

## **Anexa nr. 19**

### **GHID PRACTIC AVOCAȚII ȘI REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR (RGPD)**

Ediția 1

CONSILIUL NAȚIONAL AL BAROURILOR  
BAROUL DIN PARIS  
CONFERINȚA PREȘEDINȚILOR BAROULUI

---

MARTIE 2018

## CUPRINS

CUVÂNT ÎNAINTE	5
CADRUL GENERAL AL PROTECȚIEI DATELOR CU CARACTER PERSONAL	7
1. Protecția datelor cu caracter personal, o problemă deosebit de delicată pentru avocați	7
2. Glosar	8
3. Principiile cheie	9
3.1. Principii reafirmate	9
3.1.1. Principiul scopului: o utilizare reglementată a datelor cu caracter personal	9
3.1.2. Principiul proporționalității	9
3.1.3. Principiul unei durate limitate de stocare a datelor	9
3.1.4. Principiile de securitate și de confidențialitate	10
3.1.5. Principiul respectării drepturilor omului	10
3.2. Noile măsuri de conformitate	12
3.2.1. Notificarea privind orice încălcare a datelor cu caracter personal	13
3.2.2. Minimizarea datelor	13
3.2.3. Dreptul de a fi uitat	13
3.2.4. Evaluările impactului	14
3.2.5. Portabilitatea datelor	14
3.2.6. Capacitatea de a monitoriza destinatarii datelor cu caracter personal	16
3.2.7. Păstrarea unui registru al activităților de prelucrare	16
FIȘE PRACTICE	17
FIȘA Nr. 1. PRELUCRAREA „RU” (RESURSE UMANE)	18
1. Ce este prelucrarea RU?	18
2. Care sunt datele pe care avocatul le poate colecta în cadrul prelucrării RU?	18
3. Este necesar ca avocatul să îndeplinească formalități în cazul prelucrării RU?	19
4. Pentru cât timp pot fi stocate datele?	20
5. Este necesară informarea persoanelor în cauză?	20
FIȘA Nr. 2. GESTIONAREA CLIENTILOR	22
1. Ce date poate colecta avocatul în cadrul gestionării clienților săi?	22
2. Este necesar ca avocatul să îndeplinească formalități?	23
3. Pentru cât timp pot fi stocate datele?	24
4. Este necesară informarea persoanelor în cauză?	24

5. Securitatea dosarelor clienților	25
6. Solicitare personalizată	25
<b>FIȘA Nr. 3. SUPRAVEGHERE VIDEO ȘI PROTECȚIE VIDEO</b>	<b>26</b>
1. Ce este supravegherea video și protecția video?	26
2. Care este obiectivul instalării camerelor?	26
3. Care sunt formalitățile care trebuie îndeplinite?	27
3.1. Înainte de intrarea în vigoare a RGPD	27
3.2. După intrarea în vigoare a RGPD	27
4. Este necesară informarea persoanelor în cauză?	28
5. Cine are acces la imaginile înregistrate de camere?	28
6. Pentru cât timp pot fi stocate imaginile?	29
<b>FIȘA Nr. 4. FURNIZORI ȘI PRESTATORI</b>	<b>30</b>
1. Ce este un subcontractant?	30
2. Ce trebuie să facem în caz de subcontractare?	30
3. Ce trebuie să facem cu subcontractanții cu care cabinetul are deja relații comerciale?	31
<b>FIȘA Nr. 5. GESTIONAREA ACCESULUI ÎN CABINET</b>	<b>31</b>
1. Utilizarea badge-urilor la locul de muncă	32
2. Dispozitivele biometrice	33
<b>FIȘA Nr. 6. COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI</b>	<b>34</b>
<b>FIȘA Nr. 7. SITE-URI WEB</b>	<b>36</b>
1. Care sunt formalitățile care trebuie îndeplinite în cazul în care avocatul colectează date cu caracter personal prin site-ul său web?	36
2. Care sunt mențiunile care trebuie să apară în mod obligatoriu pe site-ul web al avocatului?	37
3. Ce trebuie să includă diferitele mențiuni?	37
4. Ce este un cookie?	39
5. Cum putem respecta utilizarea cookie-urilor pe site-ul web al avocatului?	39
<b>FIȘA Nr. 8. BUNE PRACTICI DE SECURITATE A DATELOR</b>	<b>41</b>
1. De ce securitatea datelor cu caracter personal este importantă în special în prelucrările efectuate de către avocat?	41
2. Ce măsuri fizice de securitate trebuie să pun în aplicare?	41
3. Ce măsuri logistice/digitale de securitate trebuie să pun în aplicare?	41
4. Cum putem notifica și comunica o încălcare a datelor cu caracter personal?	42

FIȘA Nr. 9. PROCEDURA ÎN CAZ DE ÎNCĂLCARE A DATELOR	43
FIȘA Nr. 10. REGISTRUL ACTIVITĂȚILOR DE PRELUCRARE	45
FIȘA Nr. 11. RESPONSABILUL CU PROTECȚIA DATELOR	47
1. Obligația cabinetelor de avocatură de a desemna un responsabil cu protecția datelor	47
2. Obligația și misiunile responsabilului cu protecția datelor	48
3. Avocatul care acționează în calitate de responsabil cu protecția datelor	49
FIȘA Nr. 12. AUTORITATEA DE CONTROL ȘI SANCTIUNILE	51
FIȘA Nr. 13. DREPTUL DE ACCES LA DATE	52
METODOLOGIA DE CONFORMITATE	54
1. Desemnarea unui pilot	54
2. Cartografierea prelucrărilor de date cu caracter personal	54
3. Identificarea acțiunilor prioritare	56
4. Gestionarea riscurilor	56
5. Instituirea procesului de protecție a datelor cu caracter personal în cadrul cabinetului de avocatură	56
6. Documentația privind conformitatea	57
PENTRU MAI MULTE INFORMAȚII	58

## CUVÂNT ÎNAINTE

Regulamentul (UE) 2016/679 privind protecția datelor (RGPD) se va aplica direct în cadrul Statelor membre la data de 25 mai 2018.

Mai sunt două luni în care cabinetele de avocatură pot anticipa acest nou text care va schimba radical regulile aplicabile mediului digital al acestora.

Prelucrarea datelor cu caracter personal ale clienților cabinetului de avocatură este una deosebit de delicată. Aceasta urmează o logică specifică, însă nu o logică a unei întreprinderi pur comerciale: protecția datelor sensibile despre care ia la cunoștință este inherentă cu privire la relația de încredere dintre avocat și clientul acestuia și cu privire la obligațiile sale deontologice.

Consiliul național al barourilor, Baroul din Paris și Conferința președinților baroului sunt alături de avocați pentru a-i ajuta cu referire la respectarea RGPD, securizarea datelor acestora și a datelor clienților.

Acest ghid practic oferă răspunsuri concrete la întrebările avocaților și le va permite acestora să aibă un rol esențial cu privire la protecția datelor și a vieții private, atât în calitate de operator, cât și de consultant pentru clienții săi.

Într-adevăr, RGPD nu are doar rolul de a consolida încrederea și securitatea necesare în relațiile cu clienții, ci reprezintă și o oportunitate formidabilă pentru avocați de a investi într-un nou domeniu de intervenție pentru clienții lor.

Avocatul apare ca un tehnician de drept care este competent în special pentru a-și ajuta clienții să respecte RGPD și pentru a exercita funcția de responsabil cu protecția datelor. Deși avocații CIL (corespondent informatică și libertăți) sunt încă puțini la număr, avocatul are propriul loc pe această piață care se deschide astăzi într-un număr foarte mare de întreprinderi. Această nouă funcție permite ca profesia să își extindă în mod natural oferta de servicii și de consultanță, incluzând relația sa cu clientul într-o perspectivă durabilă și *full service* strict cu privire la regulile noastre profesionale.

Numeroasele recomandări incluse în acest ghid trebuie să permită avocaților să ocupe un loc din ce în ce mai important în acest domeniu al dreptului.

**Christiane Féral-Schuhl,**  
președintele Consiliului  
național al barourilor

**Marie-Aimée Peyron,**  
vicepreședintele  
Consiliului național  
al barourilor,  
Președintele Baroului  
din Paris

**Jérôme Gavaudan,**  
vicepreședintele  
Consiliului național  
al barourilor,  
președintele  
Conferinței  
Președinților Baroului

## **CADRUL GENERAL AL PROTECȚIEI DATELOR CU CARACTER PERSONAL**

---

Regulamentul nr. 2016/679 al Parlamentului european și al Consiliului din 27 aprilie 2016 privind protecția datelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (regulamentul general privind protecția datelor – RGPD) intră în vigoare la data de 25 mai 2018. Acesta abrogă directiva 95/44/CE.

RGPD este un regulament european obligatoriu care reformează și consolidează drepturile și protecția datelor cu caracter personal ale persoanelor fizice.

RGPD se aplică pentru toate cabinetele de avocatură, indiferent de dimensiunea, structura și domeniul de activitate al acestora.

### **1. Protecția datelor personale, o problemă deosebit de delicată pentru avocați**

---

Datele la care avocatul are acces în exercitarea funcțiilor sale au foarte adesea legătură cu viața privată a clienților acestora și, prin natura lor, sunt foarte sensibile: date referitoare la sănătate, cazier judiciar, opinii publice și religioase, situație familială, etc...

Divulgarea acestora poate aduce atingere drepturilor și libertăților persoanelor în cauză. Informațiile prelucrate de către avocați pentru exercitarea profesiei lor trebuie să fie protejate în mod special.

Respectarea secretului profesional, așa cum se definește în articolul 66-5 al legii din 31 decembrie 1971, articolul 4 al decretului din 12 iulie 2005, articolul 2 al Regulamentului intern național (RIN) și protejată prin articolul 226-13 al codului penal, trebuie să îl facă pe avocat să fie vigilent mai ales cu privire la protecția datelor cu caracter personal ale clienților săi și, prin consecință, să se conformeze obligațiilor legale și de reglementare aplicabile în speță.

Protecția datelor cu caracter personal ale clientului său este esențială pentru garantarea secretului profesional.

Respectarea de către avocați a regulilor de protecție a datelor cu caracter personal este un factor de transparență și de încredere cu privire la clienții acestora.

De asemenea, reprezintă o garanție a securității juridice pentru avocații care, fiind responsabili cu prelucrările efectuate, trebuie, în special, să se asigure că:

- scopul fiecărei prelucrări și eventualele transmiteri de informații sunt clar definite;
- dispozitivele informatice și fizice de securitate sunt determinate cu precizie;
- măsurile de informare a persoanelor în cauză sunt aplicate.

Prelucrarea datelor cu caracter personal ale clienților cabinetelor de avocatură este deosebit de delicată. Aceasta urmează o logică specifică, însă nu o logică a unei întreprinderi pur comerciale:

protecția datelor sensibile despre care ia la cunoștință este inerentă cu privire la relația de încredere dintre avocat și clientul acestuia și cu privire la obligațiile sale deontologice.

Dacă intersectarea noilor tehnologii cu deontologia poate părea delicată, trebuie să se păstreze un principiu simplu: în toate circumstanțele, avocatul trebuie să respecte regulile deontologice. Cu alte cuvinte, evoluția modalităților practice de exercitare a profesiei indusă de noile tehnologii pe care fiecare avocat le aplică în cadrul cabinetului său nu îl poate scuti nici de respectarea dispozițiilor Regulamentului interior național (RIN), nici de regulamentul intern al fiecărui barou, nici de obligația de a impune respectarea acestor reguli de către toți membrii cabinetului său și de către toți prestatorii externi la care apelează acesta pentru nevoile activității sale.

Această regulă imperativă are legătură atât cu externalizarea anumitor servicii ale cabinetului (standard la distanță, secretariat la distanță, traducător, etc.), cât și cu externalizarea stocării datelor cabinetului (Cloud Computing) sau cu externalizarea instrumentelor de comunicare (site web, blog, site-uri de referențiere, site-uri terțe, consultații online, etc.).

Această dorință constantă de a-și respecta obligațiile deontologice în universul digital și de a asigura în special protecția datelor cabinetului și a respectării secretului profesional îi ajută pe avocați să poată să urmeze cu seninătate calea digitală fără a-și pierde valoarea și încrederea din partea clienților.

Avocatul, garantul secretului profesional, piatra de temelie a profesiei, trebuie să fie deosebit de exemplar în această privință.

## **2. Glosar**

---

- **Date cu caracter personal:** orice informații referitoare la o persoană fizică identificată sau identificabilă (numită în continuare „persoana în cauză”); este acea „persoană fizică identificabilă”, care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi numele, numărul de identificare, datele de localizare, un element online de identificare, sau la unul sau mai multe elemente specifice identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
- **Prelucrare:** orice operațiune sau ansamblu de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea sau combinarea, blocarea, ștergerea sau distrugerea.
- **Operator:** orice persoană fizică sau juridică, autoritate publică, serviciu sau alt organism care, independent sau împreună cu alte autorități, stabilește scopurile și mijloacele de prelucrare; dacă scopurile și mijloacele de prelucrare sunt determinate printr-o lege a Uniunii sau o lege a unui Stat membru, se poate desemna operatorul sau se pot stipula criteriile specifice aplicabile desemnării acestuia prin legea unui Stat membru.
- **Subcontractant:** orice persoană fizică sau juridică, autoritate publică, serviciu sau alt organism care prelucrează date cu caracter personal în numele operatorului.
- **Destinatar:** orice persoană fizică sau juridică, autoritate publică, serviciu sau orice alt organism căruia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu

terț. Cu toate acestea, autoritățile publice cărora li se dezvăluie date cu caracter personal în cadrul unei competențe speciale de anchetă conformă cu legea Uniunii sau cu legea unui Stat membru nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice în cauză este conformă cu regulile aplicabile cu privire la protecția datelor în funcție de scopurile prelucrării.

