ATELIERUL 2

1. Persoana vizată
2. Operatorul de date cu caracter personal/Operatori asociați
3. Persoana împuternicită să prelucreze datele cu caracter personal
4. Destinatarii datelor cu caracter personal

1. Persoana vizată

Potrivit definiției din Regulament – art.4 pct. 1, persoana vizată este o *persoană fizică identificată* sau *identificabilă*;

- o persoană **fizică** identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

-persoana vizată poate fi copil sau adult.

2. Operatorul de date cu caracter personal/Operatori asociați

Potrivit definiției de la art. 4 pct. 7 din Regulament, operatorul este *persoana fizică sau juridică, autoritatea publică, agenția sau alt organism* care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

Una dintre caracteristicile esențiale ale unui operator este aceea că el este cel care decide singur (stabilește singur) cum se face prelucrarea de date, respectiv ce și cum se prelucrează.

2.1. Obligațiile operatorului

2.1.1. Implementarea de măsuri tehnice și organizatorice adecvate-obligație de rezultat

Aceste măsuri diferă de la caz la caz, de la un operator la altul, în funcție de natura activității desfășurate de fiecare operator în parte, natura și volumul datelor prelucrate, scopurile și temeiurile prelucrării ori categoria de persoane vizate.

Art. 32 din Regulament - *Securitatea prelucrării* vine cu exemple concrete de măsuri tehnice și organizatorice pe care operatorii le pot lua, lista nefiind una exhaustivă. Aceste măsuri pot să constea în:

- pseudonimizarea și criptarea datelor cu caracter personal;
- capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare; (în instalarea unui antivirus licențiat, a unor parole puternice)

În cazul prelucrării imaginii prin intermediul sistemului CCTV, pot fi folosite măsuri cum ar fi: protecția întregii infrastructuri CCTV (inclusiv camerele de la distanță, cablarea și alimentarea cu energie electrică) împotriva manipulării fizice frauduloase și a furtului fizic; protecția transmiterii înregistrărilor împotriva interceptării prin canale de comunicare sigure; criptarea datelor; utilizarea de

soluții bazate pe hardware și software, cum ar fi sisteme firewall, antivirus sau de detectare a intruziunilor împotriva atacurilor cibernetice; detectarea disfuncționalităților la nivel de componente, software și interconectări[1].

- capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.
- accesul utilizatorilor la datele cu caracter personal să se facă pe baza unui user și a unei parole unice, parola care să fie schimbată la intervale de timp regulate;
- accesul diferențiat la baza de date, astfel încât fiecare angajat să poată accesa doar acele categorii de date necesare pentru îndeplinirea atribuțiilor de serviciu, indiferent de suportul pe care sunt păstrate datele: hârtie, suport informatic, acces pe imaginile preluate de către sistemul CCTV sau datele prelucrate prin GPS;
- păstrarea serverelor în camere cu acces securizat, la care să nu aibă acces decât un număr limitat de persoane;
- păstrarea datelor cu caracter personal, indiferent de suportul pe care se află, în locuri care pot fi securizate; de exemplu, cele aflate pe suport de hârtie, să fie păstrate în dulapuri sau birouri ce pot fi închise cu cheie;
- instruirea permanentă a angajaților cu privire la prelucrarea datelor cu caracter personal; instruirea ar trebui să aibă loc, în mod obligatoriu, atât cu ocazia angajării, cât și ulterior, periodic;
- introducerea în fișa postului de atribuții specifice prelucrării datelor cu caracter personal, ceea ce duce la o responsabilizare a angajatului;
- elaborarea unei politici cu privire la prelucrarea datelor cu caracter personal, adusă la cunoștința angajaților și care să fie actualizată periodic;

2.1.2. Aplicarea principiilor privacy by default și privacy by design

Potrivit art. 25 *Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.*

Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării.

Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

De exemplu, atunci când se creeaza o aplicație, aspectele care țin de securitatea și confidențialitatea datelor trebuie să fie avute în vedere încă din stadiul de proiectare.

---

1 CEPD, Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video (*https://edpb.europa.eu/sites/edpb/files/files/ file1/edpb_guidelines_201903_video_devices_ro.pdf*), p. 36.

2.1.3. Obligația de a păstra o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa

Art. 30 din Regulament, respectiv *obligația de a păstra o evidență a activităților de prelucrare desfășurate sub responsabilitatea sa.*

Respectiva evidență trebuie să cuprindă următoarele informații:

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

(b) scopurile prelucrării; scopurile prelucrării trebuie să fie indicate pentru fiecare categorie de date în parte.

(c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal; este important faptul că se menționează categoriile de persoane vizate și categoriile de date, iar nu fiecare persoană vizată în parte; astfel, în ceea ce privește categoriile de persoane vizate, se vor menționa, după caz: angajați, clienți, colaboratori, membri de familie ai angajaților, vizitatori; în ceea ce privește categoriile de date, se vor menționa, spre exemplu: date medicale, date privind apartenența politică, imaginea, vocea, date biometrice, etc.

