Revista Română de PROTECȚIA DATELOR

Revistă realizată de RENTROP & STRATON, nr. 14, martie 2019

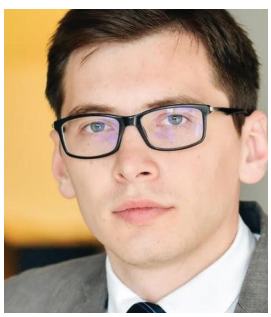
DIN SUMAR

R&S RENTROP & STRATON
Informații Specializate

SĂVESCU & ASOCIAȚII
LITIGATORS

GDPR: Lecții învățate și perspective din cel mai recent raport al ANSPDCP

av. Silvia Axinescu
Senior Managing Associate Reff & Associates SCA – Member of Deloitte Legal



av. Dragoș Șărban
Associate REFF & ASSOCIATES SCA – Member of Deloitte Legal

În contextul creșterii interesului pentru domeniul protecției datelor și a primelor amenzi impuse de la aplicarea GDPR în Portugalia, Germania, Austria și, de curând, în Franța, o analiză a celui mai recent raport al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) ne ajută să extragem cele mai relevante situații care ar putea deveni subiectul unor plângeri și/sau sancțiuni. Deși se bazează pe legislația anterioară GDPR (în principal, pe Legea nr. 677/2001), concluziile rămân valabile și în baza reglementărilor prezente.

Evident, de la an la an, activitatea ANSPDCP a fost una semnificativ crescută, atât la nivelul investigațiilor, precum și al plângerilor, fiind așteptat ca, pentru 2018 și 2019, tendința să se mențină. Am sintetizat în continuare cele mai importante constatări ale autorității care pot fi lecții pentru viitor:

Cookies

A fost verificată modalitatea de obținere a acordului pentru instalarea cookies pe device-ul persoanei vizate, precum și furnizarea informațiilor privind scopul prelucrării, tipurile de cookies stocate și accesate, durata acestora de stocare etc.

În contextul unor decizii aparent contradictorii la nivel european referitoare la opțiunile de acord pentru cookies oferite de paginile media (autoritatea din Austria și, respectiv, autoritatea din Marea Britanie) privind analiza valabilității acordului cu privire la acceptarea anumitor cookies pentru vizualizarea gratuită a conținutului versus achitarea unei sume de bani și, mai ales, al actualității subiectului la nivel european, așteptăm cu interes ca verificarea acestui aspect să fie manifestată și de către ANSPDCP, cât și poziția față de care se va alinia.

Date incluse în procese-verbale încheiate în cadrul unor proceduri disciplinare

Datele personale prelucrate în temeiul relațiilor de muncă dintr-un proces-verbal încheiat în cadrul unei proceduri disciplinare nu pot fi transmise, de exemplu, prin e-mail, către toți angajații operatorului, pentru a discuta situația în cadrul unui instructaj privind normele de securitate și sănătate în muncă.

Verificarea identității persoanei vizate

Facebook a solicitat copie a actului de identitate al unei persoanei vizate care voia să își recupereze parola și contul de pe această rețea de socializare. S-a considerat că Facebook pune la dispoziție proceduri diverse ce pot fi parcurse de către persoanele interesate (inclusiv pentru schimbarea parolei, raportarea de abuzuri). Însă parcurgerea acestor proceduri poate presupune furnizarea de informații suplimentare cerute de Facebook tocmai pentru a putea identifica cu exactitate persoana sau problema la care se face referire.

Considerăm că precizarea este foarte importantă în contextul dreptului de acces, când, în multe situații, se pune problema necesității verificării identității persoanei vizate și, implicit, solicitarea unor informații (documente) în acest sens. Cu toate acestea, o copie a actului de identitate nu poate fi so-

ATENȚIE!

Ce va urma? Având în vedere rolul activ al ANSPDCP în ceea ce privește publicarea de acte normative ulterior datei de 25 mai 2018, campaniile de informare desfășurate anterior prezenței subiectului în presă, există așteptări ca aceasta să fie cel puțin la fel de prezentă, atât din proprie inițiativă, cât și urmare a miilor de sesizări ale persoanelor vizate, tot mai active cu privire la conștientizarea, exercitarea drepturilor lor și cerința unor comportamente adecvate ale persoanelor care le prelucrează datele cu caracter personal.

licitată în toate situațiile în care o persoană vizată își exercită dreptul de acces sau oricare alt drept recunoscut în materie. Operatorul poate condiționa exercitarea unui drept atunci când informațiile pe care ar trebui să le furnizeze (ori să le prelucreze în alt mod, după caz, în funcție de dreptul exercitat) prezintă un grad de sensibilitate cel puțin mediu (precum date de sănătate – în cazul clinicilor medicale, comunicări cu terți – în cazul platformelor de social media, date financiare – în cazul băncilor).

