AGENȚIA NAȚIONALĂ A FUNCȚIONARILOR PUBLICI

Bd. Mircea Vodă, nr. 44
tronsonul III, sector 3
București, cod poștal 030669

tel: 0374 112 741
0374 112 714
Fax: 021 312 44 04
www.anfp.gov.ro

Proiect *„Instruire în domeniul prelucrării datelor cu caracter personal pentru structurile din cadrul sistemului de coordonare, gestionare și control al FESI în România”*, cod proiect 3.1.107, cod SMIS 2014+ 128212

COMPENDIU

privind cazuistica și spețele relevante în domeniul prelucrării datelor cu caracter personal[1]

- Document suport -

CUPRINS – SECȚIUNI

[1] Date preluate din Rapoartele anuale de activitate al ANSPDCP (2018 și 2019) - rapoarte anuale (dataprotection.ro)

1. PUNCTE DE VEDERE EMISE DE ANSPDCP PRIVIND DIVERSE CHESTIUNI DE PROTECŢIA DATELOR

1.1 Prelucrarea codului numeric personal de către unitățile de cazare

Referitor la modalitatea de prelucrare a datelor cu caracter personal, inclusiv sub aspectul colectării, stocării, divulgării prin transmitere, diseminării sau punerii la dispoziţie în orice alt mod, potrivit Regulamentului (UE) 2016/679, aceasta se realizează cu consimțământul persoanei vizate sau în condițiile de excepție de la consimțământ, prevăzute de art. 6, art. 9 și art. 10 în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În ceea ce privește prelucrarea unui număr de identificare național (printre care 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) codul numeric personal, seria şi numărul actului de identitate), inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, art. 4 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) prevede următoarele:

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

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

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

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

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

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

Astfel, în contextul prelucrării datelor personale, este necesară analizarea temeiului legal al efectuării acesteia, în conformitate cu dispozițiile Regulamentului (UE) 2016/679 și ale Legii nr. 190/2018, mai sus enumerate. În acest sens, în măsura în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau există o obligație legală pentru prelucrarea datelor ori în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, datele pot fi prelucrate fără consimțământul persoanei vizate.

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

Totodată, potrivit art. 2 alin. (6) din normele sus-menţionate *„fișele de anunțare a sosirii și plecării, completate și semnate de turiștii cazați, se preiau, împreună cu actele de identitate, de către recepționeri, care sunt obligați să confrunte datele din fișe cu cele din actul de identitate, să semneze fișele pentru confirmarea completării corecte a acestora și să restituie imediat actele de identitate turiștilor.”*

Sub aspectul informării persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe bază de excepții), art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menționate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic.

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

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

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

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

În ceea ce privește responsabilitatea operatorului, art. 24 din Regulamentul (UE) 2016/679 prevede că ”Ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta și a fi în 22 măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar.” Totodată, s-a precizat că, potrivit prevederilor Regulamentului (UE) 2016/679, persoana vizată beneficiază de o serie de drepturi menționate în cadrul art. 12-23 din Regulament.

1.2 Publicarea datelor pe Internet de către autorități și instituții publice

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

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

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

Raportat la publicarea pe Internet a unor date cu caracter personal, Autoritatea națională de supraveghere a subliniat în mod constant faptul că diseminarea în spațiul virtual a datelor persoanelor fizice și, implicit, punerea la dispoziția unui număr potențial foarte mare de persoane, fără niciun control asupra utilizării ulterioare a datelor în scopuri posibil incompatibile cu scopul inițial, reprezintă o ingerință gravă în drepturile la viaţă privată și protecția datelor cu caracter personal, astfel cum sunt garantate de art. 26 din Constituție, art. 8 din Convenţia Europeană a Drepturilor Omului, precum și art. 7 și 8 din Carta Drepturilor Fundamentale a UE.

În sprijinul acestor argumente amintim jurisprudența relevantă a Curții Constituționale (Decizia nr. 440/2014, par. 44 și 45), referitoare la faptul că reglementarea unei obligaţii pozitive care privește limitarea în mod necontenit a exerciţiului unui drept fundamental (cum este dreptul la viaţă privată) face să dispară însăşi esența dreptului, prin îndepărtarea garanţiilor privind exercitarea acestuia, persoanele fizice în cauză fiind supuse în permanență acestei ingerințe în exerciţiul drepturilor lor.

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

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

1.3 Monitorizarea angajaților la locul de muncă

În mai multe situații, s-a solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la monitorizarea angajaților la locul de muncă, în special prin intermediul mijloacelor de supraveghere video. În acest context, s-a precizat faptul că dispozițiile art. 5 din Legea nr. 190/2018 stabilesc următoarele: „În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;
- angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;
- angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

- alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa;
- durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate."

Prin urmare, supravegherea video a angajaților la locul de muncă se poate institui în condițiile art. 6 din Regulamnetul General privind Protecția Datelor, coroborate, după caz cu prevederile art. 5 din Legea nr. 190/2019.

În cazul invocării interesului legitim al operatorului, s-a precizat că justificarea trebuie să se regăsească la angajator într-o documentație argumentată temeinic, din care să rezulte prevalența interesului legitim asupra intereselor sau drepturilor şi libertăţilor angajaților.

Referitor la interesul legitim, s-a subliniat faptul că se impune ca acesta să fie temeinic justificat de către operator, având în vedere că prelucrarea are loc fără consimțământul persoanelor vizate. În acest sens, se poate recurge la o monitorizare prin videosupraveghere, în temeiul dispoziţiilor legale de mai sus, dar numai dacă această măsură este proporţională cu riscurile cu care se confruntă operatorul şi determină luarea unei asemenea măsuri intruzive în viaţa privată a persoanelor vizate.

În toate situațiile, în cazul în care se apelează la o altă entitate care gestionează sistemul de supraveghere video (prelucrează datele) pe seama operatorului (angajatorul), în calitate de împuternicit, se impune respectarea dispozițiilor art. 28 din Regulamentul General privind Protecția Datelor.

Totodată, devin aplicabile celelalte dispoziții ale Regulamentului General privind Protecția Datelor, cum ar fi principiile de prelucrare statuate de art. 5, drepturile persoanelor vizate, inclusiv sub aspectul transparenței și al informării, garantate de art. 12-22, responsabilitatea operatorului stabilită de art. 24, obligația operatorului de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit, prevăzută de art. 25, obligația de implementare a măsurilor tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, prevăzută de art. 32 etc.

De asemenea, Autoritatea Națională de Supraveghere a subliniat că instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video urmează să respecte și Legea nr. 333/2003 şi normele metodologice de aplicare a acesteia.

1.4 Calitatea de operator, împuternicit sau operatori asociați

La stabilirea calității entităților care prelucrează date cu caracter personal, este necesar a se lua în considerare următoarele dispoziții din Regulamentul (UE) 2016/679:

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

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

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

dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

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

(3) Indiferent de clauzele acordului menționat la alineatul (1), persoana vizată își poate exercita drepturile în temeiul prezentului regulament cu privire la și în raport cu fiecare dintre operatori." 39

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.5 Transferul datelor cu caracter personal într-un stat terț

Mai multe entități din domeniul privat au solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la condițiile în care se poate realiza transferul datelor cu caracter personal către un stat terț care nu oferă un nivel adecvat de protecție. Cu privire la acest aspect, art. 46 alin. (1) din Regulamentul General privind Protecția Datelor prevede că în absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

Garanțiile adecvate menționate mai sus pot fi furnizate fără să fie nevoie de vreo autorizație specifică din partea unei autorități de supraveghere, prin:

a) existența unui instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
b) reguli corporatiste obligatorii;
c) clauze standard de protecție a datelor adoptate de Comisie;
d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie;

e) un cod de conduită, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau
f) existența unui mecanism de certificare, aprobat în conformitate cu articolul 42, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.
Totodată, art. 46 alin. (3) din Regulament stabilește că pot fi furnizate, de asemenea, garanţii adecvate prin clauze contractuale încheiate între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională sub rezerva autorizării din partea autorității de supraveghere competente. În acest context, considerentul (109) din Regulament subliniază că „*Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate*.” Raportat la prevederile legale sus-menționate, transferul datelor cu caracter personal către state terțe care nu oferă un nivel adecvat de protecție se poate realiza în temeiul art. 46 din Regulament, cu respectarea principiilor de prelucrare a datelor cu caracter personal.

