4 Aprilie 2018

GHID DE BUNE PRACTICI

privind principalele obligații ale avocaților conform Regulamentului General privind Protecția Datelor (GDPR)

CUPRINS

PARTEA I – ASPECTE GENERALE

I. GLOSAR

„GDPR”, „Regulamentul”	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 (Regulamentul general privind protecția datelor, în limba engleză *General Data Protection Regulation*)
„date cu caracter personal”	orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
”prelucrare”	înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
„operator”	înseamnă 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;

„persoană împuternicită de operator”	înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
„destinatar”	înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
„parte terță”	înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
„consimțământ”	al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
„încălcarea securității datelor cu caracter personal”	înseamnă o încălcare a securității 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;
„reprezentant”	înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27 din GDPR, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR;
„reguli corporatiste obligatorii”	înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de

	întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;
„autoritate de supraveghere”	înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 GDPR;
DPO	responsabilului cu protecția datelor (în limba engleză, *data protection officer*)
FEPA	Forme de exercitare a profesiei de avocat
A29 GL, WP29	Grupul de Lucru Art. 29 (în limba engleză, Article 29 Working Party), organism consultativ independent al Uniunii Europene în domeniul protecției și securității datelor, format din reprezentanții autorităților de supraveghere a prelucrării datelor personale din statele membre ale Uniunii Europene
DPIA	Evaluarea impactului asupra protecției datelor (în limba engleză, *data-protection impact assessment, DPIA*);

II. PRIVIRE GENERALĂ ASUPRA NOULUI CADRU LEGAL ÎN MATERIA PROTECȚIEI DATELOR CU CARACTER PERSONAL

A. SFERA DE CUPRINDERE A GHIDULUI. LIMITĂRI AFERENTE

1. Prezentul Ghid a fost adoptat de Consiliul Uniunii Naționale a Barourilor din România și are drept scop explicitarea principalelor prevederi ale Regulamentului 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 (în continuare **„Regulamentul”**, **“GDPR”**), pentru a facilita aplicarea acestora la nivelul organelor profesiei și al formelor de exercitare a profesiei.

2. Ghidul urmărește două scopuri fundamentale:

   a) Să constituie un instrument de clarificare și interpretare a prevederilor Regulamentului, particularizat la specificul profesiei de avocat; și

   b) Să propună o serie de bune practici menite să asigure aplicarea adecvată și unitară a normelor care guvernează prelucrarea datelor cu caracter personal în activitatea organelor profesiei și a formelor de exercitare a profesiei.

B. REGULAMENTUL ȘI IMPACTUL SĂU ASUPRA PROFESIEI

3. Începând cu 25 mai 2018, Regulamentul abrogă și înlocuiește Directiva nr. 95/46/EC privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (art. 94 din Regulament).

4. Regulamentul are aplicabilitate directă în toate Statele Membre în baza Tratatului pentru Funcționarea Uniunii Europene. În consecință, începând cu 25 mai 2018, Regulamentul înlocuiește și actul normativ-cadru de reglementare internă a acestui domeniu special, Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

5. Având în vedere că, în desfășurarea activității lor specifice, organele profesiei și formele de exercitare a profesiei prelucrează date cu caracter personal, Regulamentul va fi incident și acestora.

6. Prelucrarea datelor cu caracter personal de către organele profesiei și de către formele de exercitare a profesiei se va realiza cu respectarea principiilor prevăzute în art. 5 din Regulament:

   a) datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent;

   b) datele cu caracter personal trebuie prelucrate pentru scopuri determinate, explicite și legitime;

c) datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive;

d) datele cu caracter personal trebuie să fie exacte și actualizate;

e) datele cu caracter personal trebuie să fie păstrate pe o perioadă care nu depășește perioada necesară prelucrării pentru scopul identificat;

f) datele cu caracter personal trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora.

III. CALIFICAREA AVOCATULUI DIN PERSPECTIVA REGULAMENTULUI

7. Regulamentul consacră regimuri juridice distincte pentru *operator* și *persoană împuternicită*, caracterizate, în esență, prin faptul că:

   a) Obligațiile *operatorului* sunt mai numeroase decât cele ale *persoanei împuternicite*. Spre pildă, cu excepția unor situații limitate, operatorul este obligat să informeze persoanele vizate cu privire la prelucrare și caracteristicile acesteia.

   b) Răspunderea *operatorului* este mai extinsă decât cea a *persoanei vizate*, în special din perspectiva cazurilor de răspundere.

   c) Drepturile persoanelor vizate se exercită, în principal, în relația cu *operatorul*, *persoana împuternicită* având, de principiu, un rol de asistare a *operatorului* în exercitarea acestor drepturi.

8. Raportat la cele de mai sus, **va fi esențial ca organele profesiei sau, după caz, fiecare FEPA să stabilească dacă, pentru fiecare prelucrare de date cu caracter personal, se califică drept *operator* sau *persoană împuternicită*.**

9. Conform art. 4 din Regulament:

   a) *operatorul* este 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;

   b) *persoana împuternicită* de operator este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal pe seama operatorului.

10. Avocatul prestează un serviciu în favoarea clientului său. Totuși, aceasta nu înseamnă în mod necesar că avocatul este *persoană împuternicită* în sensul Regulamentului. Recomandăm ca FEPA să analizeze de la caz la caz, în funcție de rolul lor în contextul fiecărei prelucrări de date cu caracter personal, dacă respectiva prelucrare se realizează în calitate de *operator* sau de *persoană împuternicită* de operator.

11. În calificarea avocatului ca *operator*, un rol esențial îl va avea gradul de control al avocatului în ce privește respectiva prelucrare, mai concret:

    a) Stabilește avocatul care vor fi persoanele vizate de prelucrare? (”*Cine?*”)

    b) Stabilește avocatul ce categorii de date vor fi prelucrate? (”*Ce?*”)

    c) Stabilește avocatul pentru ce scop se va realiza prelucrarea? (”*Pentru ce?*”)

    d) Stabilește avocatul cum se va realiza prelucrarea? (”*Cum?*”) – de pildă, cui se dezvăluie datele cu caracter personal, pentru cât timp se rețin datele cu caracter personal etc.

12. Dacă răspunsurile la întrebările de mai sus sunt majoritar ”DA”, atunci avocatul va acționa ca *operator* de date cu caracter personal, iar nu ca *persoană împuternicită* de operator.

13. În cele mai multe cazuri avocatul este operator, întrucât el este cel care stabilește care sunt datele cu caracter personal de care are nevoie în vederea pregătirii apărării (”Ce?”) și cum vor fi utilizate aceste date pentru apărarea drepturilor și intereselor legitime ale clientului său (”Cum?”).

***Exemplu**: o persoană se adresează unui avocat pentru introducerea unei cereri de divorț. Clientul are reprezentarea serviciului pe care avocatul îl va presta, însă avocatul este cel care decide: 1. ce date cu caracter personal solicită clientului, 2. care dintre acestea vor fi utilizate în demersul judiciar și 3. cum vor fi acestea folosite.*

Din momentul în care clientul transmite datele cu caracter personal avocatului, acesta exercită un control semnificativ în ce privește modul în care le va prelucra, chiar dacă prelucrarea se face pentru client. În consecință, în exemplul de mai sus, avocatul va acționa în calitate de operator de date cu caracter personal.

---

14. În situația în care controlul pe care avocatul îl exercită asupra datelor cu caracter personal primite de la client nu există sau este redus, avocatul va acționa în calitate de *persoană împuternicită* de operator.

***Exemplu**: o societate transmite unui avocat un contract de ipotecă mobiliară, solicitând înscrierea garanției în arhiva electronică de garanții reale mobiliare.*

În acest caz, intervenția avocatului în procesul de prelucrare a datelor cu caracter personal este minimă. El nu decide asupra

modului cum vor fi prelucrate datele cu caracter personal, ci doar completează pe avizul de ipotecă datele pe care le preia din contract și transmite acest aviz către arhivă.

PARTEA A II-A – REGULI DE BUNĂ PRACTICĂ PENTRU CONFORMAREA CU REGULAMENTUL

I. TEMEIURI LEGALE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE FORMELE DE EXERCITARE A PROFESIEI DE AVOCAT

A. ASPECTE GENERALE

15. Prelucrarea datelor cu caracter personal se poate realiza în mod legal numai dacă se bazează pe unul din temeiurile juridice prevăzute la art. 6 alin. (1) din Regulament, respectiv:

    a) Consimţământul persoanei vizate;

    b) Prelucrare necesară pentru încheierea sau executarea unui contract;

    c) Prelucrare necesară pentru îndeplinirea unei obligații legale;

    d) Prelucrare necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

    e) Prelucrare necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

    f) Prelucrare necesară 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.

16. Sunt necesare câteva precizări privind selectarea temeiului juridic de prelucrare adecvat fiecărei categorii de prelucrare de date cu caracter personal:

    a) Ținând cont de scopurile urmărite prin prelucrarea datelor cu caracter personal, primul pas în evaluarea conformității unei prelucrări de date este determinarea temeiului juridic în baza căruia se face prelucrarea. Fără un temei juridic corect identificat, prelucrarea este ilegală;

    b) Alegerea temeiului de prelucrare trebuie făcută corect de la început, schimbarea ulterioară a temeiului, fără justificare adecvată, este echivalentă cu o neconformitate;

    c) Alegerea temeiului de prelucrare trebuie documentat (cel mai frecvent, prin evidența activităților de prelucrare);

    d) Persoanele vizate trebuie informate cu privire la temeiul prelucrării, ca principiu, înainte de începerea prelucrării.

17. Art. 6 nu conține vreo referință specifică la situația prelucrărilor de date cu caracter personal de către formele de exercitare a profesiei.

18. Totuși, lit. e) a alin. (1) al art. 6 din Regulament prevede că prelucrarea se poate realiza în mod legal dacă *„e) [...] este necesară pentru îndeplinirea unei sarcini care servește unui interes public [...];"*

19. Conform art. 39 din Legea nr. 51/1995, în exercitarea profesiei, avocații sunt parteneri indispensabili ai justiției. Prin urmare, activitatea profesională a avocatului se exercită în scopul înfăptuirii justiției, servind astfel unui interes public. În acest caz, temeiul pe baza căruia formele de exercitare a profesiei prelucrează datele cu caracter personal ar putea fi cel prevăzut în art. 6 alin. (1) lit. e) din Regulament.

20. Pe de altă parte, temeiul sus-menționat (i.e. art. 6 alin. (1) lit. e) din Regulament) nu va fi incident tuturor prelucrărilor realizate de formele de exercitare a profesiei. Spre pildă, datele cu caracter personal ale angajaților din societățile civile profesionale nu sunt prelucrate în temeiul acestui articol. De asemenea, datele cu caracter personal ale clienților nu sunt prelucrate în temeiul art. 6 alin. (1) lit. e) din Regulament atunci când formele de exercitare transmit mesaje care conțin anunțuri de participare la conferințe.

21. **În concluzie, formele de exercitare a profesiei vor trebui să analizeze, stabilească și să documenteze temeiul legal care stă la baza prelucrării datelor cu caracter personal, în funcție de particularitățile fiecărei prelucrări de date cu caracter personal.**

B. TEMEIURI JURIDICE DE PRELUCRARE IN DETALIU

B.1. Prelucrare pe bază de consimțământ (Art. 6 alin. (1) lit. (a) din Regulament)

22. În lumina noilor prevederi ale Regulamentului, prelucrarea datelor pe bază de consimțământ presupune respectarea unor standarde legale specifice. A prelucra date pe baza consimțământului, înseamnă a da persoanei vizate reală libertate de alegere și control sporit asupra prelucrării. Enumerăm mai jos câteva din cele mai importante reguli de obținere și gestionare a consimțământului:

    a) Consimțământ explicit. Consimțământul trebuie să fie exprimat în mod explicit, într-o manieră clară și specifică (manifestare pozitivă a consimțământului). Utilizarea unor metode de exprimare implicită / tacită a consimțământului (e.g. căsuțe de acord pre-bifate) nu este o practică legală;

    b) Consimțământ nelegat. Furnizarea unui serviciu solicitat de / oferit persoanei vizate nu poate fi condiționată de acordarea consimțământului pentru prelucrare din partea respectivei persoane, întrucât astfel, consimțământul nu ar fi liber exprimat;

c) Consimțământ separat. Consimțământul trebuie solicitat (i) în mod separat de termeni și condiții ori alte documente de informare și prezentare și (ii) în mod specific pentru fiecare scop pentru care se face prelucrare pe acest temei juridic;

d) Consimțământ documentat. Consimțământul trebuie documentat și dovada acestuia trebuie păstrată. Ca principiu, operatorul trebuie să poată demonstra cine a dat consimțământul, când, prin ce metodă și ce informații au fost furnizate cu ocazia preluării consimțământului;

e) Consimțământ revocabil. Persoana vizată are dreptul de a retrage consimțământul în orice moment (formă de manifestare a „*dreptului de a fi uitat*"), iar operatorul trebuie să ofere un mecanism de retragere facil și să acționeze pentru a da eficiență retragerii în cel mai scurt timp posibil.