### **3. Principii cheie**

---

RGPD reafirmă principiile esențiale în vigoare în conformitate cu Directiva 95/46. De asemenea, au fost introduse noi măsuri de conformitate.

#### **3.1. Principii reafirmate**

---

##### **3.1.1. Principiul scopului: o utilizare reglementată a datelor cu caracter personal**

**Datele cu caracter personal nu pot fi colectate și prelucrate decât în scopul determinat explicit și legitim, care corespunde cu obiectivele urmărite de avocatul operator.**

Astfel, în scop ilustrativ, atunci când accesează serverul profesional de date cadastrale al direcției generale de impozite, un avocat nu trebuie să compromită viața privată a persoanei la care se referă aceste informații, în special prin utilizarea informațiilor în scopuri de prospectare comercială, demersuri politice sau electorale.

Orice utilizarea necorespunzătoare se pedepsește cu 5 ani de închisoare și amendă de 300.000 euro (articolul 226-21 al codului penal).

##### **3.1.2. Principiul proporționalității**

Doar informațiile adecvate, pertinente și necesare scopului prelucrării pot reprezenta obiectului prelucrării de date cu caracter personal.

De exemplu, nu trebuie să se înregistreze informațiile referitoare la familia unei persoane atunci când, cu privire la scopurile prelucrării și la natura cauzei, sunt necesare doar elementele referitoare la viața profesională a acesteia.

##### **3.1.3. Principiul unei durate limitate de stocare a datelor**

Informațiile care figurează într-un fișier nu pot fi stocate pe termen nelimitat. Durata de stocare trebuie să fie stabilită în funcție de scopul fiecărui fișier.

De exemplu, înregistrările de supraveghere și protecție video nu trebuie, în principiu, să fie stocate mai mult de o lună. Datele cu caracter personal referitoare la clienți nu trebuie să fie stocate mai mult de un an de la sfârșitul relației contractuale, în dosarele actuale. Totuși, această obligație de a stabili o durată de limitată de stocare nu privează operatorii de posibilitatea de a arhiva informațiile, în special în scopuri probatorii. Atunci când arhivarea se realizează în formă electronică, trebuie să se respecte recomandarea nr. 2005-213 a CNIL



(Comisia Națională pentru Informatică și Libertăți) din 11 octombrie 2005 privind arhivarea electronică a datelor cu caracter personal în sectorul privat.

#### **3.1.4. Principiile de securitate și de confidențialitate**

Datele incluse în fișiere nu pot fi consultate decât de persoanele autorizate să aibă acces la acestea în funcție de misiunea lor. Dosarele avocaților nu pot fi comunicate decât persoanelor autorizate în acest scop, în special în aplicarea dispozițiilor legislative specifice și sub rezerva respectării secretului profesional.

Avocatul, în calitate de operator, are obligația de securitate. De asemenea, acesta trebuie să ia toate măsurile necesare pentru a garanta confidențialitatea și pentru a evita divulgarea informațiilor.

De exemplu, este necesar să se asigure faptul că fiecare persoană autorizată să aibă acces la informații are o parolă individuală (în cazul în care autentificarea se bazează doar pe un element de identificare și o parolă, aceasta trebuie să aibă minim 12 caractere, mici și majuscule, cifre și caractere speciale și să fie reînnoită cu regularitate) și că drepturile de acces sunt definite cu precizie în funcție de necesitățile reale.

#### **3.1.5. Principiul respectării drepturilor omului**

Articolul 13 al RGPD stipulează comunicarea informațiilor de mai jos atunci când datele sunt colectate de la persoanele în cauză:

- coordonatele operatorului și, dacă este cazul, cele ale reprezentantului operatorului;
- dacă este cazul, coordonatele responsabilului cu protecția datelor;
- scopurile prelucrării pentru care sunt destinate datele cu caracter personal;
- baza juridică a prelucrării;
- interesele legitime urmărite de către operator sau de către un terț atunci când aceste interese legitime reprezintă condiția legalității prelucrării;
- faptul că operatorul are intenția de a efectua un transfer de date cu caracter personal către o țară terță;
- dacă este cazul, existența sau absența unei decizii de adecvare emisă de CNIL, referirea la garanțiile corespunzătoare sau adaptate și mijloacele de obținere a unei copii sau locul în care acestea au fost puse la dispoziție;
- durata de stocare a datelor cu caracter personal sau, atunci când acest lucru nu este posibil, criteriile utilizate pentru determinarea acestei durate;
- existența dreptului de a solicita operatorului accesul la datele cu caracter personal, rectificarea sau ștergerea acestora, sau limitarea prelucrării cu referire la persoana în cauză, sau a dreptului de a se opune prelucrării și dreptului la portabilitatea datelor;
- atunci când prelucrarea este fondată pe consimțământul persoanei în cauză, existența dreptului de a-și retrage consimțământul în orice moment, fără a aduce prejudicii legalității prelucrării fondate pe consimțământ, efectuată înainte de retragerea acestuia;
- dreptul de a depune o plângere la autoritatea de control;

- informațiile referitoare la posibilitatea în care obligația de furnizare a datelor cu caracter personal este de reglementare sau contractuală sau la posibilitatea în care aceasta condiționează încheierea unui contract și în care persoana în cauză trebuie să furnizeze datele cu caracter personal, precum și cu privire la consecințele eventuale ale nefurnizării acestor date;
- existența luării automate a deciziilor, inclusiv a unei profilări și, cel puțin în aceste cazuri, informațiile utile referitoare la logica subiacentă, precum și importanța și consecințele prevăzute de prelucrare pentru persoana în cauză.

Articolul 14 al RGPD prezintă informațiile care trebuie să fie furnizate atunci când datele cu caracter personal nu sunt colectate direct de la persoana în cauză. Acesta este cazul în special atunci când, în cadrul unui dosar, clientul transmite avocatului informații referitoare la partea adversă. Aceste informații includ datele cu caracter personal ale părții adverse care, prin urmare, vor fi colectate indirect de către avocat.

Articolul 14 al RGPD prevede faptul că persoana trebuie să fie informată cu privire la elementele stipulate în articolul 13 al RGPD, dar și cu privire la categoriile de date cu caracter personal în cauză și sursa de proveniență a datelor cu caracter personal și, dacă este cazul, o mențiune care să indice faptul că acestea provin sau nu din surse accesibile publicului.

Astfel de informații ar pune avocatul în dificultate, întrucât respectarea acestei obligații ar implica informarea părții adverse cu privire la constituirea dosarului de către avocat și, prin urmare, punerea în pericol a intereselor clientului său. Din acest motiv, RGPD stipulează în articolul 14 alineatul 5, d) o excepție de la informarea persoanelor ale căror date cu caracter personal sunt colectate indirect, atâta timp cât datele respective trebuie să rămână confidențiale în virtutea obligației reglementate privind secretul profesional.

Atunci când acționează în calitate de operator, avocații au libertatea de a determina mijloacele care trebuie aplicate pentru a asigura informarea persoanelor.

Orice persoană are dreptul de a se opune, din motive legale, la prelucrarea datelor cu caracter personal, cu excepția cazului în care prelucrarea în cauză este obligatorie.

De asemenea, persoanele fizice care își justifică identitatea au dreptul de a adresa întrebări operatorului de date cu caracter personal în special pentru:

- verificarea existenței datelor lor;
- obținerea comunicării de date într-o formă ușor de înțeles, pe de o parte, și a tuturor informațiilor disponibile privind originea lor, pe de altă parte;
- obținerea de informații cu privire la scopul prelucrării, datele colectate și destinatari.

### **3.2. Noile măsuri de conformitate**

RGPD are drept obiectiv modernizarea cadrului european al protecției datelor cu caracter personal cu scopul de a lua în considerare progresele tehnologice și de a armoniza legislațiile Statelor membre ale Uniunii Europene.

Practic, scopul este:

- De a consolida drepturile persoanelor, în special prin crearea de drepturi la limitare, dreptul de a fi uitat, dreptul la portabilitatea datelor cu caracter personal și prin crearea de dispoziții specifice minorilor;
- De a responsabiliza persoanele care prelucrează datele (operatori și subcontractanți);
- De a favoriza reglementarea datorită unei cooperări consolidate între autoritățile de protecție a datelor, care vor putea, în special, să adopte sancțiuni consolidate și decizii comune cu privire la prelucrările transnaționale.

Prin RGPD, responsabilitatea organismelor este consolidată: acestea vor trebui să asigure în permanență protecția optimă a datelor și să fie în măsură să demonstreze conformitatea prelucrării acestora, lucru care implică documentarea acestei conformități.

Principalele măsuri impuse de RGPD sunt următoarele:

- Integrarea conceptelor de protecție a datelor în momentul proiectării de produse noi sau servicii și în mod implicit. Atunci când avocatul își dezvoltă practicile, acesta trebuie să își pună întrebări ab initio cu privire la impactul dezvoltării asupra datelor pe care le prelucrează. Acest lucru implică în special integrarea dispozitivelor tehnice de protecție a datelor cu caracter personal și a măsurilor organizaționale care permit limitarea riscurilor de a prejudicia drepturile și libertățile omului;
- Conformarea cu principiul de răspundere care impune cabinetelor să preconstituie dovada conformității acestora;
- Notificarea către CNIL a oricărei încălcări cu privire la datele cu caracter personal;
- Desemnarea, în cazul îndeplinirii condițiilor, unui responsabil cu protecția datelor sau a unui Data Protection Officer (DPO).

Atunci când acționează în calitate de operator, avocatul are obligația, în termenii articolului 28 al RGPD, de a asigura faptul că furnizorul de servicii IT, în calitate de subcontractant, a aplicat măsuri tehnice și organizatorice adaptate care îi permit să respecte securitatea și confidențialitatea datelor. Încheierea unui contract este obligatorie între avocat și subcontractanții acestuia și trebuie să rezerve un audit pentru a permite verificarea aplicării conforme a măsurilor menționate anterior.

### **3.2.1. Notificarea privind orice încălcare a datelor cu caracter personal**

În virtutea articolelor 33 și 34 ale RGPD, un cabinet de avocatură care acționează în calitate de operator trebuie să notifice orice încălcare a datelor cu caracter personal autorității de control și să informeze persoanele în cauză în caz de risc ridicat asupra drepturilor și libertăților omului. În acest sens, se face trimitere la fișa practică nr. 9 „Procedura în caz de încălcare a datelor”.

### **3.2.2. Minimizarea datelor**

Principiul de minimizare a datelor, sau „limitarea datelor la minim” este principiul conform căruia datele cu caracter personal nu pot fi prelucrate decât dacă scopurile prelucrării nu pot fi realizate prin prelucrarea informațiilor care nu conțin date cu caracter personal.

Acest lucru constă în:

- analiza necesității prelucrării datelor cu caracter personal pentru realizarea scopurilor urmărite prin prelucrare;

- dacă prelucrarea datelor cu caracter personal se dovedește necesară, limitarea prelucrării datelor la minim, cu privire la:
- categoriile datelor prelucrate;
- volumul sau cantitatea datelor prelucrate;
- cunoașterea posibilității în care datele colectate sunt mai mult sau mai puțin necesare pentru prelucrare.

### **3.2.3. Dreptul de fi uitat**

Articolul 17 din RGPD stipulează dreptul la ștergere („dreptul de a fi uitat”): persoanele în cauză au dreptul de a obține din partea operatorului, cât mai curând posibil, ștergerea datelor lor cu caracter personal.

Această prevedere își are originea în cauza Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, în care Curtea a judecat faptul că persoanele fizice au dreptul (sub rezerva anumitor condiții și garanții) de a solicita un motor de căutare pentru ștergerea link-urilor care fac trimitere la datele personale ale acestora. Dreptul de a fi uitat sau dreptul la ștergere, înscris în RGPD, depășește deferirea vizată în decretul menționat de Google. Este relativ și presupune efectuarea unui control al proporționalității dintre interesele persoanei în cauză și cele ale operatorului sau, dacă este cazul, ale publicului în general (dreptul la informații sau interes istoric).

Pentru avocat, ștergerea ireversibilă a datelor unui client nu va putea să fie aplicată înainte de expirarea duratei de prescripție a răspunderii civile profesionale a avocatului. Într-adevăr, este important să reținem că, în mod evident, dreptul de a fi uitat nu prevalează asupra anumitor obligații de arhivare a datelor pe perioade determinate, de exemplu din motive referitoare la respectarea obligațiilor fiscale sau de prescripție.

### **3.2.4. Evaluările impactului**

În virtutea articolului 35 al RGPD, atunci când există posibilitatea ca un tip de prelucrare să genereze un **risc ridicat pentru drepturile și libertățile persoanelor fizice**, în special **prelucrarea la scară largă a categoriilor speciale de date**, operatorul trebuie să efectueze, înainte de orice implementare, o evaluare a impactului.