1.6 Prelucrarea datelor cu caracter personal de către asociațiile de proprietari în scopul supravegherii video

Numeroase asociații de proprietari au solicitat Autorității Naționale de Supraveghere exprimarea unui punct de vedere cu privire la condițiile de prelucrare a datelor cu caracter personal ale proprietarilor/locatarilor unui imobil prin mijloace de supraveghere video.

Față de aceste solicitări, Autoritatea Națională de Supraveghere a menționat că prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune prevederilor Regulamentului General privind Protecția Datelor.

Instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video se realizează și în conformitate cu Legea nr. 333/2003 şi normele metodologice de aplicare a acesteia.
În acest context, operatorii au fost informați cu privire la condițiile de legalitate care trebuie îndeplinite potrivit art. 6 din Regulamentul General privind Protecția Datelor.
Totodată, s-a subliniat că prelucrările de date efectuate vor fi precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din Regulament, care obligă operatorul să furnizeze persoanei vizate o serie de informații.
În ceea ce privește informarea persoanelor vizate, Autoritatea Națională de Supraveghere a precizat faptul că în spaţiile monitorizate trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

În plus, s-a recomandat ca perioada de stocare a datelor cu caracter personal (imaginea) prelucrate de asociaţie ca urmare a instalării sistemului de supraveghere video să nu depăşească 30 zile. În acelaşi timp, s-a precizat că, potrivit art. 48 alin. (1) din Legea nr. 196/2018 privind înfiinţarea, organizarea şi funcţionarea asociaţiilor de proprietari, adunarea generală poate adopta hotărâri, dacă majoritatea proprietarilor membri ai asociației de proprietari sunt prezenți personal sau prin reprezentanți care au o împuternicire scrisă și semnată de către proprietarii în numele cărora votează.

1.7 Prelucrarea datelor privind starea de sănătate

Art. 4 din Regulamentul General privind Protecția Datelor stabilește o serie de definiții, printre care și cea a datelor cu caracter personal. De asemenea, datele privind sănătatea sunt definite de aceleași dispoziții legale sus-menționate, ca fiind ”date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informaţii despre starea de sănătate a acesteia” (art. 4 pct. 15).
Prin urmare, în accepțiunea definițiilor sus-citate, Autoritatea Națională de Supraveghere a precizat că informațiile precum codurile diagnosticelor ce aparțin unor persoane fizice (angajații) reprezintă date cu caracter personal ce vizează starea de sănătate.

În ceea ce privește legitimitatea prelucrării (inclusiv a dezvăluirii) acestor categorii de date speciale, art. 9 din Regulamentul General privind Protecția Datelor precizează condițiile în care se pot prelucra. Astfel, regula instituită de aceste dispoziții legale este aceea de interzicere a prelucrării de date privind starea de sănătate, cu unele excepții de strictă interpretare și aplicare, reglementate de art. 9 alin. (2) din Regulament.

În ceea ce privește prelucrarea bazată pe consimțământul persoanei vizate, Autoritatea Națională de Supraveghere a subliniat faptul că este necesară respectarea dispozițiilor art. 4 pct. 11 și art. 7 din Regulamentul General privind Protecția Datelor. În același timp, alin. (4) al art. 9 din Regulamentul General privind Protecția Datelor prevede că: „Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea de date genetice, date biometrice sau date privind sănătatea.”

În acest context, prin art. 3 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 au fost stabilite aceste condiții de prelucrare, astfel:

„(1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

(2) Prelucrarea datelor privind sănătatea realizată în scopul asigurării sănătăţii publice, astfel cum este definită în Regulamentul (CE) nr. 1338/2008 al Parlamentului European şi al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum şi la sănătatea şi siguranţa la locul de muncă, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 354/70 din 31 decembrie 2008, nu se poate efectua ulterior, în alte scopuri, de către terţe entităţi.”

S-a subliniat, totodată, necesitatea respectării principiilor privind prelucrarea, statuate de art. 5 din Regulamentul General privind Protecția Datelor, a asigurării transparenței prelucrării datelor potrivit art. 12, 13 și 14 din Regulament, prin furnizarea în mod adecvat și complet a informațiilor stabilite de aceste dispoziții, precum și a respectării art. 24 din actul normativ european menționat mai sus. În ceea ce privește prelucrarea datelor privind starea de sănătate de către angajații din cadrul compartimentelor de resurse umane,

precizăm faptul că art. 29 din Regulamentul General privind Protecția Datelor prevede că orice persoană care acţionează sub autoritatea operatorului (angajații) care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

Prin urmare, Autoritatea Națională de Supraveghere a apreciat că datele privind starea de sănătate pot fi prelucrate (dezvăluite) fie cu consimțământul persoanei vizate, fie în celelalte condiții de excepție, de strictă interpretare și aplicare prevăzute de Regulamentul General privind Protecția Datelor, iar în îndeplinirea anumitor scopuri, datele se prelucrează de către un profesionist supus obligaţiei de păstrare a secretului profesional sau de către o altă persoană supusă unei obligaţii de confidenţialitate.

2. INVESTIGAȚII DIN OFICIU – FIȘE DE CAZ ANSPDCP[2]

2.1 Încălcarea dreptului de acces

FIȘĂ DE CAZ - Autoritatea Națională de Supraveghere s-a sesizat din oficiu cu privire la răspunsul comunicat de către o societate comercială unei persoane vizate (persoană fizică) ca urmare a exercitării de către aceasta a dreptului de acces la date, conform art. 13 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.
Persoana vizată, fost angajat al operatorului, s-a adresat acestuia printr-o cerere prin care își exercita dreptul de acces la datele sale cu caracter personal, solicitând informații referitoare la: scopul prelucrării datelor sale cu caracter personal, destinatarii/categoriile de destinatari ai datelor, datele care fac obiectul prelucrării, orice informații disponibile cu privire la originea datelor, activitatea desfășurată de către persoana vizată, durata activității persoanei vizate, veniturile realizate, salariul brut, încadrarea în grupe de muncă, vechime în muncă și în specialitate, conform contractului individual de muncă pe perioada în care aceasta a fost angajată.
Societatea a transmis un răspuns persoanei vizate, prin care i-a oferit informații generale cu privire la operațiunile de prelucrare a datelor efectuate, însă nu i-a furnizat informații cu privire la toate datele necesare, conform art. 13 alin. (1) din Legea nr. 677/2001.
În urma investigației efectuate, operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, raportat la art. 13 din aceeași lege, întrucât nu a comunicat persoanei vizate toate informațiile pe care avea obligația să i le comunice.
Totodată, Autoritatea Națională de Supraveghere a recomandat operatorului să transmită persoanei vizate un răspuns complet la cererea sa, cu respectarea art. 13 din Legea nr. 677/2001.

