Compendiu / legislație /jurisprudență europeană privind protecția datelor cu caracter personal

Europa se află în avangarda protecției datelor la nivel mondial. Standardele UE în materie de protecție a datelor se bazează pe Convenția 108 a Consiliului Europei, pe instrumentele UE – inclusiv Regulamentul general privind protecția datelor și Directiva privind protecția datelor pentru autoritățile polițienești și judiciare din sectorul penal – și pe jurisprudența Curții Europene a Drepturilor Omului și a Curții de Justiție a Uniunii Europene.

Abrevieri și acronime

AELS	Asociația Europeană a Liberului Schimb
AEPD	Autoritatea Europeană pentru Protecția Datelor
APD	Autoritate pentru protecția datelor
BCR	Reguli corporatiste obligatorii
Carta	Carta drepturilor fundamentale a Uniunii Europene
CE	Comunitatea Europeană
CEaDO	Convenția europeană a drepturilor omului
CEDO	Curtea Europeană a Drepturilor Omului
CEPD	Comitetul European pentru Protecția Datelor
CETS	Seria de tratate ale Consiliului Europei
CJUE	Curtea de Justiție a Uniunii Europene (înainte de decembrie 2009, denumită Curtea Europeană de Justiție, CEJ)
CoE	Consiliul Europei
Convenția 108	Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Consiliul Europei) Protocolul de modificare (CETS nr. 223) a Convenției 108 („Convenția 108 modernizată") a fost adoptat cu ocazia celei de a 128-a reuniuni a Comitetului de Miniștri al Consiliului Europei, care a avut loc la Elsinore, Danemarca (17-18 mai 2018). Trimiterile la „Convenția 108 modernizată" se referă la convenția modificată prin Protocolul CETS nr. 223.
CRM	Gestionarea relațiilor cu clienții
C-SIS	Sistemul Central de Informații Schengen
DUDO	Declarația universală a drepturilor omului
EFSA	Autoritatea Europeană pentru Siguranța Alimentară
ENISA	Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor
EPPO	Parchetul European
ESMA	Autoritatea Europeană pentru Valori Mobiliare și Piețe
eTEN	Rețele de telecomunicații transeuropene

eu-LISA	Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție
EuroPriSe	Marca europeană de protecție a vieții private
FRA	Agenția pentru Drepturi Fundamentale a Uniunii Europene
GCS	Grupul de coordonare a supravegherii
GPS	Sistem de poziționare globală
ISP	Furnizor de servicii de internet
JO	Jurnalul Oficial
MEA	Mandat european de arestare
N-SIS	Sistemul Național de Informații Schengen
OCDE	Organizația pentru Cooperare și Dezvoltare Economică
OCS	Organism comun de supraveghere
ONG	Organizație neguvernamentală
ONU	Organizația Națiunilor Unite
PIDCP	Pactul internațional cu privire la drepturile civile și politice
PIN	Număr personal de identificare
PNR	Registrul cu numele pasagerilor
RGPD	Regulamentul general privind protecția datelor
RPD	Responsabil cu protecția datelor
SEE	Spațiul Economic European
SEPA	Zona unică de plăți în euro
SIS	Sistemul de informații Schengen
SIV	Sistemul de informații al vămilor
SWIFT	Societatea pentru Telecomunicații Financiare Interbancare Mondiale
TFUE	Tratatul privind funcționarea Uniunii Europene
TIC	Tehnologia informației și comunicațiilor
TUE	Tratatul privind Uniunea Europeană
TVCI	Televiziune cu circuit închis
UE	Uniunea Europeană
UNE	Unitate națională Europol
VIS	Sistemul de informații privind vizele

1. PRINCIPIILE ESENȚIALE ALE LEGISLAȚIEI EUROPENE PRIVIND PROTECȚIA DATELOR

Articolul 5 din Regulamentul general privind protecția datelor stabilește principiile care reglementează prelucrarea datelor cu caracter personal. Aceste principii se referă la următoarele:

- **legalitate, echitate și transparență;**
- **limitări legate de scop;**
- **reducerea la minimum a datelor;**
- **exactitatea datelor;**
- **limitări legate de stocare;**
- **integritate și confidențialitate.**

Principiile servesc ca punct de plecare pentru dispoziții mai detaliate în articolele ulterioare ale regulamentului. Acestea apar, de asemenea, la articolele 5, 7, 8 și 10 din Convenția 108 modernizată.

1.1. Principiile de legalitate, echitate și transparență a prelucrării

Principalele elemente

- **Principiile de legalitate, echitate și transparență se aplică tuturor prelucrărilor de date cu caracter personal.**
- **În conformitate cu RGPD, legalitatea implică următoarele elemente:**
  - **consimțământul persoanei vizate;**
  - **necesitatea de a încheia un contract;**
  - **o obligație legală;**
  - **necesitatea protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane;**
  - **necesitatea de a realiza o activitate în interes public;**
  - **necesitatea protejării intereselor legitime ale operatorului**

- **Prelucrarea datelor cu caracter personal trebuie efectuată în mod transparent.**
  - **Înainte de a prelucra datele persoanelor vizate, operatorii trebuie să informeze aceste persoane, printre altele, cu privire la scopul prelucrării, precizând identitatea și adresa operatorului.**
  - **Informațiile privind operațiunile de prelucrare trebuie furnizate în limbaj clar și simplu, pentru a permite persoanelor vizate să înțeleagă cu ușurință normele, riscurile, garanțiile și drepturile implicate.**
  - **Persoanele vizate au dreptul de acces la datele lor, indiferent de locul unde sunt prelucrate acestea.**

1.1.1. Legalitatea prelucrării

Legislația UE și a CoE în materie de protecție a datelor impune ca prelucrarea datelor cu caracter personal să respecte principiul legalității[1]. Prelucrarea legală implică consimțământul persoanei vizate sau un alt temei juridic prevăzut de legislația în materie de protecție a datelor[2]. **Pe lângă consimțământ, articolul 6 alineatul (1) din RGPD menționează cinci temeiuri juridice pentru prelucrare, și anume atunci când prelucrarea datelor cu caracter personal este necesară: pentru executarea unui contract, pentru îndeplinirea unei sarcini care rezultă din exercitarea autorității publice, în vederea îndeplinirii unei obligații legale, în scopul intereselor legitime urmărite de operator sau de părți terțe sau pentru a proteja interesele vitale ale persoanei vizate**.

1.1.2. Echitatea prelucrării

Pe lângă legalitatea prelucrării, legislația UE și a CoE în materie de protecție a datelor impun ca datele cu caracter personal să fie prelucrate în mod echitabil[3]. **Principiul echității prelucrării reglementează în primul rând relația dintre operator și persoana vizată.**

---

1 Convenția 108 modernizată, articolul 5 alineatul (3); Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a).

2 Carta drepturilor fundamentale a Uniunii Europene, articolul 8 alineatul (2); Regulamentul general privind protecția datelor, considerentul 40 și articolele 6-9; Convenția 108 modernizată, articolul 5 alineatul (2); Raportul explicativ privind Convenția 108 modernizată, punctul 41.

3 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (a); Convenția 108 modernizată, articolul 5 alineatul (4) litera (a).

Operatorii ar trebui să înștiințeze persoanele vizate și publicul larg că vor prelucra datele într-un mod legal și transparent și trebuie să fie în măsură să demonstreze conformitatea operațiunilor de prelucrare cu RGPD. Operațiunile de prelucrare nu trebuie efectuate în secret, iar persoanele vizate ar trebui să fie conștiente de riscurile potențiale. În plus, operatorii, în măsura în care este posibil, trebuie să acționeze într-un mod care să respecte cu promptitudine voința persoanei vizate, în special atunci când consimțământul acesteia constituie temeiul juridic al prelucrării datelor.

