Orientările 07/2020 privind conceptele de operator și persoană împuternicită de operator în cadrul RGPD

Versiunea 2.0

Adoptată la 7 iulie 2021

Istoric versiuni

Versiunea 2.0	7 iulie 2021	Adoptarea orientărilor în urma consultării publice
Versiunea 1.0	2 septembrie 2020	Adoptarea orientărilor pentru consultare publică

REZUMAT

Conceptele de operator, operator asociat și persoană împuternicită de operator joacă un rol esențial în aplicarea Regulamentului general privind protecția datelor 2016/679 (RGPD), deoarece acestea stabilesc cine este responsabil de respectarea diferitelor norme privind protecția datelor cu caracter personal și modul în care persoanele vizate își pot exercita drepturile în practică. Sensul precis al acestor concepte și criteriile pentru interpretarea lor corectă trebuie să fie suficient de clare și de coerente la nivelul Spațiului Economic European (SEE).

Conceptele de operator, operator asociat și persoană împuternicită de operator sunt concepte *funcționale* în sensul că vizează atribuirea responsabilităților în conformitate cu rolurile efective ale părților și concepte *autonome* în sensul că trebuie interpretate în principal în conformitate cu legislația UE privind protecția datelor cu caracter personal.

Operator

În principiu, nu există nicio limitare în legătură cu tipul de entitate care își poate asuma rolul de operator, însă, în practică, organizația ca atare, de obicei, și nu o persoană anume din cadrul organizației (precum directorul general executiv, un angajat sau un membru al consiliului de administrație) este cea care acționează în calitate de operator.

Operatorul este un organism care *decide* anumite elemente-cheie ale prelucrării. Calitatea de operator poate fi definită prin lege sau poate rezulta dintr-o analiză a elementelor factuale sau a circumstanțelor cazului. Anumite activități de prelucrare se pot interpreta ca fiind legate în mod natural de rolul unei entități (angajatorul față de angajați, editorul față de abonați sau o asociație față de membrii acesteia). În multe situații, clauzele contractuale pot contribui la identificarea operatorului, deși nu au o influență decisivă în toate circumstanțele.

Operatorul determină scopurile și mijloacele de prelucrare, și anume *motivul pentru care* și *mijlocul în care* se realizează prelucrarea. Operatorul trebuie să decidă atât scopurile, cât și mijloacele. Cu toate acestea, unele aspecte mai practice privind punerea în aplicare („mijloace neesențiale”) pot fi lăsate la aprecierea persoanei împuternicite de operator. Nu este necesar ca operatorul să aibă acces efectiv la datele care sunt prelucrate pentru a fi calificat ca operator.

Operatori asociați

Calificarea ca operatori asociați poate apărea atunci când mai multe părți sunt implicate în prelucrare. RGPD introduce norme specifice pentru operatorii asociați și stabilește cadrul pentru reglementarea raporturilor dintre aceștia. Criteriul general pentru existența controlului comun este participarea comună a două sau mai multe entități la stabilirea scopurilor și a mijloacelor unei operațiuni de prelucrare. Participarea comună poate lua forma unei *decizii comune* luate de două sau mai multe entități sau poate reieși din *deciziile convergente* a două sau mai multe entități, în cazul în care deciziile se completează și sunt necesare pentru ca prelucrarea să aibă loc într-un asemenea mod încât aceasta să aibă un impact tangibil privind stabilirea scopurilor și a mijloacelor de prelucrare. Un criteriu important este că prelucrarea nu ar putea fi posibilă fără participarea ambelor părți, în sensul că prelucrările de către fiecare parte nu se pot separa, adică sunt legate în mod indisolubil. Participarea comună trebuie să includă stabilirea scopurilor, pe de o parte, și stabilirea mijloacelor, de cealaltă parte.

Persoană împuternicită de operator

Persoana împuternicită de operator este o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism, care prelucrează date cu caracter personal în numele operatorului. Există două condiții elementare pentru a se califica drept persoană împuternicită de operator: aceasta trebuie să fie o entitate separată în relație cu operatorul și să prelucreze date cu caracter personal în numele operatorului.

Persoana împuternicită de operator trebuie să prelucreze datele cu caracter personal exclusiv în conformitate cu instrucțiunile operatorului. Cu toate acestea, instrucțiunile operatorului pot lăsa la aprecierea persoanei împuternicite de operator un anume grad de libertate privind modul în care poate sluji cel mai bine intereselor operatorului, permițându-i acesteia alegerea celor mai adecvate mijloace tehnice și organizatorice. O persoană împuternicită de operator încalcă RGPD, totuși, dacă nu se limitează la instrucțiunile operatorului și începe să-și stabilească propriile scopuri și mijloace de prelucrare. Persoana împuternicită de operator va fi atunci considerată operator cu privire la respectiva prelucrare și poate face obiectul sancțiunilor pentru că nu s-a limitat la instrucțiunile operatorului.