(d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale; o mențiune importantă este aceea că angajații operatorului care prelucrează date cu caracter personal – cum ar fi angajații din cadrul departamentului de resurse umane sau a celui de IT nu au calitatea de destinatari ai datelor; o astfel de calitate o pot avea doar niște terți, respectiv alți operatori, către care se face un transfer de date: spre exemplu, un operator în calitate de angajator furnizează datele cu caracter personal ale angajaților săi către un cabinet de medicina muncii în vederea îndeplinirii obligațiilor sale legale.

2.1.4. Obligația de a recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate

Aceasta obligație a operatorului exista în virtutea principiului responsabilității.

Potrivit CEPD, îndeplinirea acestei obligații necesită un schimb de documentație relevantă – de exemplu, politica de confidențialitate, condițiile de furnizare a serviciilor, înregistrarea activității de prelucrare, politica de gestionare a înregistrărilor, politica de securitate a informațiilor, rapoarte de audit extern, certificări internaționale recunoscute, precum seria ISO 27000.

Evaluarea operatorului, dacă garanțiile sunt suficiente, este o formă de evaluare a riscurilor, care va depinde în mare măsură de tipul de prelucrare încredințată persoanei împuternicite, care trebuie făcută de la caz la caz, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile pentru drepturile și libertățile persoanelor fizice.

Următoarele elemente ar trebui să fie luate în considerare de către operator pentru a evalua suficiente garanții: cunoștințele de specialitate ale persoanei împuternicite (de exemplu, expertiza tehnică în ceea ce privește măsuri de securitate și încălcări de date); fiabilitatea și resursele sale; reputația sa pe piață poate fi, de asemenea, un factor relevant pentru controlori.

Mai mult, poate fi utilizată respectarea unui cod de conduită aprobat sau a unui mecanism de certificare ca element prin care se pot demonstra suficiente garanții[2].

2 *https://www.dataprotection.ro/servlet/ViewDocument?id=1950, pct. 93-96.*

2.1.5. Obligația de a respecta drepturile persoanei vizate

Nu în ultimul rând, operatorul are obligația de a respecta drepturile persoanei vizate și de a-și îndeplini obligațiile față de aceasta: astfel, în această categorie intră îndeplinirea obligației de informare a persoanei vizate, a obligației de a da curs solicitărilor de acces și celorlalte cereri pe care persoana vizată le formulează în temeiul Regulamentului, în limitele și termenele stabilite de acesta.

2.2. Operatorii asociați

Situația operatorilor asociați apare atunci când un operator nu acționează singur, ci deciziile legate de prelucrarea datelor sunt luate de către doi sau mai mulți operatori.

Potrivit art. 26 din Regulament: *În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați.*

Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentului regulament, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute de Regulament, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

Acest Acord trebuie să cuprindă rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate, iar esența acestui acord este făcută cunoscută persoanei vizate.

Potrivit practicii CJUE, există operatori asociați și atunci când entitățile nu au același scop pentru prelucrare, dar ele urmăresc *scopuri* care sunt strâns legate sau complementare.

În ceea ce privește mijloacele, entitățile trebuie să poată să își exercite controlul asupra mijloacelor, dar aceasta nu înseamnă că fiecare dintre ele trebuie să stabilească, împreună, toate mijloacele, ci pot fi implicate în diferite etape ale procesării respective și în diferite grade.

- CJUE a decis că, prin încorporarea pe site-ul său web a butonului Like Facebook pus la dispoziție de Facebook către operatorii de site-uri web, Fashion ID a exercitat o influență decisivă în ceea ce privește operațiunile care implică colectarea și transmiterea datelor personale ale vizitatorilor site-ului său către Facebook și astfel au stabilit împreună cu Facebook mijloacele procesării respective.

Referitor la obligațiile care le revin operatorilor asociați, Regulamentul arată că aceștia trebuie să stabilească clar *în special* aspectele referitoare la exercitarea drepturilor persoanelor vizate și obligația de furnizare a informațiilor prevăzute de art. 13 și 14, de unde rezultă faptul că există și alte aspecte cu privire la care trebuie să se înțeleagă și că enumerarea nu este una exhaustivă ci, dimpotrivă.

Astfel, ei ar trebui să stabilească într-o manieră clară și modul în care își împart responsabilitățile cu privire la implementarea principiilor generale de protecție a datelor (art. 5), temeiul juridic al prelucrării (art. 6), măsuri de securitate (art. 32), notificarea unei încălcări a datelor cu caracter personal către autoritatea de supraveghere și către persoana vizată (art. 33 și 34) – evaluări ale impactului asupra protecției datelor (art. 35 și 36) – utilizarea unei persoane împuternicite (art. 28) – transferuri de date către țări terțe (capitolul V) – organizarea contactului cu persoanele vizate și autoritățile de supraveghere.

