca obiect de activitate închirierea și leasing-ul de autoturisme și vehicule rutiere ușoare**

Autoritatea națională de supraveghere a dispus efectuarea unor investigații la entități care prelucrează date cu caracter personal în cadrul activităților de închiriere și leasing de autoturisme și vehicule rutiere ușoare. Au fost supuși controlului un număr de 16 operatori.

Ca urmare a investigațiilor desfășurate, s-a constatat că datele personale prelucrate pentru scopul de închiriere de autoturisme sunt, în general, aceleași, și anume cele necesare încheierii contractului de închiriere: nume, prenume, adresă domiciliu, nr. telefon, adresă e-mail, data nașterii, permis de conducere, alte date din cartea de identitate sau pașaport.

Pe lângă acestea, majoritatea operatorilor colectează copii ale actelor de identitate, cum ar fi: cărți de identitate, pașapoarte, permise de conducere. Colectarea acestor copii se efectuează atât direct, la punctele de închiriere autoturisme, cât și on-line, prin formulare de rezervare existente pe site-urile operatorilor. Refuzul de a anexa copii ale actelor de identitate la formularele de rezervare on-line, conform declarațiilor operatorilor, duce la anularea rezervării.

De asemenea, copii ale actelor de identitate erau solicitate clienților și în alte situații, precum în cazul solicitărilor de împuternicire pentru ieșire din țară cu autoturismul sau în cazul accidentelor auto, în vederea întocmirii dosarelor de daună.

Pentru colectarea și prelucrarea datelor cu caracter personal existente în copiile actelor de identitate, majoritatea operatorilor controlați nu au putut face dovada existenței consimțământului expres prevăzut de art. 5 din Legea nr. 677/2001, în lipsa unui temei legal sau a unui aviz al Autorității naționale de supraveghere, și nici nu au făcut dovada informării persoanelor vizate potrivit art. 12 din Legea nr. 677/2001.

O parte dintre operatorii verificați aveau instalate sisteme de monitorizare prin geolocalizare (GPS), iar alții urmau să instaleze asemenea sisteme. Prin utilizarea acestor dispozitive de monitorizare sunt prelucrate date cu caracter personal care permit, direct sau indirect, localizarea geografică a persoanelor fizice, chiar dacă acestea sunt instalate pe autoturismele închiriate.

În majoritatea cazurilor, persoanele fizice care solicitau închirierea de autoturisme erau informate în ceea ce privește existența acestor dispozitive, dar nu erau informate potrivit art. 12 din Legea nr. 677/2001 și nici cu privire la faptul că li se prelucrau datele personale furnizate de sistemele de monitorizare prin GPS. Niciunul dintre operatorii investigați nu notificase prelucrarea datelor cu caracter personal în scopul de monitorizare prin geolocalizare.

În ceea ce privește asigurarea măsurilor minime de securitate și confidențialitate a prelucrărilor de date cu caracter personal, majoritatea operatorilor controlați nu au putut demonstra îndeplinirea unor astfel de măsuri tehnice și organizatorice pentru a asigura confidențialitatea și integritatea datelor personale.

Ca urmare a verificărilor efectuate de Autoritatea națională de supraveghere la operatorii care prelucrează date cu caracter personal având ca obiect principal de activitate închirierea și leasing-ul de autoturisme și vehicule rutiere ușoare, au fost recomandate măsuri de remediere a deficiențelor constatate, precum:

- notificarea prelucrărilor de date cu caracter personal efectuate pentru cazurile în care subzistă obligativitatea notificării;

- întocmirea și implementarea politicilor sau a procedurilor privind măsurile minime de securitate și luarea măsurilor tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal;

- informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001;

- respectarea prevederilor art. 8 din Legea nr. 677/2001 și a art. 2 și art. 6 din Decizia Președintelui ANSPDCP nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

Totodată, au fost aplicate măsuri contravenționale pentru prelucrarea nelegală a datelor cu caracter personal și neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate conform legislației în vigoare.

**4. Respectarea prevederilor Legii nr. 677/2001 și ale Legii nr. 506/2004, referitor la prelucrările de date cu caracter personal efectuate în cadrul activității desfășurate de către societățile de salubritate**

Au fost supuse controlului Autorității naționale de supraveghere un număr de 9 entități care prelucrează date cu caracter personal în scopul prestării serviciilor de salubritate. Ca urmare a neregulilor constatate, au fost aplicate sancțiuni cu amendă în cuantum total de 62000 lei.

În cadrul controalelor efectuate au fost verificate, în principal, următoarele aspecte: respectarea drepturilor persoanelor vizate, realizarea informării persoanelor vizate potrivit art. 12 din Legea nr. 677/2001, respectarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal, respectarea condițiilor prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004 la nivelul site-urilor proprii.

Ca urmare a controalelor efectuate, s-a constatat că societățile care prestează servicii de salubritate prelucrează date cu caracter personal în mai multe scopuri: prestări servicii salubritate; resurse umane; monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor publice/private; prelucrarea datelor cu caracter personal care permit, direct sau indirect, localizarea geografică a persoanelor fizice prin intermediul sistemelor de geolocalizare; prelucrarea datelor cu caracter personal prin utilizarea tahografelor digitale în scopul înregistrării activității conducătorilor auto în ceea ce privește perioadele de conducere, pauzele și perioadele de odihnă.

Principalele deficiențe constatate în activitatea de prelucrare a datelor cu caracter personal realizată de către societățile de salubritate au fost următoarele:

- prelucrarea datelor cu caracter personal cu încălcarea dispozițiilor art. 12 din Legea nr. 677/2001, privind informarea persoanelor vizate;

- nerespectarea art. 8 din Legea nr. 677/2001 și a art. 2 și art. 6 din Decizia Președintelui ANSPDCP nr. 132/2011, prin colectarea și stocarea codului numeric personal și a seriei și numărului actului de identitate, cât și a celorlalte date conținute în actul de identitate, prin reținerea unei copii a actului de identitate al persoanelor fizice cu care operatorul investigat a încheiat contracte de prestări servicii de salubritate, fără a avea consimțământul expres al acestora, în lipsa unui temei legal sau a unui aviz al ANSPDCP;

- neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate a prelucrărilor de date cu caracter personal. În cadrul controalelor efectuate, s-a constatat că

operatorii investigați nu au întocmit și implementat o politică/procedură privind măsurile minime de securitate a prelucrărilor de date cu caracter personal pe care le efectuează și nu au luat măsuri tehnice și organizatorice pentru a asigura confidențialitatea și integritatea datelor cu caracter personal;

- nerespectarea condițiilor prevăzute la art. 4 alin. (5) din Legea nr. 506/2004, modificată și completată, întrucât societățile de salubritate supuse controlului, la nivelul site-urilor proprii, nu au îndeplinit, în mod cumulativ, cerințele de obținere a acordului utilizatorului pentru cookie-urile existente la nivelul site-urilor proprii și de furnizare, anterior exprimării acordului, a informațiilor privind scopul general al procesării informațiilor stocate, durata de viață, ce informații sunt stocate și accesate, precum și permiterea stocării și/sau accesului unor terți la informațiile stocate în echipamentul terminal al utilizatorului;

- omisiunea de a notifica prelucrarea datelor cu caracter personal, cu încălcarea dispozițiilor art. 22 din Legea nr. 677/2001.

Față de aspectele constatate în urma controalelor efectuate, s-au emis următoarele recomandări: realizarea informării persoanelor vizate pentru toate scopurile de prelucrare a datelor cu caracter personal, conform art. 12 din Legea nr. 677/2001; întocmirea și implementarea de proceduri privind măsurile minime de securitate a prelucrărilor de date cu caracter personal și luarea de măsuri tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal, pentru toate sistemele de evidență utilizate; luarea de măsuri pentru respectarea prevederilor Deciziei Președintelui ANSPDCP nr. 132/2011, în ceea ce privește reținerea unei copii a actului de identitate al persoanelor fizice, precum și distrugerea copiilor colectate cu încălcarea prevederilor legale privind protecția datelor cu caracter personal; luarea de măsuri privind respectarea dispozițiilor Legii nr. 506/2004 la nivelul website-urilor proprii; notificarea prelucrării datelor cu caracter personal potrivit art. 22 din Legea nr. 677/2001 și având în vedere prevederile Deciziei Președintelui ANSPDCP nr. 200/2015.

**PREZENTARE CAZURI**

**1. FIȘĂ DE CAZ** – Afișare listă datornici pe site-ul unei companii regionale de apă

Ca urmare a unei sesizări privind afișarea pe website-ul unei companii regionale de apă a unei liste a datornicilor, în care sunt menționate adresele exacte ale abonaților cu restanțe (nume, prenume, adresă, datorie) de către o companie regională de apă, a fost dispusă o investigație în scris de la sediul ANSPDCP.

La data desfășurării controlului, din verificările efectuate la adresa de website unde a fost postată lista datorniciilor, s-a constatat că operatorul, respectiv compania regională de apă, care postase inițial o listă a utilizatorilor – particulari (persoane fizice), din centrul zonal al municipiului respectiv, cu facturi emise până la data de 30.06.2017, neachitate la data de 27.09.2017 (cu peste 80 zile întârziere de la data emiterii facturii), care conținea nume, prenume, localitate, adresă, sold restant, a intervenit asupra conținutului datelor postate, modificând lista utilizatorilor din punct de vedere al conținutului datelor (nume, prenume și sold restant).

Raportat la prevederile art. 2 lit. i), art. 36 alin. (3), art. 42 alin. (11) din Legea nr. 51 din 2006 a serviciilor comunitare de utilități publice, s-a reținut că există reglementări în cazul neachitării facturilor emise și că nu se prevede posibilitatea notificării utilizatorilor prin publicarea datelor personale ale acestora pe Internet.

Cu toate acestea, respectiva companie regională de apă a prelucrat datele cu caracter personal ale utilizatorilor (nume, prenume și sold restant), fără ca Legea nr. 51 din 2006 a serviciilor comunitare de utilități publice, republicată, să prevadă posibilitatea notificării prin publicarea datelor utilizatorilor pe Internet.

Acest fapt a demonstrat că operatorul, respectiva companie regională de apă, a încălcat art. 4 alin. 1 lit. a) din Legea nr. 677/2001, deoarece a prelucrat datele cu caracter personal ale utilizatorilor (nume, prenume și sold restant), fără ca prelucrarea să fie legitimată în baza unor prevederi legale, și art. 4 alin. 1 lit. c), întrucât datele cu caracter personal trebuie să fie adecvate, pertinente și neexcesive prin raportare la scopul prelucrării, existând posibilitatea utilizării unui element de identificare a utilizatorilor (cod client, nr. contract, ID) pentru numele și prenumele utilizatorilor din listă.

S-a constatat săvârşirea următoarelor fapte:

*„Prelucrarea nelegală a datelor cu caracter personal”,* prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 4 lit a) și c) din Legea nr. 677/2001.

Pentru faptele constatate, s-a aplicat amendă contravențională în cuantum de 5.000 lei.

**2. FIȘĂ DE CAZ** – Dezvăluirea codului numeric personal de către o asociație județeană a vânătorilor și pescarilor sportivi

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în îndeplinirea atribuțiilor sale legale prevăzute de Legea nr. 677/2001 și de Legea nr. 102/2005, s-a autosesizat cu privire la o posibilă dezvăluire neautorizată, de către o Asociație, a codului numeric personal al mai multor membri ai asociației, prin publicarea în presa locală a unei liste cu membrii care au fost sancționați.

În contextul Legii nr. 677/2001 și al Deciziei Președintelui ANSPDCP nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, potrivit art. 8 din Legea nr. 677/2001, prelucrarea datelor cu caracter personal având funcție de identificare, respectiv prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, poate fi efectuată numai dacă persoana vizată și-a dat în mod expres consimțământul sau prelucrarea este prevăzută în mod expres de o dispoziție legală.

Totodată, art. 2 din Decizia Președintelui ANSPDCP nr. 132/2011 prevede că prelucrarea (de ex. colectarea, utilizarea, dezvăluirea etc.) codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală se realizează numai în condițiile stabilite la art. 8 din Legea nr. 677/2001, și anume:

a) persoana vizată și-a dat în mod expres consimțământul; sau

b) prelucrarea este prevăzută în mod expres de o dispoziție legală; sau

c) în alte cazuri, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

Ca urmare a verificărilor efectuate de către Autoritatea națională de supraveghere, s-a constatat că respectiva Asociație a solicitat unei publicații locale, publicarea Hotărârii privind sancționarea și excluderea unor membri din cadrul asociației, care conținea datele personale ale membrilor asociației, inclusiv CNP, fiind dezvăluite publicului larg date cu caracter personal, inclusiv codul numeric personal, prin încălcarea art. 5 și art. 8 din Legea nr. 677/2001 și a art. 2 din Decizia Președintelui ANSPDCP nr. 132/2011.

Față de cele constatate, operatorul a fost sancționat contravențional în baza art. 32 raportat la art. 5 și art. 8 din Legea nr. 677/2001 și art. 2 din Decizia Președintelui ANSPDCP nr. 132/2011, coroborat cu art. 8 din Ordonanța Guvernului nr. 2/2001.

**3. FIȘĂ DE CAZ** – Dezvăluire neautorizată a rezultatelor unor analize medicale de către un centru medical

Ca urmare a unor informații apărute în spațiul public, Autoritatea națională de supraveghere s-a sesizat din oficiu referitor la cazul unei persoane fizice care, în urma efectuării unor analize medicale (RMN), a primit rezultatul conținând analizele medicale ale unei alte persoane fizice.

Operatorul investigat a precizat că raportul medical RMN introdus în aplicația informatică utilizată pentru evidența pacienților, pe numele unui pacient, a fost completat în mod eronat cu descrierea anatomică a investigației unui alt pacient, examinat anterior, și a fost transmis prin intermediul poștei electronice către primul pacient.

În cadrul investigației efectuate, s-a constatat că operatorul investigat nu a luat suficiente măsuri tehnice și organizatorice în ceea ce privește reglementarea accesului la aplicația informatică utilizată pentru evidența propriilor pacienți, precum și transmiterea rezultatelor analizelor pacienților prin intermediul poștei electronice, ceea ce a condus la accesul neautorizat la datele cu caracter personal privind starea de sănătate a persoanelor vizate (pacienți), modificarea datelor de sănătate ale acestora înregistrate în aplicația informatică și dezvăluirea neautorizată către terți.

În baza acestor constatări, operatorul investigat a fost sancţionat contravenţional pentru săvârșirea contravențiilor prevăzute de art. 32 și art. 33 din Legea nr. 677/2001, întrucât acesta **nu a luat măsurile necesare pentru ca datele de sănătate ale pacienților proprii să fie exacte și actualizate**, ceea ce a permis ca în aplicația informatică să fie prelucrate date de sănătate inexacte, prin introducerea în raportul medical al unui pacient, a descrierii anatomice a investigației altui pacient, și **nu a aplicat măsurile tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii**, **modificării, dezvăluirii sau accesului neautorizat**, ceea ce a permis accesul neautorizat la datele cu caracter personal privind starea de sănătate a

persoanelor vizate/pacienți, modificarea datelor de sănătate înregistrate în aplicația informatică și dezvăluirea acestora către alți pacienți decât cei cărora le aparțineau datele de sănătate.

## Secţiunea a 3-a Activitatea de soluţionare a plângerilor şi sesizărilor

### I. Prezentare generală

Una dintre principalele atribuții legale prin care Autoritatea națională de supraveghere își îndeplinește obiectivul pentru care a fost înființată prin Legea nr. 102/2005, acela de apărare a drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, în legătură cu prelucrarea datelor personale și cu libera circulație a acestor date, constă în soluționarea plângerilor și a sesizărilor ce vizează încălcarea acestui drept.

Persoanele fizice se pot adresa cu plângeri în cazul în care se consideră lezate prin modul de prelucrare a datelor lor personale de către operatorii de date sau persoanele împuternicite de aceștia; de asemenea, orice persoană poate sesiza Autoritatea națională de supraveghere asupra aspectelor legate de prelucrarea datelor personale, care ar putea să contravină dispozițiilor legale. În scopul informării celor interesați, pe pagina de Internet a autorității sunt disponibile atât modele de plângere, cât și o procedură detaliată privind condițiile în care sunt înregistrate, analizate și soluționate plângerile și sesizările ce privesc posibile încălcări ale Legii nr. 677/2001 sau ale Legii nr. 506/2004.

Pentru a fi considerate admisibile plângerile, Legea nr. 677/2001 stipulează o serie de condiții: persoanele vizate nu trebuie să fi introdus anterior o acţiune în justiţie cu acelaşi obiect şi cu aceleași părți; persoanele vizate trebuie să fi înaintat anterior (15 zile) o cerere cu acelaşi conţinut către operatorul de date de la care nu a primit un răspuns sau răspunsul a fost unul nesatisfăcător.

În anul 2017 majoritatea plângerilor primite au fost soluționate prin efectuarea de investigații, în condițiile prevăzute de art. 25 și art. 27 din Legea nr. 677/2001.

Astfel, spre deosebire de anii precedenți, se observă un număr mult mai mic al plângerilor care au fost respinse pentru neîndeplinirea procedurii legale prealabile de către petenţi. O explicație a acestei situații ar putea fi formularea unui număr considerabil al

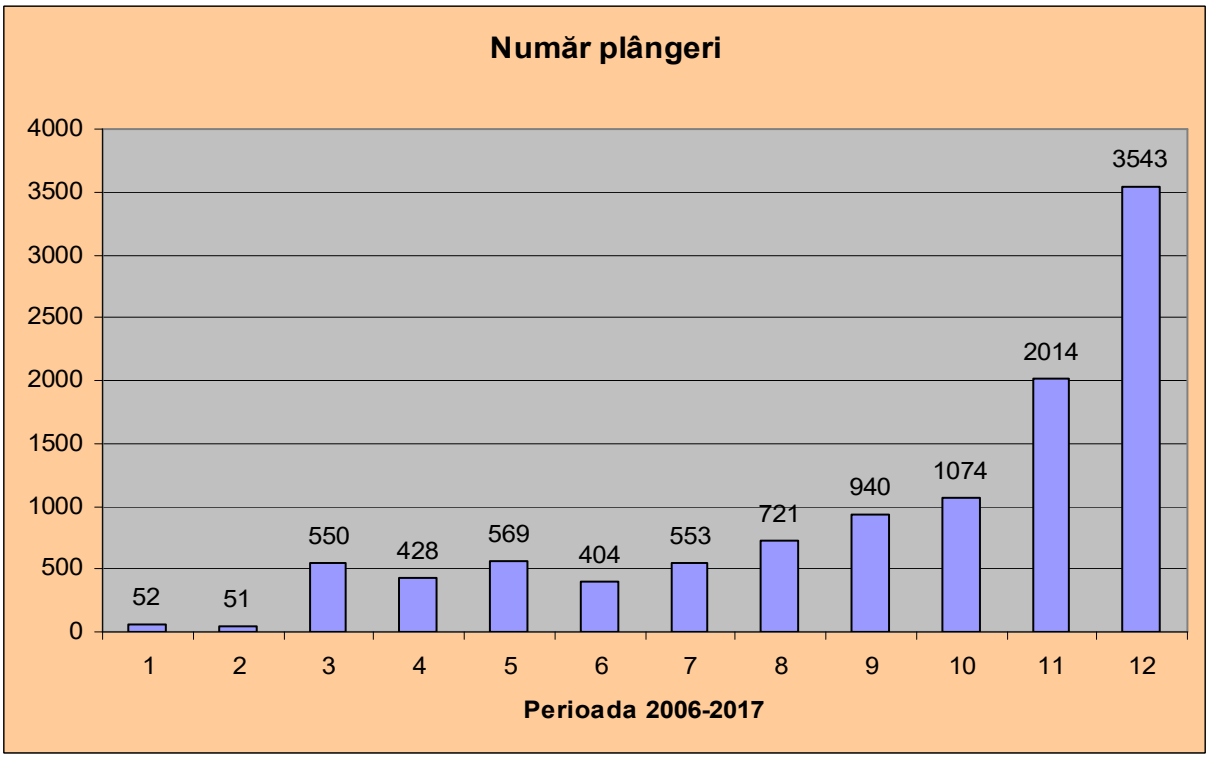
plângerilor prin intermediul reprezentanților (cabinete de avocatură, asociații, societăți de consultanță etc.).