Relația dintre operator și persoana împuternicită de operator

Operatorul trebuie să folosească doar persoane împuternicite de operator care oferă garanții suficiente pentru punerea în practică a măsurilor tehnice și organizatorice adecvate astfel încât prelucrarea să îndeplinească cerințele RGPD. Elemente de avut în vedere ar putea fi cunoștințele de specialitate ale persoanei împuternicite de operator (de exemplu, expertiză tehnică cu privire la măsurile de securitate și încălcări ale securității datelor), fiabilitatea persoanei împuternicite de operator, resursele persoanei împuternicite de operator și aderarea persoanei împuternicite de operator la un cod de conduită sau un mecanism de certificare aprobat.

Orice prelucrare a datelor cu caracter personal de către persoana împuternicită de operator trebuie să fie reglementată printr-un contract sau orice alt act juridic care se încheie în scris, inclusiv în formă electronică, și este obligatoriu. Operatorul și persoana împuternicită de operator pot alege să-și negocieze propriul contract, inclusiv toate elementele obligatorii, sau să se bazeze, integral sau parțial, pe clauzele contractuale standard.

RGPD enumeră elementele care trebuie să fie prevăzute în acordul de prelucrare. Cu toate acestea, acordul de prelucrare nu trebuie să reia dispozițiile RGPD pur și simplu; mai curând, trebuie să includă informații mai specifice, concrete, cu privire la modul în care se vor îndeplini cerințele și ce nivel de securitate este necesar pentru prelucrarea datelor cu caracter personal care fac obiectul acordului de prelucrare.

Raportul dintre operatorii asociați

Operatorii asociați stabilesc și agrează în mod transparent responsabilitățile lor corespunzătoare de respectare a obligațiilor în temeiul RGPD asupra cărora convin. Stabilirea responsabilităților corespunzătoare ale acestora trebuie se refere, în special, la exercitarea drepturilor de către persoanele vizate și la obligațiile de furnizare de informații. În plus față de aceasta, distribuția responsabilităților trebuie să acopere alte obligații ale operatorului, precum cele privind principiile generale de protecție a datelor, temeiul juridic, măsurile de securitate, obligația de notificare a încălcării securității datelor cu caracter personal, evaluările impactului asupra protecției datelor,

utilizarea persoanelor împuternicite de operatori, transferurile în țările terțe și contactele cu persoanele vizate și autoritățile de supraveghere.

Fiecare operator asociat are obligația de a se asigura că există un temei juridic pentru prelucrare și că datele cu caracter personal nu sunt prelucrate ulterior într-un mod incompatibil cu scopurile pentru care au fost colectate inițial de către operatorul care realizează schimbul de date.

Forma juridică a acordului dintre operatorii asociați nu este specificată în RGPD. În scopul securității juridice și pentru a furniza transparență și responsabilizare, CEPD recomandă ca acest acord să fie încheiat sub forma unui document obligatoriu, de exemplu un contract sau alt act juridic obligatoriu în temeiul dreptului UE sau al legislației statului membru aplicabilă operatorilor.

Acordul trebuie să reflecte în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate, iar esența acordului trebuie să fie pusă la dispoziția persoanei vizate.

Indiferent de clauzele acordului, persoanele vizate își pot exercita drepturile cu privire la și în raport cu fiecare dintre operatorii asociați. Clauzele acordului nu sunt aplicabile autorităților de supraveghere, indiferent dacă se referă la calificarea părților ca operatori asociați sau la punctul de contact desemnat.

CUPRINS

Comitetul european pentru protecția datelor

având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD" sau „regulamentul"),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

întrucât lucrările pregătitoare pentru prezentele orientări au implicat colectarea de contribuții de la părțile interesate, atât în scris, cât și în cadrul unui eveniment al părților interesate, pentru a identifica cele mai presante provocări,

A ADOPTAT URMĂTOARELE ORIENTĂRI:

INTRODUCERE

1. Scopul prezentului document este să ofere orientări privind conceptele de operator și persoană împuternicită de operator pe baza normelor din RGPD privind definițiile de la articolul 4 și dispozițiile privind obligațiile, din capitolul IV. Obiectivul principal este de a clarifica sensul conceptelor, precum și rolurile diferite și distribuția responsabilităților între acești actori.

