

## PROCEDURI ȘI AUTORITĂȚI ÎN NOUL DREPT EUROPEAN AL PROTECȚIEI DATELOR CU CARACTER PERSONAL (II)



*Prof. univ. dr. Călina JUGASTRU*  
Universitatea „Lucian Blaga” din Sibiu  
Facultatea de Drept

### Abstract

*Regulation (EU) 2016/679 regulates the international cooperation between the authorities of the Member States (between themselves and with the European data protection Committee) and establishes a complex mechanism of coherence. The purpose of the coherence mechanism is to ensure the rigorous and uniform application of the Regulation in the European area, to periodically review the guidelines, recommendations and good practices developed in the framework of the tasks assigned to the relevant authorities.*

*The regulatory rules contain benchmarks regarding the identification method of the main supervisory authority, where more than one supervisory authority for the processing of personal data operates in the Member State. Also, the European legislative act defines the supervisory authorities concerned and delimits the duties and competences of each type of supervisory authority.*

**Keywords:** *Regulation (EU) 2016/679, personal character data, the main supervisory authority, the supervisory authorities concerned, the European Data Protection Board, the cohesion enforcement mechanism*

### Preliminarii

Cele două niveluri la care se regăesc autoritățile de protecție a datelor identifică autoritatea independentă/autoritățile independente din statele membre și Comitetul european de protecție a datelor. **La nivel național**, statutul autorităților de supraveghere a datelor cu caracter personal se caracterizează prin independență în exercitarea atribuțiilor pe care Regulamentul (UE) 2016/679 le pune în sarcina acestora. **La nivelul Uniunii**, responsabilitatea revine Comitetului european de protecție a datelor – entitate nou creată prin dispozițiile Regulamentului, cu rol de coordonare a autorităților independente din statele membre. Sistemul instituit de actul normativ european este structurat de manieră a asigura protecția optimă a drepturilor și libertăților persoanelor fizice, în special a

dreptului la respectarea vieții private. Statele membre au la dispoziție un termen rezonabil, care se întinde până în luna mai 2018, pentru a finaliza demersurile de transpunere în practică a prevederilor Regulamentului. Dificultăți pot să apară în statele membre care au instituit mai multe autorități de supraveghere, în condițiile în care o singură autoritate va avea atribuții de reprezentare la nivel european. Autoritatea principală de supraveghere are atribuții delimitate de atribuțiile autorităților de supraveghere vizate – în cadrul național.

### I. Autoritățile de supraveghere independente

Statele membre instituie una sau mai multe autorități de supraveghere, care reflectă structura lor constituțională, organizatorică și administrativă.

#### *Tipuri de autorități de supraveghere*

Regulamentul operează cu noțiuni care desemnează autorități de supraveghere ce se determină după criterii distincte și care au propriul rol, în ansamblul operațiunilor de prelucrare a datelor. Noul act normativ european conține un „dicționar” util în precizarea termenilor – demersul de identificare a autorităților fiind indispensabil și prealabil discutării competențelor și sarcinilor conferite fiecăreia dintre acestea (autoritatea principală, autoritatea vizată). Un sprijin semnificativ este oferit de *Ghidul pentru stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator*, revizuit și adoptat de Grupul 29, la 5 aprilie 2017<sup>1</sup>.

**Autoritate de supraveghere.** „Autoritatea de supraveghere” este autoritatea publică independentă instituită de statul membru, în scop de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal în Uniune (art. 4 pct. 21).

**Rolul autorității de supraveghere** este de a contribui la aplicarea coerentă a prevederilor Regulamentului în spațiul european, utilizând mecanismul cooperării, între autorități și cu Comisia. Principiul independenței caracterizează activitatea fiecărei autorități de supraveghere, în îndeplinirea sarcinilor trasate de Regulament.