Exemplu: În cauza K.H. și alții/Slovacia reclamantele – mai multe femei de etnie romă – fuseseră tratate în două spitale din estul Slovaciei în timpul sarcinii și al nașterii. Ulterior, niciuna dintre ele nu a mai reușit să conceapă copii, în ciuda încercărilor repetate. Instanțele naționale au impus spitalelor să permită reclamantelor și reprezentanților acestora să consulte evidențele medicale și să extragă manual fragmente din acestea, dar au respins cererea de a realiza fotocopii după documente, invocând ca motiv prevenirea abu- zurilor. Obligațiile pozitive ale statelor în temeiul articolului 8 din Convenția europeană a drepturilor omului includ în mod necesar o obligație de a pune la dispoziția persoanei vizate copii ale fișierelor sale de date. Statului îi revenea sarcina de a stabili modalitățile de copiere a fișierelor de date cu caracter personal sau, după caz, de a prezenta motivele imperioase ale refuzului de a face acest lucru. În cazul reclamantelor, instanțele naționale au justificat interzicerea realizării de copii după documentele medicale în principal prin necesitatea de a proteja informațiile în cauză împotriva abuzului. CEDO nu a reușit totuși să identifice în ce fel reclamantele, cărora li se acordase, oricum, accesul la întreaga documentație medicală care le privea, ar fi putut utiliza abuziv informații referitoare la ele însele. În plus, riscul unui astfel de abuz ar fi putut fi împiedicat prin alte mijloace decât refuzul de a acorda reclamantelor permisiunea realizării de fotocopii după documentele medicale, de exemplu prin limitarea categoriilor de persoane care aveau dreptul de acces la aceste documente. Statul nu a demonstrat existența unor motive suficient de convingătoare pentru a refuza reclamantelor accesul eficace la informațiile referitoare la sănătatea lor. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

În ceea ce privește serviciile internet, caracteristicile sistemelor de prelucrare a datelor trebuie să permită ca persoanele vizate să înțeleagă cu adevărat ce se întâmplă cu datele lor.

Exemplu: Un departament de cercetare al unei universități efectuează un experiment prin care analizează schimbările de dispoziție a 50 de subiecți. Aceștia trebuie să își consemneze gândurile într-un fișier electronic, din oră în oră, la anumite momente stabilite. Cele 50 de persoane și-au dat consimțământul pentru acest proiect și pentru această utilizare specifică a datelor lor de către universitate. Departamentul de cercetare descoperă în curând că înregistrarea în format electronic a gândurilor persoanelor ar fi foarte utilă pentru un alt proiect, axat pe sănătatea mintală, sub coordonarea unei alte echipe. Chiar dacă universitatea, în calitate de operator, ar fi putut să folosească aceleași date pentru activitatea unei alte echipe fără a mai lua măsuri suplimentare pentru a asigura legalitatea prelucrării acestor date, având în vedere compatibilitatea scopurilor, universitatea a informat totuși subiecții și a cerut din nou consimțământul, urmând codul său de etică în domeniul cercetării și principiul echității prelucrării.

1.1.3. Transparența prelucrării

Legislația UE și a CoE în materie de protecție a datelor impune ca prelucrarea datelor cu caracter personal să se facă „în mod [...] transparent față de persoana vizată”[4].

Acest principiu stabilește obligația operatorului de a lua toate măsurile adecvate pentru a informa persoanele vizate – care pot fi utilizatori sau clienți – cu privire la modul în care sunt utilizate datele lor[5]. Transparența se poate referi la informațiile furnizate persoanei fizice înainte de începerea prelucrării, la informațiile care ar trebui să fie ușor accesibile persoanelor vizate în timpul prelucrării, precum și la informațiile furnizate persoanelor vizate în urma unei cereri de acces la propriile lor date.

4 Regulamentul general privind protecția datelor, articolul 5 alineatul (1); Convenția 108 modernizată, articolul 5 alineatul (4) litera (a) și articolul 8.

5 Regulamentul general privind protecția datelor, articolul 12

Exemplu: În cauza Haralambie/România, reclamantului i s-a acordat accesul la informațiile deținute despre el de serviciul secret doar la cinci ani de la cererea sa. CEDO a reiterat faptul că persoanele care fac obiectul unor dosare cu caracter personal deținute de autoritățile publice au un interes vital să acceadă la aceste dosare. Autoritățile aveau obligația de a pune la dispoziție o procedură eficace de obținere a accesului la aceste informații. CEDO a considerat că nici cantitatea fișierelor transmise, nici deficiențele sistemului de arhivare nu justificau întârzierea de cinci ani în acordarea accesului reclamantului la dosarele care îl priveau. Autoritățile nu au furnizat reclamantului o procedură eficace și accesibilă pentru a-i permite să obțină accesul la dosarele care îl priveau într-un termen rezonabil. Curtea a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

Operațiunile de prelucrare trebuie să le fie explicate persoanelor vizate într-un mod ușor accesibil, care să garanteze că acestea înțeleg ce se va întâmpla cu datele lor. Aceasta înseamnă că persoana vizată ar trebui să cunoască scopul specific al prelucrării datelor cu caracter personal în momentul colectării acestora. Transparența prelucrării necesită utilizarea unui limbaj clar și simplu. Persoanele vizate ar trebui să înțeleagă riscurile, normele, garanțiile și drepturile aferente prelucrării datelor lor cu caracter personal.

Legislația CoE precizează, de asemenea, că este obligatoriu ca operatorul să furnizeze persoanei vizate, în mod proactiv, anumite informații esențiale. Informați- ile privind numele și adresa operatorului (sau a operatorilor asociați), temeiul juridic și scopurile prelucrării datelor, categoriile de date prelucrate și destinatarii, precum și modalitățile de exercitare a drepturilor pot fi furnizate în orice format adecvat (printr-un site web, prin instrumente tehnologice instalate pe dispozitive personale etc.), atât timp cât informațiile sunt prezentate persoanei vizate în mod corect și eficace. Informațiile prezentate trebuie să fie ușor accesibile, lizibile, ușor de înțeles și adaptate persoanelor vizate în cauză (de exemplu, după caz, într-un limbaj accesibil copiilor).

Trebuie furnizate, de asemenea, orice informații suplimentare necesare sau utile pentru a asigura o prelucrare echitabilă a datelor, cum ar fi perioada de păstrare a datelor, explicarea raționamentului care stă la baza prelucrării datelor sau informații despre transferurile de date către un destinatar dintr-o altă parte membră sau nemembră (precizându-se inclusiv dacă o anumită parte nemembră oferă un nivel adecvat de protecție sau măsurile luate de operator pentru a garanta un astfel de nivel adecvat de protecție a datelor)[6].

6 Regulamentul general privind protecția datelor, articolele 13 și 14.

În temeiul dreptului de acces, persoana vizată are dreptul de a i se comunica, la cerere, de către operator, dacă datele sale sunt prelucrate și, în caz afirmativ, care date fac obiectul respectivei prelucrări. În plus, în temeiul dreptului la informare, persoanele ale căror date sunt prelucrate trebuie să fie informate în mod proactiv de operatori sau de persoanele împuternicite de aceștia, în principiu înainte de începerea activității de prelucrare, cu privire la scopurile, durata și mijloacele de prelucrare, printre alte detalii.

În anumite situații sunt permise derogări de la obligația de a informa persoanele vizate cu privire la prelucrarea datelor.

Exemplu: Cauza *Smaranda Bara și alții/Președintele Casei Naționale de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)* viza transmiterea datelor fiscale referitoare la venitul persoanelor fizice care desfășoară activități independente de la Agenția Națională de Administrare Fiscală către Casa Națională de Asigurări de Sănătate din România, pe baza acestor date solicitându-se plata contribuțiilor datorate la asigurările de sănătate. CJUE i s-a solicitat să stabilească dacă persoanei vizate ar fi trebuit să i se furnizeze informații privind identitatea operatorului de date și scopul transmiterii datelor înainte de prelucrarea acestor date de către Casa Națională de Asigurări de Sănătate. CJUE a stabilit că, atunci când o autoritate a administrației publice dintr-un stat membru transmite date cu caracter personal unei alte autorități a administrației publice care prelucrează ulterior aceste date, persoanele vizate trebuie să fie informate cu privire la această transmitere sau prelucrare.

1.2. Principiul limitărilor legate de scop

Principalele elemente

- **Scopul prelucrării datelor trebuie să fie definit înainte de începerea prelucrării.**
- Nu se poate face o prelucrare ulterioară a datelor într-un mod care să fie incompatibil cu scopul inițial, deși Regulamentul general privind protecția datelor prevede excepții de la această regulă în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică și în scopuri statistice.
- În esență, principiul limitărilor legate de scop înseamnă că orice prelucrare a datelor cu caracter personal trebuie realizată doar pentru un anumit scop inițial bine definit și pentru scopuri suplimentare determinate și compatibile cu cel inițial.