2.2 Utilizarea de tehnologii de plasare de informații, web-bug sau tracking code

FIȘĂ DE CAZ - Autoritatea Națională de Supraveghere a primit, la adresa de e-mail, mai multe plângeri care conțineau următorul text: *„NOTA! Mesajul, are atașat un cod de urmărire și raportare continuă a stării (TRAKING CODE) motiv pentru care vă rugăm să evitați posibilitatea de a nega faptul că acest mesaj a fost expediat la adresa Dumneavoastră de mail, respectiv că nu ați primit mesajul”.*

Ca urmare a verificărilor demarate la nivelul aplicației proprii de management al documentelor, s-a constatat că plângerile erau transmise de pe adrese de e-mail ale unor domenii de internet care conțineau „web-bug” sau „tracking pixel”.
Totodată, ca urmare a verificărilor efectuate, Autoritatea Națională de Supraveghere a constatat că, de la mai multe adrese de e-mail ale domeniilor de internet menționate anterior, au fost transmise e-mailuri care conțineau un „web-bug” sau „tracking pixel” (identificat sub denumirea de „tracking code”) în corpul mesajelor primite și către alți operatori economici.
Față de cele de mai sus, Autoritatea Națională de Supraveghere s-a sesizat din oficiu referitor la utilizarea de web-bug sau tracking code – tehnologii de plasare de informații și accesarea acestor informații din echipamentul terminal (stații de lucru –calculatoare), demarând o investigație la deținătorul domeniilor de internet ale adreselor de e-mail de la care au fost transmise plângerile.

[2] O componentă importantă a activității ANSPDCP 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.

Astfel, Autoritatea Națională de Supraveghere a solicitat informații referitoare la scopul utilizării de web-bug/tracking pixel/tracking code în cadrul comunicărilor electronice (e-mail); sursa acestui web-bug/tracking pixel/tracking code (dacă este dezvoltat de către deținătorul domeniilor sau de o terță parte), modul de funcționare, precum și o descriere a elementelor HTML ale acestui web-bug/tracking pixel/tracking code; data la care a început această prelucrare (colectare, urmărire și raportare continuă a stării), precum și, dacă este cazul, data încetării acestei prelucrări de informații prin aceste comunicări electronice; de câte ori s-a utilizat, la nivelul domeniilor deținute, această metodă de urmărire și raportare continuă a stării comunicațiilor electronice; modalitatea prin care s-au adus la cunoștința persoanelor vizate (utilizatori ai adreselor de e-mail) drepturile prevăzute de art. 12-18 din Legea nr. 677/2001; modalitatea de obținere a consimțământului persoanelor vizate privind această prelucrare/colectare (urmărire și raportare continuă a stării) prin aceste comunicări electronice; care este perioada de stocare a informațiilor colectate prin urmărirea și raportarea continuă a stării comunicațiilor electronice, precum și destinația acestor informații colectate.
Ca urmare a investigației efectuate, s-a constatat că operatorul investigat, la nivelul domeniilor proprii de Internet utilizate, servicii ale societății informaționale, a încălcat confidențialitatea comunicărilor, contrar dispozițiilor art. 4 alin. (2) din Legea nr. 506/2004, modificată și completată, care statuează că „Ascultarea, înregistrarea, stocarea şi orice altă formă de interceptare ori supraveghere a comunicărilor şi a datelor de trafic aferente sunt interzise, cu excepţia cazurilor următoare:
a) se realizează de utilizatorii care participă la comunicarea respectivă;
b) utilizatorii care participă la comunicarea respectivă şi-au dat, în prealabil, consimţământul scris cu privire la efectuarea acestor operaţiuni;
c) se realizează de autorităţile competente, în condiţiile legii.”
De asemenea, s-a constatat că la nivelul domeniilor de Internet proprii, servicii ale societății informaționale, pentru informațiile stocate în echipamentele terminale ale utilizatorilor, operatorul nu a îndeplinit în mod cumulativ condițiile prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004, respectiv obținerea acordului utilizatorului în cauză pentru modulele web-bug/tracking pixel/tracking code utilizate în corespondența electronică cu diferite adrese de e-mail și furnizarea informațiilor anterior exprimării acordului privind scopul general al procesării informațiilor stocate, durata de viață, informațiile stocate și accesate, precum și permiterea stocării și/sau accesului unor terți la informațiile stocate în echipamentul terminal al utilizatorului (stații de lucru, smartphones – mijloace automate de prelucrare a datelor cu caracter personal).
Precizăm că Grupul de lucru Articolul 29 (Grupul privind protecția datelor personale de pe lângă Comisia Europeană, în prezent Comitetul European pentru Protecția Datelor), în Avizul nr. 2/2010, subliniază că publicitatea comportamentală implică prelucrarea unor identificatori unici, indiferent dacă acest lucru se realizează prin utilizarea modulelor cookie sau a oricărui tip de dispozitive de identificare. Utilizarea acestor identificatori unici permite urmărirea utilizatorilor unui anumit calculator, chiar și în cazul în care adresele IP sunt șterse sau anonimizate.
Cu alte cuvinte, acești identificatori unici permit ca persoanele vizate să fie „recunoscute” în vederea urmăririi comportamentului lor ca utilizatori în timp ce navighează pe diferite site-uri și, prin urmare, se poate considera că sunt date cu caracter personal. Totodată, art. 5 alin. (3) din Directiva 2002/58/CE, astfel cum a fost modificată prin Directiva 2009/136/CE, a consolidat protecția utilizatorilor de rețele și servicii de comunicații electronice, introducând obligația operatorilor/furnizorilor de a obține consimțământul exprimat în cunoștință de cauză al utilizatorului (sau al abonatului) înainte de a stoca informații sau de a dobândi accesul la informațiile stocate în echipamentul terminal al acestuia. Cerința se aplică tuturor tipurilor de informații stocate sau accesate în echipamentul terminal al utilizatorului [...].

Față de cele de mai sus, în urma investigaţiei efectuate, operatorul reclamat a fost sancționat contravențional pentru încălcarea art. 4 alin. (5) din Legea nr. 506/2004, modificată și completată, întrucât operatorul, la nivelul domeniilor proprii de Internet utilizate, servicii ale societății informaționale, pentru informațiile stocate în echipamentele terminale ale utilizatorilor nu a îndeplinit în mod cumulativ condițiile prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004, respectiv:
a) obținerea acordului utilizatorului în cauză pentru modulele web-bug/tracking pixel/tracking code utilizate în corespondența electronică cu diferite adrese de email și
b) furnizarea informațiilor anterior exprimării acordului 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 (stații de lucru, smartphones, mijloace automate de prelucrare a datelor cu caracter personal), contravenție prevăzută de art. 13 alin. (1) lit. i) din Legea nr. 506/2004, modificată și completată.
De asemenea, operatorul a fost sancționat pentru nerespectarea prevederilor art. 4 alin. (2) referitoare la interdicţia interceptării şi supravegherii comunicărilor şi datelor de trafic aferente, respectiv stocarea şi orice altă formă de interceptare ori supraveghere a comunicărilor şi a datelor de trafic aferente, întrucât, la nivelul domeniilor proprii de Internet, servicii ale societății informaționale, prin utilizarea modulelor web-bug/tracking pixel/tracking code, supraveghează e-mailurile transmise (comunicările transmise prin intermediul serviciilor de comunicații electronice), fără ca destinatarii acestora să-și fi dat în prealabil consimțământul scris cu privire la efectuarea acestor operațiuni, fiind colectate informaţii privind data la care a fost deschis respectivul e-mail, adresa IP de la care a fost deschis şi chiar dispozitivul folosit, contrar articolului 4, alineatul (2), din Legea nr. 506/2004, modificată și completată.

FIȘĂ DE CAZ – Divulgare neautorizată de date cu caracter personal prin intermediul e-mail-ului

O instituție bancară a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679.

