



Revista Română de **PROTECȚIA DATELOR**

Revistă realizată de RENTROP & STRATON, nr. 12, ianuarie 2019

DIN SUMAR

- ✓ Scurtă retrospectivă privind activitatea Autorităților de Supraveghere UE și practica GDPR pentru anul 2018
- ✓ Adevărul gol-goluț despre dreptul de a fi uitat: Datele cu caracter personal se șterg foarte greu, aproape deloc
- ✓ Pentru cât timp pot fi păstrate datele cu caracter personal și când este necesar să le actualizați?

Revista Română de Protecția Datelor

Editorial: av. dr. Andrei Săvescu,
Managing Partner SĂVESCU &
ASOCIAȚII, președinte al SOCIETĂȚII de
ȘTIINTE JURIDICE

Coordonator colectiv autori:
av. Laurențiu Petre, Expert Data
Protection, Partner SĂVESCU &
ASOCIAȚII, Director JURIDICE.ro

Redactor-șef:
av. Andreea Coman, Managing Associate
SĂVESCU & ASOCIAȚII

Autori: av. Alexandru Matei, Senior
Associate SĂVESCU & ASOCIAȚII,
Vlad Bercu, Research Assistant

Manager proiect: Georgiana Istudor

Director Creație-Producție:
Cristina Straton

Tehnoredactare: Mirela Vasilescu
Corectură: Elvira Panaitescu

Fotografii: Adobestock

Redacția: Bdul Națiunile Unite
nr. 4, sector 5, București;
Telefon: 021.317.25.87,
E-mail: info@rs.ro; Internet: www.rs.ro
Corespondență:
Chișeu ext. 3 – O.P. 39, sector 3, București

Publicație editată de:
RENTROP & STRATON

Senior Editor: George Straton
Director General: Octavian Breban

© 2018 – RENTROP & STRATON
ISSN 2601 - 4289
ISSN-L 2601 - 4289

Toate drepturile rezervate. Nicio parte din această lucrare nu poate fi reprodușă, arhivată sau transmisă sub nicio formă și prin niciun fel de mijloace, mecanice sau electronice, fotocopiare, înregistrare audio sau video, fără permisiunea în scris din partea editorului. Autorii sau editorii nu sunt responsabili pentru nicio pierdere provocată vreunei persoane fizice sau juridice care acționează sau se abține de la acțiuni ca urmare a citirii materialelor publicate în această lucrare.

În această ediție:

- ✘ Editorial – Care este linia de practică cea mai avantajoasă pentru avocați, Avocat-pentru-operator sau Avocat-vânător-de-greșeli-ale-operatorilor? 2

- ✘ Scurtă retrospectivă privind activitatea Autorităților de Supraveghere UE și practica GDPR pentru anul 2018 3

- ✘ E-Privacy, *lex specialis* în raport cu GDPR 6

- ✘ Consimțământul – obținere, dovada, gestionare și revocare. Registrul de evidență a consimțământului 11

- ✘ Adevărul gol-goluț despre dreptul de a fi uitat: Datele cu caracter personal se șterg foarte greu, aproape deloc 16

- ✘ Inteligența artificială – un pericol pentru protecția datelor cu caracter personal sau un instrument de conformare la GDPR 19

- ✘ Pentru cât timp pot fi păstrate datele cu caracter personal și când este necesar să le actualizați? 23

Care este linia de practică cea mai avantajoasă pentru avocați, Avocat-pentru-operator sau Avocat-vânător-de-greșeli-ale-operatorilor?