Principiul limitărilor legate de scop este unul dintre principiile fundamentale ale legislației europene în materie de protecție a datelor. **Este strâns legat de transparență, de previzibilitate și de controlul de către utilizatori: dacă scopul prelucrării este suficient de bine determinat și de clar, persoanele vizate știu**

la ce să se aștepte, iar transparența și securitatea juridică sunt sporite. În același timp, este importantă o delimitare clară a scopului pentru a permite persoanelor vizate să își exercite în mod efectiv drepturile, cum ar fi dreptul de a se opune prelucrării[7].

Principiul impune ca orice prelucrare a datelor cu caracter personal să se facă în scopuri determinate, bine definite, și doar în acele scopuri suplimentare care sunt compatibile cu scopul inițial[8]. Prelucrarea datelor cu caracter personal în scopuri nedefinite și/sau nelimitate este, așadar, ilegală. Nu este legală nici prelucrarea datelor cu caracter personal fără un scop determinat, bazată exclusiv pe considerația că ar putea fi utilă la un moment dat în viitor. Legitimitatea prelucrării datelor cu caracter personal va depinde de scopul prelucrării, care trebuie să fie explicit, determinat și legitim.

Orice scop nou de prelucrare a datelor care nu este compatibil cu scopul inițial trebuie să aibă propriul temei juridic special și nu se poate baza pe faptul că datele au fost dobândite sau prelucrate inițial în alt scop legitim. Prelucrarea legitimă este limitată la scopul specificat inițial și orice scop nou de prelucrare va necesita un nou temei juridic separat.

Exemplu: O companie aeriană colectează date de la pasagerii săi pentru ca agențiile de rezervare de bilete să gestioneze zborurile în mod adecvat. Compania aeriană va avea nevoie de date privind: numerele de loc ale pasa- gerilor, limitări fizice speciale, cum ar fi necesitatea unui scaun cu rotile, și cerințe alimentare speciale, cum ar fi alimente de tip cușer sau halal. În cazul în care companiilor aeriene li se solicită să transmită aceste date, care sunt incluse în registrele cu numele pasagerilor, către autoritățile în domeniul imigrației de la aeroportul de debarcare, aceste date sunt astfel utilizate în scopuri de control al imigrației, care diferă de scopul inițial pentru care au fost colectate. Prin urmare, transmiterea acestor date către o autoritate din domeniul imigrației va necesita un temei juridic nou și separat.

De exemplu, divulgarea datelor cu caracter personal către părți terțe pentru un scop nou va trebui să fie luată în considerare cu atenție, deoarece o astfel de divulgare va necesita probabil un temei juridic suplimentar distinct de cel al colectării datelor.

Atunci când analizează întinderea și limitele unui anumit scop, Convenția 108 modernizată și Regulamentul general privind protecția datelor recurg la conceptul de compatibilitate: utilizarea datelor în scopuri compatibile este permisă în baza temeiului juridic inițial. În consecință, prelucrarea ulterioară a datelor nu poate fi efectuată într-un mod neașteptat, inadecvat sau inacceptabil pentru persoana vizată. Pentru a evalua dacă prelucrarea ulterioară trebuie considerată compatibilă, operatorul trebuie să ia în considerare, printre altele, următoarele elemente:

---

7 Avizul 3/2013 al Grupului de lucru „Articolul 29" privind limitările legate de scop, WP 203, Bruxelles, 2 aprilie 2013

8 Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (b).

- **„orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;**

- **contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește [așteptările rezonabile ale persoanelor vizate cu privire la utilizarea ulterioară a datelor, având în vedere] relația dintre persoanele vizate și operator;**

- **natura datelor cu caracter personal [...];**
- **posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;**
- **existența unor garanții adecvate [atât în cadrul operațiunilor de prelucrare inițiale, cât și al celor ulterioare preconizate]"[9]. Acest lucru se poate face, de exemplu, prin criptare sau pseudonimizare.**

Exemplu: Societatea Sunshine achiziționează date despre clienți în cadrul operațiunilor de gestionare a relațiilor cu clienții (GRC). Ulterior, transmite aceste date către o societate de marketing direct, societatea Moonlight, care dorește să utilizeze aceste date pentru a oferi asistență în cadrul campaniilor de marketing ale unor societăți terțe. Transmiterea datelor de către Sunshine în scopul utilizării în campanii de marketing ale altor societăți constituie o utilizare ulterioară a datelor într-un scop nou, care este incompatibil cu GRC, scopul inițial în care colectase societatea Sunshine datele despre cli- enți. Prin urmare, transmiterea datelor către societatea Moonlight necesită propriul temei juridic.

În schimb, utilizarea de către societatea Sunshine a datelor GRC pentru propriul scop de marketing, și anume transmiterea de mesaje de marketing către clienți în legătură cu produsele sale, este general acceptată drept scop compatibil.

Regulamentul general privind protecția datelor și Convenția 108 modernizată prevăd că „prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice" este considerată *a priori* compatibilă cu scopul inițial. Cu toate acestea, trebuie aplicate măsuri de protecție adecvate, cum ar fi anonimizarea, criptarea sau pseudonimizarea datelor și restricționarea accesului la date în cazul unei prelucrări ulterioare a datelor cu caracter personal. Regulamentul general privind protecția datelor adaugă că „în cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare

9 Regulamentul general privind protecția datelor, considerentul 50 și articolul 6 alineatul (4); Raportul explicativ privind Convenția 108 modernizată, punctul 49.

datele cu caracter personal, indiferent de compatibilitatea scopurilor”[10]. **Prin urmare, atunci când se întreprinde o prelucrare ulterioară, persoana vizată ar trebui să fie informată cu privire la scopurile prelucrării, precum și la drepturile sale, cum ar fi dreptul de a se opune prelucrării[11].**

Exemplu: Societatea Sunshine a colectat și stocat date de gestionare a relațiilor cu clienții (GRC) cu privire la clienții săi. Utilizarea ulterioară a aces- tor date de către societatea Sunshine pentru o analiză statistică a comportamentului de cumpărare al clienților săi este permisă, deoarece statisticile reprezintă un scop compatibil. Nu este necesar un temei juridic suplimentar, cum ar fi consimțământul persoanelor vizate. Cu toate acestea, în vederea prelucrării ulterioare a datelor cu caracter personal în scopuri statistice, societatea Sunshine trebuie să instituie garanții adecvate pentru drepturile și libertățile persoanei vizate. Măsurile tehnice și organizatorice pe care trebuie să le pună în aplicare Sunshine pot include pseudonimizarea datelor.

1.3. Principiul reducerii la minimum a datelor

Principalele elemente

- Prelucrarea datelor trebuie să se limiteze la ceea ce este necesar pentru îndeplinirea **unui scop legitim.**
- Prelucrarea datelor cu caracter personal ar trebui să aibă loc numai atunci când scopul **prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace.**
- Prelucrarea datelor nu poate interveni în mod disproporționat asupra intereselor, **drepturilor și libertăților în cauză.**

Vor fi prelucrate numai datele care sunt „adecvate, relevante și nu depășesc ceea ce este necesar în raport cu scopurile în care sunt colectate și/sau prelucrate ulterior”. Categoriile de date alese pentru prelucrare trebuie să fie necesare pentru a atinge scopul general declarat al operațiunilor de prelucrare, iar un operator ar

10 Regulamentul general privind protecția datelor, considerentul 50.

11 Convenția 108 modernizată, articolul 5 alineatul (4) litera (c); Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (c).

trebui să limiteze colectarea de date strict la acele informații direct relevante pentru scopul specific urmărit de prelucrare.

Exemplu: În cauza *Digital Rights Ireland*, CJUE a examinat valabilitatea Directivei privind păstrarea datelor, care urmărea armonizarea dispozițiilor naționale privind păstrarea datelor cu caracter personal generate sau pre- lucrate de către serviciile sau rețelele de comunicații electronice accesibile publicului pentru a fi transmise eventual autorităților competente în scopul combaterii infracțiunilor grave, cum ar fi criminalitatea organizată și terorismul. Deși s-a constatat că acest scop răspunde efectiv unui obiectiv de interes general, modul generalizat în care directiva viza „toate persoanele și toate mijloacele de comunicare electronică, precum și ansamblul datelor de trafic, fără a face vreo diferențiere, limitare sau excepție în funcție de obiectivul combaterii infracțiunilor grave" a fost considerat problematic.