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

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

În urma investigaţiei efectuate la instituția bancară, Autoritatea națională de supraveghere a constatat că instituţia bancară nu a implementat măsuri tehnice și organizatorice adecvate, în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, prin transmiterea formularelor pentru definire și actualizare date personale – persoane fizice (clienți) către adrese de e-mail eronate, din cauza unei erori tehnice a aplicației, fiind afectate de incident un număr de 56 de persoane fizice vizate. Aceasta a condus la încălcarea confidențialității datelor cu caracter personal (nume, prenume, data nașterii, codul numeric personal, numărul și seria actului de identitate, data nașterii, locul nașterii, profesie, loc de muncă, număr de telefon, adresa de e-mail, adresa de domiciliu, situație familială, date privind bunurile deținute, salariu), deși instituţia bancară avea aceste obligații, inclusiv potrivit prevederilor art. 5 lit. f), „integritate și confidențialitate” din Regulamentul (UE) 2016/679.
În acest caz, Autoritatea națională de supraveghere a constatat că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) din Regulamentul (UE) 2016/679și a dispus operatorului o măsură corectivă, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, respectiv instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

2.3 Accesul neautorizat la datele cu caracter personal ale unor persoane fizice de pe teritoriul României, prelucrate de către un operator care nu este stabilit în România

FIȘĂ DE CAZ - Autoritatea Națională de Supraveghere s-a sesizat din oficiu privind accesul neautorizat la datele cu caracter personal ale unor persoane fizice de pe teritoriul României/utilizatori din România, prelucrate de către un operator care nu este stabilit în România (Statele Unite ale Americii), prin intermediul unor aplicații disponibile doar pentru telefoane inteligente, oferite pe platforma electronică a operatorului. Potrivit prevederilor art. 2 alin. (2) lit. c) și art. 2 alin. (3) din Legea nr. 677/2001, prevederile acestei legi se aplică și prelucrărilor de date cu caracter personal efectuate în cadrul activităţilor desfăşurate de operatori care nu sunt stabiliţi în România, prin utilizarea de mijloace de orice natură situate pe teritoriul României, cu excepţia cazului în care aceste mijloace nu sunt utilizate decât în scopul tranzitării pe teritoriul României a datelor cu caracter personal care fac obiectul prelucrărilor respective.
În acest caz operatorul își va desemna un reprezentant care trebuie să fie o persoană stabilită în România. Față de cele de mai sus, investigația s-a desfășurat la reprezentantul operatorului, o societate comercială cu sediul în România, având în vedere că, potrivit prevederilor art. 2 alin. (3) din Legea nr. 677/2001, prevederile legii aplicabile operatorului sunt aplicabile şi reprezentantului acestuia, fără a aduce atingere posibilităţii de a introduce acţiune în justiţie direct împotriva operatorului. Ca urmare a investigației efectuate, Autoritatea Națională de Supraveghere a fost informată că incidentul de încălcare a securității datelor cu caracter personal, de tip hacking, a presupus accesarea de informații privind aproximativ 57 de milioane de utilizatori din întreaga lume (aproximativ 32 de milioane de persoane dintre acestea se găsesc în afara Statelor Unite ale Americii, inclusiv aproximativ 30.000 de persoane din România). La nivelul Uniunii Europene, acest incident de încălcare a securității datelor cu caracter personal a afectat utilizatori din toate cele 28 de state membre. Astfel, în mod ilegal au fost accesate date cu caracter personal și s-au efectuat copii ale acestora.
Pentru aproximativ toți utilizatorii, fișierele descărcate au inclus numele, adresele de e-mail și numerele de telefon mobil. În unele cazuri, fișierele includeau și alte informații

colectate de la utilizatori sau create de operator în legătură cu utilizatorii, de exemplu ID-ul intern de utilizator; fișierul unui utilizator care a invitat un alt utilizator să se înregistreze în aplicație sau cu care utilizatorii au partajat călătorii dacă au optat pentru anumite programe; o serie de scurte observații privind șoferii (profile automate); anumite informații unice de localizare (date de geolocalizare), precum latitudinea și longitudinea corespunzătoare locului unde utilizatorul s-a înregistrat pentru prima oară în aplicație; precum și alte informații de cont, inclusiv token-urile de utilizator și parole de utilizator hash sau salted.
Aplicațiile oferite de platforma electronică a operatorului se subscriu serviciilor societății informaționale și reprezintă servicii de comunicații electronice care constau în întregime/în principal în transmiterea semnalelor prin rețelele de comunicaţii electronice, prin intermediul Internetului, privind prelucrările de date cu caracter personal efectuate prin mijloace automate (aplicații/terminale mobile smartphone) pe teritoriul României.
Incidentul produs intră în categoria unei încălcări a securității datelor cu caracter personal, așa cum este definit de Legea nr. 506/2004, modificată și completată, respectiv distrugerea accidentală sau ilicită, pierderea, alterarea, divulgarea neautorizată ori accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate. Față de cele de mai sus, în urma investigaţiei efectuate, operatorul a fost sancţionat contravențional pentru neîndeplinirea obligației de informare prevăzute la art. 3 alin. (6) din Legea nr. 506/2004, modificată și completată, întrucât operatorul nu a îndeplinit obligația de informare, prin notificarea fără întârziere către ANSPDCP a încălcării securității datelor cu caracter personal, precum și pentru neîndeplinirea obligației de informare prevăzute la art. 3 alin. (7) din Legea nr. 506/2004, modificată și completată, întrucât operatorul nu a îndeplinit obligația de informare, prin notificarea în mod individual, fără întârziere, a tuturor persoanelor vizate/utilizatori din România afectați de incidentul de securitate a datelor cu caracter personal.
Totodată, Autoritatea Națională de Supraveghere a solicitat operatorului investigat notificarea/informarea încălcării securității datelor cu caracter personal, în mod individual, a tuturor persoanelor vizate/utilizatori din România afectați de incidentul de securitate a datelor cu caracter personal. Ca urmare a solicitării ANSPDCP, operatorul investigat a notificat în mod individual persoanele vizate afectate.

2.4 Prelucrarea nelegală a datelor cu caracter personal ale unui abonat de către un partener contractual al operatorului

FIȘĂ DE CAZ - Autoritatea Națională de Supraveghere a efectuat o investigație la un furnizor de servicii de telefonie mobilă, referitor la prelucrarea nelegală a datelor cu caracter personal ale unei persoane fizice/abonat, de către un partener contractual al operatorului, în scopul emiterii unei facturi, prin accesarea ilegală a bonusului Phone credit acordat de către furnizorul de servicii de telefonie mobilă persoanei fizice în cauză.
Ca urmare a investigației efectuate, s-a constatat că incidentul s-a datorat unei erori umane de natură internă a unui angajat al partenerului contractual al operatorului, care avea calitatea de împuternicit pentru prelucrarea datelor cu caracter personal. Față de cele de mai sus, operatorul investigat a fost sancționat contravențional pentru „Prelucrarea nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, întrucât operatorul, prin împuternicitul său, a prelucrat datele cu caracter personal ale persoanei vizate/abonat, fără consimțământul acesteia, în scopul emiterii unei facturi prin accesarea bonusului acordat acesteia de către operator, precum și pentru „Neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate”, prevăzută de art. 33 din Legea nr. 677/2001, întrucât operatorul, prin împuternicitul său, nu a luat măsuri suficiente împotriva accesului neautorizat, al unui angajat al împuternicitului, la datele cu caracter personal ale persoanei vizate/abonat din aplicația

de facturare a operatorului și folosirii acestora în vederea emiterii unei facturi în mod ilegal.
Ca urmare a constatărilor de mai sus, raportat la prevederile art. 2 lit. h) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, modificată şi completată, Autoritatea Națională de Supraveghere a apreciat că incidentul produs intră în categoria unei încălcări a securității datelor cu caracter personal așa cum este definită de legea susmențională, respectiv încălcarea securităţii având ca rezultat distrugerea accidentală sau ilicită, pierderea, alterarea, divulgarea neautorizată ori accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod în legătură cu furnizarea de servicii de comunicaţii electronice destinate publicului.
Astfel, operatorul investigat a fost sancționat contravențional și pentru neîndeplinirea obligaţiei de informare prevăzută la art. 3 alin. (6) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, modificată şi completată, întrucât acesta nu a îndeplinit obligația de informare, prin notificarea fără întârziere către Autoritatea Națională de Supraveghere a încălcării securității datelor cu caracter personal, deși operatorul avea cunoștință de acest incident de securitate, așa cum este definit de Legea nr. 506/2004, precum și de obligațiile legale aflate în sarcina sa.
Totodată, s-a recomandat operatorului să respecte prevederile Deciziei nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, în conformitate cu Regulamentul (UE) 2013/611 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice.