**Competența** autorității de supraveghere se exercită pe teritoriul statului membru de care aparține autoritatea. Autoritatea națională nu este abilitată să supravegheze operațiunile de prelucrare ale instanțelor care acționează în exercițiul funcției lor judiciare. În aria de competență a autorității de supraveghere se includ (cu tilu de exemplu): efectuarea auditului privind protecția datelor;

---

<sup>1</sup> Ghidul poate fi consultat pe pagina Autorității Naționale de Supraveghere a Prelucrării datelor cu Caracter Personal, <http://www.dataprotection.ro/servlet/ViewDocument?id=1382>, accesată la data de 14 mai 2017.

notificarea responsabilului prelucrării/împuțernicitului, în ce privește presupusa încălcare a Regulamentului (competențe de investigare); emiterea avertizărilor adresate responsabilului prelucrării/împuțernicitului cu privire la posibilitatea ca operațiunile pe care acesta le desfășoară să încalce dispozițiile Regulamentului; obligarea responsabilului prelucrării/împuțernicitului la informarea persoanei vizate cu privire la încălcarea protecției datelor; obligarea la rectificarea/ștergerea datelor/restricționarea prelucrării și la notificarea acestei conduite destinatarilor cărora le-au fost divulgate datele cu caracter personal (competențe corective); consilierea responsabilului prelucrării cu privire la procedura de consultare prealabilă; avizarea/aprobarea codurilor de conduită, în condițiile stabilite de Regulament; acreditarea organismelor de certificare; aprobarea regulilor corporatiste obligatorii (competențe de autorizare și de consiliere).

Statul membru de care aparține autoritatea poate să reglementeze competențe suplimentare, sub rezerva ca acestea să nu aducă atingere modului de operare eficientă prevăzut de Regulament.

Considerentele Regulamentului menționează că ansamblul competențelor conferite autorităților de supraveghere trebuie să se fundamenteze pe un arsenal de garanții procedurale prevăzute în dreptul Uniunii și în dreptul intern, în mod imparțial, echitabil și într-un termen rezonabil. Pentru aceasta, fiecare măsură se impune a fi adecvată, necesară și proporțională, în scopul de a asigura conformitatea cu dispozițiile Regulamentului, luând în considerare circumstanțele fiecărui caz în parte; fiecare persoană are dreptul de a fi ascultată înainte de luarea oricărei măsuri individuale ce ar putea să îi aducă atingere; se impune evitarea costurilor inutile și a inconvenientelor excesive pentru persoanele în cauză. Se recomandă ca fiecare măsură obligatorie din punct de vedere juridic, luată de autoritatea de supraveghere, să fie prezentată în scris, să fie clar formulată și lipsită de ambiguitate, să indice autoritatea de supraveghere care a emis măsura, data emiterii măsurii, să poarte semnătura șefului sau a unui membru al autorității de supraveghere autorizat, să furnizeze motivele pentru care s-a luat măsura și să facă trimitere la dreptul la o cale de atac eficientă (împrejurări care nu exclud cerințele suplimentare, în conformitate cu dreptul procedural național)<sup>2</sup>.

Exemplificativ, fiecărei autorități de supraveghere îi revin următoarele **sarcini**: monitorizarea aplicării dispozițiilor Regulamentului (UE) 2016/679; promovarea acțiunilor de înțelegere, de către public (în special de către minori), a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare a datelor; oferirea consilierii adresate parlamentului național, guvernului, altor instituții și organisme, în ce privește măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor în raport cu prelucrarea datelor;

---

<sup>2</sup> Potrivit considerentului 129, adoptarea unor decizii obligatorii din punct de vedere juridic implică faptul că se poate da naștere unui control jurisdicțional în statul membru al autorității de supraveghere care a adoptat decizia.

promovarea acțiunilor de diseminare a obligațiilor ce revin responsabililor prelucrărilor/împuterniciților; furnizarea de informații către persoanele vizate în legătură cu drepturile conferite de Regulament, cooperând, dacă este cazul, cu autorități de supraveghere din alte state membre; soluționarea plângerilor depuse de persoanele vizate, de organisme sau asociații și informarea reclamanților cu privire la evoluția și rezultatul investigațiilor; cooperarea cu alte autorități de supraveghere și asistența reciprocă, în contextul asigurării funcționării mecanismului coerentei; monitorizarea evoluțiilor relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal – mai ales evoluția tehnologiilor informației și a practicilor comerciale; întocmirea și actualizarea evidențelor referitoare la evaluarea impactului asupra protecției datelor; avizarea/aprobarea codurilor de conduită, în conformitate cu prevederile regulamentare; contribuția la activitățile Comitetului european pentru protecția datelor.