În plus, prin utilizarea tehnologiilor speciale de îmbunătățire a confidențialității, uneori se poate evita complet utilizarea datelor cu caracter personal sau se pot aplica măsuri de reducere a posibilității de a asocia datele cu persoana vizată (de exemplu, prin pseudonimizare), ceea ce are ca rezultat o soluție care protejează viața privată. Acest lucru este potrivit în special pentru sistemele de prelucrare mai extinse.

Exemplu: Consiliul local al unui oraș oferă un card inteligent utilizatorilor frecvenți ai sistemului public de transport în schimbul unei taxe. Cardul poartă numele utilizatorului în formă scrisă pe suprafața sa și, de asemenea, în format electronic, în cip. Ori de câte ori persoana folosește autobuzul sau tramvaiul, cardul inteligent trebuie validat cu ajutorul dispozitivelor de citire instalate, de exemplu, în autobuze și tramvaie. Datele citite de dispozitiv sunt comparate electronic cu o bază de date care conține numele persoanelor care au cumpărat cardul de călătorie. Acest sistem nu respectă în mod optim principiul reducerii la minimum a datelor, întrucât verificarea aspectului dacă o persoană are permisiunea de a utiliza mijloacele de transport se poate realiza fără compararea datelor cu caracter personal de pe cipul cardului cu baza de date. Ar fi suficient, de exemplu, ca cipul cardului să conțină o imagine electronică specială, cum ar fi un cod de bare, care, la validarea cu ajutorul dispozitivului de citire, ar confirma valabilitatea cardului. Un astfel de sistem nu înregistrează cine, când și ce mijloc de transport a folosit. Aceasta ar fi soluția optimă în sensul principiului reducerii la minimum a datelor, întrucât acest principiu are ca rezultat obligația de a reduce la minimum colectarea de date.

Articolul 5 alineatul (1) din Convenția 108 modernizată conține o cerință de proporționalitate pentru prelucrarea datelor cu caracter personal în raport cu scopul legitim urmărit.

1.4. Principiul exactității datelor

Principalele elemente

- Operatorul trebuie să pună în aplicare principiul exactității datelor în cadrul tuturor **operațiunilor de prelucrare.**
- **Datele inexacte trebuie să fie șterse sau rectificate fără întârziere.**
- Este posibil să fie necesar ca datele să fie verificate periodic și actualizate pentru a se **asigura exactitatea acestora.**

Un operator care deține informații cu caracter personal nu utilizează aceste informații fără a lua măsuri pentru a se asigura cu suficientă certitudine că datele sunt exacte și actualizate.

Obligația de a asigura exactitatea datelor trebuie analizată în contextul scopului prelucrării datelor. [12]

Exemplu : În cauza *Rijkeboer*, CJUE a examinat solicitarea unui cetățean neerlandez de a primi de la administrația locală din orașul Amsterdam informații cu privire la identitatea persoanelor cărora le-au fost comunicate evidențele despre el deținute de autoritatea locală în cei doi ani anteriori, precum și cu privire la conținutul datelor divulgate. CJUE a stabilit că „[dreptul] la respectarea vieții private presupune ca persoana vizată să poată să se asi- gure că datele sale cu caracter personal sunt prelucrate în mod exact și legal, cu alte cuvinte, în special, că datele de bază care o privesc sunt exacte și sunt adresate unor destinatari autorizați". În continuare, CJUE a făcut trimitere la preambulul Directivei privind protecția datelor, care prevede că persoanele vizate trebuie să poată beneficia de dreptul de acces la datele lor cu caracter personal, pentru a se asigura de exactitatea datelor.·

Pot exista și cazuri în care actualizarea datelor stocate este interzisă prin lege, întrucât scopul stocării datelor este, în principal, acela de a consemna evenimente sub forma unor „instantanee istorice".

12 Hotărârea CJUE din 7 mai 2009 în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*.

Exemplu: Dosarul medical aferent unei intervenţii chirurgicale nu trebuie modificat sau, cu alte cuvinte, „actualizat", chiar dacă ulterior se dovedeşte că unele observaţii menţionate în dosar au fost greşite. În astfel de situaţii, pot fi făcute numai completări la observaţiile din dosar, atât timp cât acestea sunt marcate în mod clar ca fiind contribuţii adăugate ulterior.

Pe de altă parte, există situaţii în care verificarea periodică a exactităţii datelor, inclusiv actualizarea, constituie o necesitate absolută, date fiind daunele potenţiale care pot fi cauzate persoanei vizate în cazul în care datele ar rămâne inexacte.

Exemplu: Dacă o persoană doreşte să încheie un contract de creditare cu o instituţie bancară, banca va verifica în mod normal bonitatea potenţialului client. În acest sens există baze de date speciale, care conţin date privind istoricul creditării persoanelor fizice. Dacă o astfel de bază de date furnizează date incorecte sau perimate cu privire la o persoană, această persoană se poate confrunta cu efecte negative. Prin urmare, operatorii unor astfel de baze de date trebuie să depună eforturi deosebite pentru a respecta principiul exactităţii datelor

1.5. Principiul limitărilor legate de stocare

Principalele elemente

- Principiul limitărilor legate de stocare implică eliminarea sau anonimizarea datelor **imediat ce acestea nu mai servesc scopurilor pentru care au fost colectate.**

Articolul 5 alineatul (1) litera (e) din RGPD şi, de asemenea, articolul 5 alineatul (4) litera (e) din Convenţia 108 modernizată impune ca datele cu caracter personal să fie „păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele". Prin urmare, datele trebuie şterse sau anonimizate după atingerea acestor scopuri. În acest scop, „ar trebui să se stabilească de către operator termene pentru ştergere sau revizuirea periodică" pentru a asigura faptul că datele nu sunt păstrate mai mult decât este necesar.

În cauza *S. și Marper*, CEDO a concluzionat că principiile fundamentale ale instrumentelor relevante ale Consiliului Europei, precum și dreptul și practica celorlalte părți contractante impun ca durata de păstrare a datelor să fie proporțională cu scopul colectării și limitată, în special în sectorul polițienesc[13].

Exemplu: În cauza *S. și Marper*, CEDO a statuat că păstrarea pe durată nedeterminată a amprentelor digitale, a probelor celulare și a profilurilor ADN ale celor doi reclamanți a fost disproporționată și nenecesară într-o societate democratică, având în vedere că procedurile penale împotriva celor doi reclamanți se încheiaseră prin achitare, respectiv suspendare.

Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04

Limitarea duratei de stocare a datelor cu caracter personal se aplică numai datelor păstrate într-o formă care permite identificarea persoanelor vizate. Prin urmare, sto- carea legală a datelor care nu mai sunt necesare se poate realiza prin anonimizarea acestora.

Datele arhivate în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice pot fi păstrate pe perioade mai lungi, cu condiția ca respectivele date să fie utilizate exclusiv în aceste scopuri. Trebuie să se pună în aplicare măsuri de ordin tehnic și organizatoric adecvate pentru stocarea și utilizarea continuă a datelor cu caracter personal în vederea garantării drepturilor și libertăților persoanei vizate.

Exemplu: În cauza Digital Rights Ireland, CJUE a examinat valabilitatea Directivei privind păstrarea datelor, care urmărea armonizarea dispozițiilor naționale privind păstrarea datelor cu caracter personal generate sau pre- lucrate de către serviciile sau rețelele de comunicații electronice accesibile publicului în scopul combaterii infracțiunilor grave, cum ar fi criminalitatea organizată și terorismul. Directiva privind păstrarea datelor a impus o perioadă de păstrare a datelor de „cel puțin șase luni, fără a se face vreo distincție între categoriile de date prevăzute la articolul 5 din această directivă în funcție de utilitatea lor eventuală în scopul realizării obiectivului urmărit sau în funcție de persoanele vizate". CJUE a menționat, de asemenea, problema absenței criteriilor obiective în Directiva privind păstrarea datelor, pe baza cărora ar trebui stabilită perioada exactă de păstrare a datelor – care poate varia de la minimum șase luni până la maximum 24 de luni – pentru a se asigura faptul că această perioadă este limitată la strictul necesar.

