

## **Impactul Regulamentului general privind protecția datelor personale asupra activității avocaților.**

### **Noi responsabilități, noi oportunități**

**Av. Dr. Gheorghe Florea, președinte UNBR**

A mai rămas extrem de puțin timp până la intrarea în vigoare a noilor reglementări europene privind protecția datelor personale, care vor produce o schimbare de paradigmă în activitatea de zi cu zi a avocaților, în legătură cu modul în care abordăm datele personale ale clienților, dar și pe cele ale terților, atunci când luăm cunoștință de acestea de la clienți, de exemplu.

Este important să regândim aceste reguli noi în contextul principiilor fundamentale privind secretul profesional și confidențialitatea comunicărilor avocat client. De asemenea, trebuie să abordăm noile reglementări și în contextul tendințelor de interprofesionalitate, ale relațiilor avocaților cu autoritățile ce dețin baze de date sau, eventual, solicită date personale de la avocați. Nu în ultimul rând, să fim atenți cum echilibrăm libertatea de exprimare a avocatului cu dreptul la protecția datelor personale, care se conturează ca un drept fundamental de sine stătător, autonom<sup>1</sup>.

Este vorba de două acte normative europene ce vor avea impact puternic asupra avocaturii:

*[Regulamentul \(UE\) 2016/679](#) al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind*

---

<sup>1</sup> A se vedea par. (1) din [Regulamentul \(UE\) 2016/679](#) al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (GDPR) : ”Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.”

*libera circulație a acestor date și de abrogare a Directivei 95/46/CE (GDPR) , care se va aplica direct, începând cu data de 25 mai 2018, fără a fi necesară vreo transpunere.*

*[Directiva \(UE\) 2016/680](#) a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului , care are termen limită de implementare 6 mai 2018. Această directivă va trebui transpusă, desigur. Deocamdată, există un proiect, care a fost în dezbateri publice pe site-ul Ministerului Afacerilor Interne, autoritatea desemnată pentru implementarea Directivei (UE) 2016/680.*

[Proiectul de lege](#) care implementează GDPR și Directiva (UE) 2016/680 a fost publicat pentru dezbateri publice pe [site-ul MAI](#), la data de 5.09.2017<sup>2</sup>. Este un proiect de modificare și completare a nr. Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. **Acesta abrogă și Legea nr. 677/2001** pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, întrucât Regulamentul GDPR este aplicabil direct, în toate țările UE, nefiind necesară nicio transpunere. Acest proiect n-a mai avansat după faza dezbaterilor publice, însă, probabil, acest lucru se va întâmpla în următoarele două luni, pentru a nu intra în procedura de infringement.

Ce aduce nou acest proiect este, în principal, asigurarea competențelor și sarcinilor de monitorizare și control ale Autorității Naționale de Supraveghere în acord cu prevederile art. 55-59 din Regulamentul (UE) 2016/679, în scopul de a avea un cadru legal adecvat pentru respectarea drepturilor specifice ale persoanelor fizice în domeniul prelucrării datelor cu caracter

---

<sup>2</sup> [Proiect de Lege](#) pentru modificarea și completarea nr. Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date

personal (dreptul de informare, dreptul de acces, dreptul la rectificare, dreptul la restricționarea prelucrării, dreptul la ștergerea datelor – dreptul ”de a fi uitat”, dreptul de opoziție, dreptul la portabilitatea datelor). Sunt stabilite principalele atribuții ale Autorității Naționale de Supraveghere și ale președintelui acesteia, în acord cu elementele de noutate aduse de cele două acte normative ale Uniunii Europene, Regulamentul (UE) 2016/679 și Directiva (UE) 2016/680<sup>3</sup>.

### **Incidența reglementărilor privind protecția datelor în cadrul cabinetelor de avocatura**

Practic, va trebui să regândim activitatea de zi cu zi, astfel încât să acordăm o atenție sporită protecției datelor cu caracter personal pe care le prelucrăm și să implementăm noile reguli în cadrul cabinetelor și societăților profesionale, pentru că amenziile vor fi usturătoare.

Încă din decembrie 2016, CCBE a atenționat uniunile profesionale membre cu privire la impactul pe care îl va avea Regulamentul (UE) 2016/679 asupra avocaturii și a emis un set de [recomandări](#) pentru implementarea acestuia în cadrul profesiei de avocat. În mai 2017, CCBE a publicat un [GHID](#) privind principalele măsuri de conformitate pentru avocați în materie de protecție a datelor. **La UNBR se lucrează la un asemenea Ghid de aplicare a reglementărilor europene privind protecția datelor la nivelul cabinetelor de avocatură din România.** Însă, acest ghid trebuie să fie unul dinamic, să fie adaptat permanent în funcție de practica judiciară și de reglementările în materie pentru că urmează schimbări în legislația națională privind protecția datelor personale. Inclusiv la nivelul UE așteptăm orientări/documente ale grupul de lucru instituit prin articolul 29, în vederea punerii în aplicare a regulamentului, referitoare la aspecte foarte importante, cum ar fi: încălcarea securității datelor, consimțământul, transparența, certificarea și acreditarea etc, și care sunt în curs de elaborare<sup>4</sup>.