Transmiterea datelor către alte autorități publice

S-a stabilit că fapta unei autorități publice de a nu informa persoanele vizate despre transmiterea datelor acestora către alte autorități publice și organisme private cu care avea încheiate protocoale nu respectă exigențele necesare aplicării efective a principiului transparenței, persoana vizată nefiind informată în mod complet, fapt care face ca prelucrarea să fie nelegală. În această speță, care a fost dedusă judecății, instanța a făcut aplicarea binecunoscutei decizii CJUE în *Cauza C-201/14 Bara și alții împotriva Președintelui CNAS, CNAS și ANAF* și a menținut sancțiunea aplicată.

Respectarea drepturilor persoanelor vizate

Din lectura raportului anterior, nu ne surprinde că una dintre principalele încălcări a fost legată de **nerespectarea dreptului la informare a persoanei vizate**. De altfel, și în prezent, o parte consistentă a operatorilor nu îndeplinesc ori îndeplinesc doar parțial această cerință, nefurnizând note de informare adecvate, mai ales în ceea ce privește zona de online. Asigurarea dreptului la informare este, până la urmă, expresia prin care se materializează posibilitatea persoanelor vizate de a se afla în deplină cunoștință a modului în care le sunt prelucrate datele, acesta fiind *mobilul* legislației în materie. Totodată, popularitatea subiectului în rândul persoanelor vizate este de așteptat să atragă verificări și în ceea ce privește **respectarea dreptului la acces**, mai ales în situația transmiterii unor răspunsuri generale sau incomplete.

O altă zonă care este de așteptat să se mențină în atenția ANSPDCP și pentru viitor este **nerespectarea măsurilor de protecție (securitate și confidențialitate) a datelor**, mai ales în contextul obligației de notificare a încălcărilor de securitate și, respectiv, informare a persoanei vizate. În acest sens, printre altele, în practică, (i) accesul angajaților se descoperă a fi unul general, iar nu agregat, doar pentru datele la care ar trebui să aibă acces, necesare pentru îndeplinirea activităților, (ii) sistemele de operare nu sunt prevăzute cu un sistem care să oblige utilizatorii (respectiv, angajații) să seteze parole complexe ori să expire la un interval de timp, (iii) salvarea documentelor pe un server cu acces restricționat este înlocuită de salvarea și dublarea acestora în diferite aplicații ori în memoria calculatorului fiecărui angajat.

Ce va urma?

Având în vedere rolul activ al ANSPDCP în ceea ce privește publicarea de acte normative ulterior datei de 25 mai 2018, campaniile de informare desfășurate anterior prezenței subiectului în presă, există așteptări ca aceasta să fie cel puțin la fel de prezentă, atât din proprie inițiativă, cât și urmare a miilor de sesizări ale persoanelor vizate, tot mai active cu privire la conștientizarea, exercitarea drepturilor lor și cerința unor comportamente adecvate ale persoanelor care le prelucrează datele cu caracter personal.

Rămâne de văzut dacă, la nivelul României, va avea loc o creștere a cuantumului amenzilor (cel puțin în cazul încălcării cu rea-credință ori gravă neglijență a dispozițiilor în materie, respectiv a celor care nu au depus minime eforturi pentru a se conforma legislației ori au făcut-o într-un mod superficial, doar pe hârtie) sau, din contră, preocuparea va fi de a formula avertismente însoțite de recomandări (urmate de verificări ulterioare cu privire la modul de redresare și respectare a acestora) în locul aplicării din start a unor amenzi.

A șaptea Plenară a Comitetului European pentru Protecția Datelor (CEPD)

Comitetul European pentru Protecția Datelor a publicat un scurt rezumat al celor discutate în cadrul celei de a șaptea Plenare CEPD.

Programul de lucru al Comitetului pentru perioada 2019-2020

Board-ul a adoptat programul său de lucru pentru doi ani: 2019-2020, în conformitate cu articolul 29 din Regulamentul de procedură al CEPD. Programul de lucru CEPD se bazează pe nevoile identificate de către membri drept prioritate pentru indivizi, părțile interesate, precum și activitățile planificate de legiuitorul UE.

Proiectul de aranjament administrativ în domeniul supravegherii piețelor financiare

Comitetul a adoptat primul său aviz privind un acord administrativ (AA), bazat pe articolul 46 alin. (3) lit. b) din GDPR, privind transferurile de date cu caracter personal între autoritățile de supraveghere financiară din SEE, inclusiv Autoritatea europeană pentru valori mobiliare și piețe (AEVMP) și țările din afara UE afiliate. Acest acord va fi prezentat autorităților de supraveghere competente pentru autorizare la nivel național.