13 Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04; vezi, de asemenea, de exemplu, Hotărârea CEDO din 13 noiembrie 2012 în cauza *M. M./ Regatul Unit*, nr. 24029/07

1.6. Principiul securității datelor

Principalele elemente

- Securitatea și confidențialitatea datelor cu caracter personal sunt esențiale pentru **prevenirea efectelor negative asupra persoanei vizate.**
- **Măsurile de securitate pot fi de natură tehnică și/sau organizatorică.**
- **Pseudonimizarea este un proces care poate proteja datele cu caracter personal.**
- Adecvarea măsurilor de securitate trebuie să fie stabilită de la caz la caz și revizuită **periodic.**

Exemplu: Propoziția „Charles Spencer, născut la 3 aprilie 1967, este tatăl a patru copii, doi băieți și două fete" poate fi, de exemplu, pseudonimizată după cum urmează:

„C. S. 1967 este tatăl a patru copii, doi băieți și două fete"; sau

„324 este tatăl a patru copii, doi băieți și două fete"; sau

„YESz3201 este tatăl a patru copii, doi băieți și două fete".

Principiul securității datelor implică punerea în aplicare, în cadrul prelucrării datelor cu caracter personal, a măsurilor tehnice sau organizatorice adecvate pentru a asigura protecția datelor împotriva accesului, utilizării, modificării, divulgării, pierderii, distrugerii sau deteriorării accidentale, neautorizate sau ilegale. RGPD prevede că operatorul și persoana împuternicită de acesta ar trebui să țină seama, la punerea în aplicare a acestor măsuri, de „stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoane- lor fizice"[14]. În funcție de circumstanțele specifice ale fiecărui caz, măsurile tehnice și organizatorice adecvate ar putea include, de exemplu, pseudonimizarea și criptarea datelor cu caracter personal și/sau testarea și evaluarea periodică a eficacității măsurilor, pentru a asigura faptul că prelucrarea datelor se face în condiții de siguranță.

[14] Regulamentul general privind protecția datelor, articolul 32 alineatul (1).

Pseudonimizarea datelor înseamnă înlocuirea cu un pseudonim a acelor atribute conținute în datele cu caracter personal care permit identificarea persoanei vizate și păstrarea acestor atribute separat de date, prin intermediul unor măsuri tehnice sau organizatorice. Procesul de pseudonimizare nu trebuie confundat cu cel de anonimizare.

Datele cu caracter personal care au atribute criptate sau păstrate separat sunt utilizate în multe situații ca mijloc de păstrare a secretului identității persoanelor. Acest lucru este foarte util atunci când operatorii de date trebuie să se asigure că lucrează cu aceleași persoane vizate, însă nu au nevoie, sau ar trebui să nu aibă nevoie, să cunoască identitatea reală a persoanelor vizate. Acest lucru este valabil, de exemplu, atunci când un cercetător studiază evoluția unei boli la pacienți a căror identitate este cunoscută numai de spitalul la care aceștia sunt tratați și de la care cercetătorul obține antecedentele pseudonimizate. Prin urmare, pseudonimizarea este o verigă puternică în cadrul arsenalului tehnologiei de îmbunătățire a confidențialității. Poate funcționa ca element important în aplicarea principiilor referitoare la protejarea vieții private din faza de proiectare. Aceasta înseamnă că protecția datelor este integrată în structura sistemelor de prelucrare a datelor.

Exemplu: Site-urile de socializare în rețea și furnizorii de servicii e-mail permit utilizatorilor să adauge un nivel suplimentar de securitate a datelor la ser- viciile furnizate, prin introducerea autentificării pe două niveluri. Pe lângă introducerea unei parole personale, utilizatorii trebuie să parcurgă o etapă suplimentară de conectare pentru a intra în contul personal. Aceasta ar putea consta, de exemplu, în introducerea unui cod de securitate trimis către numărul de telefon mobil asociat contului personal. Astfel, verificarea în două etape oferă o protecție superioară a informațiilor cu caracter personal împotriva accesului neautorizat la conturile personale prin spargerea de parole.

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate contribui la demonstrarea îndeplinirii cerinței de securitate a prelucrării[15]. În Avizul privind implicațiile prelucrării datelor din registrele cu numele pasagerilor asupra protecției datelor, Consiliul Europei oferă alte exemple de măsuri de securitate adecvate pentru protecția datelor cu caracter personal în sistemele de registre cu numele pasagerilor. Acestea includ stocarea datelor într-un mediu fizic securizat, controlul și limitarea accesului prin nivel stratificat de coduri de acces și protejarea comunicării datelor printr-o criptografie puternică.

15 Regulamentul general privind protecția datelor, articolul 34 alineatul (2).

Raportul explicativ privind Convenția 108 modernizată oferă exemple suplimentare de măsuri de protecție adecvate, cum ar fi punerea în aplicare a obligației de păstrare a secretului profesional sau adoptarea unor măsuri tehnice de securitate calificate, cum ar fi criptarea datelor. La punerea în aplicare a unor măsuri de securitate specifice, operatorul – sau, după caz, persoana împuternicită de acesta – trebuie să ia în considerare mai multe elemente, cum ar fi natura și volumul datelor cu caracter personal prelucrate, posibilele consecințe negative asupra persoanelor vizate și necesitatea restricționării accesului la date. La punerea în aplicare a măsurilor de securitate adecvate, trebuie să se țină seama de stadiul actual al tehnologiei în materie de metode și tehnici de securitate a datelor utilizate în domeniul prelucrării datelor. Costul acestor măsuri trebuie să fie proporțional cu gravitatea și probabilitatea riscurilor potențiale. Este necesară o revizuire periodică a măsurilor de securitate, astfel încât acestea să poată fi actualizate atunci când este necesar.

În cazurile în care are loc o încălcare a securității datelor cu caracter personal, atât Convenția 108 modernizată, cât și RGPD impun operatorului să comunice autorității de supraveghere competente, fără întârzieri nejustificate, faptul că a avut loc o încăl- care care generează riscuri pentru drepturile și libertățile persoanelor· Se prevede o obligație similară de comunicare, către persoana vizată, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile respectivei persoane. Comunicarea acestor încălcări persoanelor vizate trebuie să folosească un limbaj clar și simplu. Dacă persoana împuternicită de operator ia cunoștință de o încălcare a securității datelor cu caracter personal, trebuie să informeze imediat operatorul**. În anumite situații, se pot aplica excepții de la obligația de notificare. De exemplu, operatorul nu are obligația de a anunța autoritatea de supraveghere atunci când „[încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice".** De asemenea, informarea persoanei vizate nu este necesară în cazul în care măsurile de securitate puse în aplicare asigură faptul că datele devin neinteligibile pentru persoanele neautorizate sau dacă măsurile ulterioare garantează că riscul ridicat nu mai este susceptibil să se materializeze. În cazul în care informarea persoanelor vizate cu privire la o încălcare a securității date- lor cu caracter personal ar implica eforturi disproporționate din partea operatorului, o informare publică sau o măsură similară poate asigura faptul că „persoanele vizate sunt informate într-un mod la fel de eficace".

1.7. Principiul responsabilității

Principalele elemente

- Responsabilitatea impune operatorilor și persoanelor împuternicite de aceștia să pună în aplicare în mod activ și constant măsuri de promovare și de asigurare a protecției **datelor în activitățile lor de prelucrare.**
- Operatorii și persoanele împuternicite de aceștia sunt responsabili pentru conformitatea operațiunilor de prelucrare pe care le desfășoară cu legislația în materie **de protecție a datelor și pentru respectarea obligațiilor aferente.**
- Operatorii trebuie să fie în măsură să demonstreze în orice moment persoanelor vizate, publicului larg și autorităților de supraveghere că respectă dispozițiile privind protecția datelor. Persoanele împuternicite de operatori trebuie, de asemenea, să respecte anumite obligații legate strict de responsabilitate (cum ar fi păstrarea unei evidențe a operațiunilor de prelucrare și numirea unui responsabil cu protecția datelor).

RGPD și Convenția 108 modernizată prevăd că operatorul este responsabil pentru respectarea principiilor de prelucrare a datelor cu caracter personal descrise în prezentul capitol și trebuie să o poată demonstra. În acest scop, operatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate.

Deși principiul responsabilității prevăzut la articolul 5 alineatul (2) din RGPD privește doar operatorii, se așteaptă proceduri responsabile și din partea persoanelor împuternicite de operatori, având în vedere diversele obligații ale acestora și faptul că au o legătură strânsă cu responsabilitatea.