### **Prudență sporită în obținerea consimțământului pentru prelucrarea datelor clientului**

---

<sup>3</sup> A se vedea [Expunere de motive](#) și [Tabel comparativ](#) la proiectul de lege

<sup>4</sup> A se vedea [Comunicarea Comisiei Europene din 24.01.2018](#) ”Protecție sporită, noi oportunități - Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecția datelor de la 25 mai 2018”

Este clar că avocații vor trebui să manifeste mai multă prudență în ce privește obținerea consimțământului clientului pentru prelucrarea datelor personale ale acestuia, astfel încât să vizeze toate activitățile de prelucrare și toate scopurile prelucrării. Asta înseamnă că avocatul trebuie să aprecieze, în funcție modul și condițiile în care vor fi prelucrate datele clientului, dacă trebuie să ia măsuri cum ar fi o declarație făcută în scris, inclusiv în format electronic. Va trebui să discutăm dacă nu cumva ar fi necesare și modificări ale contractului de asistență juridică, prin inserarea unei clauze de consimțământ generale (bifarea unei căsuțe), care să fie completată dacă este cazul, sau ar fi mai eficientă o declarație separată care exprimă consimțământul clientului pentru protecția datelor sale personale.

### **Notificarea autorității de supraveghere vs. secretul profesional**

Una dintre noutățile aduse de GDPR este aceea că avocații vor fi obligați să notifice autoritatea de supraveghere în cazul în care are loc o încălcare a securității datelor cu caracter personal, în cel mult 72 de ore de la data la care a luat cunoștință de aceasta. Încălcarea securității datelor cu caracter personal înseamnă "orice act care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea. Pe de altă parte, avocatul trebuie să țină seama de secretul profesional.

Așa cum arată CCBE, barourile sunt invitate să ia în considerare opțiunea de a încerca să îndemne autoritățile naționale să limiteze puterea autorităților de supraveghere de a avea acces la datele deținute de avocați, inclusiv datele deținute locațiile acestora, în conformitate cu articolul 90 din GDPR<sup>5</sup>.

Articolul 90 "Obligații privind păstrarea confidențialității", prevede, la alin. 1 că **statele membre pot adopta norme specifice pentru a stabili competențele autorităților de supraveghere în legătură cu operatori sau cu persoane împuternicite de operatori care au obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate**, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru între dreptul la protecția datelor

---

<sup>5</sup> A se vedea considerentul 164 din GDPR

cu caracter personal și obligația păstrării confidențialității. Respectivele norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

În temeiul art. 90, alin. 2, statul român trebuie să notifice normele adoptate în temeiul alineatului (1) până la 25 mai 2018.

**În opinia mea, va trebui să insistăm în adoptarea unor astfel de norme.**

Sigur că trebuie să ne gândim cum facem cu protecția datelor în cadrul relațiilor interprofesionale, având în vedere tendințele de tehnicizare a dreptului și a cererii de consultanță integrată din mai multe domenii juridice sau nejuridice, în paralel cu noile reguli mult mai stricte. Se practică interconectarea fișierelor și aici e necesară o atenție sporită.

### **Oportunități pentru avocați**

Pentru avocați, noile reglementări înseamnă nu numai responsabilități sporite, dar și oportunități, care constau într-o cerere ridicată de aria de consiliere juridică pe acest domeniu, dar și posibilitatea de a fi responsabil cu protecția datelor personale, unde ar trebui să reglementăm aspectele referitoare la compatibilitate.

Ca domeniu de expertiză, protecția datelor personale ia amploare și avocații pot folosi această oportunitate. În perioada următoare se va pune accent pe creșterea nivelului de conștientizare și de înțelegere de către publicul larg a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare a datelor. Avocații au un rol important în acest sens. Comisia Europeană a subliniat recent într-o [comunicare](#) că "aceasta nu înseamnă însă că operatorii și persoanele împuternicite de către operatori ar trebui să se aștepte să primească de la autoritățile pentru protecția datelor tipul de consiliere juridică adaptată și individualizată **pe care numai un avocat sau un responsabil cu protecția datelor ar putea să o ofere**". Deci, extinderea ariei de expertiză în acest sens ar putea aduce beneficii profesiei.