2. Conceptul de operator și interacțiunea acestuia cu conceptul de persoană împuternicită de operator joacă un rol esențial în aplicarea RGPD, deoarece ele stabilesc cine este responsabil de respectarea diferitelor norme privind protecția datelor cu caracter personal și modul în care persoanele vizate își pot exercita aceste drepturi în practică. RGPD introduce în mod explicit principiul responsabilității, și anume, că operatorul este responsabil de principiile referitoare la prelucrarea datelor cu caracter personal de la articolul 5 și trebuie să poată demonstra respectarea acestora. În plus, RGPD introduce și norme mai specifice privind utilizarea persoanei (persoanelor) împuternicite de operator, iar unele dintre dispozițiile privind prelucrarea datelor cu caracter personal se adresează nu doar operatorilor, ci și persoanelor împuternicite de operator.

3. Prin urmare, este extrem de important ca sensul precis al acestor concepte și criteriile pentru utilizarea lor corectă să fie suficient de clare și diseminate la nivelul Uniunii Europene și al SEE.

4. Grupul de lucru instituit prin articolul 29" a emis orientări privind conceptele de operator/persoană împuternicită de operator în Avizul său nr. 1/2010 (WP169)[2] pentru a furniza clarificări și exemple concrete cu privire la aceste concepte. De la intrarea în vigoare a RGPD s-au ridicat multe întrebări cu privire la măsura în care RGPD a dus la modificări ale conceptelor de operator și de persoană împuternicită de operator și, respectiv, ale rolurilor acestora. S-au ridicat întrebări în special privind

[1] Trimiterile la „Statele Membre" din prezentul document trebuie înțelese ca trimiteri la „statele membre ale SEE".
[2] Grupul de lucru Articolul 29, Avizul nr. 1/2010 privind conceptele de „operator" și „persoană împuternicită de operator" adoptat la 16 februarie 2010, 264/10/EN, WP 169.

substanța și implicațiile conceptului de control comun (de exemplu, ca cel prevăzut în articolul 26 din RGPD) și privind obligațiile specifice pentru persoanele împuternicite de operatori prevăzute la capitolul IV (de exemplu, ca cele prevăzute la articolul 28 din RGPD). Prin urmare, și întrucât recunoaște că aplicarea concretă a conceptelor necesită clarificare suplimentară, CEPD consideră în prezent că este necesar să ofere orientări mai dezvoltate și mai specifice pentru a asigura o abordare consecventă și armonizată la nivelul UE și al SEE. Orientările prezente înlocuiesc avizul anterior al Grupului de lucru articolul 29 privind aceste concepte (WP169).

5. În partea I, prezentele orientări analizează definițiile diferitelor concepte de operator, operatori asociați, persoană împuternicită de operator și parte terță/destinatar. În partea a II-a sunt furnizate orientări suplimentare privind consecințele diferitelor roluri de operator, operatori asociați și persoană împuternicită de operator.

PARTEA I – CONCEPTE

1 OBSERVAȚII GENERALE

6. La articolul 5 alineatul (2), RGPD introduce explicit principiul responsabilității care înseamnă că:

   - operatorul este *responsabil de respectarea* principiilor stabilite în articolul 5 alineatul (1) din RGPD și că
   - operatorul *trebuie să poată demonstra respectarea* principiilor stabilite în articolul 5 alineatul (1) din RGPD.

   Acest principiu a fost descris într-un aviz al Grupului de lucru instituit prin articolul 29[3] și nu va fi discutat aici în detaliu.

7. Scopul introducerii principiului responsabilității în RGPD și acordarea unui rol central acestui principiu a fost de a accentua faptul că operatorii de date trebuie să pună în practică măsuri adecvate și eficace și trebuie să poată demonstra respectarea acestui principiu. [4]

8. Principiul responsabilității a fost elaborat suplimentar în articolul 24, care prevede că operatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură **să demonstreze** că prelucrarea se efectuează în conformitate cu RGPD. Aceste măsuri trebuie să fie revizuite și actualizate dacă este necesar. Principiul responsabilității este, de asemenea, reflectat în articolul 28, care prevede obligațiile operatorului atunci când recrutează o persoană împuternicită de operator.

9. Principiul responsabilității se adresează direct operatorului. Cu toate acestea, unele dintre normele mai specifice se adresează atât operatorilor, cât și persoanelor împuternicite de operatori, precum normele privind competențele autorităților de supraveghere de la articolul 58. Atât operatorii, cât și persoanele împuternicite de operatori pot fi amendate în cazul nerespectării obligațiilor din RGPD care le sunt aplicabile și ambele categorii sunt responsabile direct față de autoritățile de supraveghere în virtutea obligațiilor de a păstra și furniza documentația adecvată la cerere, de a coopera în cazul unei investigații și de a respecta măsurile administrative. În același timp, trebuie reamintit că persoanele împuternicite de operatori trebuie să respecte mereu instrucțiunilor date de operator și să acționeze doar în baza acestora.