Grupul de lucru „Articolul 29" subliniază că „tipul de proceduri și mecanisme variază în funcție de riscurile reprezentate de prelucrare și de natura datelor"

Operatorii pot asigura respectarea acestei cerințe în diverse moduri, printre care:

- **păstrarea unor evidențe cu activitățile de prelucrare și punerea acestora la dispoziția autorității de supraveghere, la cererea acesteia;**
- **în anumite situații, desemnarea unui responsabil cu protecția datelor care să fie implicat în toate aspectele legate de protecția datelor cu caracter personal;**
- **efectuarea unor evaluări ale impactului asupra protecției datelor pentru tipurile de prelucrare care ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice;**
- **asigurarea protecției datelor din faza de proiectare și a protecției implicite a datelor;**

- **punerea în aplicare a unor metode și proceduri prin care persoanele vizate să își poată exercita drepturile;**
- **aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate.**

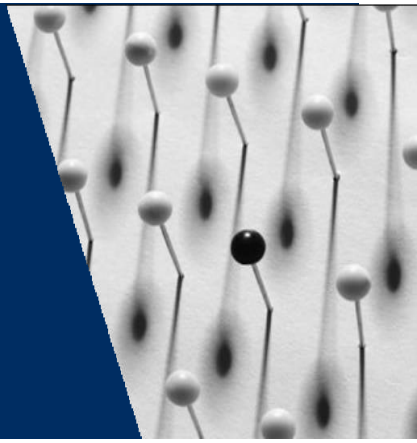
Exemplu: Un exemplu legislativ care pune în evidență principiul responsabilității este amendamentul din 2009 la Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice. Potrivit articolului 4 din versiunea modificată, directiva impune obligația de a „[asigura] punerea în aplicare a unei politici de securitate în ceea ce privește prelucrarea datelor cu caracter personal". Astfel, în ceea ce privește dispozițiile de securitate ale acestei directive, legiuitorul a decis că este necesară introducerea unei cerințe explicite pentru elaborarea și punerea în aplicare a unei politici de securitate.

Potrivit avizului Grupului de lucru „Articolul 29", esența responsabilității constă în următoarele obligații ale operatorului:

- **de a pune în aplicare măsuri care – în condiții normale – garantează respectarea normelor de protecție a datelor în contextul operațiunilor de prelucrare;**
- **de a pregăti documentația care demonstrează persoanelor vizate și autorităților de supraveghere măsurile luate în vederea respectării normelor de protecție a datelor.**

Prin urmare, principul responsabilității impune operatorilor obligația de a demonstra în mod activ conformitatea, fără să aștepte ca persoanele vizate sau autoritățile de supraveghere să semnaleze deficiențele.

Principiile au, în mod necesar, caracter general. Aplicarea lor în situații concrete lasă o anumită marjă de interpretare și de alegere a mijloacelor. În cadrul **legislației CoE**, este la latitudinea părților la Convenția 108 modernizată să clarifice această marjă de interpretare în dreptul intern. Situația în **legislația UE** este diferită: pentru stabilirea protecției datelor în cadrul pieței interne, s-a considerat necesară instituirea unor norme mai detaliate la nivelul Uniunii pentru armonizarea nivelului de protecție a datelor din cadrul legislațiilor naționale ale statelor membre. **Regulamentul general privind protecția datelor stabilește un nivel de norme detaliate, în conformitate cu principiile enunțate la articolul 5, care sunt direct aplicabile în ordinea juridică națională. Prin urmare, observațiile privind normele detaliate de protecție a datelor la nivel european prezentate în continuare privesc în principal dreptul UE.**



Jurisprudență

Jurisprudență selectată a Curții Europene a Drepturilor Omului

Accesul la datele cu caracter personal

Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83
Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09
Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81
Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09
Hotărârea CEDO [MC] din 13 februarie 2003 în cauza *Odièvre/Franța*, nr. 42326/98

Ponderarea protecției datelor cu libertatea de exprimare și cu dreptul la informare

Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Axel Springer AG/Germania*, nr. 39954/08
Hotărârea CEDO din 19 februarie 2015 în cauza *Bohlen/Germania*, nr. 53495/09
Hotărârea CEDO [MC] din 10 noiembrie 2015 în cauza *Coudec și Hachette Filipacchi Associés/Franța*, nr. 40454/07
Hotărârea CEDO [MC] din 8 noiembrie 2016 în cauza *Magyar Helsinki Bizottság/Ungaria*, nr. 18030/11
Hotărârea CEDO din 24 mai 1988 în cauza *Müller și alții/Elveția*, nr. 10737/84
Hotărârea CEDO din 25 ianuarie 2007 în cauza *Vereinigung bildender Künstler/Austria*, nr. 68354/01
Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2)*, nr. 40660/08 și 60641/08

Hotărârea CEDO [MC] din 27 iunie 2017 în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda*, nr. 931/13

Ponderarea protecției datelor cu libertatea religioasă
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05

Provocări legate de protecția datelor online
Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02

Consimțământul persoanei vizate
Hotărârea CEDO din 13 ianuarie 2015 în cauza *Elberte/Letonia*, nr. 61243/08
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05
Hotărârea CEDO din 17 februarie 2015 în cauza *Y/Turcia*, nr. 648/10

Corespondență
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 28 iunie 2007 în cauza *Association for European Integration and Human Rights și Ekimdzhiev/Bulgaria*, nr. 62540/00
Hotărârea CEDO din 14 martie 2013 în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08
Hotărârea CEDO din 18 noiembrie 2008 în cauza *Cemalettin Canli/Turcia*, nr. 22427/04
Hotărârea CEDO din 19 mai 2016 în cauza *D.L./Bulgaria*, nr. 7472/14
Hotărârea CEDO din 2 februarie 2010 în cauza *Dalea/Franța*, nr. 964/07
Hotărârea CEDO din 7 iulie 1989 în cauza *Gaskin/Regatul Unit*, nr. 10454/83
Hotărârea CEDO din 27 octombrie 2009 în cauza *Haralambie/România*, nr. 21737/03
Hotărârea CEDO din 18 octombrie 2011 în cauza *Khelili/Elveția*, nr. 16188/07
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81
Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04
Hotărârea CEDO din 21 iunie 2011 în cauza *Shimovolos/Rusia*, nr. 30194/09
Hotărârea CEDO din 25 martie 1983 în cauza *Silver și alții/Regatul Unit*, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75
Hotărârea CEDO din 26 aprilie 1979 în cauza *The Sunday Times/Regatul Unit*, nr. 6538/74

Baze de date cu caziere judiciare
Hotărârea CEDO din 22 iunie 2017 în cauza *Aycaguer/Franța*, nr. 8806/12
Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06
Hotărârea CEDO din 18 septembrie 2014 în cauza *Brunet/Franța*, nr. 21010/10
Hotărârea CEDO din 18 aprilie 2013 în cauza *M.K./Franța*, nr. 19522/09
Hotărârea CEDO din 13 noiembrie 2012 în cauza *M.M./Regatul Unit*, nr. 24029/07

Securitatea datelor
Hotărârea CEDO din 27 octombrie 2009 în cauza *Haralambie/România*, nr. 21737/03
Hotărârea CEDO din 28 aprilie 2009 în cauza *K.H. și alții/Slovacia*, nr. 32881/04

Baze de date privind ADN-ul
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04

Date GPS
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05

Date medicale personale
Hotărârea CEDO din 6 iunie 2013 în cauza *Avilkina și alții/Rusia*, nr. 1585/09
Hotărârea CEDO din 25 noiembrie 2008 în cauza *Biriuk/Lituania*, nr. 23373/03
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 29 aprilie 2014 în cauza *L.H./Letonia*, nr. 52019/07
Hotărârea CEDO din 10 octombrie 2006 în cauza *L.L./Franța*, nr. 7508/02
Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92
Hotărârea CEDO din 2 iunie 2009 în cauza *Szuluk/Regatul Unit*, nr. 36936/05
Hotărârea CEDO din 17 februarie 2015 în cauza *Y/Turcia*, nr. 648/10
Hotărârea CEDO din 25 februarie 1997 în cauza *Z/Finlanda*, nr. 22009/93

Identitate
Hotărârea CEDO din 27 aprilie 2010 în cauza *Ciubotaru/Moldova*, nr. 27138/04
Hotărârea CEDO din 25 septembrie 2012 în cauza *Godelli/Italia*, nr. 33783/09
Hotărârea CEDO [MC] din 13 februarie 2003 în cauza *Odièvre/Franța*, nr. 42326/98

Informații privind activitățile profesionale
Hotărârea CEDO din 22 decembrie 2015 în cauza *G.S.B./Elveția*, nr. 28601/11
Hotărârea CEDO din 7 iulie 2015 în cauza *M.N. și alții/San Marino*, nr. 28005/12
Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11
Hotărârea CEDO din 16 decembrie 1992 în cauza *Niemietz/Germania*, nr. 13710/88