23. Acest set de reguli face ca prelucrarea pe bază de consimțământ să ridice numeroase probleme practice. De aceea, operatorii (inclusiv FEPA) trebuie să răspundă în primul rând la întrebarea dacă consimțământul este într-adevăr temeiul juridic adecvat prelucrărilor de date cu caracter personal pe care doresc să le realizeze, sau există un alt temei juridic mai potrivit. Determinarea este cu atât mai importantă cu cât alegerea temeiului juridic este unică și, în principiu, nu poate fi schimbată ulterior începerii prelucrării.

***Exemplu**: O FEPA stabilește consimțământul ca temei juridic al prelucrării datelor clienților săi, persoane fizice. În acest scop, la începutul colaborării, în proiectul de contract de asistență juridică inserează o fereastră de consimțământ expres (cerința solicitării separate a consimțământului), prin care clienții sunt invitați să valideze / bifeze acordul lor pentru prelucrarea datelor lor personale (consimțământ expres), o dată cu semnarea contractului.*

Deși a căutat să implementeze o serie din cerințele Regulamentului privitoare la obținerea consimțământului, FEPA a făcut o eroare fundamentală de abordare. Prelucrarea datelor clienților persoane fizice este inerentă acordării serviciilor avocațiale. Dacă avocatul condiționează acordarea asistenței de acordul clientului pentru prelucrare, consimțământul este legat, deci viciat. Dacă contractul intră în vigoare și se execută indiferent de un eventual refuz al clientului, înseamnă că nu există o libertate reală a clientului de a acorda sau a refuza consimțământul pentru prelucrare. În acest caz, temeiul juridic al prelucrării datelor ar trebui să fie cel al încheierii și executării unui contract (Art. 6 alin. (1) lit. (b) din Regulament), iar nu consimțământul.

---

24. În activitatea FEPA, prelucrările de date având ca temei consimțământul persoanei vizate pot fi diverse, în funcție de modul de organizare și scopurile urmărite.

25. Prelucrarea datelor clienților nu se bazează întotdeauna pe temeiul necesității încheierii sau executării contractului de asistență juridică (a se vedea sub-secțiunea B.2 de mai jos). De exemplu, prelucrarea datelor clienților, persoane fizice, în scop de marketing (transmiterea de alerte legale / newsletters prin e-mail) va trebui să aibă la bază un consimțământ obținut în mod legal de la clienți.

B.2. Prelucrare necesară pentru încheierea și executarea unui contract (Art. 6 alin. (1) lit. (b) din Regulament)

26. Elementul cheie care justifică utilizarea acestui temei juridic este necesitatea încheierii sau executării unui contract. În acest context, prelucrarea este legală dacă:

a) Există un contract valabil, pentru a cărui executare este necesară prelucrarea de date cu caracter personal; sau

b) În faza pre-contractuală, la solicitarea persoanei vizate, este nevoie de prelucrarea anumitor date cu caracter personal în vederea încheierii contractului.

27. În mod contrar, prelucrarea nu se poate baza pe temeiul încheierii / executării contractului dacă:

a) Trebuie prelucrate datele unei persoane, alta decât cea cu care se încheie contractul;

Exemplu: *Prelucrarea datelor părții adverse nu se poate întemeia pe contractul de asistență juridică încheiat cu clientul. În acest caz, trebuie ales un alt temei al prelucrării, acesta putând fi îndeplinirea unei sarcini care servește unui interes public (Art. 6 alin. (1) lit. (e) din Regulament). A se vedea sub-secțiunea B.4 de mai jos.*

---

b) Inițiativa încheierii contractului aparține operatorului sau unei terțe persoane.

Exemplu: *Abordarea unui nou client, persoană fizică, de către un avocat, fără o manifestare de interes din partea primului nu se poate întemeia pe un eventual și viitor contract de asistență juridică. Eventual, o asemenea abordare ar fi legală dacă ar exista un alt temei al prelucrării (e.g. îndeplinirea unei sarcini care servește unui interes public sau obligație legală precum în cazuri de acordare de asistență judiciară.*

---

28. Cerința necesității prelucrării pentru încheierea sau executarea unui contract nu înseamnă întotdeauna că prelucrarea este esențială în acest scop, totuși aceasta trebuie să fie limitată la și proporțională cu scopul urmărit.

> ***Exemplu**: Prelucrarea de către o FEPA a datelor de contact ale unui nou avocat colaborator sunt necesare pentru încheierea contractului de colaborare. Spre diferență, prelucrarea datelor privind parcursul profesional / performanța avocatului colaborator (e.g. evaluări periodice) nu vor avea ca temei juridic executarea contractului (nu este necesară derulării acestuia), ci eventual, un alt temei, interesul legitim.*

B.3. Prelucrare necesară pentru îndeplinirea unei obligații legale (Art. 6 alin. (1) lit. (c) din Regulament)

29. Prelucrarea datelor cu caracter personal pe temeiul necesității conformării unei obligații legale presupune existența unei norme legale imperative aplicabile operatorului. De asemenea, prelucrarea impusă printr-o decizie administrativă / hotărâre judecătorească (ele însele, luate în temeiul unei abilitări legale) poate fi justificată tot prin necesitatea conformării unei obligații legale.

30. Prelucrarea trebuie să fie necesară conformării obligației legale. Dacă se poate asigura în mod rezonabil conformarea cu norma legală fără respectiva prelucrare sau printr-o prelucrarea mai puțin invazivă / cuprinzătoare, nu poate fi utilizat acest temei.

31. În exercitarea profesiei, FEPA cad sub incidența anumitor obligații legale care pot justifica anumite prelucrări de date cu caracter personal. Enumerăm mai jos câteva exemple:

> ***Exemplu #1**: În baza legislației privind prevenirea și sancționarea spălării banilor și prevenirea și combaterea finanțării terorismului[1], avocații au anumite obligații de implementare a unor măsuri specifice de cunoaștere a clientelei și de raportare a unor tranzacții suspecte. Prelucrările de date cu caracter personal necesare îndeplinirii acestor obligații sunt întemeiate pe obligația legală.*
>
> ***Exemplu #2**: Potrivit Art. 41 din Legea nr. 51/1995, „Avocatul este obligat să acorde asistență juridică în cauzele în care a fost desemnat din oficiu sau gratuit de către barou". Practic, o dată*

[1] Legea nr. 656/2002 pentru prevenirea și sancționarea spălării banilor, precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării terorismului.

cu înscrierea avocatului în Registrul de asistență judiciară, se activează obligația de a accepta mandate de asistență judiciară, care se concretizează în momentul desemnării concrete a avocatului în dosare de acest tip. Prelucrările de date cu caracter personal necesare în contextul unor astfel de mandate sunt întemeiate pe obligația legală. Asemenea prelucrări ar putea fi realizate și pe temeiul îndeplinirii unei sarcini care servește unui interes public (Art. 6 alin. (1) lit. (e) din Regulament).

***Exemplu #3**: Avocații au obligația de a menține anumite evidențe specifice privind activitatea lor, precum Registrul electronic al actelor întocmite de avocat. Prelucrările de date cu caracter personal realizate în acest scop au ca temei juridic îndeplinirea unei obligații legale.*

***Exemplu #4**: O parte din prelucrările de date realizate de către departamentul contabilitate al FEPA, precum reținerea și plata contribuțiilor sociale pentru personalul auxiliar, înregistrările privind concediul salariaților se întemeiază pe obligații legale reglementate de legislația muncii.*

B.4. Prelucrare necesară pentru îndeplinirea unei sarcini care servește unui interes public (Art. 6 alin. (1) lit. (e) din Regulament)

32. Lit. e) a alin. (1) al Art. 6 din Regulament prevede că prelucrarea se poate realiza în mod legal dacă *„e) [...] este necesară pentru îndeplinirea unei sarcini care servește unui interes public [...];”*

33. Conform art. 39 din Legea nr. 51/1995, în exercitarea profesiei, avocații sunt parteneri indispensabili ai justiției. Prin urmare, activitatea profesională a avocatului se exercită în scopul înfăptuirii justiției, servind astfel unui interes public. În acest caz, temeiul pe baza căruia formele de exercitare a profesiei prelucrează datele cu caracter personal ar putea fi cel prevăzut în art. 6 alin. (1) lit. e) din Regulament.

***Exemplu**: Pentru a realiza activitatea profesională în scopul înfăptuirii justiției, avocatul prelucrează datele cu caracter personal ale părților adverse sau ale unor terțe persoane. Temeiul acestei prelucrări nu poate fi consimțământul persoanelor vizate (ar fi iluzoriu să aștepte obținerea unui astfel de acord), dar nici contractul de asistență juridică cu*

clientul. Temeiul juridic este îndeplinirea unei sarcini care servește unui interes public.

B.5. Prelucrare necesară în scopul unui interes legitim (Art. 6 alin. (1) lit. (f) din Regulament)

34. Interesul legitim este cel mai flexibil temei juridic de prelucrare a datelor cu caracter personal și, de aceea, utilizarea sa trebuie calibrată în mod adecvat. În mod tipic, poate fi folosit doar în cazurile în care prelucrarea are un impact minimal asupra persoanelor vizate. Pentru o judicioasă întemeiere pe interesul legitim, prelucrarea datelor cu caracter personal trebuie să îndeplinească trei tipuri de caracteristici:

a) Testul scopului legitim. Operatorul trebuie să urmărească un interes legitim, al său ar al unui terț. Interesul legitim poate fi un interes comercial, profesional sau un scop mai larg, de exemplu un interes social.

b) Testul necesității. Prelucrarea trebuie să fie proporțională și limitată pentru atingerea interesului legitim urmărit. Dacă respectivul interes poate fi atins printr-o prelucrare mai puțin intruzivă / cuprinzătoare, nu poate fi utilizat acest temei.

c) Testul raportării la interesele persoanei vizate. Ca principiu, prelucrarea trebuie să fie previzibilă pentru persoana vizată și să nu creeze un prejudiciu / inconvenient nenecesar persoanei vizate. Important, nu întotdeauna interesele persoanei vizate trebuie aliniate cu cele ale operatorului. Pot exista situații in care interesele operatorului pot prevala asupra celor ale persoanei vizate în cadrul unei prelucrări legitime.

Exemplu: Prelucrările de date privind activitatea avocaților colaboratori și personalului auxiliar printr-un program de time-tracking a activităților profesionale executate, în scopul evaluării performanțelor se pot întemeia, ca principiu, pe interesul legitim de prelucrare al FEPA.

C. PRELUCRAREA DE CATEGORII SPECIALE DE DATE SAU REFERITOARE LA CONDAMNĂRI PENALE ȘI INFRACȚIUNI

35. În exercitarea activităților avocațiale, pot surveni prelucrări de categorii speciale de date sau date referitoare la condamnări speciale și infracțiuni.

C.1. Categorii speciale de date

36. Regulamentul definește categoriile speciale de date: originea rasială sau etnică, opiniile politice, confesiunea religioasă, convingerile filozofice, apartenența la sindicate, date

genetice, date biometrice pentru identificarea unică a unei persoane fizice, date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

37. Aceste categorii de date sunt considerate sensibile și se impune un standard de protecție superior. Concret, pentru prelucrarea adecvată a acestor categorii de date, pe lângă identificarea unui temei de prelucrare potrivit Art. 6 din Regulament, se impune îndeplinirea și uneia dintre condițiile reglementate de Art. 9 alin. (2) din Regulament.

38. În mod tipic, condiția suplimentară în baza căreia FEPA vor putea să prelucreze categorii speciale de date este Art. 9 alin. (2) lit. (f) din Regulament: "*prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță [...].*"

Exemplu: Un client dorește să acționeze în judecată un asigurător cu care are încheiată o poliță de asigurare de călătorie, pentru refuzul acestuia de a deconta o intervenție medicală în străinătate necesară ca urmare a unui accident suferit în timpul călătoriei. FEPA va prelucra datele clientului, inclusiv cele privind sănătatea, pe baza temeiului juridic al încheierii și executării contractului de asistență juridică și, în plus, prelucrarea datelor privind sănătatea se va baza și pe condiția menționată la Art. 9 alin. (2) lit. (f) din Regulament.

---

39. Domeniul de aplicare al condiției menționate la Art. 9 alin. (2) lit. (f) din Regulament ar trebui interpretat în mod larg, ca incluzând nu doar procedurile litigioase propriu-zise, dar și asistența juridică pre-litigioasă sau consultanța juridică acordată în legătură cu categoriile speciale de date.