[3] Grupul de lucru Articolul 29, Avizul nr. 3/2010 privind principiul responsabilității, adoptat la 13 iulie 2010, 00062/10/EN WP 173.
[4] Considerentul 74 din RGPD.

10. Principiul responsabilității, împreună cu celelalte norme mai specifice privind modul de respectare a RGPD și distribuția responsabilității impune, prin urmare, definirea rolurilor diferite ale diverșilor actori implicați într-o activitate de prelucrare a datelor cu caracter personal.

11. O observație generală privind conceptele de operator și persoană împuternicită de operator din RGPD este că acestea nu s-au modificat prin comparație cu Directiva 95/46/CE și că, în general, criteriile de atribuire a diferitelor roluri rămân aceleași.

12. Conceptele de operator și de persoană împuternicită de operator sunt concepte *funcționale*: acestea vizează alocarea responsabilităților în conformitate cu rolurile efective ale părților[5], ceea ce înseamnă că statutul juridic al unui actor de „operator" sau de „persoană împuternicită de operator" trebuie să fie determinat, în principiu, de activitățile efective ale acestuia într-o situație specifică, mai degrabă decât de desemnarea formală a unui actor ca „operator" sau ca „persoană împuternicită de operator" (de exemplu într-un contract)[6]. Acest fapt înseamnă că alocarea rolurilor trebuie să reiasă dintr-o analiză a elementelor factuale sau a circumstanțelor cazului și, ca atare, nu este negociabilă.

13. Conceptele de operator și persoană împuternicită de operator sunt și concepte *autonome* în sensul că, deși surse juridice externe pot sprijini identificarea entității care este operator, trebuie interpretate în principal în conformitate cu legislația UE de protecție a datelor. Conceptul de operator nu trebuie să fie afectat de concepte din alte domenii juridice - care uneori sunt în contradicție sau se suprapun cu acesta - precum conceptul de creator sau titular de drepturi din legislația în domeniul drepturilor de proprietate intelectuală sau al concurenței.

14. Deoarece obiectivul fundamental al atribuirii rolului de operator este garantarea responsabilității și protecția efectivă și cuprinzătoare a datelor cu caracter personal, conceptul de „operator" trebuie interpretat în sens suficient de larg, favorizând cât mai mult posibil protecția eficientă și completă a persoanelor vizate[7] astfel încât să asigure aplicarea completă a legislației UE privind protecția datelor cu caracter personal, să evite lacunele și să prevină posibila eludare a normelor, fără a diminua, în același timp, rolul persoanei împuternicite de operator.

2 DEFINIȚIA OPERATORULUI

2.1 Definiția operatorului

15. Articolul 4 punctul (7) din RGPD definește operatorul ca

> *„**persoana fizică sau juridică, autoritatea publică, agenția sau alt organism** care, **singur sau împreună cu altele, stabilește scopurile și mijloacele** de **prelucrare a datelor cu caracter personal**; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau*

[5] Grupul de lucru Articolul 29, Avizul nr. 1/2010, WP 169, p. 9.

[6] A se vedea, de asemenea, concluziile avocatului general Mengozzi în cauza *Martorii lui Iehova*, C-25/17, ECLI:EU:C:2018:57, punctul 68 [*„În vederea stabilirii «operatorului» în sensul Directivei 95/46, înclinăm să considerăm [...] că un formalism excesiv ar permite eludarea cu ușurință a dispozițiilor Directivei 95/46 și că, în consecință, trebuie utilizată o analiză mai factuală, iar nu una formală [...].*"].

[7] CJUE, Cauza C-131/12, Google Spain SL și Google Inc. împotriva Agencia Española de Protección de Datos (AEPD) și Mario Costeja González, hotărârea din 13 mai 2014, punctul 34; CJUE, Cauza C-210/16, Wirtschaftsakademie Schleswig-Holstein, hotărârea din 5 iunie 2018, punctul 28; CJUE, Cauza C-40/17, Fashion ID GmbH & Co.KG împotriva Verbraucherzentrale NRW eV, hotărârea din 29 iulie 2019, punctul 66.

dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi ***prevăzute în dreptul Uniunii sau în dreptul intern****"*.