av. dr. Andrei Săvescu
Managing Partner
SĂVESCU &
ASOCIAȚII

1. Pentru avocații care sunt aleși de către operatori pentru a-i ajuta să-și realizeze conformarea cu dispozițiile Regulamentului General European pentru Protecția Datelor cu Caracter Personal, fără îndoială că este o arie de practică avantajoasă, întrucât conformarea GDPR necesită o activitate laborioasă, precisă și relativ îndelungată. În cazul în care operatorii apelează la avocați in-house pentru asigurarea conformării, activitatea poate deveni chinuitoare, întrucât necesită un grad înalt de specializare, iar riscurile (amenziile) în caz de erori sau inexactități sunt mari.
2. Pentru ceilalți avocați, care apără interesele persoanelor vizate, vânarea greșelilor operatorilor este o sursă importantă de clientelă și avantajele pecuniare corespunzătoare. Probabil va fi așa o lungă perioadă după intrarea în aplicare a Regulamentului, întrucât conformarea este costisitoare și reprezintă, pentru mulți operatori, o cheltuială neprevăzută, care nu se va face imediat, ci trebuie bugetată. În plus, conformarea nu poate să fie o activitate uno ictu, din cauză că organizațiile au o dinamică internă permanentă, care necesită, în consecință, un efort permanent de adaptare a procedurilor privitoare la protecția datelor cu caracter personal, a fișelor de post, a regulamentului intern, a infrastructurii software și hardware.
3. Din acest motive, până la conformare și în fiecare zi, în permanență, acești operatori vor fi expuși față de Autoritatea națională de supraveghere, față de persoanele vizate și, nu în ultimul rând, față de propriii lor salariați nemulțumiți...
4. În concluzie, este dificil pentru avocați să aleagă linia de practică ideală, pentru că nu există o linie de practică ideală. Ceea ce însă toți avocații și consilierii juridici ar trebui să facă este să rămână mereu conectați la problematica protecției datelor cu caracter personal, pentru că GDPR este Codul civil 2. Se poate trăi și cu o cunoaștere superficială și fragmentară, însă documentarea permanentă este cel puțin la fel de importantă ca în domeniul dreptului civil. În ceea ce privește pericolele scăpărilor de informație, GDPR este chiar mai periculos decât Codul civil.

Scurtă retrospectivă privind activitatea Autorităților de Supraveghere UE și practica GDPR pentru anul 2018

1. Odată cu intrarea în vigoare a GDPR în luna mai 2018, entitățile juridice din România urmăresc, iar dacă nu, ar trebui să urmărească cu atenție activitatea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal („ANSPDCP”). Pe parcursul lunii ulterioare orei 0 de lansare a Regulamentului (UE) 679/2016, Autoritatea nu a făcut uz de competențele sale punitive, însă în această privință putem adăuga doar vestita încheiere utilizată în cinematografie: *to be continued...*

2. În ceea ce ne privește, considerăm că este de o importanță vitală pentru a înțelege perspectivele practicii în domeniul protecției datelor personale, urmărirea activității desfășurate de către Autoritățile de Supraveghere străine și Comitetul European pentru Protecția Datelor („CEPD”). În continuare, indicăm o compilație a celor mai interesante noutăți GDPR în spațiul european pentru perioada anului 2018.

3. Metamorfoza Grupului de lucru art. 29 (WP29) în Comitetul European pentru Protecția Datelor și activitatea acestuia. Pe parcursul anului 2018 CEPD a emis următoarele Ghiduri: Ghidul nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul 2016/679 – versiune pentru consultare publică; Ghidul nr. 2/2018 privind excepțiile prevăzute

de art. 49 din Regulamentul (UE) 2016/679; Ghidul nr. 3/2018 privind domeniul de aplicare teritorial (art. 3); Ghidul nr. 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor (2016/679).

4. CEPD s-a întrunit în cadrul a 5 Plenary, prilej cu care s-a discutat, în principal, cu privire la:

- Decizia Comisiei Europene privind recunoașterea unui nivel de protecție adecvat în Japonia raportat la prevederile art. 45 din Regulamentul General privind Protecția Datelor (*ar fi prima Decizie de adecvare emisă sub puterea Regulamentului general privind protecția datelor cu caracter personal*).
 - S-au adoptat avize privind Listele tipurilor de operațiuni de prelucrare pentru care este necesară o evaluare a impactului asupra protecției datelor (DPIA).
 - Proiectul Regulamentului E-evidence; necesitatea conceperii unui ghid sub formă de Q&A, privind interacțiunea dintre GDPR și Regulamentul (UE) nr. 536/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind studiile clinice intervenționale cu medicamente de uz uman.
5. Comisia pentru Protecția Datelor din Irlanda este una dintre cele mai active



Vlad Bercu
Research Assistant
SĂVESCU &
ASOCIAȚII

ATENȚIE!

Autoritatea de Supraveghere din Portugalia a aplicat o amendă de 400.000 de euro unui spital pentru încălcarea Regulamentului.

Autorități de Supraveghere din UE. Aceasta a pornit anchete ca urmare a notificărilor recepționate cu privire la *data breach* împotriva Facebook și Twitter. Comisia a constatat o multitudine de încălcări în privința securității datelor cu caracter personal în activitatea ambelor rețele de socializare.