C.2. Date referitoare la condamnări speciale și infracțiuni

40. Similar prelucrării categoriilor speciale de date, prelucrarea datelor referitoare la condamnări penale și infracțiuni presupune: (i) un temei juridic de prelucrare potrivit Art. 6 din Regulament; și (ii) competență legală (proprie autorităților publice) sau o autorizare legală.

41. În cazul FEPA, această a doua condiție este îndeplinită. Aceasta, întrucât autorizarea FEPA de a prelucra, în activitatea lor profesională, date referitoare la condamnări speciale și

infracțiuni rezultă din rolul, atribuțiile și îndatoririle avocatului în procesul penal, reglementat de legislația procesual penală și cea care guvernează profesia de avocat[2].

42. Prin urmare, în cazul FEPA, prelucrările de date referitoare la condamnări penale și infracțiuni realizate în exercitarea activității profesionale, nu ridică probleme particulare, fiind doar necesar un temei juridic general de prelucrare (e.g. executare de contract, sarcină care servește unui interes public, obligație legală, etc).

II. INFORMAREA PERSOANELOR VIZATE

43. Potrivit Articolelor 12-14 din Regulament, indiferent de temeiul prelucrărilor de date cu caracter personal, operatorii trebuie să se conformeze unei obligații specifice de informare a persoanelor vizate în legătură prelucrările efectuate.

A. FORMA ȘI CONȚINUTUL INFORMĂRII

44. Documentul de informare al persoanelor vizate cu privire la prelucrările datelor lor cu caracter personal trebuie să îndeplinească anumite cerințe formale și de conținut.

A.1. Cum se face informarea persoanelor vizate?

45. Potrivit Art. 12 alin. (1) din Regulament, informarea trebuie oferită într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

46. Documentul informare este pus la dispoziția persoanelor vizate în forme diferite, depinzând de scopurile prelucrării și de sursa datelor (persoana vizată sau altă sursă): de exemplu, politică de confidențialitate a unui website, anexă la contractul încheiat cu persoana fizică, notă de informare inserată într-un formular de aplicație pentru o poziție în cadrul operatorului, etc.

47. Ca principiu, nota de informare se livrează în scris inclusiv, atunci când este oportun, în format electronic[3].

48. În cazul FEPA, forme tipice de îndeplinire a obligației de informare impuse de Regulament sunt: (i) notă de informare / politică de confidențialitate inclusă în sau anexată la oferta de

---

[2] Codul de Procedură Penală conține numeroase referiri privind rolul avocatului în procesul penal. Pot fi enumerate, cu titlu exemplificativ: (i) Art. 10 alin. (1): *Părțile și subiecții procesuali principali au dreptul de a se apăra ei înșiși sau de a fi asistați de avocat*; (ii) Art. 29: *Participanții în procesul penal sunt: organele judiciare, avocatul, părțile, subiecții procesuali principali, precum și alți subiecți procesuali*; (iii) Avocatul asistă sau reprezintă părțile ori subiecții procesuali în condițiile legii; (iv) prevederile privind asistența juridică obligatorie prin avocat. Similar, potrivit Art. 2 alin. (3) din Legea nr. 51/1995: *Avocatul are dreptul să asiste și să reprezinte persoanele fizice și juridice în fața instanțelor autorității judecătorești și a altor organe de jurisdicție, a organelor de urmărire penală, a autorităților și instituțiilor publice, precum și în fața altor persoane fizice sau juridice, care au obligația să permită și să asigure avocatului desfășurarea nestingherită a activității sale, în condițiile legii.*

[3] Pot exista și informări verbale, la solicitarea persoanei vizate, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

asistență juridică și, subsecvent, la contractul de asistență juridică; (iii) politica de confidențialitate pe website-ul FEPA; (iv) note de informare privind prelucrarea datelor avocaților colaboratori / salarizați și a personalului auxiliar.

NB: Nota de informare este necesară și în cazul clienților persoane juridice. În acest caz, avocatul prelucrează datele personale ale reprezentanților sau împuterniciților clientului, persoane fizice. În plus, cu ocazia primului contact cu aceste persoane fizice, furnizarea unei note de informare către aceștia este de asemenea necesară.

A.2. Ce conține informarea?

49. Depinzând de sursa de obținere a datelor, respectiv persoana vizată însăși sau alte surse, informarea va avea un conținut specific, reglementat de Art. 13 și 14 din Regulament. Prezentăm mai jos un tabel sinoptic al principalelor categorii de informații care trebuie furnizate persoanei vizate:

TIP DE INFORMAȚIE	DATE OBȚINUTE DE LA PERSOANA VIZATĂ	DATE OBȚINUTE DIN ALTE SURSE
Identitatea și datele de contact ale operatorului și ale reprezentantului acestuia, dacă este cazul	√	√
Datele de contact ale responsabilului cu protecția datelor, dacă este cazul[4]	√	√
Scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;	√	√
În cazul în care prelucrarea se face baza temeiului legitim[5], interesele legitime urmărite;	√	√
Categoriile de date cu caracter personal vizate		

[4] A se vedea *Secțiunea* V *RESPONSABILUL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL (DPO) ÎN CADRUL FEPA*

[5] Art. 6 alineatul (1) litera (f) din Regulament.

		√
Destinatarii sau categoriile de destinatari ai datelor cu caracter personal	√	√
Informații specifice privind transferurile de date personale în străinătate, dacă există o asemenea intenție	√	√
Perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă	√	√
Existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor[6]	√	√
Atunci când prelucrarea are ca temei juridic consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia	√	√
Dreptul de a depune o plângere în fața autorității de supraveghere	√	√
Sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public		√
Dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații	√	
Existența unui proces decizional automatizat incluzând		

[6] A se vedea *Secțiunea III DREPTURILE PERSOANELOR VIZATE*

crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată	✓	✓

B. CÂND SE FACE INFORMAREA?

50. În cazul datelor cu caracter personal colectate direct de la persoana vizată, informarea se face în momentul obținerii datelor.

51. În cazul datelor cu caracter personal colectate din alte surse, informarea se face:

a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;

b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

C. EXCEPȚII DE LA OBLIGAȚIA DE INFORMARE

52. Indiferent dacă prelucrările de date cu caracter personal obținute de la persoana vizată sau din alte surse, informarea nu este necesară dacă și în măsura în care persoana vizată deține deja informațiile respective.

53. În plus, pentru cazul particular al prelucrărilor de date cu caracter personal obținute din alte surse realizate de formele de exercitare a profesiei, alte excepții de la obligația de informare pot deveni incidente:

a) în măsura în care obligația de informare este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective In astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate;

b) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații legale de a păstra secretul profesional.

D. CUM DOCUMENTĂM INFORMAREA?

54. Un element intrinsec al obligației de informare care revine operatorului este documentarea îndeplinirii obligației de informare sub toate aspecte sale: (i) care a fost forma și conținutul informării furnizate persoanei vizate; (ii) când a fost furnizată informarea; (iii) dacă informarea nu a fost necesară, se va documenta motivul exceptării.

55. Dovada îndeplinirii obligației de informare, se poate face cu orice mijloc adecvat de probă, în funcție de contextul concret, precum: (i) corespondența purtată cu clientul în faza pre-contractuală pe baza ofertei de asistență juridică (conținând nota de informare / politica de confidențialitate); (ii) semnătură a clientului pe contractul de asistență juridică (conținând nota de informare / politica de confidențialitate); (iii) semnătură a candidatului pe formularul de aplicație (conținând nota de informare) pentru o poziție în cadrul operatorului sau pe nota de informare privind prelucrarea datelor avocaților colaboratori / salarizați și a personalului auxiliar, etc.

III. DREPTURILE PERSOANELOR VIZATE

A. DREPTURI SPECIFICE INCIDENTE ÎN CONTEXTUL PRELUCRĂRILOR DESFĂȘURATE DE FORMELE DE EXERCITARE A PROFESIEI DE AVOCAT

56. Regulamentul prevede 8 drepturi specifice în materie de prelucrare a datelor cu caracter personal, care pot fi exercitate în măsura în care nu aduc atingere drepturilor și libertăților altora:

a) Dreptul de acces la date;

b) Dreptul la rectificarea datelor;

c) Dreptul la ștergerea datelor;

d) Dreptul la restricționarea prelucrării;

e) Dreptul la portabilitatea datelor;

f) Dreptul de opoziție la prelucrarea datelor;

g) Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea; și

h) Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal.

57. Atunci când avocatul acționează în contextul prelucrării în calitate de operator de date, acesta este ținut în mod direct respecte drepturile specifice în materie de prelucrare a datelor cu caracter personal (prin avocat înțelegând forma de exercitare în discuție și implicit salariații / colaboratorii săi, după caz).

58. Dacă avocatul acționează ca persoană împuternicită, în contextul operațiunilor de prelucrare (ex. dezvăluirea datelor către autorități conform legii), avocatul are obligația de a asista autoritățile, când este cazul să răspundă cererilor de exercitare a drepturilor specifice ale persoanelor vizate, prin implementarea de măsuri tehnice și organizaționale adecvate, într-o măsură rezonabilă.

59. Răspunsul la cererile persoanelor vizate trebuie să fie trimis în maximum o lună de la primirea acestora, cu posibilitatea prelungirii duratei cu maximum 2 luni, dacă vorbim despre

o prelucrare complexă ori de un volum mare de astfel de cereri (în orice caz, inclusiv informarea cu privire la întârzierea unui răspuns ori refuzul de a lua măsuri trebuie transmise în termenul de 1 lună).

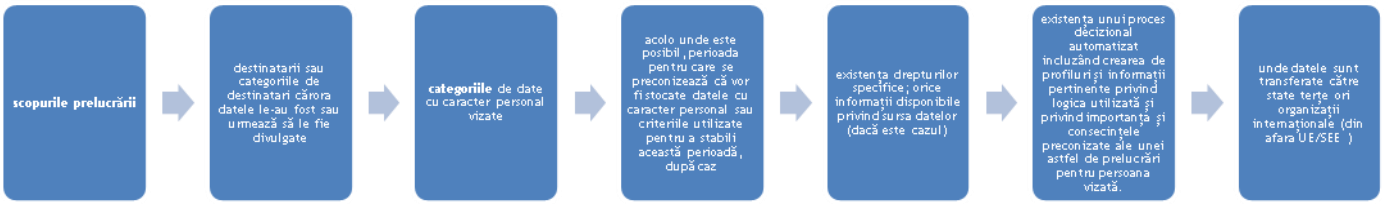
60. Orice activități desfășurate de avocat pentru a răspunde solicitărilor persoanelor vizate trebuie să fie desfășurate în mod gratuit, cu excepția cazurilor în care solicitările persoanelor vizate sunt excesive (ex. număr exagerat de solicitări identice, solicitări frecvente).

Exemplu: la solicitarea unei autorități de clarificare a surselor datelor pentru o anumită persoană vizată, avocatul implicat să aibă o evidență clară operațiunilor de prelucrare în așa fel încât să poată răspunde în termen optim unei asemenea cereri.

A.1. Dreptul de acces

61. Atunci când acționează în calitate de operator, avocatul are obligația, la cererea transmisă pe orice canal de către persoanele vizate (clienți, angajați, alte persoane fizice), de le confirma acestora ce date prelucrează și în ce condiții.

62. Informațiile minime ce ar trebui transmise în cazul primirii unor cereri de acces vizează:



63. Accesul persoanelor vizate la datele prelucrate în legătură cu acestea este limitat, în sensul că avocații sunt obligați să răspundă în măsura în care nu aduc atingere drepturilor și libertăților altor persoane, în cazul nostru, în special obligației de a păstra secretul profesional conform Statutului.

Exemplu: pârâtul dintr-un litigiu îi transmite avocatului reclamantului o solicitare de confirmare și oferire informații, respectiv o copie cu toate datele pe care avocatul le prelucrează cu privire la acesta.

În acest caz, avocatul îi va putea răspunde pârâtului și îi va putea transmite doar acele date pe care acesta fie deja le cunoaște ori care nu se califică drept secret profesional (ex. din perspectiva strategiei de apărare, invocarea inabilității sociale

a pârâtului de a interacționa cu proprii copii și respectiv acceselor violente ale acestuia într-un proces de divorț).