În ceea ce privește împărțirea sarcinilor între ei, trebuie menționat și faptul că această împărțire nu trebuie să fie una egală, CJUE arătând că existența responsabilității comune nu implică neapărat o împărțire egală a responsabilității diferiților operatori implicați în prelucrarea datelor cu caracter personal.

3. Persoana împuternicită să prelucreze datele cu caracter personal

Potrivit definiției de la art. 4 pct. 8, *persoană împuternicită de operator poate fi persoană fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.*

Principala asemănare dintre operator și persoana împuternicită este aceea că ambele prelucrează date cu caracter personal

Principala deosebire este aceea că persoana împuternicită nu prelucrează decât acele date puse la dispoziție de către operator și efectuează prelucrarea în liniile și limitele trasate de către acesta.

Întotdeauna persoana împuternicită trebuie să fie o entitate distinctă de operator. Astfel, nu poate avea rolul de persoană împuternicită un departament din cadrul operatorului – cum ar fi departamentul de resurse umane.

Una dintre cele mai des întâlnite situații în care un operator îi solicită unei persoane împuternicite să prelucreze date cu caracter personal este atunci când are loc externalizarea unor servicii, cum ar fi serviciul de contabilitate sau de resurse umane.

A acționa „în numele" cuiva = a servi interesului altcuiva și amintește de conceptul de „delegare".

Chiar dacă persoana împuternicită nu trebuie să prelucreze datele altfel decât conform instrucțiunilor operatorului, acest instrucțiuni îi pot lăsa persoanei împuternicite o anumită marjă de apreciere cu privire la modul în care își îndeplinește obligațiile, permițându-i, astfel, să aleagă cele mai potrivite măsuri tehnice și organizatorice.

A acționa „în numele" înseamnă, de asemenea, că persoana împuternicită nu poate prelucra datele în alte scopuri decât cele stabilite de către operator.

Între operator și persoana împuternicită se impune încheierea unui contract sau a unui alt act juridic care trebuie să conțină niște clauze obligatorii menționate de către Regulament. În concret, este vorba despre următoarele obligații asumate de către persoana împuternicită:

(a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

(b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;

(c) adoptă toate măsurile necesare în conformitate cu art. 32 din Regulament;

(d) respectă condițiile privind recrutarea unei alte persoane împuternicite de operator;

(e) oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor sale, așa cum sunt ele prevăzute de Regulament;

(f) ajută operatorul să asigure respectarea obligațiilor care îi revin în temeiul Regulamentului, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;

(g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

(h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor care îi revin acestuia, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

CEPD indică elementele concrete ce trebuie să fie incluse într-un contract încheiat între operator și persoana împuternicită.

- obiectul procesării (de exemplu, înregistrări de supraveghere video ale persoanelor la intrarea și ieșirea dintr-o locație);
- durata procesării: perioada exactă de timp sau criteriile utilizate pentru a o determina;
- natura prelucrării: tipul operațiunilor efectuate ca parte a procesării (de exemplu: „filmare", „înregistrare", „arhivare a imaginilor") și scopul prelucrării (pentru exemplu: detectarea intrării ilegale). Această descriere ar trebui să fie cât mai cuprinzătoare posibil, în funcție de activitatea de procesare specifică, astfel încât să permită părților externe (de exemplu, autorității naționale) să înțeleagă conținutul și riscurile prelucrării încredințate persoanei împuternicite;
- tipul de date cu caracter personal: acesta trebuie specificat în modul cel mai detaliat posibil (de exemplu: imagini video ale persoanelor care intră și ies dintr-o locație). În cazul unor categorii speciale de date, contractul sau actul juridic trebuie să specifice cel puțin ce tipuri de date sunt vizate, de exemplu, „Informații referitoare la dosarele de sănătate" sau „informații privind dacă persoana vizată este membru al unui sindicat";
- categoriile de persoane vizate: și acesta ar trebui indicat într-un mod destul de specific (pentru exemplu: „vizitatori", „angajați", servicii de livrare etc.);
- obligațiile și drepturile operatorului și ale persoanei împuternicite: în ceea ce privește obligațiile operatorului, exemplele includ obligația operatorului să îi furnizeze persoanei împuternicite datele menționate în contract, să furnizeze și să documenteze, în scris orice instrucțiune referitoare la prelucrarea datelor de către persoana împuternicită, pentru a asigura, înainte și pe tot parcursul procesării, respectarea obligațiilor stabilite de Regulament[3].

Alin. (10) al art. 28, care prevede că, în cazul în care o persoană împuternicită de operator încălcă obligațiile care îi revin în temeiul Regulamentului, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

Astfel, persoana împuternicită se va transforma în operator și, implicit, acesteia îi vor deveni aplicabile toate obligațiile pe care Regulamentul le stabilește în sarcina operatorului.

4. Destinatarii datelor cu caracter personal

„Destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță**.**

- autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

3 Idem, pct. 110-111.