Printre alte considerente pentru care plângerile și sesizările nu au putut fi reținute în vederea efectuării unor demersuri de către autoritate pot fi enumerate: neprezentarea dovezilor în susţinerea aspectelor reclamate sau a calității de reprezentant al persoanei vizate (ex. lipsa împuternicirii avocațiale sau a unui mandat emis conform dispozițiilor legale aplicabile); sesizarea unor fapte în legătură cu care Autoritatea națională de supraveghere nu deține competenţa legală materială (ex. aspecte care țin de aplicarea legislației din domeniul protecției drepturilor consumatorilor sau din domeniul dreptului penal) sau competența teritorială să intervină (ex. prelucrări efectuate pe teritorul altui stat); imposibilitatea identificării exacte a entității reclamate (ex. neidentificarea certă a expeditorului unei comunicări comerciale electronice nesolicitate sau a deținătorului unui website); preexistența unui litigiu pe rolul instanțelor judecătorești cu identitate de părți și obiect.

În anul 2017, numărul petițiilor soluționate de compartimentul de specialitate din cadrul Autorității naționale de supraveghere aproape s-a dublat prin raportare la anul 2016. Astfel, au fost primite şi soluţionate un total de **3831 petiții** (față de 2302 în 2016), din care **3543 plângeri și 191 sesizări**. Din conținutul petițiilor, se poate constata că această creștere considerabilă a numărului petițiilor primite în cursul anului 2017 este rezultatul unei mai bune cunoașteri a atribuţiilor legale ale Autorităţii naționale de supraveghere de către persoanele fizice prin comparație cu perioada anterioară și al creșterii încrederii petiționarilor în acțiunile Autorității naționale de supraveghere pentru respectarea drepturilor și libertăților lor.

Având în vedere evoluția exponențială a numărului plângerilor adresate în perioada 2006-2017 (numărul lor a crescut **de peste 75 de ori** față de primul an de activitate), considerăm ca fiind presantă necesitatea de sporire a numărului de personal al Autorității naționale de supraveghere implicat în această activitate, mai ales în perspectiva implementării din 25 mai 2018 a noului regulament general privind protecția datelor personale în toate statele membre ale Uniunii Europene. Potrivit viitorului cadru legislativ, orice persoană vizată va avea 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 a regulamentului.

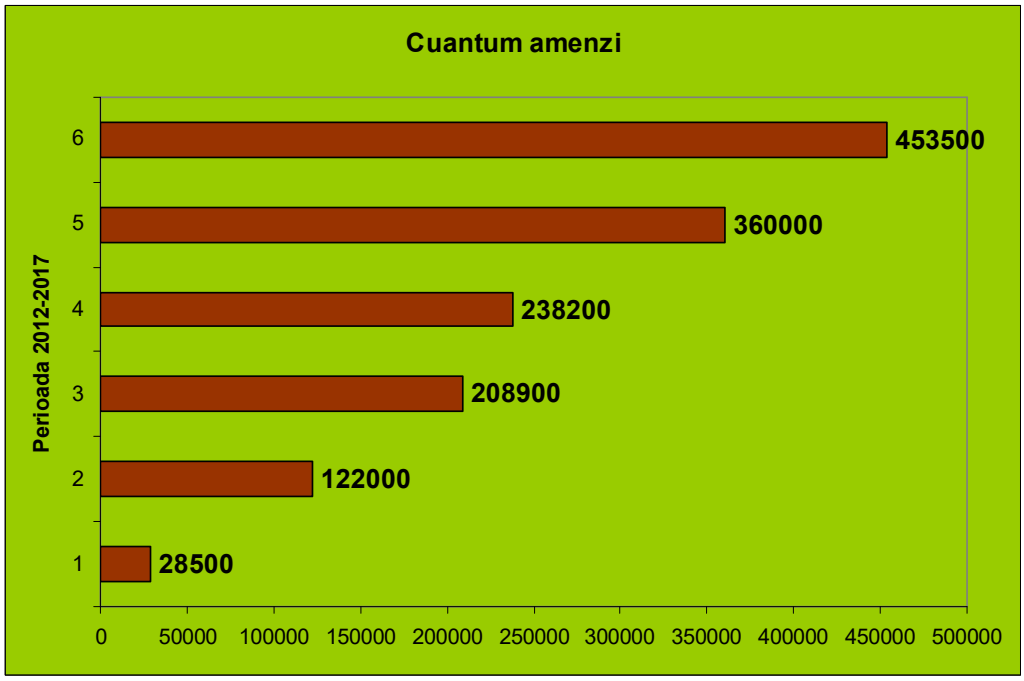
**Figura 1: Numărul plângerilor în perioada 2006-2017**




Pentru soluţionarea plângerilor şi sesizărilor primite, au fost efectuate **724** de **investigații**, dintre care **635** de **investigații în scris**. În **107 cazuri**, investigațiile au fost finalizate prin încheierea la sediul Autorității naționale de supraveghere a unor procese-verbale de constatare/sancționare.

Astfel, comparativ cu anul 2016, se poate constata că activitatea de soluționare a plângerilor/sesizărilor **aproape s-a dublat**, iar în cazul investigațiilor în scris, numărul acestora **a crescut de peste două ori**. Cu ocazia investigaţiilor efectuate pentru soluționarea plângerilor și sesizărilor, au fost aplicate sancţiuni contravenţionale, cuantumul total al amenzilor aplicate în 2017 fiind de **453.500 lei**.

**Figura 2: Cuantumul amenzilor aplicate în activitatea de soluţionare a plângerilor şi sesizărilor în perioada 2012-2017**




Totodată, în urma demersurilor de soluţionare a plângerilor şi sesizărilor adresate Autorității naționale de supraveghere, a fost emisă o **recomandare** transmisă Ministerului Justiției.

Plângerile şi sesizările primite au vizat o gamă largă de domenii, însă în anul 2017, cele mai multe dintre plângeri au vizat prelucrarea datelor personale în următoarele domenii: sectorul financiar-bancar, monitorizarea spaţiilor publice sau private prin mijloace de supraveghere video, sectorul comunicaţiilor electronice, dezvăluirea datelor către diverse entități, diseminarea datelor pe Internet. S-a remarcat, printre altele, problematica prelucrării datelor biometrice în contextul relațiilor de muncă, precum și a colectării și prelucrării ilegale a codului numeric personal și a copiei actului de identitate, care au făcut obiectul unora dintre petițiile transmise Autorității naționale de supraveghere. De asemenea, indiferent de domeniul de activitate al operatorilor, multe dintre plângerile primite au avut ca obiect nerespectarea condițiilor legale ce privesc exercitarea drepturilor persoanelor vizate (drepturile de informare, acces, intervenție, opoziție).

Astfel, în sectorul financiar-bancar, operatorii reclamați sunt, în principal, bănci, instituţii financiare nebancare, societăți de recuperări creanțe și societăți care dețin sisteme de evidență

de tipul birourilor de credit. În 2017, s-a constatat o creştere majoră a numărului petiţiilor, probabil pe fondul creșterii numărului de solicitări de credite, ocazie cu care se constată existența unui istoric negativ înregistrat la biroul de credit, ceea ce afectează implicit bonitatea și eligibilitatea unei persoane. Prin urmare, principalul motiv de nemulţumire a persoanelor vizate, care a determinat sesizarea Autorității naționale de supraveghere, a fost legat de raportarea datelor personale către sisteme de evidenţă de tip birou de credit, fără respectarea prevederilor Legii nr. 677/2001 şi ale Deciziei Președintelui ANSPDCP nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit, în vigoare din luna februarie 2008.

O serie de plângeri și sesizări s-au referit în 2017 la prelucrarea datelor personale prin mijloace de supraveghere video, domeniu reglementat de Autoritatea națională de supraveghere prin Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video. Operatorii reclamaţi au fost în principal asociaţii de proprietari, diverse categorii de angajatori care au instalat un sistem de supraveghere la locul de muncă, precum și persoane fizice care au montat camere de supraveghere video ce surprind imagini din spațiul public.

În anul 2017 au fost înregistrate, de asemenea, o serie de petiţii având ca obiect dezvăluirea datelor personale pe Internet, fără consimțământul persoanelor vizate sau alt temei legal. Operatorii reclamaţi au fost societăţi care administrează diferite site-uri de socializare, societăți care au preluat și diseminat informații din dosarele aflate pe rolul instanțelor judecătorești, precum și autorități/instituții publice. De asemenea, Autoritatea națională de supraveghere a continuat să primească plângeri în anul 2017, într-un număr mult mai scăzut față de perioada anterioară, care au vizat nerespectarea de către Google a ”dreptului de a fi uitat”, urmare a refuzului acestei companii de a da curs cererilor prin care se solicita dezindexarea de pe Internet a rezultatelor căutărilor asociate numelui unei persoane.

O pondere semnificativă a fost reprezentată de plângerile prin care petiționarii au sesizat Autoritatea națională de supraveghere cu privire la primirea de mesaje comerciale nesolicitate prin mijloace electronice de comunicare. Operatorii reclamați au fost, în principal, societați care efectuează activități de comerţ on-line sau marketing direct și furnizori de servicii de comunicații electronice.

În urma investigaţiilor realizate în 2017, au fost constatate în continuare încălcări ale prevederilor actelor normative în domeniul protecției datelor cu caracter personal de către operatori, ca urmare a nerespectării sau ignorării obligațiilor care le revin potrivit legii.

În majoritatea cazurilor investigate, operatorii au implementat măsurile dispuse de Autoritatea națională de supraveghere (ex. ștergerea datelor prelucrate ilegal, eliminarea rezultatelor afișate pe Internet, transmiterea unor răspunsuri adecvate persoanelor care și-au exercitat drepturile prevăzute de lege etc.), astfel încât să fie respectate reglementările în vigoare din materia protecției datelor personale.

## II. Principalele constatări rezultate din activitatea de soluționare a plângerilor și sesizărilor

### *1. Raportarea datelor personale către sisteme de evidență tip birou de credit*

În anul 2017 numărul plângerilor care au avut ca obiect transmiterea datelor personale către biroul de credit a crescut în mod exponențial, ocupând prima poziție ca pondere în numărul total al petițiilor primite de Autoritatea națională de supraveghere.

În general, persoanele care au formulat o astfel de plângere au luat la cunoștință despre existența datelor negative (întârzieri la plata ratelor de credit) în sistemul de evidență al biroului de credit cu ocazia solicitării altor produse bancare, uneori trecând mai mulți ani după ce datele lor fuseseră transmise de către participanții la acest sistem. Prin urmare, lipsa informării prealabile, corecte și complete, condiție obligatorie impusă de Decizia nr. 105/2007 pentru a putea fi raportate date negative de către bănci sau instituții financiare nebancare, a constituit principalul motiv pentru care s-a solicitat intervenția instituției noastre.

Numărul ridicat al plângerilor primite în acest domeniu a determinat ca efectuarea investigațiilor să se realizeze în majoritatea cazurilor în scris, solicitându-se clarificarea circumstanțelor în care au fost transmise date negative către biroul de credit pentru fiecare dintre plângerile particulare primite. În cadrul unora dintre investigaţiile desfăşurate, s-a constatat nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul biroului de credit, cu referire la: tipul de informaţii raportate de către bănci și instituțiile financiare nebancare, modalitatea şi termenul de realizare a informării prealabile impuse de Legea nr. 677/2001 şi de Decizia nr. 105/2007, termenul și frecvența raportărilor în cursul unei luni.

În cazurile în care, în urma investigațiilor efectuate, s-a constatat că băncile/instituțiile financiare nebancare nu au dat curs în mod voluntar cererilor formulate de petenți sau recomandărilor adresate cu ocazia acestor investigații, Autoritatea națională de supraveghere a dispus sancționarea contravențională a acestor operatori, cu solicitarea de a fi șterse sau modificate, după caz, datele personale transmise la biroul de credit fără respectarea legii. În toate aceste cazuri, s-a pus în vedere operatorilor să adopte măsuri pentru ca prelucrarea datelor personale pe care o realizează în legătură cu sistemele de evidență de tipul biroului de credit să se efectueze cu respectarea dispozițiilor legale.

O situație particulară o reprezintă investigațiile demarate la nivelul biroului de credit și al participanților la acest sistem, pentru clarificarea condițiilor în care se utilizează o analiză de tip scoring (FICO), reclamată în multe dintre plângerile adresate instituției noastre. În urma investigațiilor realizate în acest caz, s-a aplicat o sancțiune contravențională în baza Legii nr. 677/2001, iar în luna martie a anului 2018 s-a dispus, prin **decizia** președintelui Autorității naționale de supraveghere, suspendarea prelucrării numărului de interogări în cadrul scorului FICO până la data la care vor fi prezentate garanții privind respectarea regulilor generale de prelucrare a datelor cu caracter personal și a drepturilor persoanei vizate.

***FIȘĂ DE CAZ***

*Un petent a reclamat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o bancă, despre care susținea că i-a transmis la biroul de credit date pozitive și negative, fără înștiințarea sa prealabilă conform legii și Deciziei nr. 105/2007. Petentul s-a adresat băncii cu o cerere scrisă prin care și-a exercitat drepturile prevăzute de lege și printre altele, a solicitat ca datele sale personale, transmise fără respectarea dispozițiilor legale, să fie șterse.*

*Pentru soluționarea petiției, s-a efectuat o investigație la bancă, în urma căreia s-a constatat faptul că banca nu a furnizat dovezi din care să reiasă că a realizat informarea prealabilă a petentului cu privire la transmiterea datelor negative cu care acesta figura în continuare în evidențele biroului de credit.*

*Totodată, banca a refuzat să dea curs cererii petentului prin care acesta şi-a exercitat dreptul de intervenţie referitor la ștergerea datelor negative transmise la biroul de credit fără respectarea prevederilor legale. Răspunsurile trimise de bancă au fost transmise cu încălcarea termenului de 15 zile prevăzut de art. 14 din Legea nr. 677/2001.*

*În acest context, banca în cauză a fost sancționată contravențional pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, prin raportare la art. 4, 12 și 14 din Legea nr. 677/2001, coroborate cu prevederile Deciziei nr. 105/2007. Totodată, s-a pus în vedere băncii să șteargă informațiile negative transmise la biroul de credit fără respectarea dispozițiilor legale aplicabile.*

***FIȘĂ DE CAZ***

*Prin petiţia transmisă, petentul a reclamat faptul că o bancă a solicitat eliberarea unui raport de la biroul de credit, pe numele său, fără să existe consimțământul său. În acest sens, s-a adresat respectivei bănci cu o cerere prin care și-a exercitat dreptul de acces, în baza art. 13 din Legea nr. 677/2001.*

*În cadrul investigaţiei efectuate în acest caz, a rezultat faptul că banca a prelucrat datele petentului, în legătură cu o interogare efectuată la biroul de credit, în scopul inițierii unei relații de creditare, la care petentul a renunțat ulterior, în baza unui acord de transmitere, prelucrare și consultare a informațiilor la biroul de credit, document semnat, dar nedatat.*

*De asemenea, banca, deși a răspuns petentului în termenul legal de 15 zile la cererea sa, nu i-a furnizat toate informațiile solicitate potrivit art. 13 alin. (1) din Legea nr. 677/2001.*

*În baza acestor constatări, banca a fost sancţionată contravenţional în baza art. 32, pentru încălcarea prevederilor art. 5 și 13 din Legea nr. 677/2001 și i s-a pus în vedere să formuleze un răspuns complet la cererea petentului. Banca s-a conformat cerințelor impuse de Autoritatea națională de supraveghere.*

***FIȘĂ DE CAZ***

*Prin petiţiile transmise, mai mulți petenți au sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o bancă, prin faptul că figurează cu date negative raportate la biroul de credit, deşi nu au fost înştiinţaţi în prealabil cu 15 zile înainte de data transmiterii acestora cu privire la restanţele înregistrate şi cu privire la posibilitatea raportării la biroul de credit, așa cum prevede Decizia ANSPDCP nr. 105/2007.*

*În cadrul investigaţiei efectuate, în urma analizării tuturor documentelor prezentate de operator, a rezultat că nu s-a realizat informarea prealabilă a petenților pentru fiecare dintre*

*raportările de date negative efectuate la biroul de credit, potrivit Deciziei ANSPDCP nr. 105/2007. De asemenea, în mai multe cazuri au fost trimise notificări (informări prealabile) cu depăşirea termenului de 15 zile prevăzut de decizie. În plus, unele dintre notificări nu conţineau informaţii exacte privind sumele datorate ce urmau să fie raportate la biroul de credit ca date negative.*

*În baza acestor constatări, banca a fost sancţionată contravenţional conform art. 32 din Legea nr. 677/2001, pentru încălcarea art. 4, 12 și 14 din această lege, prin raportare la prevederile Deciziei nr. 105/2007. Totodată, s-a pus în vedere băncii să șteargă informațiile negative transmise la biroul de credit fără respectarea dispozițiilor legale aplicabile.*

## 2. Prelucrarea datelor personale prin mijloace de supraveghere video

În anul 2017, petițiile având ca obiect prelucrarea datelor cu caracter personal prin intermediul unor sisteme de supraveghere video au fost într-un număr semnificativ, atât ca urmare a utilizării tot mai frecvente a acestor sisteme de către operatorii de date, persoane juridice de drept public sau privat ori persoane fizice, cât și ca urmare a creșterii gradului de conștientizare a persoanelor fizice cu privire la drepturile de care beneficiază și la atribuțiile Autorităţii naționale de supraveghere pentru apărarea acestora.

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de supraveghere video cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune atât prevederilor Legii nr. 677/2001, modificată şi completată, și ale Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată. Autoritatea națională de supraveghere își poate exercita competențele legale în legătură cu respectarea prevederilor din primele două acte normative.

Petițiile adresate instituției noastre având ca scop instalarea sistemelor de supraveghere video au fost îndreptate, în special, împotriva unor angajatori ai persoanelor vizate (societăți comerciale sau unități de învățământ), împotriva asociațiilor de proprietari unde locuiesc petiționarii sau împotriva unor entități ce dețin spații comerciale frecventate de către persoanele care ni s-au adresat.

În cadrul investigațiilor efectuate la nivelul primei categorii de operatori, Autoritatea națională de supraveghere a apreciat faptul că efectuarea supravegherii video la locul de muncă nu poate fi admisă în situațiile în care există mijloace mult mai puțin intruzive pentru atingerea scopurilor declarate. În acelaşi timp, trebuie făcută dovada faptului că a fost efectuată în prealabil consultarea sindicatului sau a reprezentanţilor angajaţilor cu privire la scopurile pentru care se ia decizia de montare a camerelor de supraveghere video, cu argumentarea necesității prelucrării datelor personale ale angajaților prin aceste mijloace. De asemenea, pe tot parcursul funcționării sistemelor de supraveghere video este necesară realizarea unei informări permanente, care de obicei se asigură prin afișarea unor pictograme reprezentative, în apropierea locurilor monitorizate, însoțite de o serie de informații impuse prin Legea nr. 677/2001 și Decizia ANSPDCP nr. 52/2012.

În urma investigaţiilor efectuate la mai multe categorii de operatori, în special la asociaţiile de proprietari, s-a constatat că aceştia nu au cunoștință sau nu respectă prevederile Legii nr. 677/2001 şi ale Deciziei ANSPDCP nr. 52/2012. Cu ocazia investigațiilor efectuate la asociațiile de proprietari reclamate, pentru o mai bună înțelegere a obligațiilor ce le revin, reprezentanților acestora le-a fost făcut cunoscut *Ghidul privind prelucrările de date cu caracter personal efectuate prin intermediul sistemelor de supraveghere video instalate în cadrul asociațiilor de proprietari*, emis de Autoritatea națională de supraveghere în anul 2014 (disponibil pe pagina de Internet a autorității).