16. Definiția operatorului conține cinci elemente constitutive principale, care vor fi analizate separat în scopurile prezentelor orientări. Acestea sunt următoarele:

- „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism"
- „stabilește"
- „singur sau împreună cu altele"
- „scopurile și mijloacele"
- „prelucrare a datelor cu caracter personal"

2.1.1 „Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism"

17. Primul „element constitutiv" se referă la tipul de entitate care poate fi un operator. În temeiul RGPD, operatorul poate fi „*persoana fizică sau juridică, autoritatea publică, agenția sau alt organism*". Acest fapt înseamnă că, în principiu, nu există o limitare în legătură cu tipul de entitate care își poate asuma rolul de operator. Ar putea fi o organizație, dar ar putea fi și o persoană fizică sau un grup de persoane fizice.[8] Cu toate acestea, în practică, de obicei, organizația ca atare, și nu o persoană din cadrul organizației (precum directorul general executiv, un angajat sau un membru al consiliului de administrație) acționează în calitate de operator în sensul RGPD. În ceea ce privește prelucrarea datelor cu caracter personal în cadrul unui grup de întreprinderi, trebuie să se acorde o atenție specială situației în care o entitate poate acționa ca operator sau persoană împuternicită, de exemplu în cazul prelucrării datelor cu caracter personal în numele întreprinderii-mamă.

18. Uneori, întreprinderile și organismele publice numesc o persoană specifică responsabilă de punerea în practică a activității de prelucrare. Chiar dacă este desemnată o anumită persoană fizică pentru a asigura respectarea normelor de protecție a datelor, această persoană nu va fi operatorul, ci va acționa în numele entității juridice (întreprindere sau organism public) care va fi responsabilă în ultimă instanță în cazul încălcării normelor, în calitatea acesteia de operator. În mod asemănător, chiar dacă un departament sau o unitate anume a unei organizații are responsabilitatea operațională de a asigura respectarea în cazul unei anumite activități de prelucrare, acest fapt nu înseamnă că departamentul sau unitatea respectivă (mai curând decât organizația ca întreg) devine operatorul.

Exemplu:

Departamentul de marketing al întreprinderii ABC lansează o campanie publicitară de promovare a produselor ABC. Departamentul de marketing decide natura campaniei, mijloacele care vor fi utilizate (e-mail, platforme de comunicare socială etc.), clienții vizați și ce date să utilizeze pentru a face campania cât mai reușită cu putință. Chiar dacă departamentul de marketing a acționat cu independență considerabilă, în principiu, întreprinderea ABC va fi considerată operator deoarece campania publicitară este lansată de întreprindere și are loc în sfera domeniului activităților sale comerciale și în scopurile acesteia.

[8] De exemplu, în hotărârea pronunțată în cauza *Martorii lui Iehova*, C-25/17, ECLI:EU:C:2018:551, punctul 75, CJUE a considerat că o comunitate religioasă a Martorilor lui Iehova a acționat ca un operator, împreună cu membrii individuali ai acesteia. Hotărârea pronunțată în cauza *Martorii lui Iehova*, C-25/17, ECLI:EU:C:2018:551, punctul 75.

19. În principiu, se poate presupune că orice prelucrare a datelor cu caracter personal de către angajați care are loc în sfera domeniului de activitate al unei organizații are loc sub controlul organizației respective.[9] Cu toate acestea, în circumstanțe excepționale, se poate întâmpla ca un angajat să decidă să utilizeze date cu caracter personal în scopuri proprii, depășind astfel în mod ilegal autoritatea ce i-a fost conferită (de exemplu, pentru înființarea unei întreprinderi proprii sau în scopuri similare). Prin urmare, este obligația organizației, ca operator, să se asigure că există măsuri tehnice și organizatorice adecvate, inclusiv, de exemplu, formarea și informarea angajaților, pentru a asigura conformitatea cu RGPD. [10]

2.1.2 „Stabilește"

20. Cel de-al doilea element constitutiv al conceptului de operator se referă la *influența* operatorului asupra prelucrării, în virtutea *exercitării competenței decizionale*. Operatorul este un organism care *decide* anumite elemente-cheie referitoare la prelucrare. Această calitate de operator poate fi definită prin lege sau poate reieși dintr-o analiză a elementelor factuale sau a circumstanțelor cazului. Trebuie analizate operațiunile specifice de prelucrare în cauză și trebuie înțeles cine le stabilește, având în vedere mai întâi următoarele întrebări: *„De ce are loc această prelucrare*?" și *„cine a decis că prelucrarea trebuie să aibă loc într-un anumit scop?"*.