**Autoritate de supraveghere principală.** Fiecare stat membru este ținut să desemneze o autoritate de supraveghere principală, pentru prelucrarea transfrontalieră efectuată de respectivul operator sau de către împuternicitul persoanei responsabile. Utilitatea autorității de supraveghere principale se vedește în contextul prelucrărilor transfrontaliere de date, întrucât acest tip de prelucrare creează o conexiune aparte pe circuitul autorității naționale – Comisie – Comitetul european.

**Prelucrarea transfrontalieră.** Noțiunea de „prelucrare transfrontalieră” are două accepțiuni, potrivit vocabularului terminologic al Regulamentului (art. 4 pct. 23).

a. *Prelucrarea transfrontalieră semnifică operațiunile de prelucrare a datelor cu caracter personal care au loc în contextul activităților sediilor de pe teritoriile mai multor state ale Uniunii și care aparțin responsabilului prelucrării sau împuternicitului acestuia.* Condiția cerută de Regulament este ca sediile să fie plasate pe teritoriile a cel puțin două dintre statele membre.

b. Dacă responsabilul prelucrării sau împuternicitul acestuia dețin un singur sediu pe teritoriul Uniunii, *prelucrarea transfrontalieră desemnează operațiunile efectuate în contextului respectivului sediu, operațiuni care afectează sau care sunt susceptibile să afecteze în mod semnificativ, persoane vizate din cel puțin două state membre.*

Sintagma „operațiuni care afectează în mod semnificativ” desemnează un anumit tip de efecte ale operațiunilor de prelucrare cu privire la persoana vizată. Dintre înțelesurile termenului „semnificativ”, credem că legiuitorul a avut în vedere sinonimele „important”, „însemnat”. Operațiuni semnificative sunt operațiunile care au efecte importante cu privire la destinatarii prelucrărilor. Cu alte cuvinte, nu orice operațiune de prelucrare a datelor cu caracter personal atrage aplicarea dispozițiilor referitoare la prelucrarea transfrontalieră. Se vor lua în considerare numai operațiunile relevante, în ceea ce privește efectele asupra persoanei vizate. Aceasta ar însemna că, în accepțiunea noului Regulament, suntem în

prezența unei prelucrări transfrontaliere (în varianta a doua a definiției) atunci când impactul prelucrării este semnificativ în raport cu persoana vizată.

*Ghidul pentru stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator* reține că prelucrarea întrunește cerințele definiției legale «dacă există posibilitatea unui efect semnificativ, nu doar a unui efect semnificativ concret [...] „probabil” nu înseamnă că există o posibilitate îndepărtată a unui efect semnificativ. Efectul semnificativ trebuie să fie mai mult decât probabil. Pe de altă parte, aceasta înseamnă, de asemenea, că persoanele fizice nu trebuie să fie realmente afectate: probabilitatea unui efect semnificativ este suficientă pentru a încadra prelucrarea în definiția „prelucrării transfrontaliere”». Între liniile de recomandare se înscrie sugestia de a lua în considerare contextul prelucrării, tipul de date, scopul prelucrării, precum și factori cum sunt: prelucrarea are consecințe neprevăzute sau nedorite pentru persoanele fizice; prelucrarea generează sentimente de jenă sau alte efecte negative, inclusiv un prejudiciu de imagine; prelucrarea implică analiza unor categorii de date cu caracter special sau a altor date intruzive, în special referitoare la minori; prelucrarea permite ca persoanele fizice să fie vulnerabile la discriminare/tratament inechitabil; prelucrarea afectează ori este de natură a afecta statutul sau resursele financiare/economice ale persoanelor fizice; prelucrarea este de natură să afecteze sănătatea fizică sau mentală a persoanelor fizice; prelucrarea este aptă să genereze restrângerea drepturilor persoanei fizice<sup>3</sup>.

**Identificarea autorității de supraveghere principale.** În ipoteza existenței mai multor autorități de supraveghere pe teritoriul statului membru, autoritatea de supraveghere principală este „autoritatea care are responsabilitatea principală în activitatea de prelucrare transfrontalieră a datelor, de exemplu, în cazul în care persoana vizată depune o plângere referitoare la prelucrarea datelor sale personale”<sup>4</sup>.

Punctul de legătură la care face apel Regulamentul este *sediul principal* al responsabilului prelucrării: „[...] autoritatea de supraveghere a sediului principal sau a sediului unic al responsabilului sau al persoanei împuternicite de acesta este competentă să acționeze în calitate de autoritatea de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită, în conformitate cu procedura prevăzută la articolul 60” (art. 56 alin. 1 din Regulament).