2.5 Verificarea respectării prevederilor legale referitoare la prelucrarea datelor cu caracter personal de către operatorii care au ca obiect de activitate furnizarea de servicii de comunicații mobile.

Autoritatea Națională de Supraveghere a dispus efectuarea de investigații la mai multe entități care prelucrează date cu caracter personal având ca obiect principal de activitate „Activități de telecomunicații prin rețele fără cablu (exclusiv prin satelit)”.
Autoritatea Națională de Supraveghere a controlat, până la data de 25 mai 2018, patru mari furnizori de servicii de comunicații mobile. Referitor la entitățile controlate, specificăm că, în vederea realizării obiectului de activitate, acestea încheie cu clienți persoane fizice (abonați) contracte pentru furnizarea de servicii de telefonie mobilă, pentru clienții noi și clienții existenți (prelungire contract), și reziliază contracte în baza cererilor de reziliere.
Datele personale prelucrate în scopul încheierii de contracte pentru furnizarea de servicii de comunicații mobile, în general, sunt aceleași pentru toți operatorii controlați, și anume: nume, prenume, telefon, adresă de e-mail, cetățenie, serie și număr BI/CI, CNP, semnătură și adresă de domiciliu. Pe lângă acestea, operatorii controlați colectează copii ale actelor de identitate ale persoanelor fizice, respectiv copii ale BI/CI/pașaport/permis de ședere. Colectarea acestor copii de acte de identitate se efectuează atât la punctele de lucru ale operatorilor, cât și la punctele de lucru ale împuterniciților.
În contracte există clauze referitoare la acordul clientului, unde se precizează că acesta își exprimă acordul cu privire la prelucrarea CNP și a copiei actului de identitate, însă nu se oferea clientului posibilitatea de a opta pentru o astfel de prelucrare.
În urma investigațiilor efectuate de Autoritatea Națională de Supraveghere, s-a constatat că toți operatorii controlați au prelucrat în mod excesiv date cu caracter personal ce intrau

sub incidența art. 8 din Legea nr. 677/2001, modificată și completată, și au reținut prin colectare și stocare copii ale actelor de identitate ale persoanelor fizice cu care au încheiat contracte de furnizare de servicii de comunicații electronice, fără a avea consimțământul expres al acestor persoane fizice, în lipsa unui temei legal sau a unui aviz al Autorității Naționale de Supraveghere.
În temeiul prevederilor art. 4 alin. (1) lit. c), ale art. 5 și art. 8 din Legea nr. 677/2001 și ale art. 2 și art. 6 din Decizia ANSPDCP nr. 132/2011, coroborate cu prevederile art. 21 alin. (3) lit. d) și ale art. 27 din Legea nr. 677/2001, raportate la art. 3 alin. (5) coroborat cu art. 13 din Legea nr. 102/2005, Președintele Autorității Naționale de Supraveghere a emis decizii de ștergere/distrugere a datelor cu caracter personal privind codul numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, inclusiv a copiilor după actele de identitate care le conțin, deja colectate de către operatorii investigați, fără consimțământul expres al persoanelor vizate, fără temei legal sau fără avizul Autorității Naționale de Supraveghere.

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

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

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

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

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

O societate de telefonie mobilă a notificat Autoritatea națională de supraveghere cu privire la o încălcare a securității datelor cu caracter personal, care a constat în faptul că 8 dintre angajații săi au accesat neautorizat, în mod individual, aplicația care stochează datele de trafic existente pe factura detaliată a abonaților, în scop personal, cu depășirea

atribuțiilor din fișa postului. Datele cu caracter personal accesate neautorizat au fost doar vizualizate de către respectivii angajați, acestea neputând fi tipărite, copiate, exportate sau descărcate din aplicație.

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

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

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

În cadrul analizei interne, efectuate ca urmare a sesizării unei persoane vizate, societatea a concluzionat faptul că, dintr-o eroare tehnică, website-ul societății nu a fost securizat în mod corespunzător nici la momentul realizării, nici ulterior, când a fost copiat în mod identic pe serverul din România, astfel încât anumite informații, care în mod uzual pot fi vizualizate doar de deținătorul website-ului și/sau de persoana care îl gestionează, au putut fi accesibile și unor terți, în situația efectuării unor căutări precise, prin utilizarea de criterii precum denumirea societății și numele persoanelor care au aplicat pe website.
În urma investigației efectuate de Autoritatea națională de supraveghere, societatea a fost sancționată cu avertisment pentru săvârșirea contravenției prevăzute de art. 25 și art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, întrucât nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, deși avea această obligație potrivit art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679, ceea ce a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale persoanelor care și-au depus CV-urile pe website-ul societății.

2.6 Prelucrarea datelor personale prin mijloace de supraveghere video

FIŞĂ DE CAZ - Printr-o petiție s-a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o asociație de proprietari, în sensul că aceasta a instalat un sistem de supraveghere video la scara pe care o administrează, pe holuri și în lift, fără respectarea prevederilor legale.
Ca urmare a efectuării 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, pentru protecția proprietarilor și a bunurilor din condominiu. Cu privire la accesarea imaginilor înregistrate, s-a precizat că această operațiune se poate face doar de către persoanele anume desemnate, în cazuri justificate și în mod securizat; imaginile au fost dezvăluite doar organelor de poliție, în cadrul unor anchete.
Întrucât s-a constatat că asociația de proprietari nu a realizat informarea persoanelor vizate în conformitate cu prevederile art. 12 din Legea nr. 677/2001, deşi avea această obligaţie încă de la data instalării camerelor de supraveghere, aceasta a fost sancționată pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001.

FIȘĂ DE CAZ - Prin petițiile înregistrate, Autoritatea Națională de Supraveghere a fost sesizată că o Direcţie Generală de Asistenţă Socială şi Protecţia Copilului prelucrează imaginea prin intermediul sistemului de supraveghere video instalat fără respectarea tuturor dispozițiilor legale. În urma investigației efectuate, s-a constatat că Direcția prelucra imaginea angajaților și a minorilor instituționalizați, fără respectarea dispozițiilor legale în vigoare la acea dată și, ca urmare, operatorul a fost sancționat pentru contravențiile prevăzute de art. 31, art. 32 raportat la art. 12, respectiv art. 32 raportat la art. 4 din Legea nr. 677/2001.
De asemenea, s-a dispus operatorului, printre altele, suspendarea prelucrării datelor angajaților (imaginii) captate/colectate prin intermediul camerelor de supraveghere instalate în bucătărie și spălătorie, informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001, luarea măsurilor necesare în vederea respectării prevederilor Legii nr. 272/2004 privind protecţia şi promovarea drepturilor copilului în situația în care se prelucrează și date cu caracter personal ale minorilor (imaginea).