Este important să se rețină **considerentul 91 al RGPD care stipulează că prelucrarea datelor cu caracter personal ale clienților de către un avocat independent nu trebuie să fie considerată o prelucrare la scară largă.**

**Cu toate acestea, chiar dacă nu ar prelucra datele la „scară largă”, un cabinet de avocatură, indiferent de dimensiunea acestuia, este posibil să trebuiască să efectueze evaluări ale impactului în cazul în care prelucrările implementate respectă anumite caracteristici.**

Într-adevăr, atunci când sunt îndeplinite mai mult de două noi criterii stabilite de către CNIL și prin G29 (evaluare/scoring, decizie automată cu efect juridic sau similar; supraveghere sistematică; colectare de date sensibile; colectare de date cu caracter personal la scară largă;

încrucișarea datelor; persoane vulnerabile; utilizare inovatoare; excluderea beneficiului de drept / contract), prelucrarea va fi, din principiu, supusă unei evaluări a impactului.

Deși reprezintă o sarcină suplimentară, scopul evaluărilor impactului este de a permite operatorilor să identifice și să trateze riscurile care nu ar fi detectate în alte momente și de a împiedica încălcările care s-ar produce în caz contrar.

Pentru a explica articolul 35 și prin propunerea unei interpretări comune, autoritățile de protecție a datelor europene (G29) au adoptat „liniile directoare” privind DPIA (Evaluarea Impactului asupra Protecției Datelor) și prelucrările care pot produce riscuri:

<http://www.cnil.fr/fr/reglement-europeen/lignes-directrices>

La data de 29 ianuarie 2018, CNIL a publicat online pe pagina sa de internet noua versiune a software-ului său open source PIA, facilitând efectuarea și formalizarea evaluării impactului asupra protecției datelor așa cum se stipulează în RGPD:

<http://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel>.

De asemenea, CNIL a publicat trei cataloage de bune practici pentru tratarea riscurilor pe care prelucrările datelor cu caracter personal (DCP) le pot genera cu privire la libertățile și viața privată a persoanelor în cauză:

<http://www.cnil.fr/fr/PIA-privacy-impact-assessment>

### **3.2.5. Portabilitatea datelor**

**Definiție.** Dreptul la portabilitatea datelor permite persoanelor în cauză să solicite operatorilor să transmită datele lor cu caracter personal unui alt operator, fără ca operatorul care a colectat inițial datele să se opună acestui transfer.

Portabilitatea înseamnă:

- „dreptul de a primi datele cu caracter personal pe care le-au furnizat unui operator, în format structurat, utilizat în mod frecvent și în formă lizibilă electronică și de a le transmite unui alt operator [...]”
- dreptul de a obține doar datele care sunt transmise direct de un operator la altul atunci când „acest lucru este posibil din punct de vedere tehnic”<sup>1</sup>.

**Condiții.** Acest lucru înseamnă că avocatul care a prelucrat inițial datele cu caracter personal este obligat să comunice datele cu caracter personal referitoare la clientul său unui coleg, atunci când prelucrarea inițială se bazează pe unul dintre următoarele fundamente:

- clientul și-a exprimat consimțământul pentru prelucrarea datelor sale cu caracter personal sau prelucrarea este necesară pentru executarea unui contract încheiat de către client sau pentru implementarea măsurilor precontractuale luate la cererea clientului;
- și prelucrarea este efectuată cu ajutorul proceselor automatizate.

---

<sup>1</sup> Regulamentul (UE) nr. 2016-679 din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, articolul 20§2.

Astfel, avocatul va trebui să respecte solicitarea clientului său în cazul în care acesta din urmă solicită transmiterea datelor sale cu caracter personal către un coleg sau transmiterea acestora în format structurat, utilizat în mod frecvent și în formă lizibilă electronică.

În schimb, dreptul la portabilitatea datelor nu se exercită atunci când prelucrarea este necesară pentru executarea unei misiuni de interes public sau relevantă pentru exercitarea autorității publice cu care este investit operatorul<sup>2</sup>.

**Excepția dosarelor tipărite.** În conformitate cu G29<sup>3</sup>, „dreptul la portabilitatea datelor se aplică doar dacă prelucrarea datelor «este efectuată cu ajutorul proceselor automatizate» și, prin consecință, nu acoperă majoritatea dosarelor tipărite. Prin urmare, s-ar părea că dosarele tipărite ale avocaților sunt excluse de la dreptul la portabilitatea datelor personale.

**Sucesiunea avocaților în același dosar.** În orice caz, avocații trebuie să respecte reguli specifice referitoare la succesiunea avocaților în același dosar. Într-adevăr, articolul 9.2 al Regulamentului intern național privind profesia de avocat stipulează că „avocatul destituit, care nu dispune de niciun drept de retenție, trebuie să transmită imediat toate elementele necesare pentru cunoașterea deplină a dosarului”.

### **3.2.6. Capacitatea de a monitoriza destinarii datelor cu caracter personal**

Operatorii de date trebuie să fie în măsură să monitorizeze și să identifice destinarii datelor cu caracter personal pe care le prelucrează.

### **3.2.7. Păstrarea unui registru al activităților de prelucrare**

În anumite cazuri, RGPD impune operatorilor să păstreze un registru al activităților de prelucrare efectuate sub responsabilitatea acestora.

În acest sens, aceștia trebuie să consulte fișa practică nr. 10 „Registrul activităților de prelucrare”.

---

<sup>2</sup> Regulamentul (UE) nr. 2016-679 din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, articolul 20§3.

<sup>3</sup> Linii directoare WP 242 ale G29, pag. 11.

## FIȘA PRACTICE

### FIȘA NR. 1. PRELUCRAREA „RU” (RESURSE UMANE)

---

#### **1. Ce este prelucrarea RH?**

---

În cadrul recrutării unui colaborator sau a personalului de sprijin (de exemplu, un informatician sau o secretară), gestionarea salariilor și gestionarea administrativă a personalului, avocatul angajator este obligat să prelucreze date cu caracter personal.

Astfel, este necesar ca avocații să prelucreze datele în conformitate cu RGPD.

În acest sens, trebuie remarcat faptul că articolul 88 al RGPD privind prelucrarea datelor cu caracter personal în cadrul relațiilor de muncă dispune ca Statele membre să păstreze flexibilitatea cu privire la regulile care urmează să fie adoptate.

#### **2. Care sunt datele pe care avocatul le poate colecta în cadrul prelucrării RU?**

---

**Recrutare.** În cadrul recrutării, datele nu trebuie să fie utilizate decât pentru evaluarea capacității candidatului de a ocupa locul pe muncă propus.

Pot fi colectate doar datele referitoare la calificarea și experiența colaboratorului (exemple: diplome, locuri de muncă anterioare, etc.)

Astfel, se interzice:

- Solicitarea exprimată unui candidat de a-și furniza numărul de securitate socială;
- Colectarea de date referitoare la familia candidatului;
- Colectarea de date referitoare la opiniile politice sau la calitatea candidatului de membru al sindicatului.

**Gestionarea administrativă a personalului.** În cadrul gestionării referitoare la colaboratorii săi și, într-un mod mai general, la personalul său, avocatul angajator poate colecta, în principal, două tipuri de date:

- Datele necesare pentru respectarea unei obligații legale.
- Datele utilizate pentru (i) gestionarea administrativă a personalului, (ii) organizarea activității și (iii) acțiunea socială.

**Respectarea minimizării.** În cadrul prelucrărilor RH și în conformitate cu articolul 5 al RGPD, avocatul nu trebuie să colecteze decât datele corespunzătoare, pertinente și strict necesare scopului prelucrării.

**Controlarea activității personalului.** Avocatul angajator poate utiliza diferite instrumente cu scopul de controla activitatea colaboratorilor sau a personalului.

De exemplu, cabinetele de avocatură ar putea să încadreze condițiile de utilizare a internetului de către colaboratorii și personalul său la locul de muncă. Acestea pot utiliza filtre pentru a bloca anumite conținuturi (pronografie, pedofilie, etc.). De asemenea, este posibilă limitarea utilizării internetului din motive de securitate, de exemplu descărcarea de software-uri, conectarea la un forum, etc.

**Controlarea timpului.** Un cabinet poate utiliza un software care permite calcularea timpului necesar avocatului pentru a lucra la un dosar sau la un caz. Cu toate acestea, software-ul respectiv nu poate fi folosit pentru controlarea activității colaboratorilor.

**Gestionarea și controlarea accesului la cabinetul de avocatură.** Un cabinet de avocatură poate utiliza dispozitive pentru a controla programul și accesul colaboratorilor și personalului.

### **3. Este necesar ca avocatul să îndeplinească formalități în cazul prelucrării RU?**

**Înainte de 25 mai 2018.** Prin aplicarea legii privind informatica și libertățile din 6 ianuarie 1978, operatorii trebuiau să depună declarații la CNIL înainte de efectuarea unei prelucrări de date cu caracter personal.

În ceea ce privește resursele umane, CNIL a adoptat standardele și autorizațiile pentru simplificarea acestui proces, în special standardul simplificat nr. 46 referitor la gestionarea resurselor umane ale organismelor publice și private, precum și scutirea DI-002 privind salariile angajaților sectorului privat. Aceste standarde pot fi de ajutor pentru cabinetele de avocatură în vederea stabilirii limitelor prelucrării datelor cu caracter personal.

**După 25 mai 2018.** RGDP reduce foarte mult formalitățile, dar, în schimb, introduce noi obligații pentru operator.

**Registrul activităților de prelucrare.** Registrul activităților de prelucrare prezintă informațiile referitoare la caracteristicile prelucrărilor efectuate de operator.

Această obligație nu se impune decât în anumite cazuri. A priori, cabinetele de avocatură trebuie să păstreze un registru al activităților de prelucrare în măsura în care acesta prelucrează ocazional date cu caracter personal și, în special, date sensibile (ex: date referitoare la sănătate, la originea rasială, etc.) sau date referitoare la condamnări și infracțiuni penale.

Prin urmare, este indicat să se includă în registrul activităților de prelucrare o fișă dedicată gestionării resurselor umane care trebuie să conțină următoarele elemente:

- Identitatea și coordonatele operatorului;
- Scopurile;
- Categoriile de persoane în cauză;
- Categoriile de date cu caracter personal;
- Categoriile de destinatari;



- Transferurile către o țară terță sau o organizație internațională;
- Termenul prevăzut pentru ștergere;
- Descrierea generală a măsurilor de securitate tehnice și organizatorice.

#### **4. Pentru cât timp pot fi stocate datele?**

---

Avocatul operator trebuie să definească o politică pentru durata stocării datelor în cadrul cabinetului său. Datele cu caracter personal nu pot fi stocate decât pentru perioada necesară îndeplinirii obiectivului urmărit în momentul colectării acestora. În general, datele referitoare la colaboratori sau la personal sunt stocate pe perioada prezenței acestora în cadrul cabinetului de avocatură prelungită cu durata prescripției legale.

#### **5. Este necesară informarea persoanelor în cauză?**

---

- În conformitate cu cerințele articolului 12 al RGPD, colaboratorii și angajați cabinetului de avocatură trebuie să fie informați cu privire la:
- Identitatea și coordonatele operatorului;
- Coordonatele responsabilului cu protecția datelor atunci când există unul;
- Obiectivul urmărit (gestionarea administrativă a personalului și recrutării);
- Baza juridică a prelucrării;
- Interesul legitim dacă este vorba de baza juridică a prelucrării;
- Destinatarul datelor (subcontractanții gestionării salarizării, etc.);
- Fluxurile transfrontaliere
- Durata stocării;
- Condițiile de exercitare a drepturilor de opoziție, de acces, de rectificare și de limitare, etc.;
- Dreptul de retragere a consimțământului dacă este vorba de baza juridică a prelucrării;
- Dreptul de a depune o plângere la o autoritate de control;
- Informațiile privind caracterul de reglementare sau contractual al prelucrării atunci când este vorba despre baza juridică a prelucrării.

Aceste informații pot figura în contractul de colaborare sau în contractul de muncă. Aceste informații pot, de asemenea, să reprezinte obiectul unui afiș sau al unei comunicări prin e-mail, în special pentru reglementarea situației cu privire la colaboratorii și la angajații care nu au fost informați în mod corespunzător.

#### **SARCINI DE EFECTUAT**

Asigurarea faptului că datele colectate nu sunt excesive cu privire la scopul prelucrării ☐  
Asigurarea faptului că există o bază juridică cu privire la prelucrarea datelor cu caracter personal ☐  
Respectarea principiului de minimizare ☐  
Verificarea dispozitivelor de controlare a activității angajaților și relevanța acestora ☐  
Înainte de 25 mai 2018: îndeplinirea formalităților necesare ☐  
După 25 mai 2018: păstrarea unui registru al prelucrărilor ☐  
Definirea unei politici privind durata stocării ☐

Informarea persoanelor în cauză privind prelucrarea datelor lor cu caracter personal ☐

## **FIȘA Nr. 2. GESTIONAREA CLIEŢILOR**

---

### **1. Ce date poate colecta avocatul în cadrul gestionării clienţilor săi?**

---

În cadrul exercitării profesiei de avocat, datele cu caracter personal referitoare la gestionarea clientelei corespund cu toate datele cu caracter personal necesare în constituirea dosarului clientului şi în apărarea intereselor acestora.