***FIŞĂ DE CAZ***

*O petentă a sesizat că o unitate de învățământ ar fi încălcat prevederile Legii nr. 677/2001, deoarece realiza prelucrarea imaginii/vocii elevilor prin intermediul sistemului de supraveghere video instalat, fără acordul și informarea persoanelor vizate.*

*În cadrul controlului efectuat pentru soluționarea sesizării, a rezultat că instalarea sistemului de supraveghere video în sălile de clasă a fost efectuată în anul 2010 și funcționează în fiecare an numai în perioada examenelor de evaluare națională, pentru respectarea prevederilor ordinelor emise de Ministerul Educației Naționale privind organizarea şi desfăşurarea evaluării naţionale pentru absolvenţii clasei a VIII-a, în scopul asigurării supravegherii operațiunilor efectuate în timpul examenelor. Din anul 2016 s-a instituit obligația (prin Ordinul nr. 5071/2016 privind organizarea şi desfăşurarea evaluării naţionale pentru*

*absolvenţii clasei a VIII-a în anul şcolar 2016-2017) dotării tuturor sălilor de examen cu camere funcţionale de supraveghere video şi audio. Prin urmare, aceste camere de supraveghere video au fost instalate pentru îndeplinirea unor obligaţii legale exprese ale operatorului, nefiind necesar în acest caz consimțământul persoanelor vizate (elevi, profesori, vizitatori).*

*Deoarece în cursul investigației a reieșit că o cameră de supraveghere video era montată în cancelarie din anul 2016, unitatea școlară a fost sancționată contravențional în baza art. 32 din Legea nr. 677/2001, întrucât a prelucrat în mod excesiv datele cu caracter personal ale persoanelor vizate (profesori), raportat la scopul prelucrării (supravegherea bunurilor din cancelarie). Totodată, a fost dispusă încetarea prelucrării datelor prin intermediul camerei respective, operatorul informând Autoritatea națională de supraveghere despre aducerea la îndeplinire a acestei măsuri. De asemenea, a mai fost constatată contravenția prevăzută de art. 32 din Legea nr. 677/2001, ca urmare a lipsei unei informări corespunzătoare a persoanelor vizate, conform art. 12 din lege, cu privire la prelucrările de date (imagine și voce) efectuate prin intermediul sistemului de supraveghere instalat în incinta școlii, măsură ce a fost ulterior adusă la îndeplinire de către operatorul de date.*

***FIŞĂ DE CAZ***

*Mai mulți petiționari au reclamat faptul că o societate comercială a montat pe microbuzele și autobuzele din dotare camere de supraveghere video și audio, fără a-i informa pe conducătorii auto și pe călători.*

*În urma investigației efectuate, s-a constatat că societatea în cauză prelucra imaginile persoanelor vizate prin intermediul unui sistem de supraveghere video instalat în interiorul autovehiculelor deținute, fără notificarea acestor prelucrări înainte de începerea lor la Autoritatea națională de supraveghere și fără a asigura o informare completă a persoanelor, conform art. 12 din Legea nr. 677/2001. Ca atare, au fost constatate și sancționate contravențiile prevăzute la art. 31 și art. 32 din Legea nr. 677/2001.*

*Întrucât operatorul montase în autovehiculele pe care le deținea inclusiv o cameră de supraveghere video îndreptată spre șoferi/angajați, aflați în spațiile în care își desfășoară activitatea permanent la locul lor de muncă, s-a aplicat o sancțiune contravențională în baza art. 32 din Legea nr. 677/2001, deoarece operatorul a prelucrat în mod excesiv datele*

*personale (imaginea) ale angajaţilor săi, fără respectarea prevederilor legale, respectiv, contrar art. 4 din Legea nr. 677/2001, raportat la Decizia ANSPDCP nr. 52/2012.*

*Autoritatea națională de supraveghere a subliniat faptul că dreptul la viață privată al șoferilor trebuie să fie considerat prioritar în fața necesității de supraveghere permanentă prin camere video.*

***FIŞĂ DE CAZ***

*O petentă ne-a sesizat că o asociaţie de proprietari a instalat camere de supraveghere video fără a avea consimţământul tuturor proprietarilor. De asemenea, petenta a susţinut că i s-a încălcat dreptul de acces la date, deoarece asociaţia de proprietari respectivă nu i-a comunicat un răspuns la solicitarea adresată în baza Legii nr. 677/2001.*

*Ca urmare a investigației, a reieșit că decizia de a instala un sistem de supraveghere video în cadrul asociației a fost votată în adunarea generală a proprietarilor, în scopul supravegherii spațiilor comune, respectiv: calea de acces în bloc, accesul la lift, scara care duce la primul etaj, pentru protecția proprietarilor și a bunurilor din condominiu. Cu privire la accesarea imaginilor, s-a precizat că această operațiune se face în cazul producerii unor evenimente corespunzătoare scopului prelucrării datelor, de către un membru al comitetului executiv al asociației.*

*Întrucât s-a constatat că asociația de proprietari nu a notificat la Autoritatea națională de supraveghere prelucrările de date efectuate prin intermediul sistemului de supraveghere video, aceasta a fost sancționată pentru săvârșirea contravenției prevăzute de art. 31 din Legea nr. 677/2001. De asemenea, deoarece nu a făcut dovada că a informat persoanele vizate (proprietari, locatari, vizitatori) cu privire la existența sistemului de supraveghere video, precum și cu privire la celelalte informații pe care operatorul este obligat să le furnizeze persoanelor vizate (scopul prelucrării datelor, drepturile persoanelor vizate, modul lor de exercitare etc.), conform art. 12 din lege și nu a comunicat un răspuns petentei în termen de 15 zile la petiția prin care aceasta și-a exercitat dreptul de acces (art. 13 din lege), asociația de proprietari a fost sancționată pentru săvârșirea contravenției prevăzute de art. 32.*

***FIŞĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată de un petiționar cu privire la faptul că o societate comercială ce deține un hipermarket ar fi prelucrat imaginea sa prin intermediul sistemului de supraveghere video, fără respectarea tuturor dispozițiilor legale.*

*Din verificările întreprinse, a reieșit că operatorul exercită o activitate comercială în structuri de tip hipermagazin – structură de vânzare cu amănuntul, cu suprafață de peste 2.500 mp, utilizată pentru comercializarea unor mărfuri alimentare și nealimentare. Operatorul a declarat că, în urma sustragerii de la raft a câtorva produse de mici dimensiuni, petentul a fost deranjat de faptul că s-a constatat acest fapt de către personalul de pază al societății și a încercat să se apere prin invocarea legislației în materie de protecție a datelor cu caracter personal.*

*Ca urmare a investigației efectuate, operatorul, deși a prezentat informații și documente din care a reieșit necesitatea instalării unui asemenea sistem și luarea unor măsuri în vederea respectării prevederilor Legii nr. 677/2001, întrucât nu a prezentat suficiente dovezi privind existența unor instrucțiuni date angajaților/dispecerilor pentru prelucrarea datelor cu caracter personal și nu a prevăzut suficiente elemente cu privire la securitatea și confidențialitatea datelor cu caracter personal prelucrate prin intermediul sistemului de supraveghere video în procedurile sale specifice, în special din punct de vedere tehnic (restricționare, copiere/printare imagini fără o autorizare în acest sens etc), obligații prevăzute de art. 19 și 20 din aceeași lege, a fost sancționat pentru contravenția prevăzută de art. 33 din Legea nr. 677/2001.*

***FIŞĂ DE CAZ***

*Printr-o petiție, Autoritatea națională de supraveghere a fost sesizată că o societate comercială care deține un mall prelucrează date cu caracter personal prin intermediul unui sistem de supraveghere video montat în toaletele din interiorul acestuia.*

*În cadrul investigației a reieșit că, prin intermediul camerelor de supraveghere montate în interiorul clădirii, sunt surprinse imagini din zona grupurilor sanitare, unde se află oglinzile și accesul spre cabine, încălcându-se astfel intimitatea persoanelor care tranzitează această zonă. De asemenea, a rezultat că imaginile surprinse de aceste camere sunt stocate până la 60 de*

*zile, contrar prevederilor Deciziei ANSPDCP nr. 52/2012 ("durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video trebuie să fie proporţională cu scopul pentru care se prelucrează datele, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate").*

*Față de aceste constatări, operatorul a fost sancționat pentru contravenția prevăzută la art. 32 din Legea nr. 677/2001, deoarece a prelucrat în mod excesiv datele personale (imaginea) ale persoanelor vizate prin intermediul acestor camere video, fără respectarea prevederilor legale, contrar art. 4 din Legea nr. 677/2001, raportat la Decizia ANSPDCP nr. 52/2012, precum și fără respectarea termenului de stocare limitată a imaginilor prevăzut în Decizia ANSPDCP nr. 52/2012.*

### *3. Dezvăluirea datelor personale către diverse entități*

În anul 2017, o pondere însemnată în numărul plângerilor și sesizărilor 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 (prin publicarea pe Internet, de exemplu), 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. În unele dintre aceste plângeri s-a reclamat publicarea fără consimțământul petentului a unor imagini (fotografii sau înregistrări video) pe rețelele de socializare, de către alți utilizatori persoane fizice ori crearea unor conturi false pe website-uri de *dating* prin folosirea unor date personale și fotografii însoțite de informații defăimătoare la adresa persoanelor vizate. În aceste ultime cazuri, instituția noastră a efectuat demersuri de investigare numai în măsura în care a fost posibilă identificarea deținătorilor respectivelor website-uri ca fiind operatori ce intră în sfera de competență teritorială a Autorității naționale de supraveghere.

Din investigațiile efectuate în anul 2017 s-a constatat faptul că, în anumite cazuri, dezvăluirea ilegală a datelor personale s-a produs ca urmare a neadoptării de către operatori a măsurilor de securitate și confidențialitate necesare pentru a preveni accesul unor persoane neautorizate la date, datorate în special necunoașterii regulilor de protecție a datelor personale aplicabile în activitatea pe care o desfășoară.

***FIȘĂ DE CAZ***

*Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că datele sale personale au fost dezvăluite către terți de fostul angajator.*

*În cadrul investigației efectuate, s-a constatat că datele personale ale petentului (date de identificare, date din contractul individual de muncă și din fișa postului, date privind starea de sănătate), cuprinse într-un proces-verbal încheiat în cadrul unei proceduri disciplinare, au fost transmise prin intermediul poștei electronice către toți angajații operatorului, în vederea discutării situației în cadrul unui instructaj privind normele de securitate și sănătate în muncă.*

*La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat contravențional operatorul pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a dezvăluit către terți, fără temei legal, datele cu caracter personal ale petentului, precum și pentru fapta prevăzută de art. 33 din Legea nr. 677/2001, întrucât operatorul nu a asigurat confidențialitatea datelor cu caracter personal ale petentului, prelucrate inclusiv prin persoane împuternicite, și nu a luat măsuri tehnice și organizatorice adecvate împotriva dezvăluirii datelor cu caracter personal ale acestuia.*

***FIȘĂ DE CAZ***

*Un petent a reclamat că asociaţia de proprietari din imobilul unde locuiește a prelucrat ilegal datele sale de identitate prin afișarea unui înscris în care sunt menționate adresa sa de domiciliu și codul numeric personal. Petentul a susținut că s-a adresat asociației de proprietari în baza Legii nr. 677/2001, însă nu a primit niciun răspuns în termenul legal de 15 zile.*

*În urma investigației efectuate, s-a constatat că înscrisul menționat de petent a fost afișat la avizierul blocului și se referea la stadiul dosarului de recuperare debite pe care acesta le avea față de asociația de proprietari, ca urmare a unei hotărâri judecătorești.*

*În ceea ce privește cererea petentului, adresată asociației de proprietari, operatorul a afirmat că a depus un răspuns la cutia poștală a petentului, fără a prezenta o dovadă în acest sens.*

*La finalizarea demersurilor întreprinse, operatorul a fost sancționat în baza art. 32 din Legea nr. 677/2001, întrucât a dezvăluit la avizierul blocului datele cu caracter personal, inclusiv codul numeric personal, ale petentului, fără consimţământul acestuia sau alt temei legal și fără*

*să facă dovada informării acestuia. De asemenea, operatorul a fost sancționat întrucât nu a făcut dovada comunicării unui răspuns petentului, la cererea sa de exercitare a dreptului de opoziție prevăzut de art. 15 din Legea nr. 677/2001.*

***FIȘĂ DE CAZ***

*O petentă a reclamat faptul că datele sale cu caracter personal ar fi fost dezvăluite ilegal de către o societate comercială (magazin de vânzare produse).*

*Petenta a menționat că la o zi după procesul de divorț, fostul soț, invocând calitatea de "actual soț", a obținut de la operator o copie a unui bon de achiziție a unui produs electrocasnic cumpărat de petentă în anul 2015, pretextând că îi este necesar în scopul trimiterii acestuia în unitatea service pentru remedierea unor neconformități.*

*În cadrul investigației realizate, s-a constatat că reprezentanții magazinului au eliberat fostului soț al petentei o copie după extrasul din sistem (factură) privind achiziția efectuată de petentă în anul 2015, în urma unei cereri scrise și a prezentării unor documente.*

*În notificarea depusă la Autoritatea naţională de supraveghere pentru prelucrările de date efectuate în scop de "furnizare de bunuri și servicii", operatorul a declarat ca destinatari ai datelor personale persoana vizată, angajații operatorului, autoritatea judecătorească, poliția și mass-media.*

*La finalizarea demersurilor întreprinse, operatorul a fost sancționat contravențional pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a dezvăluit date cu caracter personal, în legătură cu achiziția efectuată de petentă.*

### 4. Prelucrarea excesivă a datelor personale

Din practica de soluționare a plângerilor și sesizărilor adresate Autorității naționale de supraveghere în cursul anului 2017, se constată situații diverse de încălcare a prevederilor Legii nr. 677/2001, sub aspectul respectării principiilor legalității și proporționalității în luarea deciziei de a prelucra anumite date personale. Astfel, unii operatori au ales să prelucreze date personale (chiar din categoria celor protejate prin reguli speciale, cum sunt codul numeric personal ori datele biometrice) în scopuri pentru realizarea cărora se puteau limita categoriile de date la cele strict necesare. Coroborat cu aceste aspecte, s-a mai constatat faptul că în

anumite cazuri, datele au continuat să fie stocate sau prelucrate după expirarea perioadei legale, deși acestea nu mai erau necesare, prin raportare la justificarea colectării lor inițiale. De asemenea, Autoritatea națională de supraveghere, potrivit opiniilor sale constante, nu a permis prelucrarea datelor biometrice în scopul realizării accesului la locul de muncă sau pontării orelor de muncă, în situațiile incidente putând fi alese de către operatori mijloace mai puțin intruzive pentru viața privată a persoanelor.

În privința prelucrării codului numeric personal, s-au constatat situații în care acesta este colectat în mod obligatoriu pentru efectuarea anumitor operațiuni (de exemplu, emiterea de facturi fiscale, returnarea unor produse comercializate), prin invocarea eronată a unor prevederi legale care ar impune această prelucrare. De asemenea, s-a constatat faptul că anumiți operatori de date personale colectează în mod excesiv și în lipsa unui temei legal expres copii ale actelor de identitate, în circumstanțe precum: plata unor facturi de utilități la ghișeele unor bănci, returnarea unor produse achiziționate de la diverși comercianți, permiterea accesului la anumite evenimente sociale.

În acest context, Autoritatea națională de supraveghere a urmărit respectarea art. 8 din Legea nr. 677/2001 și a Deciziei ANSPDCP nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

a) Prelucrarea datelor biometrice

***FIŞĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate a instalat camere de supraveghere video în vestiare şi foloseşte aparatură de amprentare pentru întocmirea pontajului.*

*În cadrul investigației efectuate, s-a constatat că la nivelul conducerii societății respective, ca urmare a actelor de vandalism și a distrugerilor repetate ale echipamentelor, s-a decis instalarea unui sistem de supraveghere video în halele de lucru, în zonele de acces în incinta societății, dar și în interiorul vestiarelor, la ușile de acces. În privința sistemului de amprentare, s-a declarat faptul că acesta a fost introdus întrucât vechiul sistem de acces pe bază de cartele nu funcționa de fiecare dată, ca urmare a forțării ușilor de acces în cazul în care*

*angajații nu se aflau în posesia cartelelor, ceea ce conducea inclusiv la declanșarea sistemului de alarmare pentru situații de urgență.*

*Din verificările efectuate, s-a constatat că nu existau pictograme prin intermediul cărora persoanele vizate să fie informate cu privire la existența sistemului de supraveghere video și cu privire la drepturile prevăzute de Legea nr. 677/2001 decât pe gardul societății, la intrare.*

*De asemenea, s-a constatat că la nivelul conducerii societății respective s-a decis instalarea unui sistem de amprentare pentru întocmirea pontajului (sistem de pontaj biometric) fără obținerea prealabilă a consimțământului angajaților.*

*Societatea nu a făcut dovada notificării la Autoritatea națională de supraveghere a prelucrării datelor personale prin intermediul sistemului de pontaj biometric și prin intermediul sistemului de supraveghere video. De asemenea, societatea nu a făcut dovada existenței unei obligații legale în privința acestor prelucrări și nici dovada obținerii avizului de la instituția noastră.*

*În consecință, operatorul a fost sancționat astfel:*

- *pentru fapta prevăzută de art. 31 din Legea nr. 677/2001, întrucât nu a notificat la ANSPDCP prelucrările de date cu caracter personal pe care le efectua prin sistemul de supraveghere video și prin sistemul de pontaj biometric, deşi avea această obligaţie potrivit art. 22 din Legea 677/2001;*
- *pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât nu a putut face dovada informării prealabile explicite a angajaților care își desfășoară activitatea în halele de producție supravegheate video și nu a realizat o informare a persoanelor vizate privind drepturile prevăzute de art. 12-18 din Legea nr. 677/2001, anterior instalării sistemului de supraveghere video;*
- *pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a colectat şi prelucrat date biometrice considerate a fi excesive faţă de scopul prelucrării, respectiv, pontarea timpului de lucru al angajaţilor, putând fi utilizate şi alte mijloace pentru atingerea acestui scop, mai puţin intruzive.*

*Față de cele de mai sus, s-a pus în vedere operatorului să adopte o serie de măsuri pentru intrarea în legalitate, inclusiv să înceteze prelucrarea datelor biometrice ale angajaților în scopul efectuării pontajului și să șteargă din sistem datele colectate în acest scop.*

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate prelucrează datele biometrice (amprente) ale salariaților în scopul monitorizării timpului de lucru al acestora și al întocmirii pontajului.*

*Urmare a investigației efectuate, s-a constatat că pontajul se realiza, pentru cea mai mare parte a angajaților, pe bază de date biometrice, obținute în procesul de scanare a amprentelor digitale ale acestora. Decizia de a fi implementat un astfel de sistem s-a luat în scopul ținerii unei evidențe stricte a programului de lucru al angajaților, dar și pentru accesul în incinta în care societatea își desfășoară activitatea. Ulterior instalării acestui sistem, angajaților societății li s-a oferit posibilitatea de a opta cu privire la accesul în companie pe bază de amprentă.*

*Societatea nu a făcut dovada notificării la Autoritatea națională de supraveghere a prelucrării datelor colectate prin intermediul sistemului de pontaj cu date biometrice.*

*De asemenea, societatea nu a făcut dovada existenței unei obligații legale în privința acestor prelucrări și nici dovada obținerii avizului de la instituția noastră privind prelucrarea datelor cu caracter personal prin acest sistem.*

*Prin urmare, s-a reținut că prelucrarea datelor biometrice este excesivă față de scopul prelucrării, respectiv pontarea timpului de lucru al angajaților, solicitându-se operatorului investigat să înceteze prelucrarea datelor biometrice ale angajaților și să șteargă din sistem datele colectate în acest scop.*