FISA DE CAZ - Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că i-a fost încălcat dreptul la viaţa privată cu privire la prelucrarea datelor cu caracter personal de către o societate comercială, respectiv un hipermarket, la care petentul era angajat, prin intermediul unui sistem de supraveghere video instalat în incinta în care acesta își desfășura activitatea.
Totodată, petentul și-a exprimat nemulțumirea față de răspunsul primit de la operator la cererea prin care și-a exercitat dreptul de acces la date. Din răspunsurile transmise Autorității naționale de supraveghere a rezultat faptul că angajații operatorului (inclusiv petentul) nu au fost informați clar cu privire la scopurile utilizării sitemului de supraveghere, precum și drepturile de care beneficiază.
În temeiul art. 58 alin. (2) lit. b) și d) din RGPD, raportat la art. 14 alin. (11), art. 15 alin. (1) și (3) și art. 16 alin. (5) din Legea nr. 102/2005, precum și la art. 12 din Legea nr. 190/2018 coroborat cu art. 7 din OG nr. 2/2001, s-au dispus următoarele măsuri:

Avertisment - pentru nesocotirea dreptului de informare, drept prevăzut de art. 13 din RGPD, întrucât operatorul nu a prezentat dovezi că a realizat informarea persoanelor vizate, angajați ai acestei societăți comerciale, conform prevederilor legale, cu privire la prelucrarea datelor lor prin sistemul de supraveghere video;

Măsuri corective constând în informarea adecvată a persoanelor fizice (inclusiv angajații societății) ale căror date personale le prelucrează prin sistemul de supraveghere video instalat în magazinele proprii în conformitate cu prevederile art. 13 din RGPD;

Recomandări:
- să stabilească o perioadă de stocare a datelor cu caracter personal, raportat la scopul în care sunt prelucrate și în concordanță cu dispozițiile legale în vigoare;
- să furnizeze persoanelor vizate informaţii privind acţiunile întreprinse în urma unor cereri în temeiul articolelor 15-22, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor.
Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.

2.7 Dezvăluirea datelor personale către diverse entități/terțe persoane

FIȘĂ DE CAZ – Un petent a sesizat Autoritatea Națională de Supraveghere cu privire la faptul că angajatorul i-a prelucrat ilegal datele cu caracter personal, conținute într-un raport medical de medicina muncii, prin dezvăluirea acestui document către fosta soție, fără consimțământul său. Petentul a reclamat faptul că angajatorul a depus ulterior în instanță acest document, în cadrul unui proces care avea ca obiect obținerea unui program de vizitare a unui minor și exercitarea în comun a autorității părintești.
În cadrul investigației efectuate, s-a constatat că angajatorul a dezvăluit anumite date medicale ale petentului, fără a avea consimțământul său.
La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a sancționat contravențional operatorul pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, pentru încălcarea prevederilor art. 5 din aceeași lege.

FIȘĂ DE CAZ - Prin petiția transmisă, petentul a reclamat faptul că o asociație ar fi prelucrat ilegal date cu caracter personal prin dezvăluirea acestora pe site-ul său. În fapt, petentul a susţinut că asociația a postat pe forum o plângere penală formulată împotriva mai multor persoane, plângere ce cuprindea nume şi prenume, adresa de domiciliu și CNP – ul persoanelor vizate, fără ca aceste date să fie anonimizate.
Din verificările efectuate, s-a constatat că documentul ce conținea datele cu caracter personal fusese vizualizat de 115 persoane. Ca urmare a investigației efectuate la asociație, a fost identificată pe site-ul acesteia plângerea penală formulată de un membru al asociației împotriva a 21 de persoane, plângere postată la solicitarea acestuia.
Reprezentanții operatorului au declarat că datele cu caracter personal ale persoanelor vizate nu au fost anonimizate, din neatenție. În urma demersurilor efectuate de Autoritatea Națională de Supraveghere, documentul respectiv a fost eliminat de pe site.
Față de constatări, operatorului i-a fost aplicată o sancțiune contravențională în baza art. 32, raportat la art. 5 și 8, din Legea nr. 677/2001, în vigoare la data săvârșirii faptei.

FIȘĂ DE CAZ – Mai mulți petiționari au sesizat Autoritatea Națională de Supraveghere cu privire la faptul că datele lor personale au fost dezvăluite, fără acordul lor, de către o autoritate publică unui dezvoltator imobiliar, prin transmiterea către acest terț a copiilor petițiilor adresate de petenți autorității. Petițiile dezvăluite de autoritatea publică către terț cuprindeau numele, prenumele, adresa de domiciliu și adresa de email, aparținând petenților, precum și aspecte referitoare la o construcție care urma a fi edificată la o adresă apropiată de domiciliul lor.
În cadrul investigației efectuate, operatorul a susținut că a dezvăluit datele petenților în baza unui temei legal, respectiv Ordinul care aproba metodologia de informare şi consultare a publicului cu privire la elaborarea sau revizuirea planurilor de amenajare a teritoriului şi de urbanism. Din analizarea actului normativ menționat a reieșit că operatorul nu a respectat prevederile acestuia, deoarece autoritățile competente cu aprobarea planului de amenajare a teritoriului şi de urbanism au obligația de a notifica inițiatorul PUD numai cu privire la eventualele obiecţii primite şi de a solicita acestuia modificarea propunerilor sau răspunsul motivat de refuz, cu acordarea unui termen de transmitere a acestui răspuns.
Astfel, întrucât în prevederile legale susmenționate nu se precizează că autoritatea competentă cu aprobarea planului urbanistic de detaliu dezvăluie inițiatorului PUD datele cu caracter personal ale persoanelor vizate care au făcut obiecții la acel plan, operatorul a fost sancționat contravențional pentru încălcarea art. 5 alin. (1) și (2) din Legea nr. 677/2001, pentru dezvăluirea ilegală a datelor personale ale petenților către un terț.

FISA DE CAZ - Un petent a sesizat Autoritatea națională de supraveghere cu privire la o posibilă încălcare a prevederilor legale privind prelucrarea datelor sale cu caracter personal de către deținătorul unui website care a transmis un mesaj comercial nesolicitat conținând toate adresele de e-mail vizibile ale destinatarilor, inclusiv adresa petentului.
În urma investigației efectuate, s-a constatat o încălcare a prevederilor legale prin modul în care operatorul a diseminat adresele de e-mail ale mai multor persoane, inclusiv adresa de e-mail a petentului.
În plus, a rezultat că operatorul de date reclamat nu a realizat informarea persoanelor vizate cu privire la scopul prelucrării datelor lor personale.
Pentru faptele constatate, în temeiul art. 58 alin. (2) lit. c) și d) din RGPD, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005 și art. 12 din Legea nr. 190/2018, s-a dispus aplicarea mai multor măsuri corective împotriva operatorului reclamat, și anume:

- să ia măsuri pentru informarea adecvată a persoanelor fizice ale căror date personale le prelucrează raportat la scopul prelucrării;
- să nu mai disemineze adresele de e-mail ale persoanelor care au calitatea de persoane vizate ale acestei societăți comerciale, în lipsa unui temei legal;
- transmiterea de mesaje comerciale prin mijloace de comunicare elctronică să se efectueze numai cu consimţământul expres prealabil al utilizatorului.