În ce privește postul de responsabil cu protecția datelor care ar putea fi ocupat de avocat, aici sunt mai multe aspect de discutat, nu numai sub aspectul reglementărilor referitoare la compatibilitate, pentru că sunt totuși ocupații diferite. Așa cum remarca și CCBE, ar trebui ținut cont de complexitatea îndatoririlor acestui post, ceea ce impune că persoana care acționează ca persoana responsabilă cu protecția datelor are nevoie de mai multă pregătire în afară celei juridice. Atenție, Regulamentul este extrem de dur cu greșelile!

Pe de altă parte, în cadrul societăților de avocatură va trebui desemnat un responsabil cu protecția datelor ori de câte ori activitățile constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni<sup>6</sup>. **Se pune problema ce înseamnă prelucrare la scară largă în cadrul cabinetelor de avocatură,** întrucât numai în acest caz legea obligă la desemnarea unui responsabil cu protecția datelor. Așa cum prevede și GDPR, ”prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie.”<sup>7</sup> În principiu, nu ar trebui numit responsabil cu protecția datelor atunci când prelucrarea datelor personale referitoare la condamnările penale și infracțiuni de către un cabinet individual de avocatură. Dar, deși în unele cazuri nu este necesară desemnarea unui responsabil cu protecția datelor, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal recomandă numirea unei astfel de persoane, întrucât este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal<sup>8</sup>.

---

<sup>6</sup> art. 37, al. 1, lit c din GDPR.

<sup>7</sup> par. 91 din GDPR

<sup>8</sup> Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – Comunicare privind [”Responsabilul cu protecția datelor cu caracter personal”](#)

Va trebui să acordăm atenție noilor reguli în activitățile desfășurate de avocați în cadrul profesiilor compatibile cu profesia de avocat și în conlucrările interprofesionale pentru furnizarea de servicii integrate.

### **Protecția datelor cu caracter personal la utilizarea acestora de către autoritățile polițienești și judiciare din sectorul penal**

O altă chestiune pe care vor trebui s-o aprofundeze avocații, în calitate de apărători ai drepturilor fundamentale ale cetățenilor, se referă la protecția datelor cu caracter personal la utilizarea acestora de către autoritățile polițienești și judiciare din sectorul penal.

Aici trebuie să vedem cum se abordează transpunerea [Directivei \(UE\) 2016/680 – protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile polițienești și judiciare din sectorul penal și privind libera circulație a acestor date](#).

Așa cum am arătat mai devreme, există un proiect de transpunere a Directivei și a Regulamentului GDPR, însă pare destul de minimalist în contextul tendințelor de supraveghere electronic în masă, unde avocații sunt vizați indirect.

Directiva impune ca datele colectate de autoritățile de aplicare a legii să fie<sup>9</sup>:

- prelucrate **în mod legal și echitabil**;
- colectate în **scopuri determinate, explicite și legitime** și să fie prelucrate numai potrivit acestor scopuri;
- **adecvate, relevante și neexcesive** în ceea ce privește scopurile în care sunt prelucrate;
- **exacte și actualizate** dacă este necesar;

---

<sup>9</sup> Comisia Europeană: Sinteză privind Directiva (UE) 2016/680: [Protecția datelor cu caracter personal la utilizarea acestora de către autoritățile polițienești și judiciare din sectorul penal](#) (din 2018)

- păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective;
- **securizate adecvat**, incluzând protecția împotriva prelucrării neautorizate sau ilegale.

De asemenea, Directiva impune ca autoritățile de aplicare a legii să facă o distincție clară între datele diferitelor categorii de persoane, inclusiv: cele în privința cărora există  **motive serioase**  să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune; cele care au fost  **condamnate pentru săvârșirea unei infracțiuni** ;  **victimele unor infracțiuni**  sau persoanele în privința cărora există motive să se creadă că ar putea fi victimele unor infracțiuni; cele care sunt  **părți care au legătură cu infracțiunea** , inclusiv potențialii martori.

**Informații disponibile sau furnizate persoanei vizate.**

## **Concluzii**

În concluzie, avem în față o reformă a reglementărilor privind protecția datelor cu caracter personal, în care avocații au un rol special sub aspectul punerii în aplicare a acestor reglementări, cât și sub aspectul apărării unui drept fundamental la protecția datelor personale.

UNBR va conlucra permanent cu barourile în acest sens, pentru a lua toate măsurile necesare implementării noilor reguli, în funcție de situațiile care se vor ivi în practică.

Sunt foarte multe aspecte de realizat, în condițiile în care nici la nivel european nu avem încă pregătite toate ghidurile de aplicare a Regulamentului GDPR.

Prin aceste reglementări europene, avocații sunt provocați să facă față noilor tehnologii, care implică un risc sporit în privința protecției datelor personale.

În funcție de modul în care este aplicat GDPR, acesta poate deveni un instrument puternic de apărare a secretului profesional, de apărare a cetățenilor împotriva abuzurilor legate de supravegherea electronică în masă sau, dimpotrivă, un instrument de sancționare a avocaților.