*În consecință, operatorul a fost sancționat astfel:*

- *pentru fapta prevăzută de art. 31 din Legea nr. 677/2001, întrucât nu a notificat prelucrările de date cu caracter personal pe care le efectua prin sistemul de pontaj cu date biometrice, deşi avea această obligaţie potrivit art. 22 din Legea 677/2001;*
- *pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a colectat şi prelucrat date biometrice considerate a fi excesive faţă de scopul prelucrării, respectiv pontarea timpului de lucru al angajaţilor, putând fi utilizate şi alte mijloace pentru atingerea acestui scop, mai puţin intruzive.*

*În urma investigației, operatorul a declarat că a dezafectat sistemul de prelucrare a datelor biometrice ale angajaților, a încetat prelucrarea acestor date și a procedat la ștergerea datelor biometrice colectate.*

b) Prelucrarea codului numeric personal și a copiei actului de identitate

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată cu privire la colectarea codului numeric personal al clienților unei societăți care comercializează produse vestimentare, în situațiile în care se dorește schimbarea unui produs.*

*Urmare a investigației efectuate, s-a constatat că societatea respectivă nu prelucrează în mod curent codul numeric personal de la persoanele fizice pentru întocmirea facturilor sau la schimbarea produselor, însă în cazul petentului, în mod eronat, a colectat această dată cu caracter special la schimbarea unui produs, CNP-ul fiind menționat atât pe factură, cât și pe dispoziția de plată, dar nefiind stocat în baza de date.*

*În consecință, operatorul a fost sancționat pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a prelucrat codul numeric personal al persoanelor vizate, pentru schimbarea unui produs, fără respectarea prevederilor art. 8 din Legea nr. 677/2001, raportate la Decizia ANSPDCP nr. 132/2011.*

*Societatea a implementat un manual de contabilitate la nivelul companiei, care a fost adus la cunoștința tuturor angajaților și care descrie procedura de retur. De asemenea, angajații au fost instruiți în sensul completării documentelor legale doar cu datele prevăzute expres de legislația în vigoare.*

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată prin mai multe petiții cu privire la faptul că un organizator al unui eveniment internațional de muzică a solicitat CNP-ul participanților în procedura de verificare (check-in) a biletelor cumpărate online și a scanat cartea de identitate a acestora la intrarea la festival.*

*Art. 6 din Decizia nr. 132/2011 privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală, emisă de Autoritatea națională de supraveghere, stabilește faptul că prelucrarea datelor prevăzute la art. 1 (inclusiv CNP-ul), prin efectuarea şi reţinerea de copii de pe cartea de identitate sau de pe documente care le conţin, este interzisă, cu excepţia situaţiilor prevăzute la art. 2. În același timp, art. 2 din Decizia nr. 132/2011 prevede că prelucrarea datelor prevăzute la art. 1, inclusiv dezvăluirea acestora către terţi, se face numai în condiţiile stabilite la art. 8 din Legea nr. 677/2001, şi anume: a) persoana vizată şi-a dat în mod expres consimţământul; sau b) prelucrarea este prevăzută în mod expres de o dispoziţie legală; sau c) în alte cazuri, cu avizul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal şi numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.*

*Din verificările efectuate cu ocazia investigației deschise în acest caz, a rezultat că societatea reclamată nu a cerut avizul Autorității naționale de supraveghere anterior începerii prelucrării, în condițiile în care nu s-a putut face dovada obținerii consimțământului expres al persoanelor vizate și nici a existenței unor dispoziții legale exprese în această situație particulară de prelucrare a codului numeric personal și de scanare a actelor de identitate ale persoanelor participante la evenimentul organizat. Motivele invocate de societate, fără a fi dovedite, privind obligația societății de a colabora cu autoritățile și, pe de altă parte, obligațiile societății privind paza și protecția perimetrului festivalului, nu justifică necesitatea stringentă a colectării CNP-ului și a prelucrării copiei documentului de identitate raportat la scopul propus.*

*Urmare a investigației efectuate, s-a constatat că prelucrarea CNP-ului participanților la eveniment și scanarea actelor de identitate aparținând acestora reprezintă operațiuni de prelucrare excesivă prin raportare la scopul asigurării accesului în incinta perimetrului festivalului, motiv pentru care societatea a fost sancționată contravențional în temeiul art. 32 din Legea nr. 677/2001, pentru încălcarea prevederilor art. 4 și art. 8 din Legea nr. 677/2001, raportate la Decizia ANSPDCP nr. 132/2011.*

### *5. Nerespectarea drepturilor de informare, acces, intervenție și opoziție*

Respectarea drepturilor persoanelor vizate reglementate de Legea nr. 677/2001, în special a dreptului la informare (art. 12), a dreptului de acces la date (art. 13), a dreptului de intervenţie asupra datelor (art. 14) şi a dreptului de opoziţie (art. 15), deși reprezintă o

obligație esențială a operatorilor de date, a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere și în anul 2017.

Astfel, ca urmare a investigaţiilor efectuate, s-a constatat că operatorii nu cunosc obligaţiile care le incumbă potrivit reglementărilor legale susmenţionate ori le ignoră cu bună-ştiinţă; în alte cazuri, transmit persoanelor vizate răspunsuri incomplete sau/şi fără respectarea termenului de 15 zile prevăzut de lege. De asemenea, s-a mai constatat faptul că unii operatori nu au adoptat măsuri organizatorice interne care să se dovedească a fi eficiente pentru gestionarea cererilor adresate de persoanele vizate în baza drepturilor reglementate de Legea nr. 677/2001.

a) Nerespectarea dreptului de informare

***FIȘĂ DE CAZ***

*Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o societate de închiriere autoturisme ("rent a car"). Astfel, petentul reclama că operatorul a prelucrat date de geolocalizare cu privire la persoana sa, fără consimțământul său și fără o informare prealabilă, în conformitate cu prevederile Legii nr. 677/2001.*

*Ca urmare a investigației efectuate, s-a reținut faptul că pe toate mașinile închiriate erau instalate sisteme de localizare geografică prin GPS, datele de localizare fiind disponibile în baza accesării unei aplicații dezvoltate de un terț.*

*Datele de localizare disponibile prin aplicație, aferente mașinilor aflate în proprietate, erau următoarele: număr înmatriculare, model, data și ora pornirii motorului, viteza de deplasare curentă, șofer necunoscut, coordonatele GPS; aplicația permite transmiterea unei alerte prin SMS către un angajat al societății, în cazul în care un vehicul depășește granițele României contrar obligațiilor contractuale.*

*Din verificările efectuate, s-a constatat că nici contractele, nici celelalte anexe la acestea nu conțineau informații complete privind informarea persoanelor vizate, conform art. 12 din Legea nr. 677/2001. De asemenea, termenii și condițiile de utilizare disponibile pe site-ul societății nu făceau referire la prelucrarea datelor de localizare și nici la alte informații privind Legea nr. 677/2001.*

*Față de cele constatate, operatorul a fost sancționat astfel:*

- *pentru fapta prevăzută de art. 31 din Legea nr. 677/2001, întrucât nu a declarat în cadrul formularului de notificare la Autoritatea națională de supraveghere prelucrarea datelor de localizare;*
- *pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât nu a prezentat dovezi cu privire la asigurarea unei informări complete a persoanelor fizice cărora le închiriază vehicule, pe site-ul propriu și în contractele pe suport fizic încheiate cu acestea.*

b) Nerespectarea dreptului de acces

***FIȘĂ DE CAZ***

*O petentă a sesizat faptul că două birouri ale unor executori judecătorești i-au prelucrat datele personale cu încălcarea, printre altele, a art. 13 din Legea nr. 677/2001, întrucât au ignorat cererea sa trimisă prin e-mail, cerere prin care își exercita dreptul de acces pe lângă acești operatori.*

*Ca urmare a investigației efectuate, s-a reţinut printre altele faptul că operatorii nu au furnizat petentei informaţiile solicitate prin cererile acesteia în termenul legal de 15 zile prevăzut de art. 13 din Legea nr. 677/2001, respectiv: categoriile de date personale prelucrate cu privire la petentă, destinatarii cărora le sunt dezvăluite datele acesteia, comunicarea într-o formă inteligibilă a datelor ce fac obiectul prelucrării și a oricărei informații disponibile privind originea datelor.*

*Ca atare, la finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a aplicat birourilor executorilor judecătorești sancțiuni contravenționale în baza art. 32 din Legea nr. 677/2001, pentru nerespectarea condițiilor de exercitare a dreptului de acces, astfel cum ar fi avut obligaţia potrivit art. 13 din Legea nr. 677/2001.*

*De asemenea, s-a recomandat operatorilor să transmită fiecare câte un răspuns complet petentei.*

***FIȘĂ DE CAZ***

*Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 și ale Legii nr. 506/2004 de către o societate de telefonie. Petentul a susținut că operatorul i-a încălcat drepturile prevăzute de art. 13-15 din Legea nr. 677/2001.*

*Petentul s-a adresat operatorului printr-o cerere prin care își exercita dreptul de acces la datele sale cu caracter personal, solicitând informații referitoare la confirmarea faptului că datele sale sunt sau nu prelucrate, informații referitoare la apelurile efectuate la numărul de urgență 112 de la numărul de mobil indicat de petent, scopurile în care sunt prelucrate datele, categoriile de date, categoriile de destinatari etc.*

*Societatea de telefonie a transmis un răspuns petentului prin care i-au fost oferite informații generale cu privire la operațiunile de prelucrare a datelor efectuate de operator. Operatorul nu a indicat în răspunsul către petent, în mod clar, dacă prelucrează sau nu datele personale referitoare la acesta, fiind astfel încălcate prevederile art. 13 alin. (1) din Legea nr. 677/2001.*

*În urma investigaţiei efectuate, operatorul reclamat a fost sancţionat pentru contravenţia prevăzută de art. 32 din Legea nr. 677/2001, raportat la art. 13 din aceeași lege, întrucât a încălcat dreptul de acces la date, prin faptul că nu a răspuns concret la solicitarea petentului de a-i fi confirmat faptul că datele sale sunt sau nu prelucrate de societatea de telefonie.*

c) Nerespectarea dreptului de intervenție

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată în legătură cu o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către un minister.*

*Astfel, petentul reclama faptul că a transmis o cerere către acest minister, întemeiată inclusiv pe art. 14 din Legea nr. 677/2001, prin care a solicitat ştergerea şi/sau anonimizarea datelor, precum și încetarea prelucrării datelor sale personale afișate într-un sistem de evidență online, considerată excesivă. Petentul a susţinut că ministerul nu a răspuns solicitării sale.*

*Prin aceeași petiție înaintată instituției noastre, petentul a semnalat faptul că, în sistemul de evidență online administrat de acest minister, sunt prelucrate date cu caracter personal fără*

*a exista o informare clară şi exactă cu privire la această prelucrare şi cu privire la drepturile persoanelor vizate.*

*În urma demersurilor efectuate, s-a constatat că ministerul reclamat nu a răspuns cererii petentului, prin care acesta şi-a exercitat dreptul de intervenţie, în baza art. 14 din Legea nr. 677/2001.*

*Ca atare, ministerul a fost sancționat contravențional în baza art. 32 din Legea nr. 677/2001, raportat la art. 14 din Legea nr. 677/2001.*

*De asemenea, a fost emisă o Recomandare către acest minister și către celelalte entități care utilizează sistemul de evidență online administrat de minister, prin care s-a pus în vedere adoptarea unor măsuri corespunzătoare pentru a se asigura informarea completă a persoanelor vizate, prin introducerea informațiilor prevăzute de art. 12 din Legea nr. 677/2001 atât pe prima pagină a sistemului de evidență online, cât și pe fiecare secțiune aferentă celorlalte entități.*

d) Nerespectarea dreptului de opoziție

***FIȘĂ DE CAZ***

*Prin mai multe petiţii, un petent a sesizat Autoritatea naţională de supraveghere cu privire la faptul că i-a fost încălcat dreptul la viaţa intimă, familială şi privată cu privire la prelucrarea datelor cu caracter personal de către o instituție financiară nebancară.*

*Astfel, petentul a susţinut că societatea financiară nebancară i-a folosit în mod abuziv adresa de e-mail și numărul de telefon prin transmiterea unor mesaje, inclusiv de tip SMS, prin care era informat cu privire la înregistrarea unor restanţe la creditul contractat. În acest context, petentul și-a exercitat dreptul de opoziție față de prelucrarea datelor sale de către respectivul operator, în baza art. 15 din Legea nr. 677/2001.*

*În urma investigaţiei efectuate, instituția financiară nebancară reclamată a fost sancţionată pentru contravenţia prevăzută de art. 32 din Legea nr. 677/2001, întrucât nu a răspuns petentului la solicitarea sa în termen de 15 zile, potrivit art. 15 din Legea nr. 677/2001 și i-a folosit numărul de telefon fără consimțământul acestuia.*

### 6. *Transmiterea de comunicări comerciale prin mijloace de comunicație electronică*

În cursul anului 2017, Autoritatea națională de supraveghere a înregistrat în continuare un număr semnificativ de plângeri având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (SMS) sau prin poşta electronică. Majoritatea acestora au privit aspecte legate de protecţia vieţii private în sectorul comunicaţiilor electronice prin primirea de mesaje comerciale nesolicitate prin poşta electronică, fără consimţământul expres şi neechivoc al destinatarului în acest sens.

În vederea soluţionării plângerilor considerate admisibile, Autoritatea națională de supraveghere a efectuat o serie de investigaţii pentru a verifica existenţa consimţământului persoanei vizate de a primi mesaje comerciale pe adresa sa de poştă electronică sau prin SMS. În unele cazuri investigate, s-a constatat că 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***

*Un petent a sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o societate care i-a transmis, la numărul personal de telefon, un SMS care promova un magazin ce comercializa telefoane mobile și accesorii GSM, deși petentul și-ar fi exprimat explicit opoziția ca numărul său de telefon să fie folosit pentru mesaje publicitare. Prin aceeași petiție, petentul a sesizat și faptul că s-a adresat societății, dar nu a primit niciun răspuns.*

*În urma investigaţiei efectuate, s-a constatat faptul că operatorul colecta datele persoanelor fizice incluse în baza de date a societății din contractele de prestări servicii de voce și date; în aceste contracte, clienții își pot exprima acordul sau opoziția față de prelucrarea datelor cu caracter personal de către operatorul de telefonie mobilă, partener al operatorului de date controlat. Cu titlu excepțional, societatea prelucrează date ale persoanelor vizate, deținători ai serviciilor preplătite (prepay), numai în condițiile în care aceste date au fost furnizate în mod deliberat de către persoana vizată în scopul comunicărilor comerciale.*

*Operatorul nu a stocat date cu caracter personal privindu-l pe petent, întrucât, în cazul achiziționării de cartele preplătite, societatea nu stochează informații privind identitatea*

*clienților, în baza de date aflându-se doar numărul de telefon, fără nicio informație relativă la titularul/deținătorul numărului preplătit. Consimțământul abonaților pentru a le fi colectate, utilizate și dezvăluite datele personale, în special în scop comercial, este dovedit de contractul de prestări servicii de voce și date.*

*Întrucât operatorul i-a transmis petentului un SMS care promova un magazin, deși nu a prezentat nicio dovadă certă a obținerii în prealabil a consimțământului expres al acestuia în vederea primirii de comunicări comerciale prin poșta electronică, a fost sancționat contravențional pentru nerespectarea prevederilor referitoare la comunicările nesolicitate, contravenţie prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004.*

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate care asigură servicii de întreținere corporală și wellness a transmis comunicări comerciale prin SMS, fără respectarea prevederilor legale, unei persoane fizice care avusese calitatea de membru în cadrul acestei societăți.*

*De asemenea, persoana a reclamat și încălcarea drepturilor de intervenție și opoziție de către operator, întrucât societatea nu i-a șters datele cu caracter personal care o privesc și nu a încetat prelucrarea acestora (numărul de telefon).*

*Urmare a investigației efectuate, s-a constatat că societatea a transmis mesaje promoționale cu oferte, pe numărul de telefon al petentului, fără ca acesta să-și dea consimțământul prealabil pentru aceste solicitări. S-a mai constatat că societatea nu a asigurat o informare adecvată conform prevederilor Legii nr. 677/2001 în conținutul mesajelor transmise de operator prin intermediul persoanelor împuternicite, iar din acest motiv persoanele care primeau astfel de mesaje nu erau informate în legătură cu posibilitatea de exercitare a drepturilor de care beneficiază potrivit legii.*

*Față de cele constatate, operatorul a fost sancționat contravențional în baza art. 13 raportat la art. 12 din Legea nr. 506/2004 și în baza art. 12 din Legea nr. 677/2001. Totodată, i s-a solicitat să șteargă toate datele personale (numere de telefon), dar și adresele de e-mail colectate și utilizate fără consimțământul expres prealabil al deținătorilor în scopul trimiterii de comunicări comerciale și să înceteze trimiterea de comunicări comerciale prin mijloace*

*electronice fără consimţământul expres şi prealabil al deținătorilor adreselor de poștă electronică.*

***FIȘĂ DE CAZ***

*Autoritatea naţională de supraveghere a fost sesizată de o persoană fizică în legătură cu faptul că a primit mai multe mesaje comerciale pe adresa sa personală de e-mail, de la o adresă de e-mail care aparține unei societăți cu obiect de activitate reclamă, marketing și publicitate și servicii de comunicații electronice, cu precizarea că nu şi-a dat niciodată acordul pentru prelucrarea datelor de către respectivul operator.*

*Petentul a declarat că s-a adresat operatorului, prin intermediul poştei electronice, solicitând să îi fie eliminate datele cu caracter personal din baza de date a operatorului, dar nu a primit niciun răspuns.*

*Urmare a investigației efectuate, s-a constatat faptul că datele cu caracter personal ale petentului, respectiv nume, prenume și adresă de e-mail, au intrat în baza de date a societății respective cu ocazia participării la un concurs de pe site-ul acesteia și bifarea căsuței "sunt de acord" cu termenii de înscriere în concurs și de primire de comunicări comerciale din partea operatorului.*

*La momentul controlului, operatorul nu a prezentat nicio dovadă a obținerii consimțământului expres prealabil al petentului pentru prelucrarea datelor sale cu caracter personal (nume, prenume, adresă de e-mail) de către societate, în scopul transmiterii de mesaje comerciale.*

*Cu toate acestea, s-a identificat faptul că numele și prenumele petentului, precum și adresa de e-mail se aflau în baza de date a operatorului, la momentul controlului, având status "dezactiv" pentru transmiterea de mesaje comerciale. Dezactivarea datelor petentului de la transmiterea de mesaje comerciale s-a realizat ca urmare a deciziei operatorului, și nu la solicitarea petentului.*

*Reprezentanții operatorului au declarat că singurul mesaj comercial transmis către adresa petentului a fost în cadrul unui concurs și că nu a fost găsit în evidențele societății e-mail-ul transmis de petent prin care solicita ștergerea datelor sale din baza de date a operatorului.*

*Față de cele constatate, operatorul a fost sancționat contravențional în baza art. 13 raportat la art. 12 din Legea nr. 506/2004 și i s-a solicitat să șteargă toate datele personale (numere de telefon), dar și adrese de e-mail, colectate și utilizate fără consimțământul expres prealabil al deținătorilor în scopul trimiterii de comunicări comerciale și să înceteze trimiterea de comunicări comerciale prin mijloace electronice fără consimţământul expres şi prealabil al deținătorilor adreselor de poștă electronică.*

## *7. Încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date*

Una dintre obligațiile de bază ale operatorilor de date personale prevăzute de legislația în materie se referă la adoptarea măsurilor de securitate a prelucrărilor și de respectare a regulilor de confidențialitate, prin care să se prevină incidente de genul dezvăluirii ilegale a datelor, accesării datelor de către persoane neautorizate, pierderii sau distrugerii datelor etc.

În anul 2017, o parte din plângerile și sesizările ce au fost adresate Autorității naţionale de supraveghere 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 (comercianți, autorități publice, furnizori de servicii de telefonie, clinici medicale etc.) nu au implementat proceduri interne eficiente, de ordin tehnic sau organizatoric, care să conducă la preîntâmpinarea unor astfel de probleme.