Cu privire la diversitatea domeniilor de intervenţie ale avocaţilor, aceste date pot fi diferite şi se pot referi la datele care ţin de viaţa personală şi profesională, dar nu pot face referire şi la datele care au o anumită sensibilitate.

**Date referitoare la condamnările penale şi la infracţiuni.** Avocatul poate avea obligaţia de a colecta datele referitoare la condamnările penale şi la infracţiuni. Natura specială a acestor date necesită garanţii specifice de prelucrare. Astfel, articolul 10 al RGPD stipulează faptul că prelucrarea nu poate fi efectuată decât sub controlul autorităţii publice sau în cazul în care garanţiile specifice şi adaptate sunt prevăzute de legislaţia naţională<sup>4</sup>.

Cu toate acestea, legea privind informatica şi libertăţile<sup>5</sup> stipulează faptul că prelucrarea acestor date poate fi efectuată de către **auxiliarii justiţiei pentru exercitarea misiunilor care le sunt încredinţate în conformitate cu legea**.

Proiectul de lege referitor la protecţia datelor cu caracter personal, aşa cum este redactat în prezent, păstrează această excepţie care permite auxiliarilor justiţiei să prelucreze datele referitoare la condamnările penale, la infracţiuni sau la măsurile de securitate conexe.

**Categorii speciale de date.** Avocatul poate fi obligat să prelucreze date cu caracter personal aşanumite speciale care dezvăluie originea rasială sau etnică, opiniile publice, convingerile religioase sau filosofice sau calitatea de membru al unui sindicat, la fel ca şi prelucrarea datelor genetice şi a datelor biometrice în scopul identificării unei persoane fizice în manieră unică, date referitoare la sănătate sau date referitoare la viaţa sexuală sau orientarea sexuală a unei persoane fizice.

Or, articolul 9, alineatul 1 al RGPD stipulează interzicerea, în principiu, a prelucrării acestor date. Prelucrarea datelor speciale poate avea legătură cu un număr mare de avocaţi, în special cei specializaţi în legislaţia din domeniul sănătăţii sau în legislaţia privind vătămarea corporală.

Cu toate acestea, articolul 9 stipulează o excepţie de la alineatul 2.f) pentru „prelucrarea necesară pentru constatarea, exercitarea sau apărarea dreptului în justiţie sau de fiecare dată când jurisdicţiile acţionează în cadrul funcţiei jurisdicţionale a acestora”. Prin urmare, se pare că avocaţii beneficiază de o excepţie care le permite să prelucreze datele speciale cu scopul de a-şi

---

<sup>4</sup> Regulamentul (UE) 2016/679 din 27.04.2016, art. 10 şi prin luarea în considerare a art. 19

<sup>5</sup> Legea nr. 78-17 din 06.01.1978, modificată, art. 9.

exercita profesia atâta timp cât datele în cauză sunt strict necesare pentru constatare, pentru exercitarea sau apărarea dreptului clientului său în justiție. Se recomandă o apreciere strictă a acestei necesități.

**Respectarea principiului de minimizare.** În conformitate cu articolul 5 al RGPD, avocatul nu trebuie să colecteze decât datele corespunzătoare, pertinente și strict necesare în scopul prelucrării.

Or, se întâmplă adesea ca avocații să primească foarte multe informații referitoare la clienții săi. Cu scopul de a respecta principiul minimizării, ori de câte ori este posibil se recomandă consilierea clientului atunci când acesta furnizează date cu caracter personal avocatului cu privire la documentele care sunt necesare pentru a-l reprezenta și a-l consilia.

## **2. Este necesar ca avocatul să îndeplinească formalități?**

---

**Înainte de 25 mai 2018.** În aplicarea legii privind informatica și libertățile din 6 ianuarie 1978, operatorii trebuiau să depună declarații la CNIL înainte de prelucrarea datelor cu caracter personal.

În ceea ce privește gestionarea clienților, CNIL a adoptat scutirile și standardele pentru simplificarea acestui proces, în special standardul simplificat nr. 48 referitor la gestionarea fișierelor clienților și prospectelor, precum și scutirea DI-007 privind informarea și comunicarea externă. Aceste standarde pot fi de ajutor pentru cabinetele de avocatură în vederea stabilirii limitelor prelucrării datelor cu caracter personal.

**După 25 mai 2018.** RGPD exclude multe formalități, dar, în schimb, introduce noi obligații pentru operator.

**Registrul activităților de prelucrare.** Registrul activităților de prelucrare prezintă informațiile referitoare la caracteristicile prelucrărilor efectuate de operator.

Această obligație nu se impune decât în anumite cazuri. A priori, cabinetele de avocatură trebuie să păstreze un registru al activităților de prelucrare în măsura în care acesta prelucrează ocazional date cu caracter personal și, în special, date sensibile (ex: date referitoare la sănătate, la originea rasială, etc.) sau date referitoare la condamnări și infracțiuni penale.

Prin urmare, este indicat să se includă în registrul activităților de prelucrare o fișă dedicată gestionării resurselor umane care trebuie să conțină următoarele elemente:

- Identitatea și coordonatele operatorului;
- Scopurile;
- Categoriile de persoane în cauză;
- Categoriile de date cu caracter personal;
- Categoriile de destinatari;
- Transferurile către o țară terță sau o organizație internațională;
- Termenul prevăzut pentru ștergere;
- Descrierea generală a măsurilor de securitate tehnice și organizatorice.

### **3. Pentru cât timp pot fi stocate datele?**

---

Avocatul operator trebuie să definească o politică pentru durata stocării datelor în cadrul cabinetului său. Datele cu caracter personal nu pot fi stocate decât pentru perioada necesară îndeplinirii obiectivului urmărit în momentul colectării acestora.

În general, datele referitoare la clienți pot fi stocate pe perioada relației contractuale dintre avocat și clientul acestuia. În plus, datele trebuie să fie arhivate pentru perioada în care responsabilitatea avocatului ar putea fi implicată înainte de ștergerea definitivă a datelor.

### **4. Este necesară informarea persoanelor în cauză?**

---

În conformitate cu cerințele articolului 13 al RGPD, clienții și eventualii clienți ai cabinetului de avocatură trebuie să fie informați cu privire la:

- Cu privire la identitatea și coordonatele operatorului (cabinetul);
- Coordonatele responsabilului cu protecția datelor atunci când există unul;
- Obiectivul urmărit (gestionarea și monitorizarea dosarelor clienților);
- Baza juridică a prelucrării (executare contractuală sau precontractuală la cererea clientului);
- Interesul legitim dacă este vorba de baza juridică a prelucrării;
- Destinatarii datelor (subcontractanți, executori judecătorești, etc.);
- Fluxurile transfrontaliere;
- Durata stocării;
- Drepturile de care dispun;
- Condițiile de exercitare a acestor drepturi;
- Dreptul de retragere a consimțământului dacă este vorba de baza juridică a prelucrării;
- Dreptul de a depune o plângere la o autoritate de control;
- Informațiile privind caracterul de reglementare sau contractual al prelucrării atunci când este vorba despre baza juridică a prelucrării.

Aceste informații pot figura în cadrul acordului de taxe. Aceste informații pot, de asemenea, să reprezinte obiectul unei comunicări prin e-mail sau cu ocazia transmiterii unei note de taxe, în special pentru reglementarea situației cu privire la clienții care nu au fost informați în mod corespunzător.

### **5. Securitatea dosarelor clienților**

---

Este necesar să se ia măsuri de securitate adaptate la sensibilitatea prelucrărilor. În afară de această cerință a RGPD, avocatul trebuie să respecte secretul profesional absolut și, din acest motiv, trebuie să asigure securitatea datelor care îi sunt încredințate de către clienți.

Pentru a proceda întocmai, este necesar să se verifice faptul că accesul la spațiile în care sunt stocate dosarele este securizat îndeajuns (birourile sunt încuiate cu cheie, accesul se face cu

badge-ul, etc.). De asemenea, se recomandă verificarea securității sistemului de informații în care sunt stocate dosarele în format digital (firewall, parole puternice pentru acces, autorizații, etc.).

## **6. Solicitare personalizată**

---

În afara respectării cerințelor menționate anterior, regulile speciale se aplică pentru solicitarea personalizată pe cale electronică sau prin poștă.

În acest sens, se face trimitere la Vademecumul comunicării avocaților, publicat în 2016 de către Consiliul național al barourilor:

[http://encyclopedia.avocats.fr/GED\\_BWZ/107763592594/CNB-2016-03-17](http://encyclopedia.avocats.fr/GED_BWZ/107763592594/CNB-2016-03-17)

[Ru\\_Communication-des-avocats-Vade-mecum\[Version-2016-03-16\].pdf](#)

## **SARCINI DE EFECTUAT**

Asigurarea faptului că datele colectate nu sunt excesive cu privire la scopul prelucrării ☐

Asigurarea faptului că există o bază juridică cu privire la prelucrarea datelor cu caracter personal ☐

Respectarea principiului de minimizare ☐

Înainte de 25 mai 2018: îndeplinirea formalităților necesare ☐

După 25 mai 2018: păstrarea unui registru al prelucrărilor ☐

Definirea unei politici privind durata stocării ☐

Informarea persoanelor în cauză privind prelucrarea datelor lor cu caracter personal ☐

Asigurarea faptului că dosarele digitale și fizice ale clienților sunt protejate corespunzător ☐

Verificarea securității sistemului informatic împreună cu furnizorul de servicii IT ☐

## **FIȘA Nr. 3. SUPRAVEGHERE VIDEO ȘI PROTECȚIE VIDEO**

### **1. Ce este supravegherea video și protecția video?**

---

Regimul aplicabil diferă, în funcție de locul în care sunt instalate camerele. Într-adevăr, este necesar să se distingă între supravegherea video și protecția video deoarece fiecare are propriul regim:

- **Protecția video** face referire la camerele situate în locurile deschise publicului, și anume, de exemplu, holurile de intrare, împrejurimile unui imobil și recepția clădirii în care se situează cabinetul de avocatură.
- **Supravegherea video** face referire la camerele instalate în zonele rezervate membrilor cabinetului, ca spre exemplu birourile, rezervele sau holurile cabinetului de avocatură, etc.

Indiferent de regimul aplicabil, CNIL are competență pentru a efectua controale ale dispozitivelor de protecție video, precum și ale dispozitivelor de supraveghere.

### **2. Care este obiectivul instalării camerelor?**

---

Instalarea camerelor de protecție video și de supraveghere video trebuie să aibă drept scop siguranța bunurilor și persoanelor atunci când aceste locuri sunt expuse în special riscurilor de agresiune sau de furt, în scopul prevenirii acestora sau pentru a permite identificarea autorilor de furturi, daune sau agresiuni.

În virtutea dreptului la respectarea vieții private (articolul 9 al Codului civil), supravegherea video nu poate în niciun caz să aibă drept scop filmarea membrilor cabinetului la locul de muncă al acestora, în zonele de pauză, la toaletă sau în cadrul sediului unității sau filmarea reprezentanților sindicali.

### **3. Care sunt formalitățile care trebuie îndeplinite?**

---

#### **3.1. Înainte de intrarea în vigoare a RGPD**

---

Dispozitivele de protecție video și de supraveghere video sunt foarte reglementate și nu pot fi instalate decât după îndeplinirea anumitor formalități.

Formalitățile sunt diferite, în funcție de tipul dispozitivului instalat.

În cazul în care camerele se află sub rezerva prevederilor Codului de securitate internă, este necesară o autorizație din partea prefecturii departamentului (Prefectul de poliție din Paris) (art. L251-1 și următoarele ale Codului de securitate internă).

În cazul în care camerele se află sub rezerva prevederilor legii privind informatica și libertățile, acestea trebuie să reprezinte obiectul unei declarații normale la CNIL.

TIPUL DISPOZITIVULUI	EXEMPLU	FORMALITĂȚI DE ÎNDEPLINIT
Camera este situată în cabinetul de avocatură închis publicului	Birouri, rezerve, camera de reprografie, holurile cabinetului de avocatură, etc.	Formalități prealabile la CNIL
Camera este situată într-un spațiu public sau deschis publicului, iar <b>imaginile sunt înregistrate sau stocate</b> în prelucrările informatizate sau fișierele structurate care permit identificarea persoanelor fizice	Sala de așteptare, clădirea cabinetului de avocatură, holul de intrare, etc.	Autorizație de la prefectură
Camera este situată într-un spațiu public sau deschis publicului și <b>nicio imagine nu este înregistrată sau stocată</b> în prelucrările informatizate sau fișierele structurate care permit identificarea persoanelor fizice		

### **3.2. După intrarea în vigoare a RGPD**

RGPD introduce noi obligații pentru operatori.

**Registrul activităților de prelucrare.** Registrul activităților de prelucrare include informațiile referitoare la prelucrarea efectuată.

Această obligație nu se impune decât în anumite cazuri. A priori, cabinetul de avocatură trebuie să păstreze un registru al activităților de prelucrare în măsura în care acesta prelucrează ocazional date cu caracter personal și, în special, date sensibile (ex: date referitoare la sănătate, date referitoare la originea rasială, etc.) sau date care au legătură cu condamnările și infracțiunile penale.