Interceptarea comunicărilor
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 1 decembrie 2015 în cauza *Brito Ferrinho Bexiga Villa-Nova/Portugalia*, nr. 69436/10
Hotărârea CEDO din 3 aprilie 2007 în cauza *Copland/Regatul Unit*, nr. 62617/00
Hotărârea CEDO din 25 iunie 1997 în cauza *Halford/Regatul Unit*, nr. 20605/92
Hotărârea CEDO din 10 februarie 2009 în cauza *Iordachi și alții/Moldova*, nr. 25198/02
Hotărârea CEDO din 25 martie 1998 în cauza *Kopp/Elveția*, nr. 23224/94
Hotărârea CEDO din 1 iulie 2008 în cauza *Liberty și alții/Regatul Unit*, nr. 58243/00
Hotărârea CEDO din 2 august 1984 în cauza *Malone/Regatul Unit*, nr. 8691/79
Hotărârea CEDO din 18 iulie 2017 în cauza *Mustafa Sezgin Tanrıkulu/Turcia*, nr. 27473/06
Hotărârea CEDO din 3 februarie 2015 în cauza *Pruteanu/România*, nr. 30181/05
Hotărârea CEDO din 2 iunie 2009 în cauza *Szuluk/Regatul Unit*, nr. 36936/05

Obligații pentru persoanele responsabile
Hotărârea CEDO din 17 decembrie 2009 în cauza *B.B./Franța*, nr. 5335/06
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08

Date cu caracter personal
Hotărârea CEDO [MC] din 16 februarie 2000 în cauza *Amann/Elveția*, nr. 27798/95
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05
Hotărârea CEDO din 14 martie 2013 în cauza *Bernh Larsen Holding AS și alții/Norvegia*, nr. 24117/08

Fotografii
Hotărârea CEDO din 11 ianuarie 2005 în cauza *Sciacca/Italia*, nr. 50774/99
Hotărârea CEDO din 24 iunie 2004 în cauza *Von Hannover/Germania*, nr. 59320/00

Dreptul de a fi uitat
Hotărârea CEDO din 6 iunie 2006 în cauza *Segerstedt-Wiberg și alții/Suedia*, nr. 62332/00
Hotărârea CEDO [MC] din 27 iunie 2017 în cauza *Satakunnan Markkinapörssi Oy și Satamedia Oy/Finlanda*, nr. 931/13

Dreptul la opoziție
Hotărârea CEDO din 26 martie 1987 în cauza *Leander/Suedia*, nr. 9248/81

Hotărârea CEDO din 27 august 1997 în cauza *M.S./Suedia*, nr. 20837/92
Hotărârea CEDO din 10 mai 2011 în cauza *Mosley/Regatul Unit*, nr. 48009/08
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO din 2 februarie 2010 în cauza *Sinan Işık/Turcia*, nr. 21924/05

Categorii de date sensibile
Hotărârea CEDO din 18 septembrie 2014 în cauza *Brunet/Franța*, nr. 21010/10
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 6 decembrie 2012 în cauza *Michaud/Franța*, nr. 12323/11
Hotărârea CEDO [MC] din 4 decembrie 2008 în cauza *S. și Marper/Regatul Unit*, nr. 30562/04 și 30566/04

Supraveghere și aplicarea legii (rolul diferiților actori, inclusiv al autorităților de supraveghere)
Hotărârea CEDO din 17 iulie 2008 în cauza *I/Finlanda*, nr. 20511/03
Hotărârea CEDO din 2 decembrie 2008 în cauza *K.U./Finlanda*, nr. 2872/02
Hotărârea CEDO din 24 iunie 2004 în cauza *Von Hannover/Germania*, nr. 59320/00
Hotărârea CEDO [MC] din 7 februarie 2012 în cauza *Von Hannover/Germania (nr. 2)*, nr. 40660/08 și 60641/08

Metode de supraveghere
Hotărârea CEDO din 5 noiembrie 2002 în cauza *Allan/Regatul Unit*, nr. 48539/99
Hotărârea CEDO din 28 iunie 2007 în cauza *Association for European Integration and Human Rights și Ekimdzhiev/Bulgaria*, nr. 62540/00
Hotărârea CEDO [MC] din 5 septembrie 2017 în cauza *Bărbulescu/România*, nr. 61496/08
Hotărârea CEDO din 19 mai 2016 în cauza *D.L./Bulgaria*, nr. 7472/14
Hotărârea CEDO din 15 ianuarie 2015 în cauza *Dragojević/Croația*, nr. 68955/11
Hotărârea CEDO din 7 iunie 2016 în cauza *Karabeyoğlu/Turcia*, nr. 30083/10
Hotărârea CEDO din 6 septembrie 1978 în cauza *Klass și alții/Germania*, nr. 5029/71
Hotărârea CEDO [MC] din 4 mai 2000 în cauza *Rotaru/România*, nr. 28341/95
Hotărârea CEDO din 12 ianuarie 2016 în cauza *Szabó și Vissy/Ungaria*, nr. 37138/14
Hotărârea CEDO din 22 octombrie 2002 în cauza *Taylor-Sabori/Regatul Unit*, nr. 47114/99
Hotărârea CEDO din 2 septembrie 2010 în cauza *Uzun/Germania*, nr. 35623/05
Hotărârea CEDO din 16 iunie 2016 în cauza *Versini-Campinchi și Crasnianski/Franța*, nr. 49176/11
Hotărârea CEDO din 31 mai 2005 în cauza *Vetter/Franța*, nr. 59842/00
Hotărârea CEDO din 18 octombrie 2016 în cauza *Vukota-Bojić/Elveția*, nr. 61838/10

Hotărârea CEDO [MC] din 4 decembrie 2015 în cauza *Roman Zakharov/Rusia*, nr. 47143/06

Supraveghere video
Hotărârea CEDO din 5 octombrie 2010 în cauza *Köpke/Germania*, nr. 420/07
Hotărârea CEDO din 28 ianuarie 2003 în cauza *Peck/Regatul Unit*, nr. 44647/98

Probe de voce
Hotărârea CEDO din 20 decembrie 2005 în cauza *Wisse/Franța*, nr. 71611/01
Hotărârea CEDO din 25 septembrie 2001 în cauza *P.G. și J.H./Regatul Unit*, nr. 44787/98

Jurisprudență selectată a Curții de Justiție a Uniunii Europene

Jurisprudență legată de Directiva privind protecția datelor

Hotărârea CJUE din 4 mai 2017 în cauza C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme"*

[Principiul prelucrării legale: interes legitim urmărit de o parte terță]

Hotărârea CJUE din 9 martie 2017 în cauza C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*

[Dreptul la ștergerea datelor cu caracter personal; dreptul la opoziție față de prelucrare]

Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*

[Confidențialitatea comunicațiilor electronice; furnizori de servicii de comunicare electronică; obligația privind păstrarea generalizată și nediferențiată a datelor de transfer și de localizare; lipsa examinării prealabile de către o instanță sau o autoritate administrativă independentă; Carta drepturilor fundamentale a Uniunii Europene; compatibilitatea cu dreptul UE]

Hotărârea CJUE din 19 octombrie 2016 în cauza C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*

[Definiția „datelor cu caracter personal"; adrese IP; stocarea datelor de către un furnizor de servicii media online; reglementare națională care nu permite luarea în considerare a interesului legitim urmărit de operator]

Hotărârea CJUE [MC] din 6 octombrie 2015 în cauza C-362/14, *Maximillian Schrems/Data Protection Commissioner*

[Principiul prelucrării legale; drepturi fundamentale; anularea Deciziei privind „sfera de siguranță"; competențele autorităților de supraveghere independente]

Hotărârea CJUE din 1 octombrie 2015 în cauza C-230/14, *Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság*

[Competențele autorităților naționale de supraveghere]

Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, *Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții*
[Dreptul de a fi informat cu privire la prelucrarea datelor cu caracter personal]

Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*
[Conceptele „prelucrarea datelor" și „operator"]

Hotărârea CJUE din 7 noiembrie 2013 în cauza C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert și alții*
[Dreptul de a fi informat cu privire la prelucrarea datelor cu caracter personal]

Hotărârea CJUE din 11 martie 2013 în cauza T-462/12 R, *Pilkington Group Ltd/Comisia Europeană*, Ordonanța președintelui Tribunalului