***FIȘĂ DE CAZ***

*Un petent a reclamat că angajați ai unui magazin de vânzare produse electrocasnice au accesat în mod neautorizat contul său de poștă electronică de pe telefonul cumpărat de la această societate comercială și returnat ulterior pentru casare.*

*În urma demersurilor de investigare întreprinse de Autoritatea națională de supraveghere, s-a constatat că petentul a achiziționat un telefon de la un magazin de produse electrocasnice, iar apoi l-a predat la un punct de lucru al operatorului, pe motiv că nu funcționează corespunzător.*

*Telefonul, în stare de funcționare, a fost păstrat în magazin, cu posibilitatea de vânzare ca produs resigilat. La o dată ulterioară, telefonul a fost achiziționat de un alt client la un preț*

*de discount, fără însă a se verifica în prealabil dacă telefonul a fost readus la setările din fabrică.*

*În urma sesizării operatorului de către petent că e-mail-ul său a fost accesat de pe telefonul returnat, operatorul a încercat, fără rezultat, contactarea noului posesor al telefonului. La o dată ulterioară, posesorul telefonului s-a prezentat în magazin și a reclamat că telefonul nu funcționează corespunzător. Operatorul a stornat factura, a reținut telefonul, l-a resetat și l-a trimis spre casare.*

*În cadrul investigației, s-a constatat că operatorul nu a făcut dovada că deține o politică de securitate în ceea ce privește produsele returnate și, eventual, revândute, care pot conține date cu caracter personal ale clienților.*

*Totodată, s-a constatat că operatorul nu a luat măsuri de verificare a telefonului returnat de petent, în sensul de a fi readus la setările din fabrică înainte de a fi vândut unei alte persoane. În acest fel, a fost posibilă dezvăluirea neautorizată a datelor cu caracter personal ale petentului.*

*La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul pentru fapta prevăzută de art. 33 din Legea nr. 677/2001, întrucât acesta nu a luat măsuri suficiente împotriva dezvăluirii sau accesului neautorizat în ceea ce privește datele cu caracter personal ale petentului, stocate pe telefonul mobil returnat operatorului și revândut altei persoane.*

***FIȘĂ DE CAZ***

*Autoritatea națională de supraveghere a fost sesizată de către un petent cu privire la faptul că primește, în mod constant, pe adresa sa de e-mail, de la un operator care oferă servicii medicale (clinică), o corespondență pentru o altă persoană, fiind dezvăluite, astfel, datele cu caracter personal ale acesteia, inclusiv buletine de analize medicale.*

*În cadrul controlului, operatorul a declarat că, din cauza faptului că adresele de poștă electronică "gmail.com" nu iau în considerare semnele de punctuație (".") în compunerea unei adrese de e-mail, a fost posibilă transmiterea pe adresa de poștă electronică a petentului a unor informații care erau destinate să fie transmise unui abonat al clinicii, cu o adresă de e-mail asemănătoare.*

*Totodată, s-a constatat că, deși petentul a sesizat clinica, cu privire la dezvăluirea unor date cu caracter personal către un terț, operatorul nu a luat nicio măsură, continuând să transmită informații care cuprindeau date personale ale unui terț, pe adresa de e-mail a petentului.*

*La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul pentru săvârşirea contravenţiei prevăzute de art. 33 din Legea nr. 677/2001, întrucât nu a luat măsuri tehnice și organizatorice împotriva dezvăluirii datelor personale ale unei persoanei vizate către un terț, deși a fost sesizată cu privire la acest aspect, de către petent.*

***FIȘĂ DE CAZ***

*Un petent a sesizat Autoritatea națională de supraveghere în legătură cu o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o autoritate publică, prin faptul că această instituţie a prelucrat fără drept datele sale cu caracter personal existente în bazele de date gestionate de Direcţia pentru Evidenţa Persoanelor şi Administrarea Bazelor de Date (DEPABD), în contextul în care informații despre persoana sa și despre un autovehicul au fost interogate și depuse în cadrul unui raport aflat pe rolul unei instanțe de judecată, de către un angajat al autorității reclamate.*

*În urma exercitării dreptului de acces la date, față de mai multe instituții, petentului i s-a comunicat că datele sale cu caracter personal au fost furnizate de către autoritatea reclamată.*

*În cadrul investigației realizate, a rezultat că un angajat al autorității reclamate a solicitat telefonic unui angajat al unui serviciu local al operatorului să facă verificări, prin accesarea unei aplicații informatice, cu privire la autovehiculul petentului. Prin intermediul unui coleg care a verificat autovehiculul pe stația sa de lucru, angajatul serviciului local al operatorului a generat, imprimat și scanat raportul de interogare privind autovehiculul în cauză și l-a trimis pe e-mailul de serviciu al angajatului autorității reclamate.*

*La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul pentru săvârşirea contravenţiei prevăzute de art. 33 din Legea nr. 677/2001, faptă prevăzută de art. 33 din Legea nr. 677/2001, sub forma neîndeplinirii obligațiilor privind aplicarea măsurilor de securitate și de păstrare a confidențialității*

*prelucrărilor prevăzute la art. 20 din aceeași lege, întrucât operatorul (autoritatea reclamată) nu a aplicat suficiente măsuri tehnice și organizatorice, fiind astfel posibil accesul neautorizat la datele cu caracter personal ale petentului, de către un angajat al serviciului local al operatorului, în afara îndeplinirii sarcinilor de serviciu.*

## CAPITOLUL AL V-LEA

## ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

Activitatea în plan extern a Autorităţii naţionale de supraveghere a fost marcată și în anul 2017 de participarea la o serie de grupuri de lucru, 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.

În calitate de membru al Grupului de Lucru Articolul 29, Autoritatea națională de supraveghere s-a implicat în pregătirea pentru noul cadru de protecție a datelor care va fi aplicabil pe întreg teritoriul Uniunii Europene începând cu data de 25 mai 2018. Astfel, Autoritatea naţională de supraveghere, reprezentantă de membrii săi, a participat în 2017 la o serie de reuniuni şi diverse grupuri de lucru la nivel european. Printre acestea se numără:

- Grupul de Lucru Articolul 29 (înfiinţat în temeiul art. 29 din Directiva 95/46/CE) care reuneşte toate autorităţile europene, precum şi Autoritatea Europeană pentru Protecţia Datelor. Astfel, menționăm faptul că Autoritatea naţională de supraveghere, prin membrii săi, a participat la următoarele subgrupuri de lucru: BTLE, Cooperare, eGuvernare, Enforcement, Financial Matters, Future of Privacy, Key provisions, Tehnologie, Transferuri Internaţionale,
- Comitetul Consultativ al Convenţiei 108 al Consiliului Europei (T-PD),
- Organismul comun de control în domeniul Europol şi domeniul Vamal,
- Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II şi Grupul de coordonare comună Eurodac,
- Grupul Internaţional de Lucru pe Protecţia Datelor în domeniul Telecomunicaţiilor, dedicat protecţiei datelor cu caracter personal în sectorul comunicaţiilor electronice,
- Grupul de Lucru pe protecţia datelor în cadrul Convenţiei pentru stabilirea Centrului Sud-Est European de aplicare a legii.

### Grupul de Lucru Articolul 29

În cursul anului 2017, Grupul de Lucru Articolul 29 și-a exprimat poziția față de probleme fundamentale precum reforma în domeniul vieții private și comunicațiilor electronice, prelucrarea datelor cu caracter personal la locul de muncă, prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative, prelucrarea datelor cu

caracter personal în cadrul activității polițienești și judiciare în materie penală și, totodată, a emis o serie de orientări cu privire la aplicarea Regulamentului General privind Protecția Datelor.

Astfel, menționăm următoarele documente ce au fost adoptate fie sub formă de avize, fie sub formă de ghiduri pentru interpretarea și aplicarea Regulamentului General privind Protecția Datelor:

- *avizul cu privire la propunerea de Regulament privind viața privată și comunicațiile electronice (2002/58/CE)* – documentul oferă o analiză a propunerii de Regulament ePrivacy. În acest context, menționăm faptul că Grupul de Lucru Articolul 29 apreciază în mod favorabil alegerea regulamentului ca instrument normativ și consideră că, astfel, se asigură uniformitatea normelor în întreaga UE și claritate atât pentru autoritățile de supraveghere, cât și pentru organizații. De asemenea, se asigură coerența cu Regulamentul general privind protecția datelor. În plus, la asigurarea coerenței contribuie și opțiunea de a desemna aceeași autoritate care răspunde de monitorizarea conformității cu RGPD pentru a răspunde și de asigurarea respectării normelor privind viața privată și comunicațiile electronice. Totodată, alegerea unui instrument juridic complementar reprezintă un aspect pozitiv. Protecția comunicațiilor confidențiale și a echipamentelor terminale comportă caracteristici speciale care nu sunt abordate de RGPD. Prin urmare, sunt necesare dispoziții complementare cu privire la aceste tipuri de servicii, astfel încât să se asigure protecția corespunzătoare a dreptului fundamental la viață privată și confidențialitatea comunicațiilor, inclusiv confidențialitatea echipamentelor terminale. În această privință, Grupul de Lucru Articolul 29 sprijină abordarea principială adoptată în propunerea de Regulament, respectiv de extindere a interdicțiilor și de restrângere a excepțiilor, precum și aplicarea punctuală a conceptului de consimțământ. Cât privește consimțământul privind urmărirea („consent for tracking”), Grupul de Lucru Articolul 29 solicită interzicerea explicită a pereților de urmărire („tracking walls”), adică a opțiunilor de tipul „acceptare sau renunțare”, care îi obligă pe utilizatori să consimtă la urmărire dacă doresc să aibă acces la serviciul respectiv. Grupul de Lucru Articolul 29 a identificat și alte motive de îngrijorare, referitoare, de exemplu, la domeniul de aplicare, la protecția echipamentelor terminale și la marketingul direct. Nu în ultimul rând, Grupul de Lucru Articolul 29 a identificat aspecte care necesită clarificări, pentru a proteja mai bine utilizatorii finali și pentru a asigura un nivel mai ridicat de securitate juridică pentru toate părțile interesate implicate;

- *avizul privind prelucrarea datelor la locul de muncă* – documentul completează Avizul Grupului de Lucru Articolul 29 nr. 8/2001 privind prelucrarea datelor personale în contextul angajării și Documentul de lucru din 2002 privind supravegherea comunicațiilor electronice la locul de muncă. Documentul realizează o nouă evaluare a echilibrului dintre interesul legitim al angajatorului și așteptările angajaților în ceea ce privește confidențialitatea datelor cu caracter personal/respectarea vieții private. Astfel, luând în considerare prevederile Directivei 95/46/CE privind protecția datelor, proiectul de opinie are în vedere obligațiile suplimentare impuse angajatorilor prin Regulamentul General privind Protecția Datelor. De asemenea, prin acest document, Grupul de Lucru Articolul 29 reiterează poziția și concluziile sale exprimate prin Opinia 8/2001 și Documentul de lucru din 2002. În acest context, se subliniază faptul că, atunci când se realizează o prelucrare a datelor cu caracter personal ale angajaților: (i) angajatorii trebuie să respecte întotdeauna principiile fundamentale de protecție a datelor cu caracter personal, indiferent de tehnologia utilizată; (ii) conținutul comunicațiilor electronice realizate în afara spațiului de afaceri beneficiază de aceeași protecție a drepturilor fundamentale ca și comunicațiile analogice; (iii) este foarte puțin probabil ca temeiul legal pentru prelucrarea datelor la locul de muncă să fie reprezentat de consimțământ, cu excepția cazului în care angajații pot refuza fără a exista consecințe negative; (iv) uneori se poate invoca executarea unui contract sau interesul legitim, cu condiția ca prelucrarea să fie strict necesară pentru îndeplinirea unui scop legitim și să respecte principiul proporționalității și cel al subsidiarității; (v) angajații ar trebui să primească informații eficiente cu privire la monitorizarea respectivă; (vi) orice transfer internațional de date ale angajaților ar trebui să aibă loc numai în situația în care se asigură un nivel de protecție adecvat;

- *avizul privind prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative (STI)* – documentul elaborat la nivelul Grupului de Lucru Articolul 29 constă în furnizarea de informații generale privind prelucrarea datelor cu caracter personal în contextul STI cooperative și oferă îndrumări cu scopul de a îmbunătăți nivelul de protecție a datelor în cadrul acestor noi tipuri de aplicații. Astfel, Grupul de Lucru Articolul 29 consideră că următoarele aspecte ale protecției datelor cu caracter personal sunt deosebit de importante: Comisia ar trebui să pună în aplicare regulamente sectoriale pentru colectarea și prelucrarea de date în domeniul sistemelor de transport inteligente; Comisia ar trebui să stabilească o foaie de parcurs pentru prelucrarea legală a datelor de localizare ale cetățenilor UE în contextul STI cooperative, obiectivul final fiind adoptarea unui instrument juridic la nivelul

UE [art. 6 (1) (c) din Regulamentul General privind Protecția Datelor]; adoptarea acestor instrumente juridice ar trebui să înceapă cu o evaluare a necesității și a proporționalității dispozițiilor lor; în plus, în cursul procesului legislativ, ar trebui să se efectueze o evaluare a impactului asupra protecției datelor [art. 35 (10) din Regulamentul General privind Protecția Datelor] pentru a se clarifica de la început riscurile și măsurile de remediere; celelalte temeiuri juridice avute în vedere în documentul grupului de lucru pentru STI cooperative (și anume, consimțământul, îndeplinirea unui interes legitim al contractantului) ar putea fi invocate numai în cazul în care pot fi soluționate aspectele critice identificate pentru fiecare dintre acestea în acest document; în oricare dintre temeiurile juridice selectate, setarea implicită a tuturor funcțiilor STI cooperative instalate trebuie să fie dezactivată; dispozițiile art. 25 din Regulamentul General privind Protecția Datelor (asigurarea protecției datelor începând cu momentul conceperii și în mod implicit) ar trebui să fie puse în aplicare, permițând utilizatorilor să selecteze opțiunile de urmărire (calendar, frecvență, locații) care corespund cel mai bine preferințelor proprii; securitatea ar trebui consolidată, pentru a limita riscul unei utilizări nelegitime a datelor din cadrul STI cooperative; ar trebui să fie introduse alte măsuri corective pentru protecția vieții private începând cu momentul conceperii; categoriile speciale de date și datele referitoare la condamnări penale și infracțiuni nu ar trebui să fie transmise; calitatea datelor ar trebui să fie evaluată cu atenție pentru a reduce orice risc; perioadele de păstrare a datelor prelucrate de către toate părțile implicate în platforma STI cooperative ar trebui să fie indicate în mod clar și ar trebui să fie interzisă crearea unei baze de date centralizate a mesajelor transmise de către oricare dintre actorii din cadrul STI cooperative;

- *avizul privind anumite aspecte importante ale Directivei (UE) 2016/680* – noua Directivă (UE) 2016/680 completează Regulamentul General privind Protecția Datelor. Directiva (UE) 2016/680, care trebuie transpusă în legislația națională până la data de 6 mai 2018, supraveghează prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, cercetării, detectării sau urmăririi penale a infracțiunilor sau executării de sancțiuni penale și asupra liberei circulații a acestor date. Pentru a sugera o înțelegere și o abordare coerentă și datorită diferitelor etape ale punerii în aplicare, Grupul de Lucru Articolul 29 a decis să se concentreze asupra unor aspecte-cheie pentru care sunt necesare orientări practice sau care se referă direct la activitatea autorităților de protecție a datelor sau atunci când procedura de punere în aplicare în unul sau mai multe state membre sugerează că transpunerea nu este în deplină conformitate cu principiile directivei. Având în vedere această

abordare, Grupul de Lucru Articolul 29 oferă în acest document orientări prin recomandări și observații cu privire la următoarele articole: art. 5 – termene de stocare și de revizuire, art. 10 – prelucrarea unor categorii speciale de date cu caracter personal, art. 11 – procesul decizional individual automatizat, inclusiv crearea de profiluri, art. 13-17 – drepturile persoanei vizate, art. 25 – înregistrarea (logs), art. 47 – competențele autorităților pentru protecția datelor;

- *ghidul privind dreptul la portabilitatea datelor* – Art. 20 din Regulamentul General privind Protecția Datelor introduce un drept nou, respectiv dreptul la portabilitatea datelor. Acest drept permite persoanelor vizate să primească datele cu caracter personal pe care le-au furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat, și să transmită datele respective altui operator, fără obstacole. Dreptul la portabilitatea datelor, care se aplică sub rezerva anumitor condiții, sprijină alegerea utilizatorului („user choice"), controlul utilizatorului („user control") și responsabilizarea utilizatorului („user empowerment"). Noul drept la portabilitatea datelor are ca scop responsabilizarea persoanelor vizate în ceea ce privește propriile date cu caracter personal, întrucât facilitează capacitatea de a muta, copia sau transmite datele cu caracter personal de la un mediu IT la altul (fie la propriile sisteme, fie la sistemele unor părți terțe de încredere sau cele ale noilor operatori de date). Prin afirmarea drepturilor și controlul persoanelor vizate asupra datelor cu caracter personal care le privesc, portabilitatea datelor reprezintă, de asemenea, o oportunitate de a „re-echilibra" relația dintre persoanele vizate și operatorii de date. Cu toate că dreptul la portabilitatea datelor este un drept nou, alte tipuri de portabilitate deja există sau sunt discutate în alte domenii ale legislației (de exemplu în contextul rezilierii contractului, servicii de comunicații de roaming și accesul transfrontalier la servicii). Pot apărea unele sinergii și chiar beneficii pentru persoanele fizice între diferitele tipuri de portabilitate, în situația în care sunt prevăzute într-o abordare combinată, chiar dacă analogiile ar trebui să fie tratate cu precauție. Așadar, documentul oferă îndrumări operatorilor de date, astfel încât aceștia să-și actualizeze practicile, procesele și procedurile și clarifică înțelesul de portabilitate a datelor, pentru a permite persoanelor vizate să utilizeze acest drept în mod eficient;

- *ghidul privind responsabilul cu protecția datelor („DPO")* – Regulamentul General privind Protecția Datelor ce urmează să devină aplicabil la data de 25 mai 2018 oferă un cadru legal modernizat pentru protecția datelor în Uniunea Europeană. Responsabilul cu protecția datelor (DPO) va reprezenta centrul acestui nou cadru juridic pentru multe organizații, facilitând respectarea prevederilor Regulamentului General privind Protecția Datelor. Potrivit