Prin urmare, se recomandă includerea în registrul activităților de prelucrare a unei fișe pentru supravegherea video/ protecția video care trebuie să aibă următoarele elemente:

- Identitatea și coordonatele operatorului;
- Scopurile
- Categoriile de persoane în cauză;
- Categoriile de date cu caracter personal:

- Categoriile de destinatari;
- Transferul către o țară terță sau o organizație internațională;
- Termenul prevăzut pentru ștergerea datelor;
- Descrierea generală a măsurilor tehnice și organizatorice de securitate.

#### **4. Este necesară informarea persoanelor în cauză?**

---

Persoanele în cauză, de exemplu clienții, membrii cabinetului, colegii sau prestatorii, trebuie să fie informate în legătură cu existența dispozitivului instalat.

Această informare trebuie să fie asigurată printr-un panou afișat în mod vizibil în locurile corespunzătoare (intrarea în clădire). Aceste informații trebuie să includă cel puțin:

- existența dispozitivului;
- numele responsabilului;
- procedura care trebuie urmată pentru a solicita accesul la înregistrările video care îi interesează;
- numărul de telefon.

Organismele reprezentative ale angajaților, dacă acestea există în cadrul cabinetului, trebuie să fie consultate înainte de instalarea sistemului de supraveghere video.

În orice caz, fiecare membru al cabinetului va trebui să fie informat individual, printr-o notificare care poate fi sub formă de e-mail, de exemplu, și care respectă cerințele articolelor 13 și 14 ale RGPD.

#### **5. Cine are acces la imaginile înregistrate de camere?**

---

Imaginile înregistrate de camerele de protecție video și supraveghere video nu pot fi vizionate decât de persoanele autorizate în cadrul funcțiilor acestora (de exemplu, partener fondator sau persoana responsabilă pentru securitate). Aceste persoane trebuie să fie instruite și conștiente cu privire la regulile referitoare la instalarea unui astfel de sistem.

#### **6. Pentru cât timp pot fi stocate imaginile?**

---

Atunci când este vorba despre durata de stocare, CNIL menționează faptul că imaginile nu trebuie să fie stocate mai mult de câteva zile și că, în orice caz, durata de stocare a acestora nu poate depăși o lună.

Dacă se inițiază proceduri, imaginile trebuie să fie descărcate din dispozitiv (după înregistrarea acestei operațiuni într-un caiet special) și stocate pe durata procedurii.

TEMĂ	SARCINI DE EFECTUAT
	Identificarea camerelor <input type="checkbox"/>
	Stabilirea localizării camerelor și a locurilor filmate <input type="checkbox"/>
	Limitarea accesului la imaginile înregistrate <input type="checkbox"/>



Generalități	După 25 mai 2018: întocmirea unui registru al activităților de prelucrare (recomandat) <input type="checkbox"/>
	Afișarea unui panou vizibil în locurile corespunzătoare <input type="checkbox"/>
	Consultarea organismelor reprezentative ale angajaților înainte de instalarea camerelor <input type="checkbox"/>
	Informarea individuală a angajaților (în special prin e-mail) <input type="checkbox"/>
	Limitarea duratei de stocare a imaginilor la o lună <input type="checkbox"/>
Protecție video	Solicitarea autorizației din partea prefecturii de care aparține departamentul <input type="checkbox"/>
Supraveghere video	Înainte de 25 mai 2018: Declarație normală la CNIL în prezența prelucrării datelor cu caracter personal <input type="checkbox"/>

**Pentru mai multe informații:**

[https://www.cnil.fr/sites/default/files/atoms/files/\\_videosurveillance\\_au\\_travail.pdf](https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf)

## **FIȘA NR. 4. FURNIZORII ȘI PRESTATORII DE SERVICII**

### **1. Ce este o persoană împuternicită?**

Conform art. 4, alin. 8 din GDPR, persoana împuternicită (procesatorul) este "persoana fizică sau juridică, autoritatea publică, agenția sau un alt organism care prelucrează date cu caracter personal în numele operatorului".

În practică, este, prin urmare, persoana care prelucrează datele personale în numele cabinetului de avocatură, cum ar fi un contabil, un editor de software, un furnizor gazdă etc.

### **2. Cum se procedează în caz de numire a unei persoane împuternicite?**

Articolul 28, alin. 3 din GDPR menține obligația încheierii unui contract între procesator și operator, definind limitele acestuia și stabilind cerințe mai stricte și mai importante. Astfel, contractul care stabilește un raport între cabinet și procesator trebuie să includă:

- obiectul;
- durata;
- natura;
- scopul;
- tipul de date cu caracter personal;
- categoriile de persoane vizate;
- drepturile și obligațiile operatorului;
- măsurile de securitate implementate în ceea ce privește prelucrarea datelor cu caracter personal care va fi efectuată.

De asemenea, actul juridic în cauză trebuie să definească obligațiile persoanei împuternicite referitoare la:

- posibilitatea prelucrării datelor numai pe baza instrucțiunilor documentate ale operatorului, chiar și în ceea ce privește fluxurile transfrontaliere;
- confidențialitatea datelor;
- exercitarea drepturilor persoanelor vizate;

- asistența care trebuie furnizată operatorului prin măsuri tehnice și organizatorice adecvate, în măsura posibilului, pentru îndeplinirea obligației de a răspunde la solicitările persoanelor vizate;
- asistența oferită operatorului pentru a se asigura respectarea obligațiilor sale ținând seama de natura prelucrării și de informațiile de care dispune persoana împuternicită;
- ștergerea datelor în cauză la sfârșitul prelucrării sau trimiterea acestora la operator sau păstrarea acestora, dacă există o obligație prevăzută de o dispoziție națională sau europeană;
- punerea la dispoziția operatorului a tuturor informațiilor necesare pentru a demonstra conformitatea cu aceste obligații și a permite efectuarea de audituri, inclusiv inspecții, de către operator sau de un alt auditor pe care l-a desemnat, și pentru a contribui la aceste audituri;
- eventuala recrutare de către persoana împuternicită a unui procesator ulterior, a unui nou procesator și obținerea autorizației scrise prealabile a operatorului în legătură cu această recrutare, care trebuie să fie formalizată printr-un contract care menționează toate obligațiile enumerate mai sus.

Prin urmare, clauzele contractuale care instituie un raport între procesatori și operatori vor trebui să fie mult mai precise în ceea ce privește modalitățile de tratament, precum și gestionarea relațiilor acestora și schimbul de informații între aceștia.

În conformitate cu articolul 28 alineatul (1) din GDPR, operatorul este obligat să recurgă numai la "procesatori care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru a se asigura că tratamentul respectă cerințele GDPR și garantează protecția drepturilor persoanei vizate".

### **3. Cum se procedează cu procesatorii cu care cabinetul de avocatură se află deja în relații comerciale?**

Cabinetele de avocatură vor trebui să chestioneze procesatorii cu privire la garanțiile pe care le-au instituit pentru a asigura conformitatea cu GDPR.

În cazul în care cabinetele de avocatură identifică deficiențe ale măsurilor luate de procesator, acestea vor trebui să încheie un act adițional la contract pentru a remedia aceste lacune.

### **RECOMANDĂRI**

Identificați diferiții procesatori ☐

Verificați conformitatea procesatorilor și măsurile luate în cadrul acordului de subcontractare ☐

Dacă este necesar, încheiați un act adițional la acordul de subcontractare ☐

### **FIȘA NR. 5. GESTIONAREA ACCESULUI LA CABINET**

La locul de muncă, asociații care acționează în calitate de angajator pot fi obligați să controleze accesul la spațiu sau la gestionarea unităților de tip restaurant (ecusoane

electronice, dispozitive biometrice ...). În mod similar, pot exista controale de acces pentru persoanele care se prezintă la cabinetul de avocatură.

### **1. Utilizarea ecusoanelor la locul de muncă**

Ecusoanele electronice (cartele magnetice sau cu cip) pot fi utilizate pentru a controla accesul la spații sau la unitățile de tip restaurant. Aceste dispozitive, care prelucrează date care permit identificarea persoanelor vizate, fac obiectul GDPR și trebuie să furnizeze toate garanțiile oferite de acesta persoanelor care fac obiectul colectării și prelucrării datelor lor personale.

#### **Ce garanții trebuie prevăzute?**

Fiecare trecere a ecusonului printr-un cititor permite înregistrarea datelor referitoare la deținătorul acestuia. Aceste înregistrări prezintă riscuri de utilizare abuzivă și pot urmări deplasările avocaților și salariaților în scopuri de supraveghere.

Prin urmare, cabinetul trebuie să prezinte garanții speciale pentru a preveni aceste utilizări abuzive. În special, este important să se precizeze:

- scopul dispozitivului (de exemplu, controlul accesului, gestionarea timpilor de prezență a angajaților, accesul la unitățile de tip restaurant etc.);
- informațiile colectate;
- serviciile destinate ale datelor;
- modalitățile de exercitare a drepturilor de acces la date și de rectificare a datelor.

Membrii unui cabinet de avocatură trebuie să fie pe deplin informați cu privire la aceste modalități înainte de implementarea sistemului.

Cabinetele de avocatură pot face referire la recomandările standardului NS 42 al CNIL pentru acest tip de tratament:

<https://www.cnil.fr/fr/declaration/ns-042-badges-sur-le-lieu-de-travail>

### **RECOMANDĂRI**

Informați membrii cabinetului despre modalitățile aplicate ☐

Consultați recomandările standardului NS 42 al CNIL ☐

### **2. Dispozitive biometrice**

Gestionarea accesului se poate face prin dispozitive biometrice care permit identificarea unei persoane prin caracteristicile sale fizice, biologice sau chiar comportamentale (secvență genetică, recunoaștere facială, amprente digitale etc.).

Articolul 9 din GDPR consideră că acest tip de date este deosebit de sensibil.

Tratamentul acestui tip de date este, în principiu, interzis, cu unele excepții: aceste date pot fi prelucrate numai în cazul în care au fost îndeplinite anumite condiții specifice și trebuie prelucrate cu măsuri de precauție și de siguranță suplimentare.

Persoanele vizate de un dispozitiv biometric trebuie să fie clar informate cu privire la condițiile de utilizare a acestuia, natura sa obligatorie sau facultativă, destinatarii informațiilor și modalitățile de exercitare a drepturilor lor de opoziție, acces și rectificare.

CNIL a adoptat două autorizații unice care reglementează acum toate dispozitivele pentru controlul accesului biometric la locurile de muncă, indiferent de tipul de biometrie utilizat.

Acestea disting:

- Dispozitivele biometrice care permit persoanelor să păstreze controlul asupra șablonului lor biometric (AU-052).
- Dispozitivele biometrice care nu garantează acest control (AU-053).

Autorizările unice adoptate fac parte din logica GDPR. Acestea includ premisele evaluării impactului asupra vieții private și conceptele de protecție a datelor din etapa de proiectare a produsului și ca setare implicită („privacy by design“ și „privacy by default“), cu care operatorii trebuie să se conformeze până în luna mai 2018.

CNIL intenționează să susțină din acest moment organizațiile în vederea conformității cu aceste noi reguli.

## **RECOMANDĂRI**

Să informeze persoanele în cauză ☐

Să facă referire la autorizațiile unice adoptate de CNIL ☐

## **FIȘA NR. 6. LUPTA ÎMPOTRIVA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI**

Reglementarea privind lupta împotriva spălării banilor și finanțării terorismului prevede o serie de obligații pentru avocați, dintre care unele constau în operațiuni de colectare și prelucrare a datelor cu caracter personal, în temeiul GDPR.

Colectarea de date și prelucrarea acestora pe această bază, care este impusă prin lege, depinde în mare măsură de un regim special și specific.

Avocatul care stabilește o „relație de afaceri“ cu un client trebuie să dea dovadă de vigilență constantă pe durata acesteia și să practice „o examinare atentă a operațiunilor efectuate, asigurându-se că sunt în concordanță cu cunoștințele actualizate“ pe care le deține cu privire la relația de afaceri (articolele L. 561-6 și R. 56112 CMF).

De asemenea, trebuie să colecteze "informații referitoare la scopul și natura acestei relații și orice alte informații relevante despre acel client".

Avocatul actualizează aceste informații pe întreaga durată a relației de afaceri (articolul L. 561-5-1, alineatul 1 CMF).

Astfel, pentru o persoană fizică, avocatul trebuie să prezinte originalul unui document oficial valabil cu fotografia clientului (art. R. 561-5, 1 și R. 561-6 CMF).

## **RECOMANDĂRI**

Copiați sau scanați documentul de identitate al clientului, păstrați copia acestuia și verificați, pe cât posibil, dacă nu este fals ☐

Identificați și păstrați într-un document specific următoarele informații:

- Nume
- Prenume
- Data și locul nașterii persoanei ☐
- Natura, data și locul emiterii documentului
- Numele și calitatea autorității sau a persoanei care a emis documentul și, după caz, l-a autentificat

Consiliul Național al Barourilor pune la dispoziția avocaților un formular care poate fi furnizat clientului și care susține obiectiv cererea de documente și informații:

[https://www.cnb.avocat.fr/sites/default/files/documents/cahier\\_blanchissement\\_2ed.pdf](https://www.cnb.avocat.fr/sites/default/files/documents/cahier_blanchissement_2ed.pdf).

Măsurile de vigilență și de identificare trebuie consolidate atunci când tranzacția este deosebit de complexă sau are o valoare neobișnuit de mare sau nu pare să aibă nicio justificare economică sau un scop legal (articolul L. 561-10-2 CMF).