A.2. Dreptul la rectificarea datelor

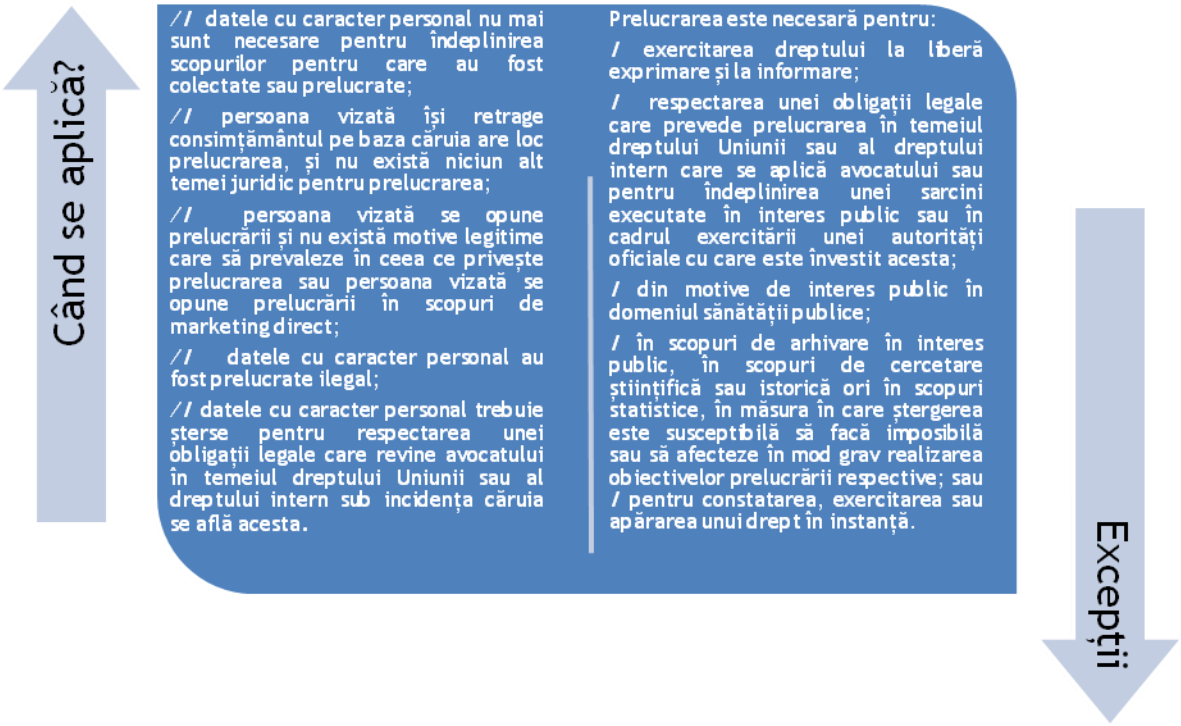
64. Atunci când acționează ca operator, avocatul are obligația de a asigura respectarea drepturilor persoanelor vizate de a obține fără întârziere rectificarea oricăror date inexacte (eronate sau incomplete) care le privesc.

Exemplu: la solicitarea unui client de actualizare a datelor sale de contact / identificare, avocatul trebuie să aibă implementate mijloace corespunzătoare pentru a introduce imediat în sistem astfel de modificări (ex. dacă vorbim despre un număr ridicat de clienți, ar trebui să aibă o persoană cu atribuții specifice pentru tratarea unor asemenea solicitări venite din partea clienților).

Exemplu: în contextul prelucrării strict a datelor în contextul unui proces de due diligence, fără posibilitatea de a cere informații suplimentare, avocatul are obligația de a asista clientul, când este cazul să răspundă cererilor de ștergere a datelor angajaților săi, prin ștergerea în mod corespunzător a datelor angajaților clientului care nu îi mai sunt necesare avocatului.

A.3. Dreptul la ștergerea datelor

65. Persoanele vizate pot solicita avocatului care acționează în calitate de operator ștergerea datelor care le privesc, fără nicio întârziere.



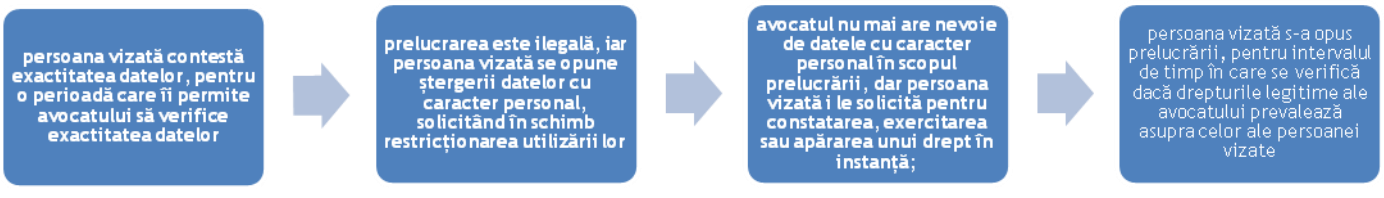
Exemplu: la solicitarea unui client persoană fizică de ștergere a datelor sale de identificare, avocatul poate invoca necesitatea păstrării acestora cel puțin pentru scopul evidenței contractelor de asistență juridică și încheierea acestuia (care conform Anexei 1 din Statut trebuie obligatoriu să conțină datele de identificare ale clienților).

66. În plus, avocatul, atunci când a făcut publice în vreun context datele a căror ștergere se solicită și persoana vizată cere inclusiv ștergerea datelor de la orice destinatari, este ținut în mod rezonabil prin măsuri adecvate (inclusiv tehnice) să asigure informarea destinatarilor datelor cu privire la o astfel de solicitare.

A.4. Dreptul la restricționarea prelucrării

67. Persoana vizată are dreptul de a obține din partea avocatului operator restricționarea prelucrării, respectiv limitarea acesteia (cu excepția stocării propriu-zise) strict la prelucrările cu care persoana vizată este de acord și /sau strict la prelucrările necesare în scopul constatării, exercitării sau apărării unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

68. Restricționarea se aplică atunci când:



A.5. Dreptul la portabilitatea datelor

69. Dreptul la portabilitatea datelor implică obligația avocatului atunci când acționează ca operator, de a asigura (i) furnizarea datelor primite de la persoana vizată într-un format accesibil la cererea acesteia și (ii) transmiterea unor astfel de date către alți operatori la cererea persoanei vizate, incidentă când următoarele condiții cumulative sunt îndeplinite:

a) prelucrarea se bazează pe consimțământ sau este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract; și

b) este realizată prin mijloace automate (nu în formă fizică / hârtie, ci prin orice mijloace automatizate).

Exemplu:

1) prima latură (furnizarea datelor / documentelor ce le conțin persoanei vizate): la solicitarea unui client persoană fizică înainte de încetarea colaborării de a preda toate documentele furnizate precum și copiile efectuate după acestea în format electronic, avocatul are obligația de a se conforma cu o asemenea cerere. În cazul încetării colaborării, prima latură a dreptului (furnizarea datelor / documentelor care le conțin) este deja reglementată prin art. 10 din Statut.

(2) portarea datelor către alt avocat - dacă la încetarea colaborării clientul solicită transmiterea datelor deținute în formă electronică către noul său avocat, conform dreptului la portabilitate, dacă este tehnic posibil, solicitarea sa ar trebui să primească un răspuns pozitiv (bineînțeles cu luarea în considerare a limitelor secretului profesional față de alți clienți, dacă spre exemplu pleacă un singur client dintr-un grup de clienți având aceeași calitate într-un litigiu).

A.6. Dreptul de opoziție la prelucrarea datelor

70. Persoanele vizate pot să se opună oricând la prelucrarea datelor lor cu caracter personal:

a) din motive legate de situația particulară în care se află, operațiunilor de prelucrare desfășurate în temeiul necesității prelucrării pentru îndeplinirea unei sarcini care servește unui interes public cu care este învestit avocatul; și/ sau prelucrărilor efectuate în temeiul intereselor legitime urmărite de avocat sau de o parte terță a datelor cu caracter personal, inclusiv creării de profiluri.

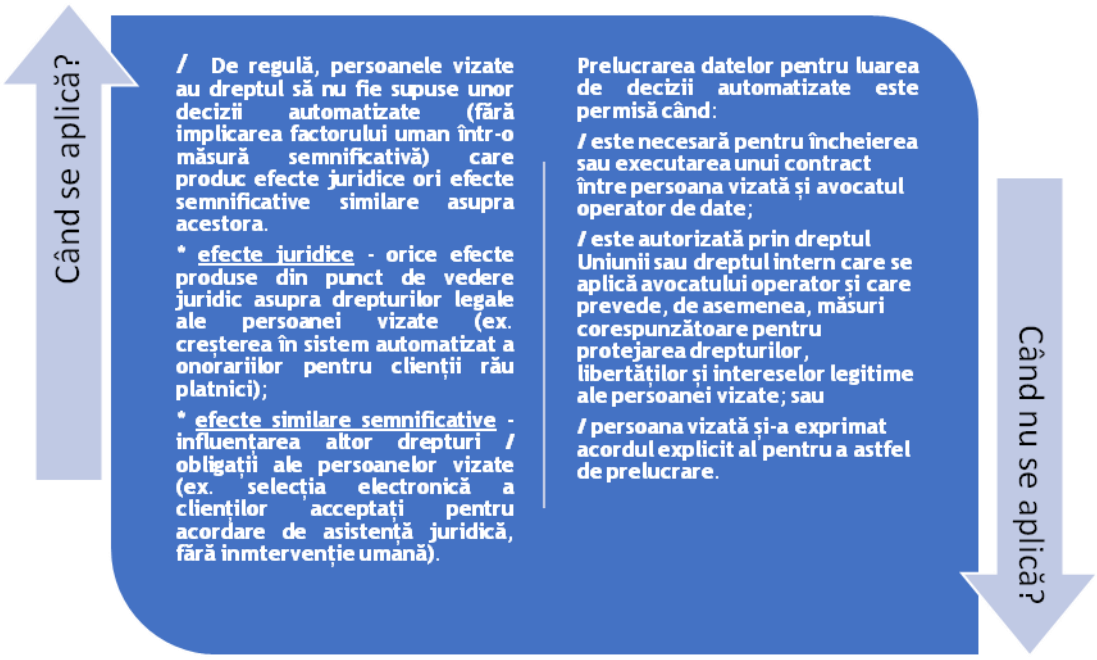
b) fără motive și justificare, în cazul prelucrării datelor în scopuri de marketing direct (ex. pentru promovarea serviciilor avocatului prin transmiterea de buletine legislative).

71. Avocatul operator nu mai poate prelucra datele cu caracter personal în cazul opunerii, cu excepția cazului în care demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul prelucrării este constatarea, exercitarea sau apărarea unui drept în instanță.

Exemplu: prelucrarea în continuare a datelor din documentele furnizate strict în scopul apărării avocatului în contextul cercetării sale urmare a unei plângeri introduse de persoana care își exercită dreptul de opoziție.

A.7. Dreptul de a nu fi supus unor decizii automatizate, inclusiv profilarea

72. Persoanele vizate au dreptul ca datele lor cu caracter personal să nu fie prelucrate în contextul luării unor decizii automatizate în următoarele condiții:



A.8. Dreptul la notificarea destinatarilor privind rectificarea, ștergerea ori restricționarea datelor cu caracter personal

73. Avocatul are obligația atunci când acționează ca operator să comunice fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal ale persoanelor vizate orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate.

74. O astfel de obligație este incidentă cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Avocatul are și obligația de a informa persoana vizată cu privire la destinatarii respectivi dacă aceasta solicită acest lucru.

B. MECANISME DE RĂSPUNS LA CERERILE DE EXERCITARE A DREPTURILOR PERSOANELOR VIZATE

75. Pentru a asigura tratarea cu celeritate a cererilor persoanelor vizate pentru exercitarea drepturilor specifice, respectiv a cererilor altor entități (pentru cazurile în care avocatul acționează în calitate de persoană împuternicită), următoarele mecanisme pot fi avute în vedere:

a) Alocarea unei / unor persoane care să se ocupe de tratarea în timp util a cererilor persoanelor vizate, care să răspundă în scris la asemenea solicitări;

b) Redactarea unor formulare de exercitare a drepturilor / răspuns tipizate care să fie utilizate atunci când clienții / angajații / alte persoane vizate își exercită drepturile specifice;

c) Dacă cererile sunt transmise prin mijloace electronice, răspunsul trebuie transmis prin aceleași mijloace, dacă persoanele vizate nu solicită altfel;

d) Implementarea unor secțiuni specifice pentru exercitarea drepturilor persoanelor vizate online, în special în cazurile în care colectarea datelor se realizează online;

e) Pentru formele de exercitare cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat în cazul primirii unor astfel de cereri, inclusiv cu principiile de avut în vedere în contextul conceperii răspunsurilor la cererile specifice.

Exemplu:

Introducerea pe website a unei secțiuni – Exercitarea drepturilor – în cadrul căreia să poată fi completat direct formularul specific pentru fiecare drept în parte, iar odată completat, formularul să ajungă la persoana care se ocupă de gestionarea unor asemenea cereri.