Regulamentului General privind Protecția Datelor, este obligatoriu ca anumiți operatori și persoane împuternicite de operatori să desemneze un DPO. Aceasta va fi situația pentru toate autoritățile și organismele publice (indiferent de tipul datelor prelucrate) și pentru celelalte organizații care – ca activitate principală – monitorizează în mod sistematic și pe scară largă persoanele fizice sau prelucrează categorii speciale de date cu caracter personal pe scară largă. Chiar și în situația în care Regulamentul General privind Protecția Datelor nu impune în mod expres numirea unui DPO, organizațiile pot găsi ca fiind utilă desemnarea unui DPO în mod voluntar. Grupul de Lucru Articolul 29 încurajează aceste eforturi voluntare. Conceptul de DPO nu este nou. Cu toate că Directiva 95/46/CE nu impune niciunei organizații să numească un DPO, această practică de numire a unui DPO s-a dezvoltat, de-a lungul anilor, în mai multe state membre. Anterior adoptării Regulamentului General privind Protecția Datelor, Grupul de Lucru Articolul 29 a susținut că DPO reprezintă un punct important al responsabilității și că numirea unui DPO poate facilita respectarea și, în plus, poate reprezenta un avantaj competitiv pentru companii. Pe lângă facilitarea respectării prin punerea în aplicare a instrumentelor de responsabilizare (precum facilitarea evaluărilor impactului asupra protecției datelor și efectuarea sau facilitarea auditurilor), DPO acționează ca intermediar între părțile interesate relevante (de exemplu autoritățile pentru protecția datelor, persoanele vizate și unitățile de afaceri din cadrul unei organizații). DPO nu este personal responsabil în caz de nerespectare a Regulamentului General privind Protecția Datelor. Regulamentul General privind Protecția Datelor stipulează că responsabil este operatorul sau persoana împuternicită de operator care trebuie să se asigure și să fie în măsură să demonstreze că prelucrarea este efectuată în conformitate cu dispozițiile sale (art. 24(1)). Respectarea normelor de protecție a datelor reprezintă responsabilitatea operatorului sau a persoanei împuternicite de operator. Operatorul sau persoana împuternicită de operator are de asemenea un rol crucial în a permite îndeplinirea eficientă a atribuțiilor DPO. Numirea unui DPO reprezintă un prim pas, dar trebuie să se asigure că DPO are autonomie și resurse suficiente pentru îndeplinirea sarcinilor într-un mod eficient. Regulamentul General privind Protecția Datelor recunoaște DPO ca un actor-cheie în noul sistem de guvernare al protecției datelor și stabilește condițiile pentru numirea sa, poziția și sarcinile sale. Obiectivul acestui ghid este de a clarifica prevederile relevante din Regulamentul General privind Protecția Datelor pentru a ajuta operatorii și persoanele împuternicite de operator în vederea respectării legii, dar și pentru a ajuta DPO în ceea ce privește rolul său. Ghidul oferă, de asemenea, recomandări de bune practici, bazându-se pe experiența acumulată în unele state membre UE;

➢ *ghidul privind stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator* – stabilirea unei autorități de supraveghere principale este importantă doar în cazul în care un operator sau o persoană împuternicită de operator efectuează prelucrări transfrontaliere de date cu caracter personal. Astfel, o „autoritate de supraveghere principală" este autoritatea care are responsabilitatea principală în activitatea de prelucrare transfrontalieră a datelor, de exemplu în cazul în care o persoană vizată depune o plângere referitoare la prelucrarea datelor sale personale. Autoritatea de supraveghere principală va coordona orice investigație, implicând alte autorități de supraveghere „vizate". Stabilirea autorității de supraveghere principale depinde de identificarea locației „sediului principal" sau a „sediului unic" al operatorului, pe teritoriul UE. Considerentul 36 al Regulamentului General privind Protecția Datelor este util în clarificarea factorului principal care va fi utilizat pentru a stabili sediul principal al operatorului în cazul în care criteriul administrației centrale nu se aplică. Acest lucru implică identificarea locului în care se exercită efectiv și real activitățile de management, care stabilesc deciziile principale privind scopurile și mijloacele de prelucrare prin acorduri stabile. Esența autorității de supraveghere principale în Regulamentul General privind Protecția Datelor este că supravegherea prelucrării transfrontaliere ar trebui să fie în sarcina unei singure autorități de supraveghere pe teritoriul UE. În cazurile în care deciziile privind diferitele activități de prelucrare transfrontalieră sunt luate în cadrul administrației centrale pe teritoriul UE, va fi o singură autoritate de supraveghere principală pentru diversele activități de prelucrare a datelor efectuate de compania multinațională;

➢ *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* – art. 35 din Regulamentul General privind Protecția Datelor introduce conceptul de Evaluarea impactului asupra protecției datelor (DPIA), așa cum prevede și Directiva (UE) 2016/680. DPIA reprezintă o parte esențială a respectării Regulamentului General privind Protecția Datelor atunci când este planificată sau are loc o prelucrare a datelor cu risc ridicat. Aceasta înseamnă că operatorii de date ar trebui să utilizeze criteriile stabilite în acest document pentru a stabili dacă trebuie sau nu să realizeze o DPIA. Politica internă a operatorului de date ar putea extinde această listă în afara cerințelor legale ale Regulamentului General privind Protecția Datelor. Acest lucru ar trebui să ducă la o mai mare încredere a persoanelor vizate și a altor operatori de date. În cazul în care este planificată o prelucrare cu risc ridicat, operatorul de date trebuie: (i) să aleagă o metodologie DPIA care să îndeplinească

criteriile stabilite în ghid sau să specifice și să implementexe un proces sistematic de DPIA care să fie în conformitate cu criteriile prezentate în documentul adoptat de Grupul de Lucru Articolul 29, care este integrat în procesele existente de proiectare, dezvoltare, schimbare, risc și revizuire operațională, în conformitate cu procedurile interne, contextul și cultura, care implică părțile interesate și care definește în mod clar responsabilitățile acestora (operatorul, DPO, persoanele vizate sau reprezentanții acestora, întreprinderi, servicii tehnice, persoanele împuternicite de operatori, ofițerii de securitate a informațiilor etc.); (ii) să furnizeze raportul DPIA autorității de supraveghere competente atunci când este necesar să o facă; (iii) să consulte autoritatea de supraveghere atunci când nu a reușit să stabilească suficiente măsuri pentru atenuarea riscurilor ridicate; (iv) să revizuiască periodic DPIA și procesele pe care le evaluează, cel puțin atunci când există o schimbare a riscului reprezentat de prelucrarea operațiunii; (v) să documenteze deciziile luate.

La sfârșitul anului 2017, Grupul de Lucru Articolul 29 a adoptat următoarele ghiduri disponibile spre consultare publică și trimitere de propuneri:

- *ghidul privind notificarea încălcărilor de securitate în sensul Regulamentului (UE) 2016/679* – Regulamentul General privind Protecția Datelor introduce cerința privind notificarea autorității naționale pentru protecția datelor în legătură cu încălcarea securității datelor și, în anumite situații, comunicarea încălcării securității datelor către persoanele fizice ale căror date cu caracter personal au fost afectate de încălcare. Grupul de Lucru Articolul 29 consideră că noua cerință de notificare are numeroase beneficii. Atunci când notifică autoritatea de supraveghere, operatorii pot obține sfaturi dacă persoanele afectate trebuie să fie informate. Într-adevăr, autoritatea de supraveghere poate solicita operatorului să informeze acele persoane în legătură cu încălcarea securității datelor. Notificarea încălcării securității datelor trebuie privită ca un instrument de îmbunătățire a respectării legii în ceea ce privește protecția datelor cu caracter personal. Regulamentul General privind Protecția Datelor conține dispoziții cu privire la momentul în care o încălcare trebuie notificată și cui, precum și ce informații ar trebui furnizate ca parte a notificării. Informațiile solicitate pentru notificare pot fi furnizate în etape, dar, în orice caz, operatorii ar trebui să acționeze în timp util asupra oricărei încălcări. Trebuie subliniat faptul că neîndeplinirea acestei obligații poate însemna o eventuală sancțiune aplicabilă operatorului în temeiul art. 83 din Regulamentul General privind Protecția Datelor. Acest document explică cerințele obligatorii de notificare și de comunicare, precum și anumiți pași pe care operatorii și persoanele împuternicite de operator trebuie să îi parcurgă pentru a

îndeplini aceste noi obligații. Ghidul oferă, de asemenea, exemple de tipuri de încălcări și diferite scenarii privind cine ar trebui să fie notificat/informat;

- *ghidul privind procesul decizional individual automatizat, inclusiv crearea de profiluri în sensul Regulamentului (UE) 2016/679* – Regulamentul General privind Protecția Datelor se referă în mod special la crearea de profiluri și procesul decizional individual automatizat, inclusiv crearea de profiluri. Profilarea și luarea automată a deciziilor sunt utilizate într-un număr tot mai mare de sectoare atât private, cât și publice. Sistemul bancar și finanțele, asistența medicală, asigurări, marketing și publicitate sunt doar câteva exemple din domeniile în care se realizează o profilare mai regulată pentru a ajuta la luarea deciziilor. Cu toate acestea, crearea de profiluri și procesul decizional automatizat pot prezenta riscuri semnificative pentru drepturile și libertățile persoanelor fizice și, implicit, necesită garanții adecvate. Regulamentul General privind Protecția Datelor introduce noi dispoziții pentru a aborda riscurile care decurg din crearea de profiluri și procesul decizional automatizat, în special, dar fără a se limita la viața privată. Scopul acestor orientări este de a clarifica aceste dispoziții. Documentul publicat de Grupul de Lucru Articolul 29 abordează următoarele aspecte: definiția profilării și a procesului decizional automatizat; prevederile generale privind crearea de profiluri și procesul decizional automatizat; prevederile specifice privind deciziile bazate exclusiv pe prelucrarea automată, așa cum este menționat la art. 22 din Regulamentul General privind Protecția Datelor; minorii și crearea de profiluri; evaluarea impactului asupra protecției datelor și responsabilii cu protecția datelor;

- *ghidul privind consimțământul în sensul Regulamentului (UE) 2016/679* – documentul oferă o analiză aprofundată a noțiunii de consimțământ din Regulamentul General privind Protecția Datelor. Conceptul de consimțământ, așa cum este menționat în Directiva 95/46/CE și Directiva ePrivacy, a evoluat. Regulamentul General privind Protecția Datelor oferă o clarificare suplimentară și o specificare a cerințelor pentru obținerea și demonstrarea consimțământului valabil. Ghidul se concentrează asupra acestor modificări și oferă orientări practice pentru a asigura conformitatea cu Regulamentul General privind Protecția Datelor, având la bază Avizul Grupului de Lucru Articolul 29 nr. 15/2011 privind consimțământul. Opiniile existente ale Grupului de Lucru Articolul 29 privind consimțământul rămân relevante, întrucât Regulamentul General privind Protecția Datelor menționează faptul că orientările și bunele practici generale ale Grupului de Lucru Articolul 29 existente și majoritatea elementelor-cheie ale consimțământului rămân aceleași. Așadar, prin acest document, Grupul de Lucru Articolul 29

extinde și completează opiniile anterioare pe teme specifice care includ trimiterea la consimțământul în temeiul Directivei 95/46/CE;

- *ghidul privind transparența în sensul Regulamentului (UE) 2016/679* – documentul oferă orientări practice și asistență interpretativă privind noua obligație de transparență în ceea ce privește prelucrarea datelor cu caracter personal în temeiul Regulamentului General privind Protecția Datelor. Transparența reprezintă o obligație generală în temeiul Regulamentului General privind Protecția Datelor care se aplică în trei domenii centrale: (1) furnizarea de informații persoanelor vizate legate de prelucrarea corectă; (2) modul în care operatorii de date comunică cu persoanele vizate în legătură cu drepturile lor în temeiul Regulamentului General privind Protecția Datelor; și (3) modul în care operatorii de date facilitează exercitarea de către persoanele vizate a drepturilor lor. În măsura în care respectarea transparenței este necesară în ceea ce privește prelucrarea datelor în conformitate cu Directiva (UE) 2016/680, aceste linii directoare se aplică, de asemenea, interpretării acestui principiu. Cerințele de transparență din Regulamentul General privind Protecția Datelor se aplică indiferent de temeiul juridic al prelucrării și pe întrega durată a acesteia. Acest lucru este clar din art. 12 care prevede că transparența se aplică în următoarele etape ale ciclului de prelucrare a datelor: (i) înainte sau la începutul ciclului de prelucrare a datelor, în cazul în care datele cu caracter personal sunt colectate fie de la persoana vizată, fie obținute în alt mod; (ii) pe parcursul întregii perioade de prelucrare, în cazul în care comunică cu persoanele vizate în legătură cu drepturile lor; și (iii) în anumite etape, în timp ce prelucrarea este în desfășurare, de exemplu atunci când apar încălcări ale securității datelor sau în cazul unor modificări semnificative ale prelucrării.

**Comitetul Consultativ al Convenţiei 108 al Consiliului Europei**

În anul 2017, au fost continuate discuțiile în contextul modernizării Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (T-PD), cunoscută sub denumirea de Convenția 108. Totodată, în urma reuniunilor Comitetului Consultativ al Convenţiei 108 al Consiliului Europei, a fost publicat Ghidul privind protecția persoanelor în legătură cu prelucrarea datelor cu caracter personal în contextul Big Data. Big Data reprezintă o nouă paradigmă în ceea ce privește modul în care datele sunt colectate, combinate și analizate. Big Data, care beneficiază de interacțiunea cu alte medii tehnologice, precum Internetul Lucrurilor și cloud computing, poate reprezenta o sursă de inovație pentru societate.

În același timp, deoarece Big Data permite colectarea și analizarea unui volum mare de date pentru a identifica și prezice comportamentul grupurilor și comunităților, trebuie luată în considerare și dimensiunea colectivă a riscurilor asociate utilizării datelor. În acest context, Comitetul Consultativ al Convenţiei 108 a considerat ca fiind necesară elaborarea acestui ghid care oferă un cadru general în ceea ce privește implementarea de proceduri și măsuri adecvate pentru a asigura eficiența principiilor și dispozițiilor Convenției 108 în contextul Big Data. Acest document a fost elaborat luând în considerare principiile Convenției 108, ținând cont de procesul continuu de modernizare a acesteia, și se adresează în primul rând factorilor de decizie, operatorilor și persoanelor împuternicite de operator. Prin intermediul acestui ghid se recomandă operatorilor și persoanelor împuternicite de operator să implementeze măsuri pentru a preveni impactul negativ al utilizării Big Data asupra demnității umane, drepturilor omului și libertăților fundamentale, în special în ceea ce privește protecția datelor cu caracter personal.

De asemenea, Comitetul Consultativ al Convenţiei 108 a publicat proiectul de Ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc. Documentul subliniază cele mai importante aspecte care pot apărea în utilizarea datelor cu caracter personal în sectorul polițienesc, dar și elementele cheie care trebuie luate în considerare în acest context. Acest ghid nu repetă prevederile Convenției 108 și nici pe cele ale Recomandării (87) 15, ci se axează pe îndrumări practice. Principiile explicate în acest document se aplică prelucrării datelor cu caracter personal în scopul prevenirii, cercetării și urmăririi penale a infracțiunilor, al executării pedepselor. Trebuie subliniat faptul că acest ghid intenționează să ofere orientări pentru situația practică cu care poliția se poate confrunta în cadrul operațiunilor sale zilnice și recunoaște faptul că pentru autoritățile de aplicare a legii colectarea și utilizarea legală a datelor cu caracter personal sunt esențiale în interesul securității naționale și al prevenirii infracționalității sau menținerii ordinii publice.

În ceea ce privește aderarea la Convenția 108, au fost primite solicitări de aderare din partea Republicii Argentina și a Statelor Unite Mexicane. Referitor la Republica Argentina, Comitetul Consultativ al Convenției 108 a considerat că legea națională referitoare la protecția datelor cu caracter personal respectă pe deplin prevederile Convenției 108. Prin urmare, pe baza analizei legislației aplicabile privind protecția datelor, Comitetul Consultativ al Convenției 108 a decis ca cererea Republicii Argentina de a fi invitată să adere la Convenția 108 să primească un răspuns favorabil. Astfel, Comitetul Consultativ al Convenției 108 recomandă, de

asemenea, ca Republica Argentina să fie invitată să adere la protocolul adițional. Față de solicitarea Statelor Unite Mexicane, Comitetul Consultativ al Convenției 108 consideră că dispozițiile legale naționale privind protecția datelor din Statele Unite Mexicane respectă, în general, principiile Convenției 108 și ale Protocolului său adițional. Comitetul Consultativ al Convenției 108 constată că sunt binevenite unele ajustări ale dispozițiilor legale. Pe baza analizei legislației aplicabile privind protecția datelor, Comitetul Consultativ al Convenției 108 a considerat că trebuie să se răspundă favorabil solicitării Statelor Unite Mexicane de a fi invitate să adere la Convenția 108 și la protocolul adițional.

**Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II, Grupul de coordonare comună Eurodac și Consiliul de Cooperare Europol**

Grupul de coordonare comună VIS a adoptat un chestionar privind implementarea art. 41 din Regulamentul VIS pentru a evalua punerea în aplicare a obligației autorităților de supraveghere de a efectua un audit independent cel puțin o dată la patru ani pentru a verifica legalitatea operațiunilor de prelucrare a datelor cu caracter personal înregistrate în sistemele VIS naționale. Una din constatările principale evidențiate în raportul redactat pe baza răspunsurilor primite este aceea că majoritatea statelor membre au efectuat deja auditul prevăzut la art. 41 sau acesta se află în curs de desfășurare. Metodologia cea mai frecvent utilizată de autoritățile pentru protecția datelor pentru realizarea auditului este aceea de investigație la fața locului. În plus, toate autoritățile de supraveghere au subliniat faptul că nu au primit nici resurse financiare, nici resurse umane suplimentare.

Referitor la activitatea în legătură cu Sistemul de Informații Schengen, în anul 2017, Grupul de coordonare comună SIS II a adoptat și a transmis către Președinția Parlamentului UE adresa ce exprimă poziția grupului față de pachetul legislativ cu privire la Sistemul de Informații Schengen. Astfel, prin acest document, Grupul de Coordonare Comună SIS II sprijină argumentele prezentate de Autoritatea Europeană privind Protecția Datelor prin Opinia sa nr. 7/2017 și subliniază aspectele care trebuie luate în considerare în cadrul viitoarelor trialoguri ce vor avea loc pe marginea pachetului legislativ SIS, respectiv:

- pregătirea unei analize prealabile cu privire la necesitatea introducerii noilor identificatori biometrici (imaginea facială, amprenta palmelor și profilele ADN),
- o mai bună definire a drepturilor și regulilor de access pentru Frontex,

- justificarea necesității extinderii perioadei de reținere a alertelor cu privire la persoane, de la 3 la 5 ani,
- introducerea posibilității pentru Biroul SIRENE de a șterge alertele cu privire la obiecte, după îndeplinirea scopului,
- desfășurarea de campanii de informare regulate în vederea creșterii conștientizării persoanelor vizate.

Drepturile persoanelor vizate reprezintă un element esențial pentru protecția datelor cu caracter personal, întrucât acestea permit un control al persoanelor fizice asupra prelucrării datelor lor cu caracter personal. În acest context, simplul fapt că se asigură persoanelor vizate accesul la datele personale proprii, într-un mod eficient, precum și corectarea sau ștergerea respectivelor informații personale poate constitui un sprijin pentru descoperirea prelucrărilor ilegale de date cu caracter personal și pentru creșterea calității datelor în ceea ce privește prelucrările legale efectuate de operatorul de date. Aceste considerații sunt cu atât mai relevante în privința cererilor de azil, având în vedere consecințele negative ale prelucrării ilegale sau eronate a datelor cu caracter personal asupra solicitanților de azil.

Grupul de Coordonare Comună Eurodac a investigat și în anii anteriori exercitarea drepturilor persoanelor vizate. În acest context, a adoptat un raport privind pregătirea națională pentru punerea în aplicare a reformei Eurodac, document ce a inclus mai multe întrebări referitoare la drepturile persoanelor vizate.

Având în vedere importanța problematicii drepturilor persoanelor vizate, Grupul de Coordonare Comună Eurodac a decis continuarea verificării modului în care drepturile persoanelor vizate sunt puse în aplicare, prin redactarea unui chestionar elaborat pe baza chestionarelor anterioare și a planului standard de inspecții în domeniul Eurodac.

Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Regulamentul Europol) a fost adoptat în data de 11 mai 2016 și a devenit aplicabil începând cu data de 1 mai 2017. De la această dată, Autoritatea Europeană privind Protecția Datelor (AEPD) a înlocuit Organismul Comun de Supraveghere în calitate de autoritate competentă pentru monitorizarea legalității prelucrării datelor cu caracter personal efectuate de Europol, în timp ce competența autorităților naționale pentru protecția datelor a rămas neschimbată. Un aspect esențial al supravegherii legalității prelucrării datelor efectuate de Europol îl reprezintă cooperarea

autorităților naționale de supraveghere cu Autoritatea Europeană privind Protecția Datelor, în special în cadrul nou-înființatului Consiliu de Cooperare Europol, un forum cu funcții consultative pentru discutarea problemelor comune, care colaborează pentru a elabora, de exemplu, avize, ghiduri, recomandări și bune practici, pentru a analiza dificultățile de interpretate sau aplicare a Regulamentului Europol. Astfel, în anul 2017 a avut loc prima reuniune a Consiliului de Cooperare Europol, în cadrul căreia au fost adoptate Regulile de procedură prin care se stabilesc competențele acestui forum, atribuțiile președintelui Consiliului de Cooperare, metodele de lucru în cadrul forului.