Este necesară informarea și obținerea unor elemente complementare, adresând niște întrebări complementare.

Dacă informațiile obținute nu sunt considerate suficiente, avocatul trebuie să înregistreze în scris și să păstreze caracteristicile operațiunii, adică informațiile colectate și documentate referitoare în special la:

- originea și destinația sumelor utilizate pentru finanțarea operațiunii,
- obiectul operațiunii,
- caracteristicile operațiunii cu privire la cele patru condiții cumulate prezentate mai sus,
- identitatea clientului ordonator și a avândului/avânzilor-drept economici, precizând pentru fiecare dintre aceștia numele, adresa, naționalitatea și profesia.

Având în vedere puterea de control de care dispune Consiliul Baroului, în conformitate cu articolul 17, 13° din Legea din 31 decembrie 1971, avocatul trebuie să poată justifica Consiliului Baroului, după caz, că amploarea măsurilor pe care le-a luat este adecvată gradului de risc (articolul L. 561-5 CMF, articolul L.561-9, I CMF). Respectarea strictă a cerințelor de reglementare de mai sus este deja o dovadă a diligențelor realizate și a respectării obligației sale de supraveghere.

Documentele și informațiile, indiferent de suportul lor, referitoare la identitatea clienților obișnuiți sau ocazionali, trebuie păstrate timp de cinci ani de la încetarea relațiilor cu aceștia (articolul L. 561-12 CMF).

Același lucru se aplică, sub rezerva obligațiilor legate de practica profesională a avocatului, documentelor referitoare la operațiunile pe care le-a efectuat și documentelor care înregistrează caracteristicile operațiunilor în nume propriu sau în numele terților, efectuate cu persoane fizice sau juridice, inclusiv filiale sau unități ale acestora, situate, înmatriculate sau stabilite într-un stat sau pe un teritoriu a cărui legislație împotriva spălării banilor este considerată insuficientă (articolul L. 561-12 CMF).

Deoarece prelucrările în cauză care identifică persoane susceptibile de a participa la infracțiuni grave, sunt deosebit de sensibile, obligația privind securitatea datelor astfel colectate, care este atribuită operatorilor de către GDPR, trebuie exprimată aici integral.

Avocații pot crea site-uri web ca parte a activității lor profesionale pentru a-și promova cabinetul, a prezenta membrii cabinetului, a-și expune abilitățile sau a publica articole, dar site-ul poate permite, de asemenea, colectarea date cu caracter personal prin diverse mijloace:

- un chestionar online;
- o consultare online;
- un formular de contact;
- crearea unui cont online;
- cookie-uri etc.

### **1. Care sunt formalitățile care trebuie îndeplinite dacă avocatul colectează date cu caracter personal prin intermediul paginii sale web?**

**Înainte de 25 mai 2018**, dosarul poate fi declarat la/poate face obiectul CNIL:

- Dacă fișierul respectă un standard simplificat, trebuie făcută o declarație de conformitate cu acest standard. De exemplu, standardul simplificat nr. 48 pentru fișierele potențialilor clienți;
- Dacă fișierul nu respectă niciun standard, se va face o declarație normală.

**După 25 mai 2018**. GDPR reduce considerabil formalitățile, dar introduce, în schimb, noi obligații pentru operator.

**Registrul activităților de prelucrare.** Registrul activităților de prelucrare conține informațiile despre caracteristicile prelucrărilor efectuate de operator.

Această obligație este necesară numai în anumite cazuri. A priori, cabinetul de avocatură trebuie să țină o evidență a activităților de prelucrare în măsura în care se ocupă de date cu caracter personal neocazional și, în special, de date sensibile (de exemplu, date privind sănătatea, date privind originea rasială etc.) sau date referitoare la condamnări și infracțiuni penale.

Prin urmare, este indicat să se includă în registrul activităților de prelucrare o fișă dedicată prelucrării datelor de pe site-ul web, care trebuie să includă următoarele elemente:

- Identitatea și datele de contact ale operatorului;
- Scopuri;
- Categoriile de persoane;
- Categoriile de date cu caracter personal;
- Categoriile de destinatari;
- Transferuri către o țară terță sau o organizație internațională;
- Termenele limită pentru ștergere;
- Descrierea generală a măsurilor de securitate tehnică și organizatorică.

### **2. Ce mențiuni trebuie să fie prezente în mod obligatoriu pe site-ul avocatului?**

Pe site-ul avocatului trebuie să apară multe informații:

- Mențiunile juridice în temeiul Legii nr. 2004-575 din 21 iunie 2004 privind încrederea în economia digitală;
- Mențiunile obligatorii în conformitate cu articolele 10.2 și 10.3 din RIN (Fișa nr. 4 din Manualul pentru comunicare al avocaților: [http://encyclopedia.avocats.fr/GED\\_BWZ/107763592594/CNB-2016-03-17\\_Ru\\_Communicationdes-avocats-Vade-mecum\[Version-2016-03-16\].pdf](http://encyclopedia.avocats.fr/GED_BWZ/107763592594/CNB-2016-03-17_Ru_Communicationdes-avocats-Vade-mecum[Version-2016-03-16].pdf));

- Mențiunile privind informațiile rezultate din articolele 13 și 14 din GDPR;
- Mențiunile privind informațiile despre cookie-uri.

### 3. Ce trebuie să conțină diferitele mențiuni?

MENȚIUNI	TEXTE	INFORMAȚII
MENȚIUNI JURIDICE	Articolul 6 din Legea nr. 2004-575 din 21 iunie 2004 privind încrederea în economia digitală	Numele și denumirea cabinetului
		Adresa cabinetului principal
		Numărul de înmatriculare în Registrul comerțului și al societăților (atunci când este necesară înregistrarea)
		Coordonate poștale, telefonice și electronice ale cabinetului
		Numele și datele de contact ale directorului publicației site-ului
		Numele, denumirea, adresa și numărul de telefon al gazdei web
MENȚIUNI OBLIGATORII	Articolul 10.2 "Dispoziții comune pentru toate comunicările" din Regulamentul Intern Național privind profesia de avocat - RIN.	Precizarea calității (avocat)
		Identificarea (Doamna X, Cabinetul X)
		Furnizarea de informații despre localizarea acestuia (adresa cabinetului)
		Elemente care permit contactarea acestuia (nr. tel., nr. fax, adresa de e-mail)
		Menționarea Baroului la care este înregistrat avocatul
		Precizarea structurii de exercițiu din care face parte
MENȚIUNI PRIVIND INFORMAȚIILE GDPR	Articolele 13 și 14 din GDPR  Articolul 32 din Legea privind protecția datelor	Identitatea și datele de contact ale persoanei responsabile de fișier
		Datele de contact ale responsabilului cu protecția datelor

		Scopul și temeiul juridic al prelucrării datelor
		Interesele legitime urmărite dacă prelucrarea se face în temeiul juridic al prelucrării datelor
		Destinatarii sau categoriile de destinatari
		Perioada pentru care vor fi stocate datele
		Eventualele transferuri de date către state din afara UE
		Drepturile persoanelor vizate (dreptul de acces, de rectificare, de ștergere, de opoziție, de restricționare etc.)
		Dreptul de a retrage consimțământul în orice moment, dacă prelucrarea se face în temeiul juridic al prelucrării datelor;
MENȚIUNI DE INFORMAȚII PRIVIND COOKIE-URILE	Directivile din 25 noiembrie 2011 numite « Pachetul telecom » 2009/136/CE și 2009/140/CE  Ordonanța « Pachetul telecom » din 24 august 2011  Articolul 32 II din legea din 06 ianuarie 1978  Proiectul e-Privacy	Informațiile privind caracterul regulamentar sau contractual al tratamentului, atunci când se aplică temeiul juridic al prelucrării datelor
		Scopurile cookie-urilor
		Obținerea consimțământului utilizatorilor prin "anunțurile de consimțământ"
		Posibilitățile de refuz al cookie-urilor

#### 4. Ce este un modul cookie?

Cookie-urile sunt marcatori plasati și cititi în timpul consultării site-ului cabinetului de avocatură, citirii unui mesaj electronic, instalării sau utilizării unui software.

Cookie-urile și alți indicatori sunt, în general, destinați să analizeze navigarea și accesarea site-ului cabinetului de avocatură.



## **5. Cum se respectă utilizarea cookie-urilor pe site-ul avocatului?**

Într-o primă etapă, avocații sunt sfătuiți să verifice prezența actuală a cookie-urilor pe site-ul lor prin departamentul IT al cabinetului, al furnizorilor de servicii sau prin verificarea instrumentelor utilizate etc.

Apoi, este necesar să se determine tipurile de cookie-uri utilizate pe site-ul web al avocatului. Într-adevăr, unele module cookie necesită consimțământul utilizatorului, acesta fiind cazul:

- cookie-urilor publicitare;
- cookie-urilor " rețele sociale" generate de butoanele de partajare atunci când colectează date cu caracter personal fără consimțământul persoanelor interesate;
- unele module cookie pentru măsurarea audienței.

În acest caz, consimțământul trebuie acordat înainte de introducerea sau citirea modulelor cookie. Atât timp cât clientul nu și-a dat consimțământul, aceste cookie-uri nu pot fi depuse sau citite pe terminalul său.

## **RECOMANDĂRI**

Integrarea mențiunilor legale și obligatorii ☐

Asimilarea mențiunilor GDPR ☐

Înainte de 25 mai 2018: declarațiile CNIL, dacă există prelucrări ale datelor cu caracter personal ☐

După 25 mai 2018: Registrul activităților de prelucrare ☐

Identificarea prezenței cookie-urilor plasate pe site-ul web al avocatului ☐

Identificarea tipului de cookie-uri pe site-ul web ☐

Utilizarea unui anunț de colectare a consimțământului ☐

Integrarea mențiunilor pe cookie-uri ☐

## **FIȘA NR. 8. BUNE PRACTICI PENTRU SECURITATEA DATELOR**

### **1. De ce securitatea datelor cu caracter personal este importantă, în special, în prelucrările de date efectuate de către avocați?**

Este esențial să se asigure securitatea și confidențialitatea datelor prelucrate de cabinetele de avocatură, prin garantarea unui nivel de securitate adaptat riscului prelucrării de date.

Într-adevăr, avocatul are obligația de respectare a secretului profesional. Această obligație consolidează necesitatea punerii în aplicare a măsurilor de securitate în cabinetele de avocatură, deoarece, în cazul încălcării datelor personale ale clienților, secretul profesional este încălcat. Problema securității nu este, așadar, neînsemnată pentru avocat.

### **2. Ce măsuri de securitate fizică trebuie puse în aplicare?**

Este necesar să adoptați unele măsuri de securitate fizică în cabinetul dvs.:

- Limitați accesul la cabinet;
- Nu depozitați sau arhivați fișiere sau documente care conțin date cu caracter personal în birouri accesibile oricui;
- Instalați alarme în incinta cabinetului etc.

### **3. Ce măsuri de securitate logice / digitale trebuie puse în aplicare?**

Implementarea măsurilor de securitate permite asigurarea unui nivel de securitate adaptat riscului.

În special, se recomandă:

- **autentificarea utilizatorilor:** setarea unei parole de cel puțin 8 caractere care să conțină o literă majusculă, o literă minusculă, o cifră și un caracter special; nu o comunicați nimănui; nu o scrieți în clar pe hârtie; evitați pre-înregistrarea acesteia; schimbați-o în mod regulat.
- **Gestionați autorizările și sensibilizați utilizatorii:** stabiliți persoanele care au dreptul să acceseze datele cu caracter personal; eliminați permisiunile de acces învechite; întocmiți o carte informatică și anexați-o regulamentului intern, dacă există unul.
- **Securizați dispozitivele informatice mobile:** asigurați mijloace de criptare pentru laptopuri și dispozitive de stocare amovibile (chei USB, CD-uri, DVD-uri ...), evitați stocarea de date personale sensibile ale clienților pe acestea.
- **Creați copii de rezervă și asigurați continuitatea activității:** configurați copii de rezervă periodice, stocați materialele de rezervă într-un loc sigur etc.

#### 4. Cum se notifică și se raportează o încălcare a datelor cu caracter personal?

Consultați următoarea fișă nr. 9 "Procedura în cazul încălcării datelor".

#### RECOMANDĂRI

**Puneți în aplicare măsuri de securitate fizice:**

- Limitați accesul la cabinet ☐
- Verificați și securizați locația de stocare a fișierelor ☐
- Instalați și activați o alarmă ☐

**Puneți în aplicare măsuri de securitate logice:**

- Instalați măsurile de autentificare a utilizatorului ☐
- Gestionați autorizările și sensibilizați utilizatorii ☐
- Securizați dispozitivele informatice mobile ☐
- Creați copii de rezervă și asigurați continuitatea activității ☐

**Puneți în aplicare o carte informatică** ☐

**Puneți în aplicare proceduri de notificare privind încălcarea datelor personale** ☐

**Mai multe:** CNIL a publicat în ianuarie 2018, un ghid conținând măsurile de precauție de bază care trebuie puse în aplicare în mod sistematic:

<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>

## **FIȘA nr. 9. PROCEDURA ÎN CAZUL ÎNCĂLCĂRII DATELOR CU CARACTER PERSONAL**

**Notificarea către CNIL.** Încălcarea datelor cu caracter personal reprezintă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau dezvăluirea neautorizată a datelor cu caracter personal transmise, păstrate sau prelucrate în alt mod sau accesul neautorizat la astfel de date.