6. În Italia, Autoritatea de Supraveghere (*Garante per la protezione dei dati personali*) informează că în primele 4 luni de la intrarea în vigoare a GDPR au fost numite 40.748 de persoane în funcția de responsabil cu protecția datelor cu caracter personal („RPD”; „DPO”); au fost transmise Autorității de Supraveghere un număr de 2.547 de plângeri; au fost emise 305 notificări către Autoritatea de Supraveghere având ca obiect încălcări ale securității datelor cu caracter personal.
7. În Germania, conform informațiilor furnizate de DLA Piper, Comisarul pentru protecția datelor și libertatea de informare din Baden-Wuerttemberg (din eng. *The State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg*, sau *LfDI* – abrevierea oficială) a fost prima autoritate germană pentru protecția datelor care a impus o amendă în baza dispozițiilor GDPR. Amendă de **20.000 de euro** a fost aplicată unei societăți din domeniul *social media* ca urmare a nerespectării obligației sale de a asigura securitatea prelucrării datelor cu caracter personal în temeiul art. 32 alin. (1) lit. a) GDPR (*obligația de pseudonimizare și criptarea datelor cu caracter personal*). *LfDI* a fost notificată privind încălcarea securității datelor în cadrul societății, ca urmare a unui atac hacker în urma căruia parolele și adresele de e-mail a aproximativ 330.000 de utilizatori au fost furate și publicate. S-a dovedit că societatea nu a criptat parolele clienților, ci le-a păstrat ca text simplu, încălcând astfel dispozițiile art. 32 GDPR.
8. Freshfields Bruckhaus Deringer Law Firm a anunțat că în octombrie, în Austria a fost aplicată prima amendă, cuantumul acesteia fiind de **4.800 de euro**. Amendă a fost aplicată unei companii care utiliza camere de supraveghere ce capturară o zonă prea mare, inclusiv o parte din trotuar pe care circulau pietonii. Astfel, Autoritatea de supraveghere austriacă a amendat compania pentru *monitorizarea ilegală a unui spațiu public fără o transparență adecvată și notificare a Autorității corespunzătoare*.
9. Autoritatea de Supraveghere din Portugalia (CNPD) a aplicat o amendă de **400.000 de euro** unui spital pentru încălcarea Regulamentului Uniunii Europene privind protecția generală a datelor (GDPR). Decizia nu a fost făcută publică, însă spitalul sancționat a anunțat că va contesta amenda. Conform surselor media portugheze, spitalul a fost amendat ca urmare a următoarelor încălcări: doctorii din cadrul spitalului, indiferent de specialitate, aveau acces la toate dosarele pacienților instituției medicale.
10. Până în prezent, Autoritatea Națională de Supraveghere a publicat lista celor mai relevante situații în care instanțele de judecată au menținut în cea mai mare parte sancțiunile contravenționale aplicate de Autoritatea de supraveghere în urma investigațiilor desfășurate până la data de 25 mai 2018, dată ce marchează aplicabilitatea efectivă a GDPR. În această listă au fost menționate societăți precum:
 - SC [...] SRL: „omisiunea de a notifica și notificarea cu rea-credință”, sub forma omisiunii de notificare întrucât societatea nu a făcut dovada notificării prelucrării datelor cu caracter personal, care permit, direct sau indirect, localizarea geografică a persoanelor fizice, deși utilizează sisteme de geolo-

calizare din anul 2017, instalate pe autovehicule; „prelucrarea nelegală a datelor cu caracter personal”, întrucât societatea nu a prezentat nicio dovadă sub nicio formă prevăzută de lege a informării persoanelor vizate cu mențiunile prevăzute de lege, pentru niciunul dintre scopurile în care prelucrează date cu caracter personal; „Neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate” deoarece [...] SRL nu a întocmit și nu a implementat o politică de securitate care să cuprindă cerințele minime de securitate a prelucrărilor de date pe care le efectuează; „Nerespectarea condițiilor prevăzute la art. 4 alin. (5) din Legea nr. 506/2004, modificată și completată”, întrucât [...] SRL, la nivelul site-ului www.[...].ro, pentru informațiile stocate în echipamentul terminal al utilizatorului nu a obținut acordul utilizatorului în cauză pentru cookie-urile existente la nivelul site-ului www.[...].ro și 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.

– SC [...] SA: „prelucrarea nelegală a datelor cu caracter personal” - întrucât compania a transmis date negative la Biroul de Credit, înainte de împlinirea termenului de 30 de zile de la data scadenței, precum și pentru faptul că nu a făcut dovada înștiințării prealabile a persoanelor vizate.

– SC [...] SA: „prelucrarea nelegală a datelor cu caracter personal” - întrucât societatea a transmis date negative la Biroul de Credit SA, raportat la 7 cazuri analizate în cuprinsul procesului-verbal, s-a constatat că pentru o parte dintre cazuri nu a realizat informarea prealabilă a clienților, deși a înregistrat

datele negative ale acestora în sistemul de evidență a Biroului de Credit.