Hotărârea CJUE din 30 mai 2013 în cauza C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*
[Conceptul „date cu caracter personal"; evidența timpului de lucru; principiile legate de calitatea datelor și criteriile care conferă legitimitate prelucrării datelor; accesul de către autoritatea națională responsabilă pentru monitorizarea condițiilor de lucru; obligația angajatorului de a pune la dispoziție evidența timpului de lucru, astfel încât să permită consultarea imediată a acesteia]

Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții* și *Kärntner Landesregierung și alții*
[Încălcarea legislației primare a UE de către Directiva privind păstrarea datelor; prelucrarea legală; limitările legate de scop și de stocare]

Hotărârea CJUE [MC] din 8 aprilie 2014 în cauza C-288/12, *Comisia Europeană/Ungaria*
[Legitimitatea încetării mandatului autorității naționale pentru protecția datelor]

Hotărârea CJUE din 17 iulie 2014 în cauzele conexate C-141/12 și C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel* și *Minister voor Immigratie, Integratie en Asiel/M și S*
[Domeniul de aplicare al dreptului de acces al unei persoane vizate; protejarea persoanelor fizice față de prelucrarea datelor cu caracter personal; conceptul „date cu caracter personal"; date referitoare la solicitantul unui permis de ședere și analiza juridică inclusă într-un document administrativ de pregătire a deciziei; Carta drepturilor fundamentale a Uniunii Europene]

Hotărârea CJUE [MC] din 13 mai 2014 în cauza C-131/12, *Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

[Obligațiile furnizorilor de servicii de motoare de căutare de a se abține, la cererea persoanei vizate, de la a afișa datele cu caracter personal în rezultatele de căutare; aplicabilitatea Directivei privind protecția datelor; conceptu „prelucrarea datelor"; sensul termenului „operator"; ponderarea protecției datelor cu libertatea de exprimare; dreptul de a fi uitat]

Hotărârea CJUE [MC] din 16 octombrie 2012 în cauza C-614/10, *Comisia Europeană/Republica Austria*

[Independența unei autorități naționale de supraveghere]

Hotărârea CJUE din 24 noiembrie 2011 în cauzele conexate C-468/10 și C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) și Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*

[Punerea în aplicare corectă a articolului 7 litera (f) din Directiva privind protecția datelor – „interesele legitime ale altor persoane" – în legislația națională]

Hotărârea CJUE din 16 februarie 2012 în cauza C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*

[Obligația furnizorilor de rețele sociale de a împiedica utilizarea ilicită a operelor muzicale și audiovizuale de către utilizatorii rețelei]

Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*

[Societatea informațională; drepturi de autor; internet; software peer-to-peer; furnizori de servicii internet; instalarea unui sistem de filtrare a comunicațiilor electronice pentru a preveni partajarea de fișiere care încalcă drepturile de autor; absența obligației generale de a monitoriza informațiile transmise]

Hotărârea CJUE din 5 mai 2011 în cauza C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*

[Necesitatea reînnoirii consimțământului]

Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, *Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen*

[Conceptul „date cu caracter personal"; proporționalitatea obligației legale de a publica date cu caracter personal privind beneficiarii unor anumite fonduri agricole ale UE]

Hotărârea CJUE din 7 mai 2009 în cauza C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*
[Dreptul de acces al persoanei vizate]

Hotărârea CJUE [MC] din 9 martie 2010 în cauza C-518/07, *Comisia Europeană/Republica Federală Germania*
[Independența unei autorități naționale de supraveghere]

Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy*
[Conceptul „activități jurnalistice", în sensul articolului 9 din Directiva privind protecția datelor]

Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-524/06, *Heinz Huber/Bundesrepublik Deutschland*
[Legitimitatea deținerii de date privind cetățenii străini într-un registru statistic]

Hotărârea CJUE [MC] din 29 ianuarie 2008 în cauza C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*
[Conceptul „date cu caracter personal"; obligația furnizorilor de servicii de acces la internet de a dezvălui identitatea utilizatorilor de programe de schimb de fișiere KaZaA unei asociații de protecție a proprietății intelectuale]

Hotărârea CJUE din 6 noiembrie 2003 în cauza C-101/01, *Proces penal/Bodil Lindqvist*
[Categorii speciale de date cu caracter personal]

Hotărârea CJUE din 20 mai 2003 în cauzele conexate C-465/00, C-138/01 și C-139/01, *Rechnungshof/Österreichischer Rundfunk și alții* și *Christa Neukomm și Joseph Lauermann/Österreichischer Rundfunk*
[Proporționalitatea obligației legale de a publica date cu caracter personal privind salariile angajaților anumitor categorii de instituții asociate sectorului public]

Concluziile avocatului general Kokott din 20 iulie 2017 în cauza C-434/16, *Peter Nowak/Data Protection Commissioner*
[Conceptul de date cu caracter personal; accesul la propria foaie de examinare; corecturile examinatorului]

Hotărârea CJUE din 17 octombrie 2013 în cauza C-291/12, *Michael Schwarz/Stadt Bochum*

[Trimitere preliminară; spațiul de libertate, securitate și justiție; pașaport biometric; amprente digitale; temei juridic; proporționalitate]

Jurisprudență legată de Directiva (UE) 2016/681

Avizul 1/15 al Curții (Marea Cameră) din 26 iulie 2017

[Temei juridic; proiect de acord între Canada și Uniunea Europeană privind transferul și prelucrarea datelor din registrul cu numele pasagerilor; compatibilitatea proiectului de acord cu articolul 16 din TFUE și cu articolele 7 și 8 și articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene]

Jurisprudență legată de Regulamentul privind protecția datelor de către instituțiile UE

Hotărârea CJUE din 16 iulie 2015 în cauza C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Autoritatea Europeană pentru Siguranța Alimentară (EFSA), Comisia Europeană*

[Accesul la documente]

Hotărârea CJUE [MC] din 29 iunie 2010 în cauza C-28/08 P, *Comisia Europeană/The Bavarian Lager Co. Ltd.*

[Accesul la documente]

Jurisprudență legată de Directiva 2002/58/CE

Hotărârea CJUE din 15 martie 2017 în cauza C-536/15, *Tele2 (Netherlands) BV și alții/Autoriteit Consument en Markt (ACM)*

[Principiul nediscriminării; punerea la dispoziție a datelor cu caracter personal ale abonaților în scopul furnizării de servicii publice de informații telefonice și de liste de abonați; consimțământul abonatului; diferențiere în funcție de statul membru în care se furnizează serviciile publice de informații telefonice și de liste de abonați]

Hotărârea CJUE [MC] din 21 decembrie 2016 în cauzele conexate C-203/15 și C-698/15, *Tele2 Sverige AB/Post- och telestryrelsen* și *Secretary of State for the Home Department/Tom Watson și alții*

[Confidențialitatea comunicațiilor electronice; furnizori de servicii de comunicare electronică; obligația privind păstrarea generalizată și nediferențiată a datelor de transfer și de localizare; lipsa examinării prealabile de către o instanță sau o autoritate administrativă independentă; Carta drepturilor fundamentale a Uniunii Europene; compatibilitatea cu dreptul UE]

Hotărârea CJUE din 24 noiembrie 2011 în cauza C-70/10, *Scarlet Extended SA/ Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*

[Societatea informațională; drepturi de autor; internet; software peer-to-peer; furnizori de servicii internet; instalarea unui sistem de filtrare a comunicațiilor electronice pentru a preveni partajarea de fișiere care încalcă drepturile de autor; absența obligației generale de a monitoriza informațiile transmise]

Hotărârea CJUE din 19 aprilie 2012 în cauza C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB/Perfect Communication Sweden AB*

[Drepturi de autor și drepturi conexe; prelucrarea datelor prin internet; încălcarea unui drept exclusiv; cărți audio puse la dispoziție prin internet, pe un server FTP, prin intermediul unei adrese IP alocate de furnizorul de servicii internet; ordin emis împotriva furnizorului de servicii internet, prin care i se impune acestuia să divulge numele și adresa fizică a utilizatorului adresei

Actualizările vor fi disponibile pe site-ul FRA, la adresa fra.europa.eu, pe site-ul Consiliului Europei, la adresa coe.int/dataprotection, pe site-ul Curții Europene a Drepturilor Omului, la adresa echr.coe.int, în meniul Case- Law (Jurisprudență) și pe site-ul Autorității Europene pentru Protecția Datelor, la adresa edps.europa.eu.