Cu excepția cazurilor în care încălcarea datelor nu este de natură să provoace un risc pentru drepturile și libertățile persoanelor fizice, este necesară notificarea acesteia în mod prompt către autoritatea de control competentă, și anume, CNIL, și, dacă este posibil, cel târziu în 72 de ore după ce a luat la cunoștință de aceasta (GDPR, articolul 33).

Această notificare trebuie să specifice, printre altele:

- natura încălcării datelor cu caracter personal (categorii și numărul aproximativ de persoane și înregistrări de date în cauză);
- numele și datele de contact ale DPO sau ale altui punct de contact de la care pot fi obținute informații suplimentare;
- consecințele probabile ale încălcării datelor;
- măsurile luate sau care trebuie luate pentru a atenua eventualele consecințe negative.
- Un formular de notificare a încălcărilor securității datelor cu caracter personal este pus la dispoziția operatorului de date pe site-ul CNIL: [https://www.cnil.fr/sites/default/files/typo/document/CNIL\\_Formulaire\\_Notification\\_de\\_Violations.pdf](https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf)

De asemenea, se recomandă:

- să se instituie măsuri de analiză a riscurilor presupuse de prelucrarea efectuată pentru drepturile și libertățile persoanelor fizice;
- să se asigure că încălcările sunt notificate în termen de 72 de ore, în caz contrar trebuie să se furnizeze explicații privind întârzierea către autoritatea de control competentă din statul în cauză;
- să se menționeze în notificare faptele privind încălcarea datelor, natura încălcării, efectele acesteia și măsurile luate pentru remedierea încălcării;
- să se depună toate eforturile pentru a documenta cât mai bine orice încălcare a datelor pentru a permite autorității de control să verifice respectarea cerințelor impuse de GDPR;
- să se pună în aplicare măsuri de urgență, astfel încât încălcarea datelor să poată fi remediată, iar consecințele acesteia atenuate.

În cazul în care cabinetul de avocatură are o persoană împuternicită, aceasta din urmă trebuie, de asemenea, să notifice operatorul despre orice încălcare a datelor cu caracter personal cât mai curând posibil după ce a luat la cunoștință de aceasta. Este recomandată indicarea acestuia contractual.

**Comunicare privind persoanele vizate.** Se va conveni, de asemenea, cu excepția cazurilor în care încălcarea datelor nu este susceptibilă să creeze un risc ridicat pentru drepturile și libertățile unei persoane fizice, să se informeze direct persoana vizată despre încălcare.

Această comunicare nu va fi necesară dacă:

- măsurile tehnice și organizatorice au făcut datele incomprehensibile oricărei persoane (de exemplu, criptarea);
- s-au luat măsuri pentru a se asigura că riscul nu mai este "probabil să se materializeze";

În plus, GDPR permite comunicarea "publică", mai degrabă decât comunicarea directă, dacă comunicarea necesită "eforturi disproporționate".

În cazul în care cabinetul de avocatură nu procedează la comunicarea privind încălcarea datelor către persoana vizată, autoritatea de control va putea, după luarea în considerare a riscului care rezultă din încălcare, să ordone operatorului să facă divulgarea.

## **RECOMANDĂRI**

- |  |                          |
|--|--------------------------|
| Mobilizați persoanele competente                             | <input type="checkbox"/> |
| Calificați încălcarea  | <input type="checkbox"/> |
| Luați măsurile necesare pentru a atenua orice consecințe     | <input type="checkbox"/> |
| Dacă există riscuri: notificarea încălcării la CNIL          | <input type="checkbox"/> |
| În cazul unui risc ridicat: comunicarea cu persoanele vizate | <input type="checkbox"/> |
| În orice caz, introducerea în registrul încălcărilor         | <input type="checkbox"/> |

## **FIȘA NR. 10. EVIDENȚA ACTIVITĂȚILOR DE PRELUCRARE**

În schimbul eliminării formalităților declarative, GDPR prevede înființarea unui registru al activităților de prelucrare care trebuie păstrat de către operator.

Fiecare operator trebuie să țină o evidență a categoriilor de prelucrări a datelor cu caracter personal efectuate sub responsabilitatea sa. Această obligație nu se impune societăților cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este de natură să genereze un risc în ceea ce privește drepturile și libertățile persoanelor vizate, dacă nu este ocazională sau dacă include date sensibile sau date referitoare la condamnări penale și infracțiuni.

Prin urmare, se pare că un număr mare de cabinete de avocatură, în cazul în care prelucrările efectuate de acestea implică date referitoare la anumite categorii de date sau date referitoare la condamnări penale și infracțiuni, vor fi supuse obligației de păstrare a evidenței activităților de prelucrare.

În orice caz, chiar și pentru cabinetele care nu vor avea această obligație, păstrarea unei evidențe contribuie la respectarea principiului responsabilității (constând în documentarea conformității, în vederea dovedirii acesteia) și, ca atare, este foarte recomandată.

Într-adevăr, lipsa obligației de a ține o evidență nu reprezintă o libertate necontrolată în gestionarea datelor cu caracter personal, dimpotrivă. Este necesar să existe, cel puțin, o cartografiere a prelucrărilor, să se respecte toate principiile menționate în GDPR, să se respecte drepturile persoanelor și să se documenteze respectarea diferitelor obligații în conformitate cu principiul responsabilității.

Evidența trebuie să includă, în conformitate cu articolul 30 din GDPR, următoarele informații:

- numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- scopurile prelucrării;
- descrierea categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizațiile internaționale;
- 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 documentația care dovedește existența unor garanții adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- în măsura în care este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate implementate.

## **RECOMANDĂRI**

### **Cartografierea prelucrărilor efectuate în cadrul cabinetului**

- Inventarierea activităților de prelucrare (gestionarea dosarelor clientului, managementul resurselor umane, managementul contabilității etc.) ☐
- Identificarea caracteristicilor fiecărei prelucrări (date colectate, destinatari, termen de valabilitate etc.) ☐

### **Elaborarea evidenței activităților de prelucrare** ☐

## **FIȘA NR. 11. RESPONSABILUL CU PROTECȚIA DATELOR**

### **1. Obligația cabinetelor de avocatură de a desemna un responsabil cu protecția datelor**

În conformitate cu articolul 37 din GDPR, operatorii și procesatorii vor avea obligația să desemneze un responsabil cu protecția datelor:

- dacă aparțin sectorului public;
- dacă activitățile de bază (principale) ale acestora îi determină să realizeze monitorizarea periodică și sistematică a persoanelor pe scară largă;
- dacă activitățile de bază (principale) ale acestora îi determină să prelucrez (tot pe scară largă) anumite categorii de date, numite date "sensibile" și date privind condamnările penale și infracțiunile;

În afara acestor cazuri, numirea unui responsabil cu protecția datelor va fi, desigur, posibilă și chiar recomandată.

Nu există o limită de personal care să impună obligativitatea numirii unui responsabil cu protecția datelor.

Responsabilii de tratament pot opta pentru un responsabil cu protecția datelor comun sau extern. Grupul de lucru "Articolul 29" (G29), compus din reprezentanți ai autorităților de protecție a datelor din statele membre ale UE, a emis orientări privind rolul responsabililor cu protecția datelor și a făcut recomandări privind bunele practici.

Dacă este desemnat un responsabil cu protecția datelor, organizația este obligată să publice informațiile privind responsabilul cu protecția datelor și să le comunice autorității de control competente.

Cu toate acestea, articolul 37 (precum și articolul 35, a se vedea mai jos) se aplică întotdeauna operatorului sau persoana împuternicite cu prelucrarea anumitor categorii de date. Aceste dispoziții impun numirea unui responsabil cu protecția datelor în cazurile în care activitățile de bază ale operatorului sau persoanei împuternicite constau în prelucrarea la scară largă a anumitor categorii de date menționate la articolul 9.

Conform orientărilor privind responsabilii cu protecția datelor, *"activitățile de bază pot fi considerate ca fiind toate activitățile pentru care prelucrarea datelor face parte integrantă din activitățile operatorului sau ale persoanei împuternicite"*.

Sensul expresiei *"pe scară largă"* are o importanță deosebită, deoarece un cabinet mic de avocatură poate prelucra dosare care implică cantități considerabile de date.

Cu toate acestea, considerentul 91 din GDPR facilitează argumentarea faptului că această cerință nu se va aplica avocaților care practică în mod individual (a se vedea secțiunea 1.3.2.4 privind evaluarea impactului).

Astfel, evaluarea obligației de desemnare sau nu a unui responsabil cu protecția datelor se va face de la caz la caz, în funcție de numărul de persoane vizate de prelucrarea datelor cu caracter personal, de volumul de date prelucrate, de durata sau permanența activităților de prelucrare, domeniul geografic al activității de prelucrare, dar se pare că, în cea mai mare parte, cabinetele de avocatură nu pot fi considerate procesatoare de date cu caracter personal la scară largă și, prin urmare, numirea unui responsabil cu protecția datelor nu va fi obligatorie

În orice caz, o astfel de desemnare, chiar dacă nu este obligatorie, trebuie, de asemenea, analizată ca o oportunitate, în măsura în care ar permite desemnarea unei persoane care să se ocupe de conformitatea cabinetului.

## **2. Obligațiile și sarcinile responsabilului cu protecția datelor**

GDPR impune obligații semnificative responsabililor cu protecția datelor. În calitate de "dirijor" al conformității în materie de protecție a datelor în cadrul organizației sale, ofițerul de protecție a datelor are, în principal, următoarele obligații:

- să informeze și să consilieze operatorul sau persoana împuternicită și angajații acestora;
- să asigure respectarea reglementărilor și a legislației naționale privind protecția datelor;
- să consilieze organizația pentru efectuarea studiilor de impact privind protecția datelor și să verifice implementarea acestora;
- să coopereze cu autoritatea de control și să fie punctul de contact al acesteia. Pentru a vă ajuta în implementarea noilor obligații impuse de regulamentul european, ofițerul de protecție a datelor trebuie, în special:
- să se informeze cu privire la conținutul noilor obligații;
- să sensibilizeze factorii de decizie cu privire la impactul acestor noi reguli;
- să efectueze un inventar al prelucrării datelor de către organizația dvs..;
- să conceapă acțiuni de sensibilizare;
- să gestioneze respectarea continuă a conformității.

În consecință, persoana care acționează în calitate de ofițer de protecție a datelor va avea responsabilități importante.

## **3. Avocatul care acționează în calitate de responsabil cu protecția datelor**

În mod oportun, GDPR a abrogat pragul de 50 de angajați care interzicea externalizarea responsabilului cu protecția datelor (DPO).

Decizia normativă de reformare a articolelor 6 "Domeniul profesional al avocatului" și 19 "Serviciile juridice online" din Regulamentul Intern național (RIN) al profesiei de avocat, adoptat de Adunarea Generală a Consiliului Național al Barourilor din 9 și 10 decembrie 2016<sup>6</sup> pe baza unui raport al Comitetului de reguli și practici și după consultarea profesiei, a modificat prevederile referitoare la misiunea avocatului-DPO:

<https://www.cnb.avocat.fr/reglement-interieur-national-de-la-profession-davocat-rin#>

### **Articolul 6.3.3 "Împuternicitul pentru protecția datelor cu caracter personal - Ofițerul de protecție a datelor cu caracter personal (DPO)" din RIN prevede următoarele:**

*"Avocatul împuternicit pentru protecția datelor cu caracter personal trebuie să-și înceteze misiunea dacă consideră că nu poate să o realizeze, după ce a informat în prealabil și a luat măsurile necesare cu persoana responsabilă de prelucrare; în niciun caz nu-și poate denunța clientul.*

*Avocatul împuternicit pentru protecția datelor cu caracter personal trebuie să refuze să reprezinte orice persoană sau organizație pentru care exercită sau a exercitat funcția de ofițer de protecție a datelor cu caracter personal în contextul procedurilor administrative sau judiciare care implică responsabilul cu prelucrarea datelor. "*

Începând cu data de 25 mai 2018, aceste dispoziții vor fi înlocuite cu următoarele dispoziții:

*"6.3.3: Responsabilul cu protecția datelor.*

*"Avocatul responsabil cu protecția datelor trebuie să-și înceteze misiunea dacă consideră că nu poate să o realizeze, după ce a informat în prealabil și a luat măsurile necesare cu persoana responsabilă de prelucrare; în niciun caz nu-și poate denunța clientul.*

*Avocatul responsabil cu protecția datelor trebuie să refuze să reprezinte orice persoană sau organizație pentru care exercită sau a exercitat misiunea de împuternicit pentru protecția datelor cu caracter personal (DPO) sau de ofițer de protecție a datelor în cadrul procedurilor administrative sau judiciare care implică operatorul."*

Avocatul-DPO a fost deja supus unor obligații care nu sunt obligatorii pentru un DPO care nu este avocat: obligația de a nu-și denunța clientul și obligația de demisie în caz de conflict de interese.

Este necesar să se precizeze că avocatul trebuie să refuze să reprezinte clienții pentru care exercită sau a exercitat misiunea de DPO în procedurile care implică responsabilul cu prelucrarea, pentru a evita orice situație de conflict de interese sau de încălcare a secretului profesional.