C. EVIDENȚA GESTIONĂRII CERERILOR DE EXERCITARE A DREPTURILOR PERSOANELOR VIZATE

76. Atât când acționează ca operator cât și ca persoană împuternicită, este recomandabilă păstrarea de către avocat a unei evidențe clare a răspunsurilor date în contextul cererilor persoanelor vizate de exercitare a drepturilor specifice în materie de prelucrare a datelor cu caracter personal, astfel:

    a) Avocatul operator trebuie să aibă dovezi clare scrise (inclusiv conținând răspunsurile și data transmiterii acestora) care să ateste îndeplinirea obligațiilor specifice în materie; recomandăm păstrarea evidenței pe două paliere: solicitări primite cu toate informațiile aferente cu evidențierea datei primirii acestora și respectiv răspunsuri transmise, cu evidențierea datei transmiterii răspunsurilor, iar unde este cazul de prelungire a termenului de răspuns după o lună, cu indicarea clară a motivului prelungirii.

    b) Avocatul persoană împuternicită trebuie să aibă dovezi scrise care să susțină transmiterea în termen util a informațiilor solicitate respectiv implementarea în mod rezonabil a măsurilor necesare pentru conformarea cu drepturile specifice ale persoanelor vizate a operatorilor care le solicită informații / luarea de măsuri specifice.

77. Este preferabilă păstrarea dovezilor în formă scrisă. Cu toate acestea, dacă persoana vizată solicită anumite informații oral, este admisibilă și păstrarea unor dovezi ale înregistrărilor care să ateste răspunsul acordat unor asemenea solicitări.

IV. EVIDENȚELE OPERAȚIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

A. ANALIZA INCIDENȚEI OBLIGAȚIEI DE ȚINERE A EVIDENȚELOR PRELUCRĂRILOR

78. Din interpretarea art. 30, para. 5 din Regulament, rezultă că obligația menținerii unei evidențe a activităților de prelucrare a datelor cu caracter personal incumbă, de principiu, întreprinderilor sau organizațiilor cu peste 250 de angajați.

79. Întreprinderile sau organizațiile cu mai puțin de 250 de angajați sunt ținuți de această obligație doar dacă *”prelucrarea pe care o efectuează este susceptibilă să genereze un risc*

pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10".

80. Deși cele mai multe FEPA s-ar afla sub pragul de 250 de angajați, categoriile de date prelucrate determină, în principiu, existența unui registru de prelucrare a datelor personale. Prelucrarea de categorii speciale de date sau date referitoare la condamnări penale și infracțiuni ocazionate de asistența juridică în materie penală sunt argumente suplimentare în sensul necesității ținerii unei astfel de evidențe.

B. FORMA ȘI CONȚINUTUL EVIDENȚEI PRELUCRĂRII DATELOR

81. Art. 30 din Regulament analizează conținutul registrului de evidență pe două paliere: nivelul operatorului și nivelul persoanei împuternicite.

82. Astfel, fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor.

83. Evidența menținută de operatori și, după caz, de reprezentanții acestora trebuie să cuprindă următoarele informații:

a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;

f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

84. Pe de altă parte, persoana împuternicită și, după caz, reprezentantul acesteia păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană (aceste persoane),

precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz și ale responsabilului pentru protecția datelor cu caracter personal;

b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf din GDPR, documentația care dovedește existența unor garanții adecvate;

d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate.

85. Desigur, lista prezentată în această secțiune nu este exhaustivă, ci reprezintă un cumul de cerințe minime obligatorii ce trebuie respectate și integrate în registrul de evidență de către FEPA ce desfășoară în mod sistematic activități de prelucrare a datelor cu caracter personal.

V. RESPONSABILUL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL (DPO) ÎN CADRUL FEPA

A. PUNCTE CHEIE

a) Este responsabilitatea FEPA să evalueze necesitatea numirii unui DPO în cadrul organizației, prin raportare la criteriile impuse de Regulament;

b) Este recomandabil să fie documentată în scris această evaluare, ca parte a proiectului de conformare Regulament și să valideze / actualizeze periodic evaluarea făcută;

c) Cele mai multe FEPA nu vor trebui să numească un DPO, dar un număr semnificativ de FEPA vor cădea sub incidența acestei obligații;

d) DPO în cadrul FEPA trebuie să îndeplinească toate sarcinile și să se bucure de toate garanțiile pentru a își desfășura activitatea în parametrii reglementați de Regulament;

e) Numirea voluntară de DPO este o recomandare de bună practică. Dacă FEPA nu numește DPO trebuie să acorde atenție tuturor celorlalte aspecte de conformare aplicabile.

B. CÂND ESTE OBLIGATORIU CA FEPA SĂ NUMEASCĂ DPO?

B.1. Norma juridică relevantă

86. Art. 37 alin. (1) din Regulament stabilește situațiile în care este obligatorie numirea DPO:

a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

b) **activitățile principale** ale operatorului sau persoanei împuternicite constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o **monitorizare periodică și sistematică** a persoanelor vizate **pe scară largă**; și

c) **activitățile principale** ale operatorului sau ale persoanei împuternicite de operator constau în **prelucrarea pe scară largă** a unor **categorii speciale de date** sau a unor **date cu caracter personal privind condamnări penale și infracțiuni**.

B.2. Clarificări conceptuale

87. Fiecare FEPA va trebui să evalueze dacă, prin raportare la propria sa organizare și activitate, se încadrează în vreuna din cazurile de mai sus (relevante pentru profesia de avocat fiind ultimele două). Câteva elemente-cheie trebuie avute în vedere pentru această evaluare:

a) Conceptul de *„activități principale”*. Potrivit A29 GL, activități principale înseamnă *„operațiuni-cheie pentru atingerea scopurilor operatorului / persoanei împuternicite”*, fără a exclude însă *„activitățile în care prelucrarea datelor cu caracter personal este o parte inextricabilă a activității operatorului / persoanei împuternicite”*.

În cazul FEPA, activitatea principală este cea de furnizare de servicii specifice profesiei (consultații și cereri cu caracter juridic, asistență și reprezentare juridică, redactarea de acte juridice, activități de mediere). Totuși, avocatul nu și-ar putea desfășura activitatea fără a dobândi, a stoca și a utiliza datele cu caracter personal ale clienților săi. Din acest punct de vedere, se poate susține că prelucrarea datelor cu caracter personal este o parte inextricabilă a activității desfășurate de FEPA.

---

b) Conceptul de *„prelucrare pe scară largă”*. Regulamentul nu oferă criterii precise pentru a valida acest element. A29 GL oferă o serie de criterii orientative de care trebuie ținut cont în calificarea unei prelucrări ca fiind *„pe scară largă”*: numărul de persoane vizate / proporția din populația relevantă, volumul și varietatea datelor personale prelucrate, durata prelucrării, întinderea geografică.

Practica unui cabinet individual de avocatură nu îndeplinește criteriul prelucrării de date personale pe scară largă[7].

---

[7] În acest sens este și punctul (91) din Preambulul Regulamentului: *“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.”*

Evaluarea devine mai nuanțată cu cât FEPA este o organizație mai mare și mai diversificată. Chiar și în privința unor societăți mari de avocatură, criteriul prelucrărilor de date pe scară largă trebuie corelat cu celelalte criterii.

---

c) Conceptul de **„*monitorizare periodică și sistematică*”** unde, conform A29 GL,

(i) ***monitorizare*** înseamnă orice formă de urmărire și profilare în mediu online, dar nu sunt excluse și forme de monitorizare „clasică”;

(ii) ***periodică*** înseamnă în principiu, fie continuă, fie recurentă / repetată la intervale fixe de timp;

(iii) ***sistematică*** înseamnă în principiu, realizată pe baza unui sistem, pre-aranjată, organizată sau metodică, fiind realizată ca parte a unui plan general sau strategie de colectare de date.

Activitatea de avocat nu implică, în sine, activități de monitorizare periodică și sistematică de date cu caracter personal. Este posibil ca anumite operațiuni realizate de FEPA să poate fi incluse în categoria monitorizării periodice și sistematice, cum ar fi profilările în legătură cu îndeplinirea obligațiilor de cunoaștere a clientelei în condițiile aplicării legislației privind prevenirea și combaterea spălării banilor.

---

d) Conceptul de **„*categorii speciale de date*** include categoriile de date stabilite prin art. 9 din Regulament: *originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice*.

La acestea, se adaugă *datele cu caracter personal privind condamnări penale și infracțiuni*, menționate la art. 10 din Regulament.

B.3. Concluzii

88. Având în vedere prevederile Regulamentului și precizările A29 GL, fiecare FEPA va trebui să evalueze necesitatea sau oportunitatea numirii unui DPO, prin raportare la dimensiunea sa, modul de organizare, tipurile de prelucrări de date cu caracter personal, volumul și varietatea acestora, durata prelucrării și stocării de date, aria geografică acoperită.

89. Ca elemente de orientare, pot fi avute în vedere următoarele:

a) Formele individuale de exercitare a profesiei (cabinet individual, cabinete asociate, chiar societăți profesionale cu un număr mic de avocați), în principiu, nu vor trebui să numească un DPO.

b) Formele mai complexe de exercitare a profesiei (formate dintr-un număr semnificativ de avocați -asociați, colaboratori, salarizați în interiorul profesiei-, departamente auxiliare, IT, contabilitate, marketing) sunt susceptibile a intra sub incidența obligației de a numi un DPO.

În mod tipic, FEPA nu realizează monitorizări periodice și sistematice, dar este probabil să prelucreze categorii speciale de date, precum: date privind apartenența la sindicate, date privind sănătatea, viața sexuală, orientarea sexuală (diferite litigii), date privind condamnări penale și infracțiuni (departamente de drept penal).

Prin urmare, ca principiu, numirea unui DPO va fi necesară în cadru unei FEPA care (i) prelucrează pe scară largă (ii) categorii speciale de date. O FEPA care acoperă numeroase arii de practică este probabil să prelucreze categorii speciale de date, precum: date privind apartenența la sindicate, date privind sănătatea, viața sexuală, orientarea sexuală (diferite litigii), date privind condamnări penale și infracțiuni (departamente de drept penal). Evaluarea internă a FEPA va trebui să determine dacă asemenea prelucrări de date sensibile se fac pe scară largă, sau, dimpotrivă, reprezintă o arie de practică secundară față de ramurile de drept care formează practica principală de activitate a FEPA.

	CRITERII		DPO OBLIGATORIU
FEPA individual	Prelucrare pe scară largă	Monitorizare periodică și sistematică	
	x	x	**NU**
	Prelucrare pe scară largă	Categorii speciale de date	
	x	x / o	**NU**
FEPA complex	Prelucrare pe scară largă	Monitorizare periodică și sistematică	
	o	x	**NU**
	Prelucrare pe scară largă	Categorii speciale de date	
	x / o		**POSIBIL**

90. Chiar dacă o FEPA ajunge la concluzia că nu este necesară numirea unui DPO, recomandarea de bună-practică a A29 GL este numirea voluntară a acestuia.

91. Chiar dacă FEPA nu numește DPO, trebuie să acorde atenție tuturor celorlalte aspecte de conformare aplicabile.

92. În plus, este recomandabil să documenteze în scris evaluarea realizată și concluziile acesteia. De asemenea, FEPA trebuie să valideze periodic concluziile unei asemenea evaluări. Dacă circumstanțele care au condus la decizia de a nu numi DPO se schimbă (e.g. FEPA se dezvoltă, accesează noi tipuri de prelucrări sau categorii de date), poate rezulta necesitatea numirii unui DPO.

C. SARCINILE DPO

93. Nu există reglementări particulare privind sarcinile DPO în cadrul unei FEPA. Ca principiu, DPO trebuie să aibă o implicare efectivă și la timp în toate aspectele privind protecția datelor din cadrul organizației.

94. Principalele sarcini ale unui DPO sunt următoarele:

La preluarea mandatului

a) Auditarea organizației cu relevarea situației existente și vulnerabilitățile de conformitate identificate;

   (i) Colectează informații privind activitățile de prelucrare desfășurate;

   (ii) Interviuri / muncă colaborativă cu personalul din departamentele relevante;

b) Consiliază conducerea FEPA cu privire la obligațiile specifice și vulnerabilitățile identificate;

c) Facilitează / coordonează planuri pentru implementarea în organizație a cerințelor Regulamentului și conformare continuă;

d) Training pentru management / salariați privind obligațiile specifice domeniului.

Dezvoltare și mentenanță

a) Facilitează (redactează) documentație specifică:

b) Evidența activităților de prelucrare;

c) Evaluarea impactului asupra protecției datelor (DPIA);

d) Proceduri interne (e.g. securitatea datelor (clean desk policy), monitorizare acces, corespondență electronică, gestionare incidente de securitate);

e) Monitorizează activitățile organizației și facilitează conformare începând cu momentul conceperii și în mod implicit (protecția datelor by design și by default);

f) Asistență în cazul survenirii unui incident de securitate.