Explicațiile privind acțiunea „*sediului principal*”, conform Regulamentului, sunt oferite de art. 4 pct. 16. *Dacă operațiunile sunt efectuate de responsabilul prelucrării*, care dispune de sedii în cel puțin două state membre, sediul principal este „locul în care se află administrația centrală a acestuia în Uniune, cu excepția

---

<sup>3</sup> A se vedea, cu privire la interpretarea art. 4 pct. 23 din Regulament, *Ghidul pentru stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator*, op. cit.

<sup>4</sup> *Ibidem*.

cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal”. *Dacă prelucrarea este efectuată de împuternicit, iar acesta are sedii în cel puțin două state membre, sediul principal este „locul în care se află administrația centrală a acestuia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament”.*

Ceea ce rămâne de identificat este administrația centrală a responsabilului/persoanei împuternicite. *Ghidul* precizează că, în mod implicit, Regulamentul abordează administrația centrală pe teritoriul Uniunii, prin prisma locului în care se iau decizii cu privire la scopurile și mijloacele de prelucrare a datelor cu caracter personal. Este avut în vedere considerentul 36, care aduce lămuriri: „Sediul principal al unui operator în Uniune ar trebui să fie locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului în Uniune. În acest caz, acesta din urmă ar trebui considerat drept sediul principal”.

Într-adevăr, determinarea administrației centrale trebuie să fie subordonată unor criterii obiective – iar reperul este locul în care sunt luate deciziile principale cu privire la scopurile și mijloacele de prelucrare în cadrul unor înțelegeri stabile. Locul în care sunt situate mijloacele tehnice și tehnologiile de prelucrare a datelor cu caracter personal și, respectiv, locul unde se derulează activitățile de prelucrare, nu constituie sedii principale și, prin urmare, nu sunt criterii determinante, în acest sens. Considerentul 36 conține și câteva explicații utile pentru ipoteze care se pot ivi în practica prelucrării transfrontaliere a datelor. *Sediul principal al persoanei împuternicite* este reprezentat de locul în care se află administrația centrală a acesteia în Uniune sau, în cazul în care nu are o administrație centrală în Uniune, locul în care se desfășoară principalele activități de prelucrare în Uniune. *Atunci când operațiunile de prelucrare implică atât operatorul, cât și persoana împuternicită de operator*, autoritatea de supraveghere principală competentă este autoritatea de supraveghere a statului membru în care operatorul își are sediul principal, iar autoritatea de supraveghere a persoanei împuternicite de operator este considerată ca fiind o autoritate de supraveghere vizată și cea autoritate de supraveghere ar trebui să participe la procedura de cooperare prevăzută de prezentul regulament. *În situația unei prelucrări efectuate de un grup de întreprinderi*, sediul principal al întreprinderii care exercită controlul este sediul principal al grupului de între-

prinderi, cu excepția cazului în care scopurile și mijloacele aferente prelucrării sunt stabilite de o altă întreprindere<sup>5</sup>.

Demersul de determinare a autorității principale de supraveghere este important, în condițiile plasării sediilor pe arii teritoriale aparținând unor state diferite. În același timp, este firesc ca imperativul monitorizării întregii activități a unui operator, să fie în sarcina unei singure autorități de supraveghere. *Ghidul* exemplifică, arătând că pot exista situații în care un sediu, altul decât locul administrației centrale, să ia decizii autonome referitoare la scopurile și mijloacele unei anumite activități de prelucrare. Ceea ce înseamnă că, în unele cazuri, s-ar putea stabili cel puțin două autorități de supraveghere principale, de pildă, atunci când o companie multinațională stabilește centre de luare a deciziilor diferite, situate pe teritoriile unor state diferite, pentru activități de prelucrare diferite. Se menționează că, pentru multinaționale, este esențial să stabilească exact care este locul în care se iau deciziile privind scopul și mijloacele prelucrării. De determinarea precisă a sediului principal depinde identificarea corectă a autorității de supraveghere principale, căreia îi revin o serie de responsabilități, conform Regulamentului (poate fi vorba, concret, de desemnarea unui responsabil cu protecția datelor, de consultarea pentru o activitate de prelucrare ce prezintă risc și pe care operatorul nu o poate diminua prin mijloace rezonabile ș.a.)<sup>6</sup>.