În plus, articolul 6.4 "Declarații către Barou" din RIN prevede:

*"Un avocat care intenționează să practice activitatea de broker imobiliar, agent portofoliu sau agent imobiliar, agent sportiv, agent de artiști și autori, intermediar în asigurări, activități de lobby, administrator de imobile și împuternicit cu protecția datelor cu caracter personal - ofițer delegat cu protecția datelor (DPO) trebuie să adreseze o declarație Baroului prin scrisoare sau e-mail către Președintele Baroului. "*

Începând cu data de 25 mai 2018, la articolul 6.4, termenii "Împuternicit cu protecția datelor cu caracter personal Ofițer de protecție a datelor (DPO)" se vor înlocui cu termenii "Responsabil cu protecția datelor".

Este o simplă obligație de a declara, fără nicio constrângere formală. Astfel, această declarație urmărește, pe de o parte, o mai bună pregătire a avocaților care doresc să exercite această funcție și, pe de altă parte, să permită Barourilor să comunice cu privire la avocații care exercită aceste misiuni în jurisdicția lor.



## **FIȘA NR. 12. AUTORITATEA DE CONTROL ȘI SANCTIUNI**

Operatorii și procesatorii pot face obiectul unor sancțiuni administrative semnificative în caz de necunoaștere a dispozițiilor GDPR.

**Autoritățile de control (în Franța, CNIL) pot, în special:**

- Pronunța un avertisment;
- Pune în întârziere întreprinderea;
- Limita un tratament temporar sau permanent;
- Suspenda fluxurile de date;
- Dispune îndeplinirea cererilor de exercitare a drepturilor persoanelor fizice;
- Dispune rectificarea, limitarea sau ștergerea datelor.

În ceea ce privește noile instrumente de conformitate care pot fi utilizate de către companii, autoritatea poate retrage certificarea acordată sau obliga organismul de certificare să-și retragă certificarea. În ceea ce privește amenzile administrative, acestea pot crește, în funcție de categoria infracțiunii, cu 10 sau 20 de milioane de euro, sau, în cazul unei companii, de la 2% până la 4% cifră de afaceri anuală la nivel global, fiind reținută cea mai mare sumă.

Această sumă trebuie să se raporteze la faptul că, pentru prelucrările transnaționale, sancțiunea va fi adoptată de comun acord între toate autoritățile competente, potențial pentru teritoriul întregii Uniuni Europene.

În acest caz, întreprinderii i se va impune o singură decizie de sancționare decisă de către mai multe autorități de control.

## **FIȘA nr. 13. DREPTUL DE ACCES LA DATE**

GDPR face următoarele modificări în materie de drept de acces:

- **Termenele limită pentru a răspunde unei solicitări:** timpul de răspuns este acum de maximum o lună de la primirea cererii (articolul 12, alineatul 3). Cu toate acestea, este prevăzută o posibilitate de prelungire a termenului cu două luni, "*având în vedere*

*complexitatea și numărul cererilor", cu condiția informării persoanei în cauză în termen de o lună de la primirea cererii (articolul 12.3).*

- **Taxele de reproducere a documentelor:** regulamentul prevede un principiu al gratuității pentru copiile furnizate ca parte a unei cereri de acces (articolul 12.5). Numai atunci când cererea este vădit nefondată sau excesivă, operatorul poate solicita plata "unor taxe rezonabile" care iau în considerare costurile administrative suportate pentru furnizarea informațiilor. Același lucru se va aplica atunci când se solicită o copie suplimentară.
- **Modalitățile de comunicare a datelor:** regulamentul prevede că, în cazul în care persoana depune o cerere pe cale electronică, informațiile solicitate sunt furnizate în format electronic de uz comun, cu excepția cazului în care persoana respectivă solicită altfel (articolul 12.3).
- **Modalitățile de comunicare a datelor:** regulamentul prevede că persoana împuternicită asistă operatorul în îndeplinirea obligațiilor sale privind dreptul de acces (articolul 28 e). De exemplu: un angajator i-ar putea solicita împuternicitului care i-a furnizat un dispozitiv de geolocalizare, sprijinul pentru a oferi angajaților care îi solicită date geografice "într-o formă accesibilă"; atunci când responsabilul de date dispune doar o analiză a datelor, acesta ar putea să se adrese împuternicitului care a păstrat datele de identificare.

## **METODOLOGIA PRIVIND CONFORMITATEA**

### **Metodologia privind conformitatea**

CNIL a dezvoltat o metodologie în șase etape pentru a facilita conformitatea operatorilor. Cele șase etape corespund:

- Desemnarea unui pilot;
- Cartografierea prelucrării datelor cu caracter personal;
- Prioritizarea acțiunilor care trebuie întreprinse;
- Managementul riscului;
- Organizarea proceselor pe plan intern;
- Documentația de conformitate.

## **1. Desemnarea unui pilot**

Articolul 37 din GDPR a introdus obligația numirii unui responsabil cu protecția datelor în diferite situații (a se vedea fișa nr. 11).

Pentru majoritatea cabinetelor de avocatură, o astfel de desemnare nu pare obligatorie, deoarece, în cazul în care se ocupă de anumite categorii de date sau date referitoare la infracțiuni și condamnări, cea mai mare parte dintre acestea nu va putea susține neprelucrarea acestor date "pe scară largă".

Cu toate acestea, chiar și în cazurile în care numirea responsabilului cu protecția datelor nu este obligatorie, CNIL recomandă o numirea acestuia pentru a facilita conformitatea cu GDPR (a se vedea fișa nr. 11).

Fără măcar să desemneze o persoană în calitate de responsabil cu protecția datelor, ar fi oportun să se desemneze dintre membrii cabinetului o persoană care să se ocupe de aspectele legate de protecția datelor și să servească drept referință pentru personal și colaboratorii cabinetului.

## **2. Cartografierea prelucrării datelor cu caracter personal**

Cartografierea oferă o imagine de ansamblu asupra prelucrării datelor personale operate în cadrul cabinetului de avocatură.

CNIL recomandă așadar să punem următoarele întrebări:

- Cine?
- Ce?
- De ce?
- Până când?
- Cum?

**Cine?** Această întrebare face posibilă identificarea diferiților factori, respectiv a operatorului, dar și a persoanelor împuternicite și a destinatarilor datelor.

- **Operatorul de date.** În cadrul cabinetului de avocatură, operatorul este cel care determină scopul și mijloacele tratamentului, și poate fi, printre altele, avocatul asociat. În acest scop, este necesar să se identifice persoana din cadrul cabinetului de avocatură care inițiază prelucrarea datelor cu caracter personal. De asemenea, poate fi chiar cabinetul în calitate de persoană juridică.
- **Persoana împuternicită.** Persoana împuternicită este "persoana fizică sau juridică, autoritatea publică, serviciul sau alt organism care prelucrează date cu caracter personal în numele operatorului" în conformitate cu articolul 4, alineatul 8, din GDPR. Prin urmare, pot fi prestatori, furnizori, editori de software, gazde web etc.
- **Destinatari.** GDPR definește la articolul 4, alineatul (9) destinatarul unei prelucrări de date cu caracter personal care este "persoana fizică sau juridică, autoritatea publică, serviciul sau orice alt organism care primește comunicarea datelor cu caracter personal, fie că este sau nu o terță parte".

**Ce?** Se referă la informațiile privind tipul de date personale pe colectează cabinetul și, în general, pe care le tratează. În plus, avocatul trebuie să identifice prezența anumitor categorii de date cu caracter personal (date privind sănătatea, date privind viața sexuală, date privind condamnările penale și infracțiunile etc.).

**De ce?** Prin această întrebare, avocatul determină scopul prelucrării datelor personale pe care le operează, adică obiectivul (de exemplu: managementul clienților, managementul resurselor umane, managementul solicitărilor personalizate etc.).

**Unde?** În acest stadiu, este vorba de determinarea locului în care sunt stocate datele personale (un anumit server, local, partajat? Fișierele sunt stocate într-o cameră la care are acces întreg cabinetul de avocatură? etc.). Această întrebare ar trebui, de asemenea, să permită avocatului să identifice eventualele transferuri de date către țări din afara UE (un dosar internațional, un avocat care depune cerere în străinătate etc.).

**Când?** Cabinetul de avocatură are o politică de păstrare, arhivare și ștergere a datelor? Cabinetul de avocatură intenționează să epuizeze datele pe care le colectează?

**Cum?** Cabinetul de avocatură trebuie să identifice măsurile de securitate fizică și logică introduse pentru a garanta protecția datelor cu caracter personal pe care le colectează.

### **3. Identificarea acțiunilor prioritare**

Operatorul poate efectua mai multe acțiuni pentru a garanta conformitatea prelucrării datelor cu GDPR.

Prin urmare, cabinetul de avocatură va trebui, să stabilească dacă respectă:

- Principiul minimalizării, adică faptul că se referă doar la datele strict necesare pentru prelucrarea acestora;
- Principiul legalității, adică determinarea temeiului juridic al prelucrării datelor cu caracter personal efectuate de cabinetul de avocatură (încheierea și executarea unui contract, necesitatea de a respecta o obligație legală, consimțământul, interes legitim, etc.);
- Obligația de a furniza informații (contract de onorariu, contract de muncă, contract de colaborare, site web etc.);
- Obligațiile contractuale referitoare la subcontractanți (contabil, gazdă a sistemului de informații, furnizor de servicii IT, editor de software pentru clienți sau pentru contabilitate, de exemplu);
- Drepturile persoanelor;
- Măsurile de securitate implementate în birou (acces la sedii, parole, autorizații etc.).

Atenție, cabinetul de avocatură trebuie să fie vigilent în prezența unor date particulare și date privind condamnările penale și infracțiunile, și în prezența fluxurilor transfrontaliere de date cu caracter personal.

### **4. Managementul riscului**

Această etapă abordează necesitatea unei analize de impact. Într-adevăr, unele cabinete de avocatură, în funcție de datele cu caracter personal pe care le colectează, ar putea fi nevoite să efectueze analize de impact.

Pentru mai multe informații privind analizele de impact, consultați punctul 1.3.2.4.

### **5. Implementarea proceselor de protecție a datelor personale în cadrul cabinetului de avocatură**

Cabinetele de avocatură pot crea procese pentru a se asigura că prelucrarea datelor cu caracter personal este compatibilă cu GDPR.

Aceste procese includ:

- Protecția datelor cu caracter personal începând cu proiectarea și securitatea implicită
- Sensibilizarea membrilor cabinetului în probleme legate de protecția datelor cu caracter personal;
- Procedurile de gestionare a cererilor referitoare la diferitele drepturi ale clienților. Într-adevăr, cu cât cabinetul de avocatură reacționează mai rapid, acordând dreptul la acces, opoziție, rectificare, etc. a clientului, cu atât mai puțin există riscul ca el să depună o plângere la autoritatea de supraveghere care ar putea conduce la un control din partea acestuia;
- Măsurile interne referitoare la încălcarea datelor cu caracter personal, respectiv notificarea către autoritatea de supraveghere și comunicarea către persoanele vizate.

## **6. Documentația de conformitate**

- Cabinetul de avocatură trebuie să păstreze dovada conformității prelucrării acestor date în ceea ce privește GDPR. Sunt disponibile mai multe instrumente pentru a documenta conformitatea acestor prelucrări:
- Registrul prelucrărilor;
- Analiza de impact;
- Instrumente de gestionare a fluxului transfrontalier, cum ar fi clauzele contractuale standard, Binding Corporate Rules, certificări etc.;
- Mențiuni de informații;
- Contractele cu persoanele împuternicite;
- Dovada obținerii consimțământului datelor cu caracter personal.

## **INFORMAȚII SUPLIMENTARE**

### **Directivile G29:**

<https://www.CNIL.fr/fr/reglement-europeen/lignes-directrices>

- Responsabilul cu protecția datelor (5/05/2017)
- Evaluarea impactului asupra protecției datelor (DPIA) (4/10/2017)
- Portabilitatea (5/05/2017)

- Desemnarea unei autorități de supraveghere principale pentru un operator sau un procesator (5/05/2017)

**Directivele Consiliului barourilor europene (CCBE) privind principalele măsuri noi de conformitate a avocaților cu GDPR (19/05/2017)**

[http://www.ccbe.eu/fileadmin/speciality\\_distribution/public/documents/IT\\_LAW/ITL\\_Position\\_papers/FR\\_ITL\\_20170519\\_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf](http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf)

**Ghiduri de informare CNIL:**

<https://www.CNIL.fr/fr/principes-cles/GDPR-se-preparer-en-6-etapes>

<https://www.CNIL.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>

<https://www.CNIL.fr/fr/video-le-youtubeur-cookie-connecte-repond-vos-questions-sur-larrivee-du-GDPR>

**Comisia Europeană:**

- Comunicare publicată la data de 24 ianuarie 2018 de către Comisie Parlamentului European și Consiliului: o mai bună protecție și noi perspective - orientări ale Comisiei referitoare la aplicarea directă a reglementărilor generale privind protecția datelor din 25 mai 2018:

<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52018DC0043>

un nou instrument online care include fișele factuale, Q & A și ilustrații practice pentru a ajuta cetățenii și întreprinderile să respecte noile norme introduse de regulament.