– SC [...] SA: „prelucrarea nelegală a datelor cu caracter personal” - întrucât au fost nerespectate drepturile de intervenție și informare a persoanelor vizate, societatea nedând curs cererilor unor persoane vizate, prin care acestea și-au exercitat dreptul de intervenție, în sensul de a fi adoptate măsuri de ștergere din evidența Biroului de Credit a datelor negative transmise, fără realizarea informării prealabile a persoanei vizate.

– SC [...] SA: „prelucrarea nelegală a datelor cu caracter personal” - întrucât societatea a transmis date negative la Biroul de Credit pentru mai multe persoane vizate, fără să facă dovada informării prealabile a acestora.

– SC [...] SA: „prelucrarea nelegală a datelor cu caracter personal” - întrucât societatea nu a dat curs cererii persoanelor vizate, prin care acestea și-au exercitat dreptul de intervenție, în sensul de a fi adoptate măsuri de ștergere a datelor negative transmise la Biroul de Credit fără informarea sa prealabilă etc.

ATENȚIE!

Amenzile pot varia între 2% și 4% din cifra de afaceri mondială.

IMPORTANT!

Cuantumul amenzilor contravenționale aplicate a variat de la 5.000 lei până la 40.000 lei, amenzi menținute prin hotărâri definitive ale instanțelor de judecată.

11. Readucem aminte că, potrivit GDPR, pot fi aplicate amenzi: 1. Sancțiuni de până la 10 milioane de euro sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri mondială; 2. Sancțiuni de până la 20 de milioane de euro sau, în cazul unei întreprinderi, de până la 4% din cifra de afaceri mondială.

12. ANSPDCP nu a emis momentan nicio amendă, însă credem că primele sancțiuni nu se vor lăsa așteptate, urmând ca în cursul anului prezent (2019) să fim „martori” la primele exemple în acest sens.
13. De asemenea Autoritatea Națională de Supraveghere a emis următoarele acte: Lista operațiunilor pentru care este obligatorie DPIA; Procedura de primire și soluționare a plângerilor; Procedura de efectuare a investigațiilor; a fost aprobat formularul tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679.
14. În ceea ce privește piața de documentare română și protecția datelor cu

caracter personal, au apărut o multitudine de așa-numite *kituri GDPR*, din promovarea cărora reiese că la un preț redus și acceptabil veți primi un instrument prin care să vă conformați 100% la GDPR. Acest fapt trezește suspiciuni, în condițiile în care conformarea la GDPR reprezintă un proces anevoios și cât se poate de individual fiecărei entități juridice în parte. Recomandăm să abordați cu rezerve astfel de instrumente.

15. În concluzie, anul 2018 a fost unul în care Regulamentul general privind protecția datelor „a tatonat terenul”. Pentru specialiștii din domeniul protecției datelor reprezintă un interes sporit ce va aduce anul 2019, care cu siguranța va fi unul *de aplicare efectivă a GDPR*.

E-Privacy, *lex specialis* în raport cu GDPR

Viitorul nostru digital poate fi construit numai pe încredere. Toată lumea trebuie protejată. Normele UE consolidate privind protecția datelor vor deveni realitate la 25 mai. Este un pas important înainte și suntem hotărâți să-i facem un succes pentru toată lumea (Andrus Ansip, vicepreședinte al Comisiei Europene pentru piața unică digitală, 24 ianuarie 2018)



av. Alexandru Matei
Senior Associate
SĂVESCU &
ASOCIAȚII

În prezent, există o propunere de Regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind viața privată și comunicațiile electronice sau ePrivacy). Acest regulament care, momentan, se află la stadiul de proiect trebuia să se aplice odată cu GDPR (Regulamentul general privind protecția datelor cu caracter personal), respectiv din data de 25 mai 2018. În cazul în care acesta se va aplica în viitor, este necesar ca operatorii de

date cu caracter personal care își desfășoară activitatea în domeniul comunicațiilor electronice să se conformeze potrivit prevederilor acestuia.

ePrivacy își propune să asigure coerența cu GDPR și cu securitatea juridică pentru utilizatori și întreprinderi, în egală măsură acționând ca *lex specialis* față de regulamentul privind protecția datelor. Ca domeniu de aplicare, vizează prelucrările datelor transmise prin intermediul comunicațiilor electronice efectuate în legătură cu prestarea și utilizarea serviciilor de comunicații