2.8 Nerespectarea drepturilor de informare, acces, intervenție și opoziție

FIȘĂ DE CAZ - Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o companie de telefonie mobilă, în sensul că aceasta i-a încălcat dreptul de acces la datele cu caracter personal. Petentul s-a adresat operatorului cu o cerere prin care solicita informații referitoare la prelucrarea datelor sale cu caracter personal, scopul prelucrării, datele prelucrate, destinatarii către care au fost dezvăluite datele, sursa de colectare a datelor și eventuale mecanisme automate, în situația în care acesta le utilizează. De asemenea, petentul a solicitat să i se comunice care sunt drepturile de care beneficiază în baza Legii nr. 677/2001. Urmare a cererii depuse, i s-a comunicat că are posibilitatea exprimării în mod gratuit a opțiunii în legătură cu primirea unor informații comerciale referitoare la oferte și programe de loialitate inițiate de operator, menționându-i-se totodată că va înceta prelucrarea datelor sale cu caracter personal la încetarea serviciilor, dacă nu se înregistrează debite restante.
Având în vedere că operatorul nu a răspuns solicitărilor efective ale petentului, la finalizarea demersurilor întreprinse, acesta a fost sancționat contravențional pentru că a încălcat dreptul de acces, întrucât nu i-a răspuns petentului în termenul legal de 15 zile și nu i-a comunicat toate informațiile solicitate prin cererea sa.

FIȘĂ DE CAZ - Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o autoritate publică. Petentul a susținut că operatorul i-a încălcat dreptul prevăzut de art. 13 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 și a fost nemulțumit că acesta nu i-a transmis toate informațiile solicitate, și anume, scopul concret al accesării datelor și categoriile de date prelucrate cu ocazia accesării.
În cadrul investigației s-a constatat că datele cu caracter personal ale petentului (CNP, nume și prenume) au fost accesate neautorizat într-o bază de date constituită la nivel național, la o anumită dată, de către un utilizator al operatorului.
De asemenea, s-a constatat că operatorul nu a transmis petentului toate informațiile pe care avea obligația să le transmită, în conformitate cu prevederile art. 13 din Legea nr. 677/2001, la cererea de exercitare a dreptului de acces la date, inclusiv informații cu

privire la scopul concret al accesării datelor sale cu caracter personal și categoriile de date prelucrate cu ocazia accesării.
În urma investigației efectuate, operatorul reclamat a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 33 din Legea nr. 677/2001, întrucât nu a adoptat suficiente măsuri de securitate şi confidenţialitate pentru a proteja datele personale ale petentului (nume, prenume, CNP) împotriva accesului neautorizat, aşa cum era prevăzut de art. 19 şi art. 20 din Legea nr. 677/2001, fapt care a permis accesarea ilegală a datelor acestuia, într-o bază de date constituită la nivel național, de către un utilizator al operatorului. Totodată, operatorul a fost sancţionat pentru contravenţia prevăzută de art. 32 din Legea nr. 677/2001, întrucât a încălcat dreptul de acces la date, prin faptul că nu a transmis petentului, în termen de 15 zile, toate informațiile pe care avea obligația să le transmită, în conformitate cu prevederile art. 13 din Legea nr. 677/2001, la cererea de exercitare a dreptului de acces la date, inclusiv informații cu privire la scopul concret al accesării datelor sale cu caracter personal și categoriile de date prelucrate cu ocazia accesării.

FIȘĂ DE CAZ - Un petent ne-a sesizat cu privire la refuzul Google de a da curs cererii de ștergere a unor adrese URL care figurau pe Internet ca fiind asociate unui site. Petentul s-a adresat Google arătând că informațiile publicate sunt false și se încearcă discreditarea sa de către un blogger. Conform informaţiilor furnizate de petent şi verificate de instituţia noastră, s-a constatat că site-ul reclamat este un blog personal pe care sunt postate şi informaţii privind unele călătorii efectuate de petent, fiind folosit un ton denigrator la adresa acestuia, dar și alte informații de natură personală care îl priveau pe petent (fără ca acesta să joace un rol în viața publică). Față de situația prezentată, Autoritatea Națională de Supraveghere a solicitat Google LLC să dea curs cererii petentului cu privire la adresa URL susmenționată, în cel mai scurt termen posibil.
Solicitarea s-a realizat având în vedere atât Decizia Curţii de Justiţie a Uniunii Europene în cauza Costeja, din 13 mai 2014, cât şi Ghidul pentru aplicarea Hotărârii Curţii de Justiţie a Uniunii Europene privind <Google Spania şi INC V. Agencia Española de Proteccion de Datos (AEPD) Mario Costeja Gonzales> C-131/12, adoptat pe 26 noiembrie 2014 de către Grupul de lucru Art. 29 din care face parte și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal din România. Google LLC nu a transmis un răspuns la adresa Autorității Naționale de Supraveghere, ci a solicitat instanței de judecată pronunțarea unei hotărâri prin care să se dispună anularea adresei ANSPDCP. Curtea de Apel București a hotărât respingerea cerererii formulate de reclamanta Google Inc. în contradictoriu cu Autoritatea Națională de Supraveghere, ca inadmisibilă. Față de cele de mai sus, instituția noastră a solicitat din nou operatorului să ia măsuri pentru soluționarea plângerii petentului.
În cadrul investigației efectuate, Google LLC a refuzat să dea curs solicitării instituției noastre, considerând că nu sunt întrunite condițiile prevăzute de lege pentru eliminarea URL-ului din rezultatele căutării. De asemenea, s-a constatat că Google LLC (fosta Google Inc.) nu și-a desemnat un reprezentant pe teritoriul României, conform art. 2 alin. (3) din Legea nr. 677/2001, cu toate că notificase la Autoritatea Națională de Supraveghere, încă din anul 2015, faptul că prelucrează date prin intermediul serviciilor de căutare web și că transferă date în SUA. Față de constatări, operatorului i-au fost aplicate sancțiuni contravenționale în baza art. 31 și art. 32 raportat la art. 14 și art. 15 din Legea nr. 677/2001, în vigoare la data constatării faptei.

2.9 Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

FIȘĂ DE CAZ - Un petent a sesizat o posibilă încălcare a dispoziţiilor legale de către o societate care i-a transmis prin SMS, la numărul personal de telefon, mesaje comerciale prin care își promova activitatea, după exercitarea dreptului de opoziție de către petent și

comunicarea unui răspuns că a fost dezabonat.
În urma investigaţiei efectuate, s-a constatat că operatorul colecta datele persoanelor fizice incluse în baza de date a societății fie ca urmare a efectuării unor comenzi on-line de către acestea, fie în urma realizării unor campanii de marketing prin diverse mijloace, respectiv radio și televiziune, urmate de contactarea telefonică a operatorului de către potențialii clienți. Cu aceste ocazii, operatorul solicita persoanelor vizate să își dea acordul pentru prelucrarea datelor, inclusiv pentru a fi informate cu privire la ofertele operatorului și „campaniile de marketing” .
Cu toate acestea, operatorul nu a ținut seama de exprimarea opoziției petiționarului de a nu mai primi mesaje comerciale și i-a transmis, prin SMS, astfel de mesaje ulterior cererii adresate de acesta și comunicării răspunsului că a luat act de solicitarea sa.
Astfel, întrucât operatorul i-a transmis petentului mesaje prin SMS, prin care își promova activitatea, ulterior opoziției manifestate de acesta și nu a putut prezenta 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 - Prin petiţia sa, un petent ne-a sesizat faptul că a primit mesaje comerciale nesolicitate, pe adresa sa de e-mail, în conținutul mesajelor fiind promovate produse comercializate de un site. De asemenea, petentul a susținut că s-a adresat operatorului prin intermediul poștei electronice, solicitând eliminarea datelor sale din baza de date a societății, dar nu a primit răspuns.
Ca urmare a investigației efectuate la această societate, s-a constatat faptul că, în ceea ce privește mesajele comerciale primite de petent pe adresa sa de e-mail, societatea nu a putut face dovada obținerii consimțământului său expres și prealabil pentru primirea de comunicări comerciale prin mijloace de comunicație electronică. De asemenea, s-a constatat faptul că operatorul nu a răspuns la cererea petentului.
Față de constatări, operatorului i-au fost aplicate sancțiuni contravenționale în baza art. 13 alin. (1) lit. q) din Legea nr. 506/2004 și a Legii nr. 677/2001 în vigoare la data săvârșirii faptei.