Altele

a) DPO este punct de contact pentru persoanele vizate;

b) DPO este punct de contact și cooperare cu autoritatea de supraveghere.

D. INTEGRAREA DPO ÎN ORGANIZAȚIE

95. Regulamentul impune o serie de garanții pe care organizația (FEPA) trebuie să le ofere DPO în vederea îndeplinirii sarcinilor și rolului acestuia stabilite prin Regulament.

Implicare în toate aspectele privind protecția datelor	DPO participă cu regularitate la ședințele managementului; Opiniile / recomandările DPO trebui luate în considerare (A29 GL recomandă documentarea motivelor pentru care nu este respectată opinia DPO); Consultare în cazul apariției unui incident de securitate.
Asigurarea resurselor necesare pentru îndeplinirea sarcinilor	FEPA trebuie să asigure că DPO dispune de resursele de timp necesare îndeplinirii sarcinilor sale (în special pentru DPO intern care cumulează și alte atribuții); Suport adecvat la resurse financiare, infrastructură (locație, facilități, echipamente), inclusiv personal; Drept de acces la toate datele cu caracter personal; Relaționare cu departamentele FEPA (resurse umane, legal, IT, marketing); Training DPO pentru perfecționare continuă.
Independența DPO	DPO „lucrează” în primul rând pentru persoanele vizate și doar în subsidiar pentru organizație; Orice relație de subordonare ierarhică este inaplicabilă în cazul DPO; DPO nu vor primi instrucțiuni despre cum să abordeze o problemă de conformitate, cum să investigheze un anumit incident; DPO nu are putere de decizie, dar este un consultant a cărui opinie trebuie ascultată la cel mai înalt nivel de management.
Stabilitate (nu poate fi sancționat sau demis pentru îndeplinirea sarcinilor)	O opinie “incomodă” nu poate constitui temei al demiterii sau sancționării (sau al încetării contractului cu DPO extern); Sancțiunile sunt de asemenea interzise (refuz la promovare, bonusuri, amenințare); DPO poate fi demis / sancționat pentru neîndeplinirea sarcinilor conform regulilor comune aplicabile oricărui alt angajat /

	colaborator (abatere gravă / abateri repetate, necorespundere profesională, neîndeplinirea obligațiilor contractuale).
Poziția de DPO nu trebuie să genereze un conflict de interese	În principiu, DPO nu poate exercita o funcție care îi permite să determine scopurile sau mijloacele unei prelucrări; DPO incompatibil cu o poziție de conducere / de decizie. În principiu, un avocat asociat al unei FEPA nu poate fi numit DPO; Bună-practică pentru evitarea conflictului de interese: a. Identificarea în organizație a pozițiilor incompatibile cu DPO; b. Proceduri interne de evitare / rezolvare a conflictului; c. Declarație formală că DPO nu se află în poziție de conflict (la momentul notificării către autoritatea de supraveghere).

VI. EVALUAREA IMPACTULUI ASUPRA PROTECTIEI DATELOR (DPIA)

A. CONCEPT

96. Conform art. 35 para. 1 din Regulament, *„având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii,* ***este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice****, operatorul efectuează,* ***înaintea prelucrării****, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.”*

97. Astfel, principalele coordonate ale DPIA sunt următoarele:

a) Obligativitatea DPIA intervine atunci când prelucrarea, în special cea bazată pe noile tehnologii, este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice.

b) O evaluare unică poate fi utilizată pentru analiza unor operațiuni de procesare multiple care prezintă similitudini din perspectiva riscului generat;

c) Evaluarea trebuie realizată anterior prelucrării datelor cu caracter personal.

98. În analiza riscului major, relevant este și numărul persoanelor vizate.

99. Dacă, în urma analizei, se constată că operațiunea de procesare este susceptibilă să genereze un risc ridicat, operatorul trebuie:

a) Fie să adopte o metodologie DPIA care îndeplinește criteriile din Regulament și din ”Ghidul privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă

o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679"[8] emis de către A29 GL ("**Ghidul A29 GL privind DPIA**") fie să implementeze un proces DPIA sistematic care:

(i) Îndeplinește condițiile din Anexa nr. 2 din Ghidul A29 GL privind DPIA;

(ii) Este integrat în procesele existente de dezvoltare și revizuire operațională și de risc în conformitate cu procesele interne, contextul și cultura organizațională;

(iii) Implică persoanele interesate relevante și le definește atribuțiile într-un mod clar (operator, DPO, persoane vizate, persoana împuternicită etc).

b) Să transmită raportul DPIA către autoritatea de supraveghere competentă atunci când i se solicită aceasta;

c) Să consulte autoritatea de supraveghere atunci când nu au reușit să determine măsuri suficiente pentru prevenirea riscului ridicat;

d) Să revizuiască periodic DPIA și procedurile aferente:

e) Să documenteze deciziile luate.

B. POTENȚIALE CAZURI CARE AR PUTEA ATRAGE NECESITATEA REALIZĂRII DPIA ÎN CADRUL ACTIVITĂȚII SPECIFICE DESFĂȘURATE DE FORMELE DE EXERCITARE A PROFESIEI DE AVOCAT

100. Astfel cum rezultă din art. 35 para. 1 din Regulament (mai sus citat), un caz ce implică necesitatea DPIA este determinat de utilizarea noilor tehnologii.

101. Conform punctului (91) din Preambulul Regulamentului: "*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*".

102. Conform Ghidului Consiliul Barourilor Europene (CCBE) privind principalele măsuri de conformitate pentru avocați în materie de protecție a datelor[9], excepția se mai sus s-ar aplica cabinetelor individuale de avocați, fără a exclude necesitatea efectuării DPIA în cazul cabinetelor de dimensiune redusă (cabinete individuale cu avocați colaboratori), deși, în cazul acestora, analiza de impact s-ar putea dovedi împovărătoare, față de resursele de care aceste entități dispun.

---

[8] Pentru versiunea în limba română a textului, a se vedea: http://www.dataprotection.ro/servlet/ViewDocument?id=1439

[9] Pentru varianta în limba engleză a documentului, a se vedea *http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf*

C. RECOMANDĂRI PRIVIND MODUL DE REALIZARE A DPIA

103. În cazul în care nu este clar dacă și în ce măsură PIA este necesară, A29 GL recomandă ca entitățile vizate să desfășoare DPIA întrucât această procedură reprezintă un instrument util pentru operatori și persoanele împuternicite în executarea obligațiilor ce le revin în baza legislației de protecție a datelor cu caracter personal.

104. Obligativitatea parcurgerii DPIA intervine în cazul operațiunilor de procesare ce îndeplinesc criteriile din art. 35 GDPR și care sunt inițiate după data de 25 mai 2018. Cu toate acestea, A29 GL recomandă parcurgerea acestei proceduri și pentru operațiunile de procesare în desfășurare la data de 25 mai 2018. În plus, *"acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare"*[10].

105. Art. 35 para. 7 din Regulament enunță o serie de elemente cu caracter minimal ce trebuie incluse în DPIA:

    a) "o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

    b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

    c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate; și

    d) *măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate."*

106. Anexa nr. 2 din Ghidul A29 GL privind DPIA stabilește o serie de criterii comune care clarifică cerințele minimale ale Regulamentului, oferind în același timp suficientă libertate în implementarea acestuia.

107. În același timp, A29 GL încurajează dezvoltarea unor proceduri specifice fiecărui sector de activitate. Date fiind particularitățile și specificitățile activității desfășurate de fiecare FEPA, este recomandabilă adaptarea în consecință a DPIA.

108. În plus, DPIA trebuie publicată, în tot sau în parte și trebuie comunicată autorității cu competență în domeniu, în speță Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Publicarea nu este o cerință legală impusă de Regulament, dar întărește încrederea persoanelor vizate în operatorul de date și îl ajută pe acesta din urmă să demonstreze respectarea principiilor responsabilității și transparenței.

[10] Art. 35 para. 11 GDPR.

109. Până la acest moment, autoritatea competentă din România nu a adoptat o metodologie de realizarea DPIA[11] însă o clarificare cu privire la modelul de urmat în ceea ce privește profesia de avocat ar fi binevenită.

VII. CONFIDENȚIALITATEA ȘI SECURITATEA DATELOR

A. ASPECTE GENERALE PRIVIND CONFIDENȚIALITATEA ȘI SECURITATEA DATELOR

110. Conform art. 32 din Regulament, *"Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:*

a) pseudonimizarea și criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării".

111. Un rol important în evaluarea nivelului adecvat de securitate îl vor avea riscurile pe care le implică prelucrarea, riscuri ce pot fi generate, accidental ori ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

112. Demonstrarea îndeplinirii condițiilor menționate se poate realiza, printre altele, prin aderarea la un cod de conduită aprobat în temeiul art. 40 din Regulament (cod care, în temeiul para. 2 al aceluiași articol, poate fi aprobat și la nivelul UNBR) sau la un mecanism de certificare aprobat în temeiul art. 42 GDPR.

B. REGULI SPECIFICE PRIVIND EXTERNALIZAREA GESTIUNII DATELOR UTILIZATE ÎN ACTIVITATEA AVOCAȚILOR (SERVICII DE CLOUD, SERVICII DE GESTIUNE A DATELOR / DOCUMENTELOR)

113. Conform art. 92 din Statutul din 3 decembrie 2011 al profesiei de avocat[12], *„avocatul este obligat să țină evidența actelor întocmite conform art. 3 alin. (1) lit. c) din Lege (*Lege nr. 51

[11] Astfel de metodologii au fost, însă, adoptate de alte State Membre UE: Marea Britanie (*https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf*), Franța (*https://www.cnil.fr/fr/PIA-privacy-impact-assessment*) etc.

din 7 iunie 1995 pentru organizarea şi exercitarea profesiei de avocat, republicată[13], *s.n.) şi să le păstreze în arhiva sa profesională, în ordinea întocmirii lor*". De asemenea, potrivit aceluiași text de lege, "*actele juridice semnate în fața avocatului care poartă o încheiere, o rezoluție, o ştampilă sau un alt mijloc verificabil de atestare a identității părților, a consimțământului și a datei actului trebuie înregistrate în Registrul electronic al actelor întocmite de avocat*".

114. Executarea în practică a acestor obligații este lăsată, însă, la latitudinea avocaților, motiv pentru care nu poate fi exclusă utilizarea unor metode și proceduri de externalizare a datelor prin servicii de cloud sau de gestiune a datelor/documentelor. Specificitățile acestor proceduri și mecanisme ce presupun transferul unor date din evidența avocaților către serverele administrate de terțe persoane (denumite generic în continuare "**prestatorii de servicii de gestiune a datelor**", persoane împuternicite în accepțiunea Regulamentului) impun o atenție sporită pentru respectarea Regulamentului și pentru evitarea oricăror breșe de securitate. De aceea, se impune luarea unor măsuri minime de siguranță:

a) Analiza tehnologiei care stă la baza infrastructurii cloud / de gestiune a datelor folosite în scopul determinării nivelului de securitate a datelor, îndeplinirea cerințelor impuse de GDPR etc.

b) Pentru a permite exercitarea drepturilor persoanelor vizate ("dreptul de a fi uitat", dreptul de acces la informații, dreptul de a fi informat etc) avocatul, în calitate de operator, trebuie să se asigure că prestatorii de servicii de gestiune a datelor cunosc locația fizică a fiecărui server prin care administrează bazele de date în discuție. Aceasta se impune întrucât documentele electronice sunt mai greu de găsit decât documentele în format fizic, primele putând fi transferate prin sisteme backup, arhive sau către terțe părți/entități (ex., Dropbox). În scopurile respectării Regulamentului, atât operatorul cât și persoana împuternicită trebuie să aibă o evidență clară cu privire la localizarea fiecărei informații. În același scop (i.e., exercitarea drepturilor de către persoanele vizate), se impune revizuirea de către operator a protocoalelor de backup și stocare utilizate de către prestatorii de servicii de gestiune a datelor.

c) Asumarea expresă de către prestatorii de servicii de gestiune a datelor a obligațiilor ce le incumbă în temeiul Regulamentului și a legislației aplicabile în raport atât cu operatorul cât și cu persoanele vizate.

d) Determinarea locației exacte a serverelor este utilă și pentru a determina legislația aplicabilă diferitelor operațiuni.

e) Pentru a evita compromiterea datelor în integralitatea lor și a breșelor de securitate cu impact major, este recomandabilă împărțirea datelor pe diverse categorii și stocarea lor pe servere diferite.