Circumstanțe care dau naștere controlului

21. Deoarece „operatorul" este un concept funcțional, prin urmare, acesta se bazează mai degrabă pe o **analiză mai factuală decât formală**. Pentru facilitarea analizei, anumite reguli generale și prezumții practice pot fi utilizate pentru ghidarea și simplificarea procesului. În majoritatea situațiilor, „organismul determinant" poate fi identificat ușor și în mod clar prin trimitere la anumite circumstanțe juridice și/sau factuale în temeiul cărora se poate deduce în mod normal „influența", cu excepția cazului în care alte elemente arată contrariul. Se pot distinge două categorii de situații: (1) controlul care decurge din *dispoziții legale*; și (2) controlul care provine din *influența factuală*.

1) *Controlul care decurge din dispozițiile legale*

22. Există cazuri în care controlul poate fi dedus din competența juridică explicită, de exemplu, atunci când operatorul sau criteriile specifice pentru desemnarea acestuia sunt prevăzute în dreptul intern sau în dreptul Uniunii. Într-adevăr, articolul 4 punctul (7) prevede că *„atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern*". Deși articolul 4 punctul (7) se referă la „operator" doar la singular, CEPD consideră că poate fi posibil, de asemenea, ca dreptul Uniunii sau dreptul intern să desemneze mai mult de un operator, poate chiar și operatori asociați.

23. În cazul în care operatorul a fost identificat în mod specific prin legislație, acest fapt va fi determinant pentru stabilirea entității care acționează ca operator. Acest fapt presupune că legiuitorul a desemnat ca operator entitatea care are o capacitate reală de a exercita controlul. În unele țări, dreptul intern prevede că autoritățile publice sunt responsabile de prelucrarea datelor cu caracter personal în contextul obligațiilor ce le revin.

24. Cu toate acestea, de obicei, decât să desemneze direct operatorul sau să stabilească criteriile pentru desemnarea acestuia, legislația va stabili o sarcină sau va impune o obligație unei persoane în vederea

[9] Angajații care au acces la date cu caracter personal în cadrul unei organizații, în general, nu sunt considerați „operatori" sau „persoane împuternicite de operatori", ci mai degrabă „persoane care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator" în sensul articolul 29 din RGPD.
[10] Articolul 24 alineatul (1) din RGPD.

colectării și prelucrării anumitor date. În aceste cazuri, scopul prelucrării este adesea stabilit prin legislație. Operatorul va fi în mod normal cel desemnat prin legislație pentru realizarea acestui scop, pentru îndeplinirea acestei sarcini publice. De exemplu, acest fapt ar fi valabil în cazul în care o entitate căreia i se atribuie anumite sarcini publice (de exemplu, securitatea socială) care nu pot fi îndeplinite fără a colecta cel puțin anumite date cu caracter personal, creează o bază de date sau un registru pentru a îndeplini sarcinile publice respective. În acest caz, deși în mod indirect, prin lege se stabilește cine este operatorul. La nivel general, prin legislație se poate impune și o obligație fie entităților publice, fie celor private de a păstra sau de a furniza anumite date. Astfel, în mod normal, aceste entități ar fi considerate operatori cu privire la prelucrarea necesară pentru executarea acestei obligații.

Exemplu: Dispoziții legale

Dreptul intern din țara A prevede obligația autorităților municipale de a furniza prestații sociale precum unele plăți lunare către cetățeni în funcție de situația financiară a acestora. Pentru a efectua aceste plăți, autoritatea municipală trebuie să colecteze și să prelucreze date privind situația financiară a solicitanților. Deși nu se prevede în mod explicit prin legislație că autoritățile municipale sunt operatori pentru această prelucrare, acest fapt reiese implicit din dispozițiile legale.

2) *Controlul care decurge din influența factuală*

25. În absența controlului care reiese din dispoziții legale, calificarea unei părți ca operator trebuie să fie stabilită pe baza unei evaluări a circumstanțelor factuale care însoțesc prelucrarea. Toate circumstanțele factuale relevante trebuie avute în vedere pentru a ajunge la o concluzie potrivit căreia o anumită entitate exercită o influență determinantă cu privire la prelucrarea datelor cu caracter personal în cauză.

26. Necesitatea unei evaluări factuale înseamnă, de asemenea, că rolul unui operator nu decurge din natura unei entități care prelucrează date, ci din activitățile concrete ale acesteia într-un context specific. Cu alte cuvinte, aceeași entitate poate acționa în același timp ca operator pentru anumite operațiuni de prelucrare și ca persoană împuternicită de operator pentru altele, iar calificarea ca operator sau persoană împuternicită de operator trebuie evaluată cu privire la fiecare activitate specifică de prelucrare de date.