FIȘĂ DE CAZ - O petentă ne-a sesizat faptul că o anumită societate i-a transmis un mesaj comercial de tip SMS prin care era promovată activitatea acesteia, deși și-a exprimat dezacordul în acest sens. Petenta a mai menționat în petiția sa și faptul că s-a adresat societății prin e-mail, solicitând să i se șteargă datele personale, dar societatea a continuat să îi trimită mesaje comerciale la numărul personal de telefon. Urmare a investigației efectuate, s-a constatat că societatea a transmis mesaje promoționale cu oferte, pe numărul de telefon al petentei, fără a prezenta o dovadă certă a obținerii în prealabil a consimțământului expres al acesteia în vederea primirii de comunicări comerciale prin telefon, încălcând astfel prevederile art. 12 alin. (1) din Legea nr. 506/2004.
În urma investigației efectuate, față de cele constatate, societatea a fost sancționată pentru săvârșirea contravenției de „Nerespectare a prevederilor art. 12 referitoare la comunicările nesolicitate” , contravenţie prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004.

2.10 Încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date

FIȘĂ DE CAZ - Autoritatea Națională de Supraveghere a fost sesizată de către un petent cu privire la faptul că i-au fost dezvăluite datele cu caracter personal ale altei persoane, în cadrul unei operațiuni de deschidere cont bancar. În cadrul investigației s-a constatat că,

din eroare, odată cu furnizarea documentelor aferente deschiderii unui cont curent, reprezentantul operatorului bancar i-a înmânat petentului un exemplar de cerere deschidere cont emisă pe numele altei persoane, dezvăluind, fără temei legal, datele cu caracter personal ale acesteia.
La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a sancționat operatorul pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, întrucât a dezvăluit fără consimțământ datele cu caracter personal (nume, prenume, CNP, serie și număr CI, număr cont) ale unei persoane fizice, precum și pentru săvârșirea contravenției prevăzute de art. 33 din Legea nr. 677/2001, întrucât nu a luat măsuri tehnice și organizatorice împotriva dezvăluirii datelor personale ale unei persoane vizate către un terț.

FIȘĂ DE CAZ - Un petent a sesizat un incident de securitate la o societate comercială al cărei angajat a fost, în sensul că puteau fi accesate de către orice angajat al acestei societăți datele cu caracter personal colectate și stocate pe serverul acestui operator, aparținând unui număr de peste 5000 de persoane fizice (solicitanți, foști angajați, parteneri etc.). În cadrul investigației efectuate, s-a constatat faptul că, la data incidentului, unele foldere, care conțineau și date cu caracter personal ale angajaților, erau accesibile tuturor angajaților din societate. Acest fapt s-ar fi datorat unei erori în stocarea informațiilor financiare și personale ale angajaților, iar din dovezile disponibile, nu au existat indicii cu privire la transferarea datelor în afara companiei sau la utilizarea necorespunzătoare a acestora.
Întrucât operatorul nu a luat măsuri suficiente împotriva dezvăluirii și/sau accesului neautorizat la datele personale ale angajaților, fapt care a făcut posibil ca datele cu caracter personal ale acestora, colectate și stocate pe serverul societății, să poată fi accesate fără drept, a fost sancționat contravențional pentru „neîndeplinirea obligațiilor privind confidenţialitatea şi aplicarea măsurilor de securitate”, conform art. 33 din Legea nr. 677/2001, pentru încălcarea art. 20 din Legea nr. 677/2001.

2.11 Investigații în alte cazuri

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

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

Ca urmare a verificărilor efectuate, Autoritatea națională de supraveghere a constatat faptul că operatorul investigat a apreciat și implementat, într-un mod total eronat, faptul că o inacțiune a utilizatorului (nebifarea unei căsuțe) poate constitui un consimțământ valabil exprimat pentru prelucrarea datelor cu caracter personal, deși consimțământul trebuia să fie granular pentru fiecare dintre scopurile avute în vedere. Astfel, societatea a transmis prin e-mail ”Personal Update”, pentru un număr de 4357 de utilizatori, a colectat date personale într-un mod nelegal și netransparent față de persoana vizată, le-a prelucrat ulterior într-un mod incompatibil cu scopul în care au fost colectate inițial, respectiv executarea contractului, și nu a putut face dovada obținerii consimțământului granular pentru fiecare dintre scopurile avute în vedere, exprimat printr-o acțiune neechivocă, care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, prin bifarea căsuței/opțiunii pentru această prelucrare.

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

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

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

În urma investigației efectuate, s-a constatat că operatorul nu a implementat măsuri tehnice şi organizatorice adecvate, în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, ceea ce a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal (nume, prenume, adresa de corespondență, email, telefon, loc de muncă, detalii tranzacții efectuate) ale persoanelor care au efectuat tranzacții recepționate de website-ul societății, documente accesibile public prin intermediul motorului de căutare Google.

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

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

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

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

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

Totodată, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, Autoritatea națională de supraveghere a dispus operatorului și măsura corectivă de a revizui și actualiza măsurile tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal.

3. HOTĂRÂRI JUDECĂTOREȘTI PRONUNȚATE ÎN DIVERSE LITIGII ÎN DOMENIUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

3.1 Hotărâri definitive în litigii referitoare la supravegherea video a angajaților

Potrivit unei investigații efectuate de către Autoritatea națională de supraveghere, ca urmare a unor plângeri prin care se sesizau încălcări ale prelucrării datelor prin utilizarea de către un operator a unui sistem de supraveghere video prin care acesta își monitoriza angajații la locul de muncă, inclusiv în birouri, s-a constatat încălcarea legislației în vigoare, fiind dispuse sancțiuni cu avertisment și amendă.

Astfel, operatorul de date a fost sancționat întrucât, pe lângă faptul că nu a notificat prelucrarea datelor înainte de începerea prelucrării, potrivit legislației în vigoare la data respectivă, a prelucrat în mod nelegal datele, deoarece nu a realizat informarea completă a persoanelor vizate și a prelucrat în mod excesiv datele personale (imaginea) ale angajaţilor săi prin intermediul camerelor video instalate în birouri.

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

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

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

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

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

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

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

3.2 Hotărâre definitivă într-un litigiu referitor la prelucrarea datelor fără consimțământ

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

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

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

Pentru faptele constatate operatorul a fost sancţionat contravenţional, procesul-verbal de constatare/sancţionare contravenţională fiind contestat la instanţa competentă. Instanţa, analizând probatoriul administrat în cauză, a constatat că "....@yahoo.com (...) a fost raportat faptul că profilul în discuție nu a fost realizat de titularul adresei de e-mail - care s-a dovedit a fi semnatara petiției prin care a solicitat ștergerea acestuia; a arătat că primește mesaje deranjante, numele și pozele sunt reale, luate în mod abuziv de pe contul de facebook, iar restul informațiilor sunt greșite, unele clar cu tentă vindicativă".

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

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

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

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

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

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

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

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

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

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

3.3 Hotărâre definitivă într-un litigiu privind dezvăluri de date

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

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

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

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

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

Ca urmare a investigației efectuate la operator, Autoritatea națională de supraveghere a dispus prin procesul-verbal de constatare/sancţionare, în temeiul art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16

alin. (5) din Legea nr. 102/2005, precum și la art. 12 din Legea nr. 190/2018, măsuri corective împotriva acestuia, precum și obligația ca în termen de 45 de zile de la data comunicării procesului-verbal să transmită Autorității dovezi cu privire la respectarea măsurilor corective dispuse.

Operatorul a contestat în instanță măsurile corective dispuse.

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

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

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

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

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

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

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

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

Hotărârea instanței favorabilă Autorității naționale de supraveghere a rămas definitivă.