**Grupul Internaţional de lucru pentru Protecţia Datelor în domeniul Telecomunicaţiilor**

În cadrul reuniunilor Grupului Internaţional de lucru pentru Protecţia Datelor în domeniul Telecomunicaţiilor, discuțiile s-au axat și în anul 2017 pe temele privind viaţa privată referitor la platformele de e-learning, aspecte privind viaţa privată cu privire la datele din registrul WHOIS, ICANN, inteligența artificială, viaţa privată şi standardizarea internaţională.

Discuțiile s-au concretizat prin adoptarea documentului de lucru privind viața privată pe platformele de tip e-learning, a documentului de lucru privind principiile sau instrumentele internaționale pentru colectarea informațiilor guvernamentale și a documentului de lucru referitor la aspecte privind viaţa privată în legătură cu datele din registrul WHOIS, ICANN.

Utilizarea platformelor de tip e-learning, care devine tot mai populară în numeroase state, conduce la creșterea numărului de date personale digitalizate generate de elevi și de comportamentul și performanța acestora. În plus, datele digitalizate detaliate despre elevi și studenți pot determina cererea de utilizare sporită a datelor în cadrul educației, inclusiv utilizarea așa-numitelor „analize de învățare”.

Această evoluție poate duce la o lipsă de transparență dacă părinții și studenții nu au acces la datele utilizate pentru a lua decizii și la procesul de luare a deciziilor. Mai mult decât atât, riscul ca societățile private care colectează date pe astfel de platforme să le folosească și dincolo de obiectivul academic este evident. În afară de scopurile evidente de marketing, astfel de date ar putea fi folosite chiar și pentru a lua decizii în lumea reală în legătură cu viitoarele oportunități ale studenților, inclusiv privind ocuparea forței de muncă, locuințele și creditele.

Documentul de lucru privind platformele de e-learning descrie și alte riscuri asociate acestor platforme în ceea ce privește confidențialitatea datelor. De asemenea, materialul oferă

recomandări instituțiilor de învățământ, furnizorilor de platforme de e-learning și autorităților pentru protecția datelor.

În ceea ce privește principiile sau instrumentele internaționale pentru guvernarea colectării inteligente, în ultimii ani a existat o creștere a gradului de conștientizare publică, precum și discuții în legătură cu interesul statelor cu privire la securitatea națională și drepturile persoanelor la viață privată.

Documentul de lucru intitulat „Către principii internaționale sau instrumente pentru colectarea informațiilor guvernamentale" subliniază recentele solicitări de consens privind standardele internaționale în acest domeniu și oferă recomandări autorităților pentru protecția datelor care contribuie la elaborarea unor noi principii.

**Grupului de Lucru pe protecţia datelor în cadrul Convenţiei pentru stabilirea Centrului Sud-Est European de aplicare a legii (PCC SEE)**

În anul 2017, discuțiile din cadrul Grupului de Lucru PCC SEE s-au axat pe proiectul de Acord de implementare privind protecția datelor referitor la Convenția de Cooperare Polițienească în Europa de Sud-Est (PCC SEE). În acest context, au fost fomulate o serie de observații și recomandări menite să aducă mai multă claritate documentului. Având în vedere contribuția importantă a reprezentantului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal la elaborarea proiectului de Acord de implementare, Secretariatul PCC SEE a propus ca partea română să își asume rolul de raportor al unui subgrup, format din experți ai Grupului de Lucru PCC SEE privind protecția datelor – reprezentanți ai autorităților naționale pentru protecția datelor și ai poliției, precum și experți în elaborarea acordurilor internaționale, care va definitiva Acordul de implementare privind protecția datelor referitor la Convenția de Cooperare Polițienească în Europa de Sud-Est.

**A 38ª Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private**

În anul 2017, cea de-a 39ª Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private a fost organizată de Autoritatea pentru protecţia datelor din Hong Kong. În cadrul conferinței au fost adoptate 3 rezoluții:

- rezoluția privind protecția datelor în legătură cu vehiculele automatizate și conectate – prin care se face apel la toate părțile relevante implicate să respecte pe deplin drepturile

utilizatorilor cu privire la protecția datelor cu caracter personal și a vieții private și să aibă în vedere aceste drepturi în cadrul fiecărei etape de creare și/sau dezvoltare de noi dispozitive sau servicii;

- rezoluția privind cooperarea dintre autoritățile pentru protecția datelor și autoritățile pentru protecția consumatorilor pentru o mai bună protejare a cetățenilor și consumatorilor într-o economie digitală – document prin care se subliniază necesitatea identificării unor modalități de îmbunătățire a colaborării la nivel internațional între autoritățile pentru protecția datelor și autoritățile pentru protecția consumatorilor în scopul asigurării unei mai bune protecții cetățenilor și consumatorilor într-o economie digitală;
- rezoluția privind explorarea viitoarelor opțiuni de cooperare internațională pentru o aplicare consolidată a prevederilor legale în domeniul protecției datelor cu caracter personal.

**Conferinţa de primăvară a autorităţilor europene pentru protecţia datelor**

În anul 2017, Conferința de primăvară a autorităților europene pentru protecția datelor cu caracter personal a fost organizată de autoritatea pentru protecția datelor din Cipru. Subiectele dezbătute au vizat aspecte precum:

- noul regim juridic în domeniul protecției datelor cu caracter personal,
- activitatea de conștientizare/informare – apropierea dintre autoritățile pentru protecția datelor, companii și publicul larg,
- asigurarea transparenței și respectarea principiului responsabilității în mediile de stocare virtuale,
- accesul autorităților de aplicare a legii la datele cu caracter personal – sisteme la scară largă, interoperabilitate și fluxuri transfrontaliere de date cu caracter personal,
- bazele de date ADN – provocări pentru viața privată.

În cadrul conferinței au fost adoptate 2 rezoluții: rezoluția privind modernizarea Convenției pentru protecția persoanelor fizice cu privire la prelucrarea automată a datelor cu caracter personal și rezoluția privind regulile și procedurile aferente Conferinței Autorității Europene pentru Protecția Datelor.

**Misiuni de evaluare Schengen**

O parte însemnată a activității Autorității naționale de supraveghere în plan extern, în cursul anului 2017, a constituit participarea instituției noastre la misiunile de evaluare Schengen în domeniul protecţiei datelor din Islanda și Portugalia.

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. Acest document conține, printre altele, constatări și evaluări privind legislația, autoritatea pentru protecția datelor, drepturile persoanelor vizate, cooperarea internațională.

**Sistemul de Informații Schengen de a doua generație (SIS II)**

În decembrie 2016, Comisia Europeană a lansat un pachet legislativ de revizuire a cadrului legal în domeniul Sistemului de Informații Schengen de a doua generație (SIS II), compus din 3 propuneri de regulament care modifică baza legală la nivel european în ceea ce privește funcționarea SIS II, respectiv:

- propunerea de regulament privind returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală,
- propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul controalelor la frontieră, modificarea Regulamentului (UE) 515/2014 și abrogarea Regulamentului (CE) 1987/2006,
- propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și judiciare în materie penală, modificarea Regulamentului (UE) 515/2014 și abrogarea Regulamentului (CE) 1986/2006, a Deciziei Consiliului 533/2007, a Deciziei Comisiei 261/2010.

[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

Propunerea de regulament privind returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală dezvoltă și îmbunătățește sistemul existent. Aceasta extinde domeniul de aplicare al actualului SIS prin introducerea unei noi categorii de alertă pentru deciziile de returnare. Impactul său asupra drepturilor fundamentale este, prin urmare, limitat, deoarece funcționarea solidă a sistemului a fost deja dovedită și au fost deja puse în aplicare garanții importante și eficiente. Cu toate acestea, deoarece propunerea implică prelucrarea datelor cu caracter personal, există un posibil impact asupra drepturilor fundamentale ale unei persoane fizice. Acest lucru a fost luat în considerare și au fost instituite garanții pentru a se respecta principiile enunțate în Carta drepturilor fundamentale a Uniunii Europene.

Față de propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul controalelor la frontieră, cadrul juridic actual al SIS II referitor la utilizarea acestuia în scopul controalelor la frontiere ale resortisanților țărilor terțe se bazează pe un instrument al fostului pilon 1, și anume Regulamentul (CE) nr. 1987/2006. Acestă propunere înlocuiește cadrul legal existent pentru:

- a obliga statele membre să introducă o alertă în SIS în toate cazurile în care a fost emisă o interdicție de intrare unui resortisant al unei țări terțe aflat în situație de ședere ilegală, în conformitate cu dispozițiile care respectă Directiva 2008/115/CE;
- a armoniza procedurile naționale de utilizare a SIS în legătură cu procedura de consultare pentru a evita ca un resortisant al unei țări terțe care face obiectul unei interdicții de intrare să dețină un permis de ședere valabil emis de un stat membru;
- a introduce modificări tehnice în vederea îmbunătățirii securității și pentru a contribui la reducerea sarcinilor administrative;
- a aborda utilizarea completă a SIS, acoperind nu numai sistemele centrale și naționale, ci și necesitățile utilizatorului final prin asigurarea faptului că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile și a respecta toate cerințele de securitate atunci când prelucrează datele SIS.

Această propunere dezvoltă și îmbunătățește un sistem existent, în loc să stabilească unul nou și, prin urmare, se bazează pe garanții importante și eficiente care au fost deja puse în aplicare. Cu toate acestea, întrucât sistemul continuă să prelucreze date cu caracter personal și va prelucra alte categorii de date biometrice sensibile, există un posibil impact asupra drepturilor fundamentale ale unei persoane fizice. Aceste aspecte au fost luate în considerare

cu atenție și au fost instituite măsuri de protecție suplimentare pentru a se limita colectarea și prelucrarea ulterioară a datelor la ceea ce este strict necesar din punct de vedere operațional.

În ceea ce privește propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și judiciare în materie penală, cadrul juridic actual al SIS II referitor la utilizarea sa în scopul cooperării polițienești și judiciare în materie penală se bazează pe un instrument al fostului pilon 3, și anume Decizia 2007/533/JAI a Consiliului și pe fostul pilon 1, respectiv Regulamentul (CE) 1986/2006.

Această propunere consolidează conținutul instrumentelor existente adăugând în același timp noi dispoziții pentru a:

- armoniza mai bine procedurile naționale de utilizare a SIS, în special în ceea ce privește infracțiunile legate de terorism, precum și copiii expuși riscului de răpire de către părinți;
- extinde domeniul de aplicare al SIS prin introducerea de noi elemente de identificare biometrică în alertele existente;
- introduce modificări tehnice în vederea îmbunătățirii securității și pentru a contribui la reducerea sarcinii administrative prin furnizarea copiilor naționale obligatorii și a standardelor tehnice comune de punere în aplicare;
- aborda utilizarea completă a SIS, acoperind sistemele centrale și naționale, cu asigurarea că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile și a respecta toate normele de securitate atunci când prelucrează datele SIS.

Deoarece SIS II va continua să prelucreze date cu caracter personal, precum și alte categorii de date cu caracter special, respectiv date biometrice, ar putea exista un impact asupra drepturilor fundamentale ale persoanelor fizice ale căror date sunt prelucrate. În acest sens, au fost implementate măsuri suplimentare de protecție pentru a se limita colectarea și prelucrarea ulterioară a datelor cu caracter personal. În plus, propunerea consolidează măsurile de protecție a drepturilor fundamentale, deoarece stabilește în legislație cerințele pentru care trebuie ștearsă o alertă și introduce o evaluare a proporționalității în cazul în care se prelungește perioada de valabilitate a unei alerte.

Față de cele 3 propuneri de regulament ce fac parte din pachetul legislativ de revizuire a cadrului legal în domeniul Sistemului de Informații Schengen de a doua generație (SIS II), Autoritatea națională de supraveghere a formulat o serie de observații și propuneri, în special cu referire la drepturile persoanelor vizate ale căror date cu caracter personal sunt prelucrate.

**Revizuirea Regulamentului (CE) 45/2001**

Dreptul la protecția datelor cu caracter personal se aplică și prelucrării datelor cu caracter personal efectuate de instituțiile, organismele, oficiile și agențiile UE. În 2001 a fost adoptat Regulamentul (CE) nr. 45/2001, principala parte a legislației UE privind protecția datelor cu caracter personal în cadrul instituțiilor Uniunii Europene, având în vedere două obiective: protejarea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal în întreaga Uniune Europeană.

În aprilie 2016, Parlamentul European și Consiliul au adoptat Regulamentul General privind Protecția Datelor, care va deveni aplicabil începând cu data de 25 mai 2018. Regulamentul General privind Protecția Datelor cere ca Regulamentul (CE) 45/2001 să fie adaptat la principiile și normele stabilite în Regulamentul General privind Protecția Datelor, pentru a asigura un cadru solid și coerent de protecție a datelor în Uniune și pentru a permite ca ambele instrumente să fie aplicabile în același timp.

Propunerea de regulament este în concordanță cu abordarea coerentă a protecției datelor cu caracter personal în întreaga Uniune pentru a alinia, în măsura posibilităților, normele de protecție a datelor pentru instituțiile, organismele, oficiile și agențiile Uniunii Europene la normele de protecție a datelor adoptate pentru statele membre.

**Sistemul european de informații și de autorizare privind călătoriile (European Travel Information and Authorisation System – ETIAS)**

ETIAS va fi un sistem automat, înființat pentru identificarea eventualelor riscuri prezentate de un vizitator exonerat de obligația de a deține viză care călătorește în spațiul Schengen, care va colecta informații cu privire la acești vizitatori înainte de începerea călătoriei, pentru a permite prelucrarea prealabilă a datelor.

Prin urmare, funcția principală a ETIAS ar consta în verificarea informațiilor transmise de către resortisanții țărilor terțe exonerați de obligația de a deține viză, prin intermediul unei cereri online, înainte de sosirea lor la frontierele externe ale UE, pentru a stabili dacă aceștia prezintă anumite riscuri în materie de migrație neregulamentară, securitate sau sănătate publică.

Propunerea de regulamentul are un impact asupra drepturilor fundamentale, în special asupra dreptului la demnitate, la libertate și securitate, la respectarea vieții private și familiale,

la protecția datelor cu caracter personal, la azil și la protecția în caz de îndepărtare, expulzare sau extrădare, la nediscriminare, asupra drepturilor copilului, precum și asupra dreptului la o cale de atac eficientă.

Interesul public legitim legat de asigurarea unui nivel ridicat de securitate este afectat în mod pozitiv de punerea în aplicare a unui sistem de tip ETIAS. O mai bună și mai precisă identificare a riscului de securitate în cazul resortisanților țărilor terțe aflați în afara regimului de vize, care traversează frontiera externă a spațiului Schengen, sprijină detectarea traficului de ființe umane (în special în cazul minorilor) și a criminalității transfrontaliere și, în general, facilitează identificarea persoanelor a căror prezență în spațiul Schengen ar reprezenta o amenințare la adresa securității. Prin urmare, ETIAS contribuie la îmbunătățirea securității cetățenilor prezenți în spațiul Schengen și la consolidarea securității interne în UE.

Față de propunerea de regulament ce va institui sistemul ETIAS, Autoritatea națională de supraveghere a formulat o serie de observații și propuneri, în special cu referire la drepturile persoanelor vizate ale căror date cu caracter personal sunt prelucrate.

**Conferinţe, seminarii și alte reuniuni privind aplicarea Regulamentului General privind Protecţia Datelor**

Pe parcursul anului 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la o serie de evenimente dedicate cadrului legal în domeniul protecției datelor și noutăților aduse de Regulamentul General privind Protecția Datelor.

În cadrul evenimentelor privind aplicarea Regulamentului General privind Protecția Datelor, participanții au fost informați în legătură cu impactul noii reglementări la nivel european, precum și cu obligațiile ce le revin potrivit Regulamentului General privind Protecția Datelor, cum ar fi desemnarea unui responsabil cu protecția datelor, notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal, efectuarea evaluării impactului asupra protecției datelor în situația în care prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, păstrarea evidenței activității de prelucrare desfășurate și, nu în ultimul rând, asigurarea securității datelor cu caracter personal.

# CAPITOLUL VI

# ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

În anul 2017, Autoritatea națională de supraveghere a soluţionat **6.437** solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări şi cereri prin care se solicita punctul de vedere sau clarificarea unor aspecte privind prelucrările de date cu caracter personal efectuate.

Au fost soluţionate **6.115** notificări privind prelucrări de date cu caracter personal, dintre care **4795** efectuate pe teritoriul României şi **1320** transferuri de date către state din Uniunea Europeană, Zona Economică Europeană şi state terţe.

Din cele **1320** notificări cu transferuri de date către entităţi din străinătate, în **1030** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terţe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield).

Totodată, au fost notificate **290** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, în baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules).

În urma analizării transferurilor de date în străinătate către state terţe, a fost emis un număr de **74** autorizaţii de transfer.

În acelaşi timp, au fost analizate **322** solicitări ale operatorilor privind aspecte referitoare la dispoziţiile Legii nr. 677/2001, modificată şi completată.

## Secțiunea 1- Activitatea de înregistrare a prelucrărilor de date

Potrivit prevederilor Deciziei nr. 200/2015, emisă în temeiul art. 22 alin. (9) din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată și completată, notificarea Autorităţii naţionale de supraveghere nu mai este necesară, cu excepţia cazurilor enumerate la art. 1 alin. (1) din Decizia nr. 200/2015.

La elaborarea acestui act normativ s-au luat în considerare prevederile Regulamentului (UE) 2016/679 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 referitoare la eliminarea obligaţiei operatorilor de a notifica autorităţile naţionale de supraveghere pentru prelucrările de date efectuate.

Deși, prin Decizia președintelui Autorității naționale de supraveghere au fost reglementate expres cazurile pentru care este necesară notificarea autorității, reprezentanții unor autorități și instituții publice au emis, contrar prevederilor deciziei susmenționate, acte normative prin care au stabilit obligația pentru operatorii din diferite domenii de activitate de a notifica Autoritatea națională de supraveghere pentru prelucrările de date care nu intrau sub incidența dispozițiilor Deciziei nr. 200/2015.

Dintre acestea, precizăm:

- Ordinul nr. 4/2017 emis de președintele Autorității Naționale pentru Protecția Consumatorului privind documentația și informațiile necesare înregistrării, precum și modalitatea și termenele de raportare pentru dezvoltatorii imobiliari, care a stabilit obligaţia acestora de a face dovada că sunt operatori de date cu caracter personal;
- Ordinul nr. 1/2017 emis de președintele Autorității Naționale pentru Protecția Consumatorului privind documentaţia şi informaţiile necesare înregistrării, precum şi modalitatea şi termenele de raportare pentru entităţile de recuperare creanţe, care a stabilit obligația acestora de a face dovada că sunt operatori de date cu caracter personal;
- Ordinul nr. 2632/2016 pentru dezvoltarea serviciilor Ministerului Finanţelor Publice puse la dispoziţia autorităţilor şi instituţiilor publice prin sistemul informatic propriu, emis de Ministrul Finanţelor Publice, prin care s-a stabilit obligaţia autorităţilor/instituţiilor publice de a se înregistra ca operatori de date cu caracter personal;
- Ordonanța de urgență a Guvernului nr. 52/2016 privind contractele de credit oferite consumatorilor pentru bunuri imobile, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 50/2010 privind contractele de credit pentru consumatori, prin care s-a stabilit obligaţia intermediarilor de credite de a se înregistra ca operatori de date cu caracter personal.

Având în vedere prevederile actelor normative menționate mai sus cu referire la obligația entităților din diferite sectoare de activitate de a se înregistra ca operatori de date cu caracter personal, Autoritatea națională de supraveghere a întreprins o serie de demersuri în vederea modificării acestor dispoziții legale, în sensul eliminării acestei obligaţii.