---

[12] Publicat în Monitorul Oficial cu numărul 898 din data de 19 decembrie 2011

[13] Republicată în Monitorul Oficial cu numărul 98 din data de 7 februarie 2011

f) Reiterarea în contractele și acordurile încheiate între avocați (în calitate de operatori) și prestatorii de servicii de gestiune a datelor (în calitate de persoane împuternicite) că prelucrarea datelor cu caracter personal transmise către cei din urmă se face în numele avocaților, aceștia menținând controlul constant asupra informațiilor.

g) Crearea unor proceduri de verificare și de analiză de risc cărora să le fie supuși prestatorii de servicii de gestiune a datelor și testarea periodică a respectării legislației aplicabile în domeniul prelucrării datelor cu caracter personal (spre exemplu, dar fără a se limita la, art. 28 GDPR).

C. DEZVĂLUIRI DE DATE LA SOLICITAREA AUTORITĂȚILOR PUBLICE. LIMITELE DEZVĂLUIRII

115. Art. 6 para. 1 lit. c) din Regulament prevede că prelucrarea datelor cu caracter personal este legală dacă, printre altele, *"prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului"*.

116. Ca atare, avocații pot transmite date cu caracter personal pe care le prelucrează ca operatori către autorități publice doar dacă și în măsura în care, *în principal*:

a) Aceasta se manifestă într-o obligație legală pentru aceștia;

b) Autoritatea care solicită aceste informații are competență în domeniu, verificată în prealabil de către avocatul căruia i se solicită transferul;

c) Avocatul asigură un nivel de protecție adecvat al datelor prelucrate și astfel transmise;

d) Transferul se realizează cu respectarea principiilor prevăzute de GDPR și sintetizate în art. 5 din acesta: legalitate, echitate și transparență; principiul limitării transferului în funcție de scop; principiul reducerii la minimum a datelor transferate; principiul exactității datelor; principiul limitării legate de stocarea datelor; principiul asigurării integrității și confidențialității datelor; principiul responsabilității.

117. Un exemplu de obligație legală de transmitere este cel prevăzut de art. 5 din 656/2002 pentru prevenirea și sancționarea spălării banilor, precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării terorismului[14] (**"Legea 656/2002"**) în baza căruia, prin coroborare cu art. 10 lit. f) din aceeași lege, avocatul care "are suspiciuni că o operațiune ce urmează să fie efectuată are ca scop spălarea banilor sau finanțarea actelor de terorism, informează persoana desemnată conform art. 20 alin. (1), care sesizează imediat Oficiul Național de Prevenire și Combatere a Spălării Banilor, denumit în continuare Oficiul. Persoana desemnată analizează informațiile primite și sesizează Oficiul cu privire la suspiciunile motivate rezonabil. Acesta confirmă primirea sesizării." Conform art. 5 alin. (9) si (11) din Legea 656/2002, avocații *"nu au obligația de a raporta către Oficiu informațiile pe care le primesc sau pe care le obțin de la unul dintre clienții lor în cursul determinării situației*

[14] Republicată în Monitorul Oficial al României, Partea I, nr. 861 din 7 decembrie 2011

juridice a acestuia ori al apărării sau reprezentării acestuia în cadrul unor proceduri judiciare ori în legătură cu acestea, inclusiv al acordării de consultanță cu privire la declanșarea unor proceduri judiciare, potrivit legii, indiferent dacă aceste informații au fost primite sau obținute înainte, în timpul ori după încheierea procedurilor" ci *"raportările se fac către persoanele desemnate de către structurile de conducere ale profesiilor liberale, care au obligația de a le transmite Oficiului în cel mult 3 zile de la primire. Informațiile se transmit Oficiului nealterate".*

VIII. BREȘELE DE SECURITATE

118. Conform art. 5 din Regulament unul din principiile de bază care guvernează prelucrarea datelor cu caracter personal este acela că datele trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a acestora. Garanțiile legale ale acestui principiu se regăsesc în principal în art. 32-34 din Regulament.

119. Formele de exercitare sunt obligate să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător (art. 32 din Regulament). Formele de exercitare trebuie să stabilească măsurile necesare și suficiente pentru a asigura securitatea datelor, pe baza criteriilor explicate în secțiunea anterioară (componenta preventivă a politicilor interne privind securitatea datelor).

120. Totodată, chiar dacă art. 33 din Regulament nu o prevede în mod expres, formele de exercitare trebuie să implementeze măsuri tehnice și organizatorice care, în cazul apariției unei breșe de securitate, asigură componenta reactivă a politicilor interne privind securitatea datelor. Aceste măsuri trebuie să ajute operatorul:

    a) să stabilească imediat dacă s-a produs o breșă de securitate (preambul, pct. 87 din Regulament);

    b) dacă este cazul, să notifice autoritatea de supraveghere a prelucrării datelor cu caracter personal (art. 33 din Regulament);

    c) după caz, să informeze persoana sau persoanele vizate afectate de apariția breșei de securitate (art. 34 din Regulament).

121. Nu în ultimul rând, incidentele de securitate trebuie documentate conform art. 33 alin. (5) din Regulament.

122. Art. 4 alin. (12) din Regulament definește breșa de securitate: „o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal (...) sau la accesul neautorizat la acestea".

123. În Ghidul privind notificarea încălcării securității datelor, A29 GL explică noțiunile de „distrugere", „pierdere", „modificare" și „divulgare neautorizată":

a) „distrugerea” se referă la situația în care datele nu mai există ori nu mai există într-o formă care să le facă utilizabile de către operatori;

b) „pierderea” are în vedere situația în care datele pot să existe, însă operatorul a pierdut controlul sau accesul la date;

c) „modificarea” desemnează situația în care datele sunt corupte sau modificate în alt mod, astfel încât ele nu mai sunt complete;

d) în fine, „divulgarea neautorizată” are în vedere situația în care datele au fost transmise către ori accesate de către persoane neautorizate să primească sau să acceseze datele personale.

124. Privind noțiunea de breșă de securitate prin prisma celor trei elemente ale securității datelor (disponibilitate, integritate, confidențialitate), rezultă că există o breșă de securitate atunci când:

a) datele devin indisponibile ca urmare a (i) distrugerii ori (ii) pierderii accesului; și/sau

b) este afectată integritatea datelor prin modificarea acestora; și/sau

c) este compromisă confidențialitatea datelor prin (i) divulgarea neautorizată sau (ii) accesul neautorizat la date.

125. Există diferite exemple de breșe de securitate: atacuri informatice tip ransomware, pierderea cheii de criptare a datelor, nefuncționarea sistemelor informatice, pierderea unor documente, transmiterea unei corespondențe la adresa greșită etc.).

126. Breșele de securitate pot avea cauze diferite: de la nefuncționarea sau funcționarea necorespunzătoare a sistemelor informatice până la erori umane. Un studiu al autorității britanice privind breșele de securitate apărute în rândul profesiei arată că cele mai multe incidente de securitate se datorează erorilor umane: situații în care documente conținând date cu caracter personal sunt uitate ori pierdute în afara sediului profesional al avocatului.

127. Este foarte important ca FEPA, în calitatea lor de operatori, să se asigure că indiferent de cauza acesteia și forma în care se manifestă, apariția unei breșe de securitate este identificată imediat și adusă în mod corespunzător la cunoștința persoanelor competente să implementeze măsurile care se impun.

128. Pentru aceasta, FEPA vor asigura instruirea persoanelor implicate în procesele de prelucrare a datelor astfel încât acestea să poată identifica breșele de securitate și să le aducă la cunoștința persoanelor responsabile pentru a lua măsurile necesare în vederea analizei și limitării consecințelor breșei de securitate și, după caz, în vederea notificării autorității de supraveghere și eventual a persoanelor vizate.

A. NOTIFICAREA AUTORITĂȚII DE SUPRAVEGHERE

129. Art. 33 din Regulament reglementează obligația operatorului de a notifica breșele de securitate către autoritatea de supraveghere a prelucrării datelor cu caracter personal. În

situația în care avocatul acționează în calitate de persoană împuternicită, este obligația operatorului să notifice autoritatea de supraveghere cu privire la breșa de securitate. Totuși, avocatul, în calitate de persoană împuternicită va informa operatorul imediat ce ia cunoștință de apariția breșei de securitate.

130. Scopul notificării autorității este ca aceasta să poată interveni pentru limitarea riscurilor asupra drepturilor și libertăților persoanelor vizate.

131. Nu orice breșă de securitate trebuie notificată autorității de supraveghere. Conform art. 32 din Regulament, nu este obligatorie notificarea dacă respectiva breșă nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate. Este obligația operatorului să analizeze dacă incidentul de securitate cu care se confruntă generează riscuri pentru drepturile și libertăților persoanelor vizate. Analiza se face de la caz la caz, pe baza următoarelor elemente:

a) tipul incidentului;

b) natura, contextul, volumul datelor afectate;

c) posibilitatea de a identifica persoanele vizate;

d) consecințele incidentului asupra persoanelor vizate;

e) consecințele incidentului asupra persoanelor vizate;

f) circumstanțele persoanelor vizate;

g) circumstanțele operatorului în cauză.

Exemplu: pierderea unor date cu caracter personal criptate cu un algoritm de criptare complex nu este susceptibilă să genereze riscuri pentru drepturile și libertățile persoanelor vizate, atât timp cât criptarea asigură că datele nu pot fi accesate de persoane neautorizate. Totuși, dacă datele nu sunt criptate, pierderea acestora ar trebui notificată.

---

132. În cazurile în care notificarea autorității este obligatorie, aceasta trebuie făcută „fără întârziere", de principiu nu mai târziu de 72 de ore de la data la care operatorul a luat la cunoștință de existența breșei.

133. Conținutul minim al notificării este reglementat de art. 33 din Regulament. La pregătirea notificării, avocații vor trebui să protejeze confidențialitatea informațiilor oferite de clienți, sens în care vor oferi autorității detalii despre categoriile și numărul persoanelor afectate, fără însă a compromite confidențialitatea datelor primite de la clienți. În anumite situații, este posibil ca nu toate datele să fie de la început la dispoziția operatorului, unele amănunte devenind disponibile pe măsură ce operatorul investighează breșa. Pentru aceste situații, Regulamentul (art. 33 alin. (4)) și A29 GL recunosc posibilitatea notificării etapizate, în care

operatorul transmite autorității de supraveghere datele relevante pe măsură ce acestea devin disponibile.

B. INFORMAREA PERSOANELOR VIZATE

134. Art. 34 din Regulament reglementează obligația operatorului de a informa persoanele vizate cu privire la breșele de securitate. Scopul informării este ca persoanele vizate să își poată lua măsuri de protecție.

135. Informarea persoanelor vizate este obligatorie numai dacă incidentul de securitate este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate. Dacă notificarea autorității de supraveghere este obligatorie ori de câte ori există un risc privind drepturile și libertățile persoanelor vizate, informarea persoanelor vizate este obligatorie atunci când există un risc ***ridicat*** pentru drepturile și libertățile acestora.

136. Regulamentul nu prevede criterii obiective în funcție de care se determină nivelul riscului generat de incidentul de securitate. Conform Ghidului privind notificarea încălcării securității datelor, la analiza nivelului de risc, operatorul va avea în vedere criteriile de mai jos:

a) tipul incidentului;

b) natura, contextul, volumul datelor afectate;

c) posibilitatea de a identifica persoanele vizate;

d) consecințele incidentului asupra persoanelor vizate;

e) consecințele incidentului asupra persoanelor vizate;

f) circumstanțele persoanelor vizate;

g) circumstanțele operatorului în cauză;

h) numărul persoanelor afectate.

137. În analiza sa, avocatul va avea în vedere severitatea riscului, însă în același timp va ține cont de probabilitatea apariției acestuia. Astfel, posibilitatea ca incidentul de securitate să genereze un risc ridicat cu privire la drepturile și libertățile persoanei/persoanelor vizate crește (i) atunci când severitatea riscului crește, dar și (ii) atunci când, chiar dacă riscul nu este foarte ridicat, totuși probabilitatea apariției sale este mai mare[15].

138. Având în vedere specificul profesiei de avocat, care de multe ori presupune prelucrarea datelor personale extrem de sensibile, pot fi imaginate multe situații în care incidente de securitate pot genera riscuri ridicate.

[15] Un ghid cu recomandări privind analiza severității incidentelor de securitate poate fi consultant la următoarea adresă: *https://www.enisa.europa.eu/publications/dbn-severity*

Exemplu: pierderea unui document care cuprinde identitatea reală a unui martor cu identitate protejată este susceptibilă să genereze riscuri ridicate pentru drepturile și libertățile respectivului martor.

139. În cazurile în care informarea persoanelor vizate este obligatorie, aceasta trebuie făcută „fără întârziere". Conținutul notificării este reglementat de art. 34 din Regulament.