**Autoritate de supraveghere vizată.** „*Autoritatea de supraveghere vizată*” este acea autoritate de supraveghere care este avută în vedere de operațiunile de prelucrare a datelor personale, fie întrucât responsabilul prelucrării/împuternicitul este stabilit pe teritoriul statului membru al acelei autorități, fie pentru că persoa-

---

<sup>5</sup> *Întreprinderea* este persoana (fizică sau juridică) ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriatele sau asociațiile care desfășoară în mod regulat o activitate economică; *grup de întreprinderi* înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta [art. 4 pct. 18-19 din Regulamentul (UE) 2016/679].

<sup>6</sup> Notăm două exemple oferite de *Ghid*, edificatoare pentru determinarea autorității de supraveghere principale: «„Un distribuitor de produse alimentare are sediul principal (adică „locul administrației centrale”) în Rotterdam, Olanda. Acesta are sedii în diferite alte state UE, care sunt în legătură cu persoane fizice de acolo. Toate sediile utilizează același software pentru a prelucra datele personale ale consumatorilor în scop de marketing. Toate deciziile privind scopurile și mijloacele de prelucrare a datelor personale ale consumatorilor în scop de marketing se iau în cadrul sediului principal din Rotterdam. Aceasta înseamnă că, în cazul companiei, autoritatea de supraveghere principală pentru activitatea de prelucrare transfrontalieră este autoritatea de supraveghere din Olanda”; „O bancă are sediul principal al corporației în Frankfurt și toate activitățile sale de prelucrări bancare sunt organizate de acolo, dar departamentul său de asigurări este situat în Viena. Dacă sediul din Viena are competența de a decide asupra întregii activități de prelucrare a datelor în scop de asigurări și de a dispune punerea în aplicare a acestor decizii pentru întreg teritoriul UE, atunci, așa cum prevede art. 4 (16) al RGPD, autoritatea de supraveghere din Austria va fi autoritatea principală privind prelucrările transfrontaliere de date cu caracter personal în scopuri de asigurări, iar autoritățile germane (autoritatea de supraveghere din Hessen) vor supraveghea prelucrarea datelor cu caracter personal în scopuri bancare, indiferent unde se află clienții».

nele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare, fie pentru că s-a depus o plângere la autoritatea în cauză (art. 4 pct. 22).

### *Statutul independent*

Autoritatea de supraveghere este o entitate care funcționează pe **principiul independenței**. Independența trebuie înțeleasă ca palier pe care converg două imperative: independența autorității *constituie o garanție* pentru persoanele fizice, în ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date; *permite controlul* (inclusiv jurisdicțional)/ monitorizarea, în ceea ce privește cheltuielile efectuate de autoritățile de supraveghere.

**Conținutul principiului independenței** autorității de supraveghere este identificabil pe următoarele direcții (art. 52):

a. fiecare autoritate de supraveghere beneficiază de independență deplină în realizarea sarcinilor care îi revin conform Regulamentului și în exercitarea competențelor sale;

b. în cadrul îndeplinirii sarcinilor/exercitării competențelor, membrii autorității de supraveghere își păstrează independența față de orice influență externă directă sau indirectă (se menționează faptul că aceștia nu primesc instrucțiuni de la o parte externă);

c. membrii autorității de supraveghere se vor abține să întreprindă acțiuni incompatibile cu atribuțiile lor, iar pe durata mandatului, nu vor desfășura activități incompatibile, remunerate sau nu;

d. fiecare autoritate de supraveghere dispune de resurse umane, tehnice și financiare, de sediu și de infrastructura necesare pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale. Sunt avute în vedere inclusiv activitățile desfășurate în contextul asistenței reciproce, al cooperării și al participării în cadrul Comitetului;

e. fiecare autoritate de supraveghere selectează personalul propriu (personal aflat sub conducerea exclusivă a autorității de supraveghere respective);

f. fiecare autoritate de supraveghere dispune de buget anual, distinct, public, ce poate face parte din bugetul general de stat sau național.