Totodată, furnizorii de asistență medicală, respectiv cabinetele medicale ambulatorii ale medicilor de familie şi de alte specialităţi, centrele de diagnostic şi tratament, centrele medicale, centrele de sănătate, laboratoarele, precum şi alte unităţi sanitare publice şi private, care își desfășoară activitatea curentă în baza Legii nr. 95/2006 privind reforma în domeniul sănătății, republicată, au notificat Autoritatea națională de supraveghere cu privire la prelucrările de date efectuate în scopul furnizării serviciilor de sănătate.

În aceste cazuri, Autoritatea națională de supraveghere a supus atenției Ministerului Sănătății propunerea de a se dispune luarea măsurilor necesare în vederea asigurării informării furnizorilor de asistență medicală cu privire la scutirea de la obligaţia de notificare, conform prevederilor Deciziei nr. 200/2015, coroborate cu cele ale Legii nr. 95/2006 privind reforma în domeniul sănătății, republicată.

În plus, operatori de date care își desfășoară activitatea în domeniul turismului, imobiliar, hotelier, precum şi entităţi care desfăşoară o activitate independentă (birouri notariale, birouri de executori judecătorești, societăți de avocatură, cabinete medicale individuale) au notificat Autorității naționale de supraveghere prelucrările pe care le efectuează în scopul îndeplinirii atribuţiilor lor legale.

Autoritatea națională de supraveghere a informat aceste entităţi că au calitatea de operator şi, implicit, obligaţia de a respecta legislaţia din domeniul protecţiei datelor, în special cu privire la dispozițiile art. 12, 19 şi 20 din Legea nr. 677/2001, modificată şi completată, însă sunt scutite de obligaţia de a notifica.

Scutirea de obligaţia de a notifica Autoritatea naţională de supraveghere nu exonerează, însă, operatorii de îndeplinirea celorlalte obligaţii care le revin potrivit dispoziţiilor legale aplicabile în domeniul protecţiei datelor cu caracter personal (ex.: informarea persoanelor vizate în condiţiile reglementate de art. 12 din Legea nr. 677/2001 şi adoptarea unor măsuri adecvate pentru asigurarea securităţii prelucrării datelor conform prevederilor art. 20 alin. 1 din acelaşi act normativ şi cerinţelor minime aprobate prin Ordinul nr. 52/2002).

Sub incidența prevederilor Deciziei nr. 200/2015, Autoritatea națională de supraveghere a înregistrat în registrul de evidenţă a prelucrărilor de date cu caracter personal, în principal, următoarele prelucrări de date:

- prelucrarea datelor care permit localizarea geografică a persoanelor fizice prin mijloace de comunicații electronice (monitorizarea/securitatea persoanelor şi/sau bunurilor publice/private prin utilizarea GPS-ului);
- prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea şi/sau evaluarea unor aspecte de personalitate, precum competenţa profesională, credibilitatea, comportamentul sau alte asemenea (crearea şi utilizarea de profiluri ale persoanelor vizate în vederea transmiterii unor newsletteruri, semnalarea încălcării codurilor de conduită în mediul privat - whistleblowing);
- prelucrarea datelor cu caracter personal ale minorilor efectuată prin intermediul internetului sau al mesageriei electronice (publicarea rezultatelor la diferite concursuri şcolare şi extraşcolare, postarea unor imagini din tabere școlare);
- prelucrarea datelor efectuată prin mijloace de supraveghere video în scopul monitorizării/securităţii persoanelor, spaţiilor şi/sau bunurilor publice/private.

În urma analizării formularelor de notificare, s-a propus efectuarea unor **investigaţii din oficiu** pentru verificarea anumitor aspecte referitoare la prelucrarea datelor cu caracter personal, şi anume:

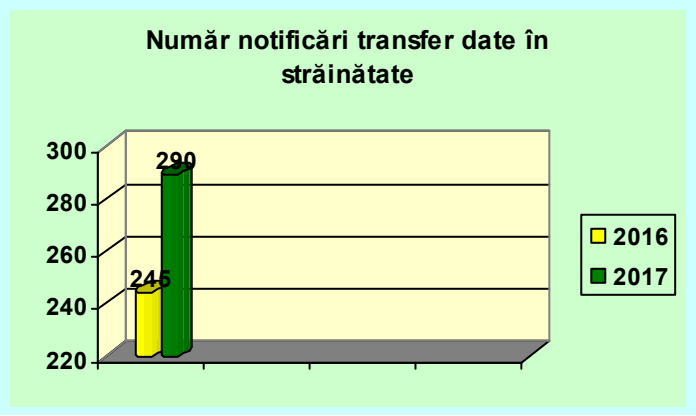
- verificarea condițiilor de prelucrare a datelor biometrice și genetice ale angajaților unei societăți în scopul monitorizării accesului în incinta acestei entități;
- verificarea condițiilor în care se efectuează prelucrarea datelor cu caracter personal în scopul ”ținerii evidenței orelor de muncă prestate de fiecare angajat (realizarea pontajelor), prin utilizarea unui sistem de control acces cu recunoaștere facială;
- controlul legitimității prelucrării datelor biometrice în scopul „resurselor umane”, respectiv „realizarea unui pontaj biometric”;
- verificarea condițiilor de funcționare a unei aplicații mobile de geolocalizare și închiriere biciclete, a necesității folosirii datelor referitoare la contul de Facebook și a celor privind locul de muncă, precum și a necesității păstrării datelor de geolocalizare după închiderea aplicației;

- verificarea condițiilor de prelucrare a datelor biometrice în scopul „îmbunătăţirii şi evaluării performanţelor algoritmilor biometrici”;
- verificarea condițiilor în care se efectuează monitorizarea video a angajaților în spațiile în care își desfășoară activitatea;
- verificarea legitimității prelucrării datelor de către o asociație de proprietari în vederea supravegherii video, în special în lifturi;
- controlul legitimității prelucrării datelor clienților, consumatorilor și debitorilor, în scopul efectuării unor rapoarte de credit, prin intermediul unui registru al facturilor neîncasate;
- verificarea modalității de prelucrare a datelor cu caracter personal efectuate în scopul „implementării unui sistem de autentificare pentru autorizarea plăților bazat pe recunoașterea amprentelor digitale prin intermediul cititorului biometric”;
- controlul respectării dreptului de acces al persoanelor vizate de către o instituție publică.

## Secțiunea a 2-a – Transferul în străinătate al datelor cu caracter personal

Din cele **1320** notificări cu transferuri de date către entităţi din străinătate, în **1030** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terţe cu nivel de protecţie adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield), precum şi transferuri către state terţe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată şi completată.

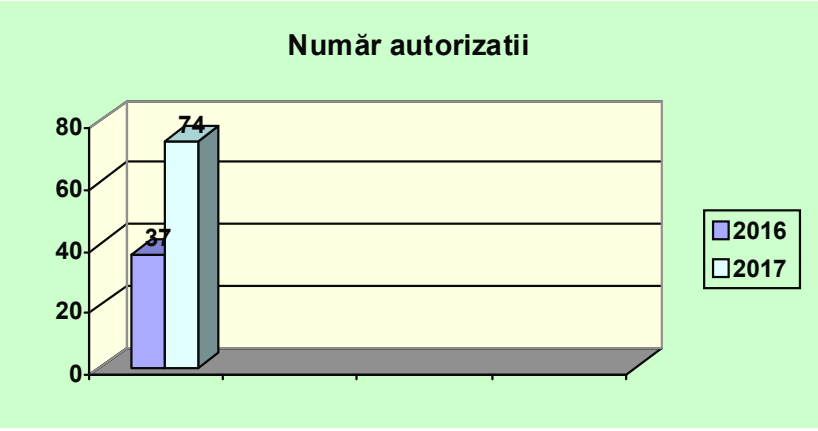
Totodată, au fost notificate **290** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, în baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules).



În anul 2017, dintre domeniile care au vizat transferurile de date către state terţe, efectuate în baza prevederilor art. 29 alin. 4 din Legea nr. 677/2001, modificată şi completată, respectiv efectuate în baza clauzelor contractuale standard și a regulilor corporatiste obligatorii, menționăm următoarele:

- gestiune economico-financiară şi administrativă, respectiv calculul rentabilității clientului, facturarea, condițiile de plată, gestionarea și raportarea de management, inclusiv raportarea și punerea în aplicare a programelor corporative, raportare financiară;
- suport cu privire la tehnologia informației și securitatea informației;
- gestionare date în domeniul farmacovigilenței;
- asigurarea conformității respectării normelor, aplicarea uniformă a regulamentelor, soluționarea sesizărilor de tip compliance formulate de orice persoană interesată cu privire la fapte de încălcare a legii, săvârșirea infracțiunilor de corupție, infracțiunilor de serviciu, abateri disciplinare, contravenții;
- resurse umane, recrutarea, evaluarea și promovarea personalului, dezvoltarea personală a angajaților, gestionarea trainingului și a formării profesionale a angajaților, a potențialilor angajați și a colaboratorilor;
- activități comerciale, realizarea de proiecte și comenzi de la clienți, achiziționarea de bunuri și servicii de la furnizori, comunicare internă, cooperare la scară globală.

În urma analizării transferurilor de date în străinătate către state terţe, a fost emis un număr de 74 de autorizaţii de transfer.



## Secțiunea a 3-a - Puncte de vedere privind diverse chestiuni de protecţia datelor

În cursul anului 2017, au fost analizate **322** solicitări ale operatorilor privind aspecte referitoare la dispoziţiile Legii nr. 677/2001, modificată şi completată, precum și la prevederile Deciziei nr. 200/2015.

În același timp, au fost înregistrate numeroase solicitări referitoare la necesitatea desemnării unui responsabil cu protecția datelor, precum și la sarcinile pe care acesta trebuie să le îndeplinească potrivit prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.

Prezentăm mai jos o serie de spețe semnificative supuse spre analiză Autorităţii naționale de supraveghere:

**1)** Președintele unei asociații de proprietari a solicitat punctul de vedere cu privire la necesitatea obținerii consimțământului tuturor proprietarilor dintr-un condominiu pentru supravegherea video a exteriorului clădirilor, curții interioare, spațiilor de parcare și aleii de acces.

S-a apreciat că se poate recurge la o monitorizare prin videosupraveghere numai dacă această măsură este proporţională cu riscurile cu care se confruntă asociaţia de proprietari şi determină luarea unei asemenea măsuri. În acelaşi timp, s-a precizat faptul că trebuie să se ţină cont şi de interesele, drepturile şi libertăţile persoanelor vizate.

Astfel, anterior implementării unui astfel de sistem de supraveghere prin camere video se impune o justificare temeinică a luării acestei măsuri (inclusiv sub aspectul numărului de camere şi al poziţionării acestora), pentru motivarea interesului legitim al asociaţiei faţă de drepturile şi libertăţile fundamentale sau interesele proprietarilor. Această analiză şi argumentare trebuie să se regăsească în conţinutul actelor asociaţiei emise în urma adunării generale a proprietarilor, realizată în condiţiile Legii nr. 230/2007 privind înfiinţarea, organizarea şi funcţionarea asociaţiilor de proprietari, în special cele privind atribuţiile Adunării generale a proprietarilor şi ale Comitetului Executiv (art. 27-30).

Regulile stabilite prin Normele metodologice de aplicare a Legii nr. 230/2007, referitoare la convocarea adunării generale, informarea prealabilă a proprietarilor, condiţiile de organizare

a adunării generale şi de cvorum/majoritate pentru adoptarea hotărârilor trebuie respectate de asociaţia de proprietari pentru ca hotărârea instalării sistemului de supraveghere video să fie adoptată legal (constituie dovezi ale convocării şi reconvocării afişul de la avizier şi tabelul nominal convocator cu semnături). Hotărârile adunării generale a asociației de proprietari trebuie aduse la cunoștința proprietarilor, conform Legii nr. 230/2007. Persoanele care nu sunt de acord cu hotărârea adoptată, o pot contesta în termenele și condițiile legale.

**2)** O societate comercială a solicitat opinia Autorității naționale de supraveghere în ceea ce privește *implementarea unui sistem de acces în sediu al angajaților pe bază de amprentă digitală.*

În acest sens, s-a precizat că amprentele digitale sunt o categorie de date cu caracter special, întrucât ele privesc caracteristicile fizice/fiziologice ale persoanelor şi pot conduce la identificarea acestora.

Totodată, s-a menționat că potrivit dispoziţiilor art. 4 alin. (1) din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, colectate în scopuri determinate, explicite şi legitime, cu respectarea dispoziţiilor în vigoare. De asemenea, datele colectate trebuie să fie strict cele necesare îndeplinirii scopului, aspect ce solicită o analiză prealabilă a necesităţii imperioase a colectării amprentelor digitale, pentru evitarea unor ingerinţe în viaţa privată a unei persoane, şi găsirea unor soluţii mai puţin intruzive.

În acelaşi timp, autoritatea a subliniat faptul că principiile privind prelucrarea datelor personale stabilite de art. 4 din Legea nr. 677/2001 se impun a fi respectate, indiferent dacă prelucrarea datelor are loc pe baza consimţământului persoanelor vizate sau în temeiul excepţiilor de la consimţământ prevăzute de lege.

Astfel, Autoritatea naţională de supraveghere a recomandat folosirea unei soluţii alternative la *sistemul de acces pe bază de amprentă digitală*.

Autoritatea naţională de supraveghere a subliniat faptul că această abordare referitoare la prelucrarea datelor biometrice a fost confirmată şi de instanţele de judecată.

**3)** Mai multe persoane juridice au solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la necesitatea declarării prin intermediul formularului de notificare a

transferului datelor cu caracter personal în Statele Unite ale Americii, ținând cont de prevederile Deciziei nr. 200/2015, precum și de Acordul UE-SUA Privacy Shield.

În contextul solicitărilor formulate, s-a menționat că în situaţia în care importatorul a aderat la principiile Privacy Shield nu este necesară notificarea autorității, întrucât sunt incidente dispozițiile art. 2 alin. (1) din Decizia nr. 200/2015, conform cărora vor face obiectul notificării Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal doar transferurile datelor cu caracter personal către statele situate în afara Uniunii Europene, a Zonei Economice Europene, precum şi către statele cărora Comisia Europeană nu le-a recunoscut, prin Decizie, un nivel de protecţie adecvat. În caz contrar, se impune identificarea altor garanţii care să permită transferul datelor către entităţi din aceste state, în conformitate cu prevederile art. 29 sau 30 din Legea nr. 677/2001, modificată şi completată.

**4)** O societate care prelucrează date cu caracter personal prin intermediul unor dispozitive mobile de geolocalizare a unor persoane fizice (pacienți cu Alzheimer sau alte forme de deficiență mintală, bătrâni singuri) pe baza unei aplicații mobile a solicitat informații cu privire la obligațiile ce-i revin în ceea ce privește prelucrarea datelor cu caracter personal. În plus, societatea menționată mai sus a precizat că datele referitoare la monitorizarea geolocației persoanelor vizate vor fi stocate pe servere în China.

În contextul celor prezentate, s-a apreciat că prelucrarea se circumscrie prevederilor art. 1 alin. (1) lit. c) din Decizia nr. 200/2015, iar notificarea Autorităţii naționale de supraveghere se impune dacă, prin intermediul aplicației, se realizează, direct sau indirect, localizarea geografică a persoanelor fizice care o utilizează.

Cât privește faptul că datele conținute în conturile private ale clienților contractanți vor fi stocate în China, s-a apreciat că se impune declararea prelucrării efectuate prin completarea formularului de notificare (inclusiv transferul datelor în China).

**5)** O societate civilă de avocatură a solicitat informații referitoare la condițiile în care pot fi prelucrate datele participanților la campanii publicitare cu acordarea de premii după încheierea acestora, în activități de marketing direct.

În acest context, s-a menționat că prelucrarea datelor personale în cadrul campaniilor publicitare se poate realiza cu consimțământul expres și neechivoc al persoanei vizate și cu informarea completă a acesteia, potrivit art. 12 din Legea nr. 677/2001. Informarea se poate

realiza atât prin intermediul regulamentului fiecărei campanii publicitare, cât și prin intermediul documentului de colectare a datelor personale.

În același timp, persoana vizată trebuie informată că, potrivit art. 15 alin. 2 din Legea nr. 677/2001, se poate opune oricând prelucrării datelor sale în activități de marketing direct, fără nici o justificare.

În consecință, prelucrarea datelor cu caracter personal ale participanților la o campanie publicitară, precum și prelucrarea ulterioară a acestor date în activități de marketing direct, se realizează doar cu respectarea prevederilor menționate mai sus.

## CAPITOLUL VII

# MANAGEMENTUL ECONOMIC AL AUTORITĂŢII

În vederea desfășurării activității, în anul 2017, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal i s-au alocat fonduri prin Legea bugetului de stat nr. 339/2017 și prin Ordonanțele Guvernului nr. 14 și nr. 86/2017 privind rectificarea bugetului de stat pe anul 2017, rezultând un buget final în sumă de 4.287.000 lei, cu următoarea structură:

- mii lei -

| Denumire indicator | Cod | Buget iniţial 2017 | Buget actualizat la 31.12.2017 | Sume cheltuite până la 31.12.2017 | Execuţie (%) |
|---|---|---|---|---|---|
| Total cheltuieli | 51.01 | 4.585 | 4.287 | 4.280 | 99,84 |
| Cheltuieli de personal | 10 | 3.878 | 3.588 | 3.587 | 99,97 |
| Bunuri și servicii | 20 | 672 | 664 | 659 | 99,22 |
| Alte cheltuieli | 59 | 10 | 10 | 10 | 100 |
| Cheltuieli de capital | 71 | 25 | 25 | 24 | 97,31 |

Pentru că, 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, ținând cont de solicitările permanente privind eficiența utilizării fondurilor publice.

În ceea ce priveşte modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorităţii naționale de supraveghere a constituit un procent de 84% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat

efectiv credite în valoare de 3.586.994 lei (prin ocuparea unor posturi temporar, prin detaşare), înregistrându-se în continuare un deficit major de personal (11 posturi neocupate, 5 posturi ocupate temporar prin detașare, reprezentând 32% din numărul total de 50 de posturi – exclusiv demnitarii – prevăzute de Legea nr. 102/2005). Majoritatea cheltuielilor de personal au fost aferente plăţilor efectuate pentru achitarea drepturilor salariale ale angajaților din compartimentele de specialitate.

Cheltuielile aferente titlului Bunuri și servicii în anul 2017 au avut o pondere de 15,5% în bugetul instituției, iar din acestea, cheltuielile cu pondere mai importantă au fost:

- 33% costuri de închiriere și cheltuieli cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI
- 37% bunuri și servicii pentru întreținere și funcționare (curățenie, abonament program legislativ, servicii de actualizare informatică etc.)

Trebuie menţionat faptul că Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal îşi realizează obiectul principal de activitate prin investigaţii şi controale efectuate la operatorii situaţi pe teritoriul României, precum şi la consulatele României.

La nivelul Uniunii Europene, Autoritatea naţională de supraveghere are obligaţia de a participa la lucrările Grupului de Lucru Articolul 29, ale subgrupurilor de lucru din cadrul acestuia, la reuniunile Grupurilor de coordonare comună (SIS II, VIS, Eurodac), precum şi la lucrările Comitetului Consultativ al Convenției 108.

În anul 2017, cheltuielile cu bunuri și servicii au scăzut cu 5% față de anul 2016, fapt cu un impact deosebit asupra activității instituției și cheltuielilor bugetare, fiind efectuate mai putin de jumătate din cheltuielile privind deplasările externe estimate.

De asemenea, trebuie precizat și faptul că s-au avut permanent în vedere mai mulți factori – 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 acestui titlu de cheltuieli.

În ceea ce privește cheltuielile de capital, în anul 2017, 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, 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 sunt verificate şi vizate.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, subliniem că acestea au fost utilizate cu maximă eficienţă şi printr-o atentă administrare de către instituţia noastră.