27. În practică, anumite activități de prelucrare pot fi considerate ca fiind legate în mod natural de rolul sau de activitățile unei entități care duc în final la responsabilități din punctul de vedere al protecției datelor. Acest fapt poate fi rezultatul unor dispoziții legale mai generale sau unei practici juridice consacrate în diferite domenii (drept civil, drept comercial, dreptul muncii etc.). În acest caz, rolurile tradiționale și expertiza profesională existente care implică în mod normal o anumită responsabilitate vor contribui la identificarea operatorului, de exemplu: un angajator în legătură cu prelucrarea datelor cu caracter personal ale angajaților acestuia, un editor care prelucrează date cu caracter personal ale abonaților săi sau o asociație care prelucrează date cu caracter personal ale membrilor sau contribuitorilor acesteia. Atunci când o entitate contribuie la prelucrarea datelor cu caracter personal ca parte a interacțiunilor sale cu angajații, clienții sau membrii acesteia, aceasta va fi, în general, entitatea care stabilește scopul și mijloacele în raport cu prelucrarea și, prin urmare, acționează în calitate de operator în sensul RGPD.

Exemplu: Firmele de avocatură

Întreprinderea ABC angajează o firmă de avocatură pentru a o reprezenta într-un litigiu. Pentru a realiza această sarcină, firma de avocatură trebuie să prelucreze datele cu caracter personal legate de caz. Mandatul firmei de avocatură de a reprezenta clientul în instanță justifică prelucrarea datelor cu caracter personal. Totuși, acest mandat nu vizează în mod specific prelucrarea datelor cu caracter personal. Firma de avocatură acționează cu un grad semnificativ de independență, de exemplu, atunci când decide ce informații să utilizeze și cum să utilizeze aceste informații și când nu există nicio instrucțiune de la întreprinderea client privind prelucrarea datelor cu caracter personal. Prelucrarea realizată de firma de avocatură pentru a îndeplini sarcina de reprezentant legal pentru întreprindere are, prin urmare, legătură cu rolul funcțional al firmei de avocatură, astfel încât aceasta trebuie considerată operator pentru această prelucrare.

Exemplu: Operatori de telecomunicații[11]:

Furnizarea unui serviciu de comunicații electronice precum un serviciu de poștă electronică implică prelucrarea de date cu caracter personal. Furnizorul unor asemenea servicii va fi considerat în mod normal un operator în ceea ce privește prelucrarea datelor cu caracter personal care sunt necesare pentru funcționarea serviciului ca atare (de exemplu, date privind traficul și facturarea). În cazul în care singurul scop și rol al furnizorului este să permită transmiterea de mesaje prin e-mail, furnizorul nu va fi considerat operator în ceea ce privește datele cu caracter personal conținute în mesajul propriu-zis. Operatorul în ceea ce privește orice date cu caracter personal conținute în mesaj va fi considerat în mod normal persoana de la care provine mesajul, și nu furnizorul de servicii care oferă serviciul de transmisie.

28. În multe cazuri, o evaluare a clauzelor contractuale dintre diferitele părți implicate poate facilita stabilirea părții (sau a părților) care acționează ca operator. Chiar dacă un contract nu menționează cine este operatorul, poate conține suficiente elemente pentru a deduce cine exercită un rol decizional cu privire la scopurile și mijloacele prelucrării. De asemenea, este posibil ca în contract să fie cuprinsă o declarație explicită referitoare la identitatea operatorului. În cazul în care nu există niciun motiv de îndoială că acest fapt reflectă întocmai realitatea, nu există motive pentru nerespectarea clauzelor contractuale. Cu toate acestea, clauzele contractuale nu sunt determinante în toate circumstanțele, deoarece acest fapt ar permite părților pur și simplu să aloce responsabilitatea după cum consideră de cuviință. O entitate nu poate să devină operator sau să se sustragă de la obligațiile operatorului pur și simplu prin redactarea contractului într-un anumit mod, atunci când circumstanțele factuale indică altceva.

29. În cazul în care una dintre părți decide în fapt modalitatea și mijloacele de prelucrare a datelor cu caracter personal, partea respectivă va fi un operator, chiar dacă contractul prevede că este o persoană împuternicită de operator. În mod similar, în cazul în care un contract comercial utilizează termenul „subcontractant”, acest fapt nu înseamnă că o entitate trebuie să fie considerată persoană împuternicită de operator din perspectiva legislației privind protecția datelor.[12]

30. În conformitate cu abordarea factuală, termenul „stabilește” înseamnă că entitatea exercită în mod efectiv o influență decisivă cu privire la scopurile și mijloacele de prelucrare în realitate este operatorul. În mod normal, un acord privind persoana împuternicită de operator stabilește care este partea

[11] CEPD consideră că acest exemplu, inclus anterior în considerentul 47 din Directiva 95/46/CE, rămâne relevant și în temeiul RGPD.