**În măsura în care un stat membru instituie mai multe autorități de supraveghere, obligațiile ce îi revin** sunt prevăzute de Regulament (51-54):

a. *statul va fi ținut să reglementeze mecanisme care să asigure participarea efectivă a autorităților de supraveghere respective la asigurarea coerenței*. Mecanismul pentru asigurarea coerenței este reglementat expres și presupune cooperarea autorităților de supraveghere, între ele și cu Comisia;

b. statul este obligat să desemneze, dintre autoritățile de supraveghere independente, instituite pe teritoriul său, acea autoritate de supraveghere care îndepli-



nește funcția de *punct unic de contact* pentru participarea efectivă a acestor autorități la mecanism. Scopul identificării autorității care joacă rolul de punct de contact este asigurarea cooperării rapide și armonioase cu alte autorități de supraveghere, cu Comitetul și cu Comisia;

c. *statul membru este obligat să se asigure că fiecare autoritate de supraveghere beneficiază de resurse financiare și umane, de spațiile și de infrastructura necesare îndeplinirii eficace a sarcinilor;*

d. *statul este ținut să se asigure că fiecare autoritate de supraveghere beneficiază de un buget public anual separat;*

e. *statul are obligația să se asigure că numirea membrilor autorităților de supraveghere are loc cu respectarea unei proceduri transparente, conform dispozițiilor legale în vigoare;*

f. *fiecare stat membru reglementează aspecte privind autoritățile de supraveghere: calificările membrilor autorității și condițiile de eligibilitate ale membrilor acesteia; procedurile de numire a membrilor autorității; durata mandatului membrilor autorității (minimum 4 ani, cu excepția primei numiri, după data de 24 mai 2016, din care o parte poate fi pe o durată mai scurtă, în cazul în care acest lucru e necesar pentru a proteja independența autorității de supraveghere prin intermediul unei proceduri de numiri eşalonate); obligațiile membrilor autorității (interdicții privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea mandatului). Distinct, este reglementată obligația de confidențialitate ce revine membrilor autorității de supraveghere, conform dreptului intern sau dreptului european. Secretul profesional privește informațiile de care aceștia au luat cunoștință cu prilejul îndeplinirii sarcinilor sau exercitării competențelor conferite prin lege. Obligația de păstrare a secretului incumbă membrilor autorității pe durata mandatului și subzistă după încetarea mandatului.*

### *Cooperarea între autoritatea de supraveghere principală și autoritățile de supraveghere vizate*

Cooperarea între autorități are la bază *comunicarea reciprocă* pe care o impune Regulamentul, așa încât autoritatea principală și autoritățile vizate (aflându-se în posesia informațiilor relevante) să ajungă la un consens. Scopul cooperării este aplicarea coerentă a prevederilor Regulamentului și instituirea asistenței reciproce. Asistența reciprocă are ca obiect cererile de informații și măsurile de supraveghere (de exemplu, cereri privind autorizări și consultări prealabile, controale și investigații)<sup>7</sup>.

---

<sup>7</sup> Se prevede că autoritatea de supraveghere principală poate solicita asistență reciprocă autorităților vizate și poate desfășura activități comune cu acestea, în vederea efectuării de investigații sau pentru monitorizarea punerii în aplicare a unei măsuri referitoare la un responsabil al prelucrării sau o persoană împuternicită aflată pe teritoriul altui stat membru (art. 60 alin. 2 din Regulament).

Actul normativ european instituie un mecanism detaliat al cooperării între autoritatea de supraveghere principală și autoritățile de supraveghere vizate, precum și al asistenței reciproce între autoritățile de supraveghere. De asemenea, reglementează operațiunile comune ale autorităților de supraveghere, inclusiv investigații comune sau măsuri comune de aplicare a legii, ce implică personal din autoritățile de supraveghere ale altor state membre.

Distinct, este prevăzut *mecanismul pentru asigurarea coerenței*, destinat să asigure aplicarea riguroasă și corelată a Regulamentului în spațiul Uniunii. Complexul mecanismului coerenței are două componente: cooperarea între autoritățile de supraveghere și cooperarea autorităților de supraveghere cu Comisia.