140. Regulamentul nu prescrie un anume formalism pentru informarea persoanelor vizate. Dacă circumstanțele concrete nu reclamă o altă abordare, informarea se va face printr-o comunicare adresată direct persoanei vizate, printr-un mijloc de comunicare corespunzător (poștă electronică, SMS etc.). Cu titlu de excepție, doar în situația în care contactarea directă a persoanei/persoanelor vizate ar presupune un efort disproporționat, se poate face o informare publică.

C. EVIDENȚA BREȘELOR DE SECURITATE

141. Toate incidentele de securitate trebuie documentate de formele de exercitare a profesiei. Obligația de a documenta incidentele de securitate se întinde și asupra acelor incidente care nu au făcut obiectul notificării.

142. Regulamentul nu prevede o formă anume a instrumentului care documentează breșele de securitate. Totuși, conținutul acestuia este reglementat în art. 33 alin. (5) din Regulament. În cazul incidentelor de securitate pentru care s-a luat decizia să nu se notifice autoritatea de supraveghere sau persoanele vizate, operatorul va face mențiune despre decizia de a nu notifica, arătând motivele care au fundamentat această decizie.

IX. STOCAREA DATELOR CU CARACTER PERSONAL

A. ASPECTE GENERALE

143. Al cincilea principiu care guvernează prelucrarea datelor cu caracter personal (supra, paragr. 7.E) prevede că datele cu caracter personal trebuie să fie păstrate pe o perioadă care nu depășește perioada necesară prelucrării pentru scopul identificat. Principiul stocării limitate a datelor cu caracter personal derivă din principiile al treilea și al patrulea:

- datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive;
- datele cu caracter personal trebuie să fie exacte și actualizate.

144. În mod evident, datele cu caracter personal stocate pentru perioade mai lungi decât cele necesare prelucrării pentru scopul identificat vor deveni în mod automat ***excesive***. Totodată, ele ar putea deveni ***nerelevate și chiar inexacte***.

145. Regulamentul nu stabilește perioada standard de stocare a datelor cu caracter personal și nici reguli detaliate care să ajute operatorii ori persoanele împuternicite să stabilească această

perioadă. Revine așadar formelor de exercitare a profesiei sarcina să stabilească perioadele de reținere a datelor cu caracter personal prelucrate. Ghidul oferă în paragrafele care urmează o serie de criterii care trebuie avute în vedere la stabilirea prelucrării duratelor de stocare a datelor cu caracter personal prelucrate în contextul activității profesionale a avocaților.

146. Stabilirea perioadei de stocare a datelor trebuie să asigure un just echilibru între nevoia avocatului de a reține datele cu caracter personal pe de o parte și drepturile și interesele legitime ale persoanelor vizate pe de altă parte. Ștergerea datelor prea devreme, în contextul în care avocatul ar putea avea (încă) nevoie să le prelucreze, l-ar putea pune pe acesta într-o situație dificilă. Totodată, stocarea datelor personale pentru mai mult timp decât este necesar riscă să încalce principiile prelucrării datelor cu caracter personal, astfel cum acestea sunt prevăzute în Regulament. De asemenea, în cazul în care datele cu caracter personal sunt stocate mai mult decât este nevoie, va crește inutil volumul de date pentru care vor trebui asigure securitatea datelor și posibilitatea exercitării drepturilor de către persoanele vizate. În consecință, adoptarea unei politici de retenție a datelor nu doar că asigură respectarea Regulamentului, ci ușurează sarcina operatorului în ce privește managementul datelor.

147. În contextul prelucrării datelor cu caracter personal, pentru a se conforma regulilor privind retenția datelor, formele de exercitare vor implementa două tipuri de reguli interne:

a) politici de arhivare, în baza cărora datele cu caracter personal care nu sunt prelucrate în activitatea curentă, dar pentru reținerea cărora există o justificare, să fie arhivate cu respectarea garanțiilor privind securitatea datelor

b) politici de ștergere, în baza cărora se vor revizui datele cu caracter personal prelucrate și se vor șterge, sau, după caz, se vor anonimiza acele date cu caracter personal de care nu mai este nevoie.

B. POLITICI DE ARHIVARE

148. Scopul politicilor de arhivare va fi acela de a asigura un flux corespunzător al dosarelor sau lucrărilor inactive și al datelor cu caracter personal din aceste dosare/lucrări. Un dosar devine inactiv atunci când pentru forma de exercitare este evident că în cauza respectivă se vor face demersuri într-un orizont de timp evaluabil. Fără ca enumerarea să fie limitativă, următoarele sunt cazuri în care un dosar devine inactiv:

- contractul de asistență juridică referitor la cauza respectivă a încetat, altfel decât prin reziliere pentru culpa uneia dintre părți;
- chiar dacă nu a survenit încetarea contractului de asistență juridică, în cauza respectivă nu s-au mai făcut demersuri în ultimele (12) luni;

149. Atunci când un dosar devine inactiv, forma de exercitare:

- va verifica dosarul în cauză și va identifica datele cu caracter personal prelucrate în dosarul respectiv;
- va analiza, pentru fiecare categorie de date prelucrate, dacă există motive justificate pentru reținerea lor în continuare.

Exemplu: la încetarea contractului de asistență juridică, dosarul sau cauza care face obiectul respectivului contract devine inactivă. Totuși, forma de exercitare are interesul să rețină date cu caracter personal din dosarul respectiv, pentru a răspunde eventualelor pretenții ale clientului privind modul în care avocatul a gestionat dosarul. Aceste date ar trebui arhivate, urmând a fi șterse doar ulterior, atunci când devine evident că o pretenție nu ar mai putea fi formulată (de ex. pentru că s-a împlinit termenul de prescripție extinctivă)

În cazul în care se vor identifica date care nu mai sunt necesare, acestea se vor anonimiza sau se vor șterge. Datele din dosare inactive pentru reținerea cărora există temei vor fi arhivate, cu respectarea garanțiilor privind securitatea datelor.

150. Important, datele cu caracter personal arhivate nu au un regim juridic derogatoriu, acestora aplicându-li-se toate prevederile privind prelucrarea datelor cu caracter personal. Spre pildă, FEPA va trebui să dea curs unei solicitări prin care se exercită dreptul de acces, chiar dacă datele vizate prin cerere vor fi fost arhivate.

C. POLITICI DE ȘTERGERE

151. Scopul politicilor de ștergere va fi acela de a stabili, pentru fiecare categorie de date cu caracter personal, perioada de stocare și procedura ce urmează a fi aplicată după expirarea acestei perioade – ștergerea definitivă sau, după caz, anonimizarea.

152. La stabilirea perioadelor de retenție se vor avea în vedere în primul rând prevederile din legislația privind organizarea și exercitarea profesiei de avocat și din actele emise de organele profesiei. Ori de câte ori există un termen de retenție stabilit în legislația aplicabilă sau în actele emise de organele profesiei, FEPA nu vor stoca datele pentru perioade mai lungi decât perioada legală.

59. Acolo unde nu există termene de stocare a datelor stabilite în actele normative ori în actele organelor profesiei, FEPA vor stabili perioadele de stocare a datelor cu caracter personal ținând cont de scopul prelucrării datelor personale și de contextul prelucrării acestora;

60. Perioada de retenție a datelor cu caracter personal trebuie stabilită de la caz la caz, în funcție de scopul pentru care au fost colectate respectivele date. Astfel, odată ce datele nu mai sunt necesare scopului pentru care au fost colectate, acestea vor fi șterse sau anonimizate.

Exemplu: un client solicită avocatului să redacteze o procură prin care un terț este împuternicit să reprezinte clientul în fața unei autorități publice pentru ridicarea unui înscris. Odată cu solicitarea, clientul transmite avocatului său o copie a cărții de identitate a mandatarului. După ce va fi redactat procura, iar aceasta a fost semnată de către client, avocatul nu mai are niciun motiv să rețină copia cărții de identitate a mandatarului. În consecință, respectiva copie va trebui ștearsă.

153. Contextul prelucrării datelor cu caracter personal oferă de cele mai multe elemente relevante pentru stabilirea perioadei de stocare a datelor.

62. De cele mai multe ori, avocații prelucrează date cu caracter personal în contextul serviciilor de asistență juridică prestate clienților. Din acest punct de vedere, atunci când contractul de asistență juridică încetează, avocatul va trebui să analizeze care sunt datele de care nu mai are nevoie (acestea urmând a fi șterse sau anonimizate) respectiv care sunt datele care trebuie menținute în continuare, în ce scop și pentru cât timp. La încetarea contractului de asistență juridică, avocatul va trebui să rețină în continuare date cu caracter personal pentru a răspunde eventualelor plângeri sau pretenții ale clientului. Cum am arătat mai sus, aceste date ar trebui păstrate în arhiva avocatului pentru o perioadă suficientă astfel ca după trecerea acestei perioade, formularea unei plângeri sau a unei pretenții în legătură cu prestația avocatului să nu mai fie posibilă.

X. TRANSFERUL DATELOR CU CARACTER PERSONAL CĂTRE STATE TERȚE

A. CONCEPT ȘI DELIMITARE

154. Conform art. 45 para. 1 din Regulament, „*transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când Comisia a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale*”. Decizia Comisiei în acest sens este obligatorie pentru toate statele membre UE.

155. Cu privire la nivelul adecvat de protecție, astfel cum a stabilit și CJUE în cauza C-362/14 Maximillian Schrems împotriva Data Protection Commissioner[16], ”*termenul „adecvat” care figurează la articolul 25 alineatul (6) din Directiva 95/46 implică faptul că nu se poate impune ca o țară terță să asigure un nivel de protecție identic cu cel garantat în ordinea juridică a Uniunii (...) chiar dacă mijloacele la care această țară terță a recurs, în această*

[16] Cauza C-362/14 Maximillian Schrems împotriva Data Protection Commissioner, 06.10.2015m para. 73-74

privință, pentru a asigura un astfel de nivel de protecție pot fi diferite de cele puse în aplicare în cadrul Uniunii pentru a garanta respectarea cerințelor care decurg din această directivă, interpretată în lumina cartei, aceste mijloace trebuie totuși să se dovedească în practică efective în scopul de a asigura o protecție în esență echivalentă cu cea garantată în cadrul Uniunii"[17].

156. Conform art. 45 din Regulament, în analiza realizată în scopul determinării dacă și în ce măsură statul terț sau organizația internațională asigură un nivel de protecție adecvat, Comisia Europeană trebuie să aibă în vedere două elemente: legislația incidentă și metodele prin care se asigură aplicarea efectivă a acesteia.

157. În concret, avocații pot realiza transferuri către state terțe sau organizații internaționale în cazul unor tranzacții ce implică mai multe jurisdicții, în cazul transferului de procedură, în situația unor proceduri arbitrale, dar în toate aceste cazuri numai dacă adresa de destinație (inclusiv adresa serverului) este localizată în afara spațiului UE și SEE.

B. CERINȚE SPECIFICE DE TRANSFER ÎN FUNCȚIE DE TEMEIUL ȘI SCOPUL TRANSFERULUI

158. În absența unei decizii a Comisiei care să constate asigurarea unui nivel adecvat de protecție, datele cu caracter personal pot fi transferate către state terțe sau organizații internaționale doar dacă (i) operatorul sau persoana împuternicită de operator a oferit garanții adecvate și (ii) cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

159. Aceste garanții adecvate pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea unei autorități de supraveghere, prin:

a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

b) reguli corporatiste obligatorii în conformitate cu articolul 47 din Regulament (în speță, reguli cu privire la transferul între mai multe entități parte ale aceluiași grup);

c) clauze standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2) din Regulament;

d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2) din Regulament;

e) un cod de conduită aprobat în conformitate cu articolul 40 din Regulament, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

[17] Directiva 95/46 va fi abrogată de către GDPR începând cu 25.05.2018 iar conform art. 94 GDPR, trimiterile la Dierctiva 95/46 vor fi interpretate ca fiind trimiteri la GDPR.

f) un mecanism de certificare aprobat în conformitate cu articolul 42 din Regulament, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

160. De menționat că Regulamentul limitează abilitatea operatorului sau persoanei împuternicite să transfere date cu caracter personal în afara UE în cazul în care acest transfer are la bază doar analiza acestora cu privire la nivelul adecvat de protecție de care beneficiază aceste date.

161. În absența unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, iar consimțământul său a fost unul informat;

b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

162. În cazul în care un transfer nu ar putea să se întemeieze pe niciunul dintre temeiurile menționate anterior, inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații specifice, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care:

a) transferul nu este repetitiv,

b) transferul se referă doar la un număr limitat de persoane vizate,

c) transferul este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și

d) în urma unei evaluări a circumstanțele aferente transferului de date, operatorul a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal.

163. În acest din urmă caz, operatorul informează atât autoritatea de supraveghere cât și persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.