Autoritățile de supraveghere competente vor monitoriza acordul și aplicarea sa practică pentru a se asigura că se respectă drepturile efective ale persoanelor vizate și se aplică mijloacele adecvate de redresare și supraveghere.

Brexit

CEPD a adoptat o notă de informare adresată entităților comerciale și autorităților publice cu privire la transferurile de date în cadrul GDPR în cazul unui brexit fără acord.

Fluxul de SEE în Regatul Unit

În absența unui acord între UE și Regatul Unit (Brexit no-deal), Regatul Unit va deveni o țară terță de la ora **00.00 CET la 30 martie 2019**.

În consecință, transferul datelor cu caracter personal din SEE către Regatul Unit va trebui să se bazeze pe unul dintre următoarele instrumente: Clauze standard sau ad hoc privind protecția datelor, Reguli corporative obligatorii, Mecanisme de conduită și de certificare și instrumentele specifice de transfer disponibile autorităților publice. În absența clauzelor standard de protecție a datelor sau a altor garanții alternative adecvate, devin aplicabile derogările existente în materie.

Ghidul privind codurile de conduită

Comitetul a adoptat Ghidul privind codurile de conduită. Obiectivul acestui Ghid este de a oferi orientări practice și asistență interpretativă în legătură cu aplicarea articolelor 40 și 41 din GDPR. Ghidul intenționează să contribuie la clarificarea procedurilor și a normelor implicate în transmiterea, aprobarea și publicarea codurilor de conduită atât la nivel național, cât și la nivel european. Ghidul ar trebui să acționeze în continuare ca un cadru clar pentru toate autoritățile de supraveghere competente, Consiliul și Comisia să evalueze codurile de conduită în mod consecvent și să eficientizeze procedurile implicate în procesul de evaluare. Ghidul va face obiectul unei consultări publice.

Vlad Bercu
Research Assistant
SĂVESCU & ASOCIAȚII

Restricționarea anumitor drepturi în contextul prelucrării datelor cu caracter personal de către CE

Elena Albu
consilier juridic

În Jurnalul Oficial al Uniunii Europene, seria L 37/144 din 8 februarie 2019 a fost publicată Decizia (UE) nr. 2019/236 a Comisiei din 7 februarie 2019 de stabilire a normelor interne privind furnizarea de informații persoanelor vizate și restricționarea anumitor drepturi ale acestora în contextul prelucrării datelor cu caracter personal de către Comisia Europeană în scopuri de securitate internă a instituțiilor Uniunii.

Comisia trebuie să își desfășoare activitatea într-un mediu de siguranță și securitate. În acest scop, Comisia are nevoie de o abordare coerentă și integrată în ceea ce privește securitatea sa, asigurând niveluri adecvate de protecție a persoanelor, a activelor și a informațiilor, în funcție de riscurile identificate, și asigurând furnizarea eficientă și la timp a securității. Comisia se confruntă cu amenințări și provocări majore în domeniul securității, în special în ceea ce privește terorismul, atacurile cibernetice și spionajul politic și comercial.

Pentru a asigura securitatea persoanelor, a activelor și a informațiilor, Comisia, în special prin intermediul Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, ia măsurile prevăzute în Decizia (UE, Euratom) nr. 2015/443 a Comisiei, care implică prelucrarea mai multor categorii de date cu caracter personal. Printre aceste măsuri se numără efectuarea de verificări ale antecedentelor în materie de securitate, în temeiul articolului 7 alineatul (5), de evaluări ale amenințărilor, în temeiul articolului 12, și de anchete privind securitatea, în temeiul articolului 13 din Decizia (UE, Euratom) nr. 2015/443. În cadrul mandatului său de investigare, Comisia colectează informații de interes pentru investigații, inclusiv date cu caracter personal, din diverse surse – autorități publice și persoane fizice – și face schimb de informații cu alte instituții, organe, oficii și agenții ale Uniunii, cu autoritățile competente ale statelor membre și ale țărilor terțe, precum și cu organizații internaționale înaintea desfășurării activităților de investigare sau coordonare, precum și în timpul și după încheierea acestor activități.

În îndeplinirea sarcinilor sale, Comisia, în calitate de operator, are obligația de a respecta drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, recunoscute la articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene și la articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene, precum și drepturile prevăzute în Regulamentul (UE) nr. 2018/1725 al Parlamentului European și al Consiliului. Totodată, Comisia are obligația de a respecta normele stricte în materie de confidențialitate prevăzute la articolul 9 din Decizia (UE, Euratom) nr. 2015/443.

Prezenta decizie stabilește normele pe care Comisia trebuie să le respecte pentru a informa persoanele vizate cu privire la prelucrarea datelor lor în conformitate cu articolele 14, 15 și 16 din Regulamentul (UE) nr. 2018/1725, atunci când își desfășoară toate sarcinile prevăzute în Decizia (UE, Euratom) nr. 2015/443.