## II. Comitetul european pentru protecția datelor

În cuprinsul Regulamentului(UE) 2016/679, acest *organ cu personalitate juridică* este desemnat prin termenul „Comitetul”. Reprezentarea Comitetului este asigurată de către președinte<sup>8</sup>, iar *componenta* include șeful unei autorități de supraveghere din fiecare stat membru și din Autoritatea Europeană pentru Protecția Datelor. Pentru statul membru în care funcționează mai multe autorități de supraveghere, responsabile de monitorizarea aplicării Regulamentului, există obligația de a numi un reprezentant comun, potrivit dreptului intern. Fără drept de vot, Comisia are dreptul de a participa la activitățile Comitetului; președintele Comitetului comunică acesteia activitățile desfășurate de Comitet (art. 68). Secretariatul Comitetului este asigurat de Autoritatea Europeană pentru Protecția Datelor. Sprijinul oferit Comitetului de către secretariat este analitic, logistic, administrativ și presupune, în principal: gestiunea curentă a activităților Comitetului; comunicarea între membrii Comitetului, comunicarea cu publicul și cu instituțiile; pregătirea și monitorizarea acțiunilor ulterioare reuniunilor Comitetului; redactarea și publicarea avizelor, deciziilor privind soluționarea litigiilor dintre autoritățile de supraveghere, redactarea și publicarea altor texte adoptate de către Comitet (art. 75).

Principiul care guvernează activitatea Comitetului este *independența* în realizarea sarcinilor și exercitarea competențelor. Comitetul nu solicită și nu acceptă instrucțiuni de la o parte externă, în îndeplinirea atribuțiilor ce îi revin.

La nivelul Uniunii, Comitetul asigură aplicarea riguroasă a Regulamentului, iar multiplele sale sarcini sunt menționate în art. 70. Între cele semnificative, se înscriu: consilierea Comisiei cu privire la orice aspect legat de protecția datelor cu caracter personal în cadrul Uniunii, inclusiv cu privire la propunerile de modificare a Regulamentului; prezentarea avizului pentru evaluarea caracterului adecvat al nivelului de protecție într-o țară terță sau o organizație internațională, inclusiv

---

<sup>8</sup> Sarcinile președintelui sunt circumscrise convocării reuniunilor Comitetului, stabilirii ordinii de zi, notificării deciziilor autorităților de supraveghere naționale, asigurării îndeplinirii la timp a atribuțiilor Comitetului, inclusiv în ce privește mecanismul coerenței.

pentru a determina dacă o țară terță, un teritoriu, unul sau mai multe sectoare specificate din acea țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat; promovarea cooperării și schimbului eficient bilateral și multilateral de informații și bune practici între autoritățile de supraveghere.

Emiterea de orientări, recomandări și bune practici este una dintre sarcinile Comitetului și funcționează pentru aspecte cum sunt: procedurile de ștergere a linkurilor către datele cu caracter personal, a copiilor sau a reproducerilor acestora, de care dispun serviciile de comunicații accesibile publicului; detalierea criteriilor și condițiilor pentru deciziile bazate pe crearea de profiluri; stabilirea încălcării securității datelor cu caracter personal, circumstanțele speciale în care un operator sau o persoană împuternicită de către operator are obligația de a notifica încălcarea securității datelor cu caracter personal; circumstanțele în care o încălcare a securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice; detalierea criteriilor și cerințelor pentru transferurile de date cu caracter personal; stabilirea procedurilor comune de raportare de către persoanele fizice a încălcărilor Regulamentului.

Activitatea Comitetului include și informarea publicului, Parlamentului European, Consiliului și Comisiei, privind protecția persoanelor și prelucrarea datelor în Uniune și, dacă este relevant, în țări terțe și organizații internaționale. Informațiile sunt diseminate prin intermediul raportului anual al Comitetului, redactat conform art. 71 din Regulament (raportul cuprinde și revizuirea aplicării practice a orientărilor, recomandărilor, bunelor practici pe care acest organism le elaborează în îndeplinirea sarcinilor sale).

### **III. Concluzii**

Articulat, mecanismul cooperării instituit prin Regulamentul (UE) 2016/679 este destinat consolidării protecției drepturilor și libertăților persoanelor fizice, în raport cu prelucrarea datelor care le privesc. Buna funcționare a relațiilor între autoritățile de supraveghere naționale, Comisie și Comitet este esențială pentru asigurarea circuitului transfrontalier de prelucrare a datelor personale. Este imperios necesară urgentarea demersurilor de adoptare/aplicare a actelor normative ce conțin norme speciale în sectorul comunicațiilor electronice, precum și actualizarea - inclusiv corelarea unora dintre regulamentele în vigoare cu noul Regulament (UE) 2016/679, care constituie cadrul comun de reglementare europeană a prelucrării datelor.