[12] A se vedea, de exemplu, Grupul de lucru Articolul 29, Avizul nr. 10/2006 privind prelucrarea datelor cu caracter personal de către Societatea pentru Telecomunicații Financiare Interbancare Mondiale (SWIFT), 22 noiembrie 2006, WP128, p. 11.

determinantă (operator) și care este partea mandatată (persoana împuternicită de operator). Chiar dacă persoana împuternicită de operator oferă un serviciu care este definit preliminar într-un mod specific, operatorul trebuie să primească o descriere detaliată a serviciului și trebuie să ia decizia finală de a aproba activ modul în care se efectuează prelucrarea și de a solicita modificări, dacă este necesar. În plus, persoana împuternicită de operator nu poate să modifice într-o etapă ulterioară elementele esențiale ale prelucrării fără aprobarea operatorului.

Exemplu: serviciu standardizat de stocare în cloud

Un mare furnizor de servicii de stocare în cloud le oferă clienților săi posibilitatea de a stoca volume mari de date cu caracter personal. Serviciul este standardizat complet, clienții având o capacitate redusă sau inexistentă de a personaliza serviciul. Clauzele contractuale sunt stabilite și redactate unilateral de furnizorul de servicii cloud, fiind puse la dispoziția clientului pe baza principiului „dacă accepți, bine, dacă nu, nu”. Întreprinderea X decide să utilizeze furnizorul de servicii cloud pentru a stoca date cu caracter personal referitoare la clienții săi. Întreprinderea X va fi considerată în continuare operator, având în vedere decizia sa de a utiliza acest furnizor de servicii cloud pentru a prelucra date cu caracter personal în scopurile sale. În măsura în care furnizorul de servicii cloud nu prelucrează datele cu caracter personal în scopuri proprii și stochează datele doar în numele clienților săi și în conformitate cu instrucțiunile, furnizorul de servicii va fi considerat o persoană împuternicită de operator.

2.1.3 „Singur sau împreună cu altele”

31. Articolul 4 punctul (7) recunoaște că „scopurile și mijloacele” prelucrării ar putea fi determinate de mai mulți actori. Acesta prevede că operatorul este actorul care, „singur sau împreună cu altele”, stabilește scopurile și mijloacele prelucrării. Aceasta înseamnă că mai multe entități diferite pot acționa ca operatori pentru aceeași prelucrare, fiecare dintre acestea făcând apoi obiectul dispozițiilor aplicabile privind protecția datelor. În același mod, o organizație poate fi în continuare un operator chiar dacă nu ia toate deciziile în ceea ce privește scopurile și mijloacele. Criteriile pentru controlul comun și măsura în care doi sau mai mulți actori exercită în comun controlul pot lua diferite forme, astfel cum s-a clarificat ulterior.[13]

2.1.4 „Scopurile și mijloacele”

32. Cel de-al patrulea element constitutiv al definiției operatorului se referă la obiectul influenței operatorului, și anume „scopurile și mijloacele” prelucrării. Acesta reprezintă partea materială a conceptului de operator: ce trebuie să stabilească o parte pentru a se califica ca operator.

33. Dicționarele definesc „scopul” ca „un rezultat anticipat avut în vedere sau care orientează acțiunile pe care le planificați” și „mijloacele” sunt definite ca „modalitatea prin care se obține un rezultat sau se atinge un scop”.

34. RGPD stabilește că datele trebuie colectate în scopuri determinate, explicite și legitime și să nu fie prelucrate ulterior într-un mod incompatibil cu aceste scopuri. Prin urmare, stabilirea „scopurilor” prelucrării și a „mijloacelor” pentru realizarea acestora este extrem de importantă.

[13] A se vedea partea I, secțiunea 3 („Definiția operatorilor asociați”).

35. Stabilirea scopurilor și a mijloacelor înseamnă a decide cu privire la „motivul” și, respectiv, la „modul” prelucrării:[14] având în vedere o anumită operațiune de prelucrare, operatorul este actorul care a stabilit *de ce* are loc prelucrarea (și anume, „în ce scop”; sau „pentru ce”) și *modul* în care va fi realizat acest obiectiv (și anume, ce mijloace trebuie utilizate pentru atingerea obiectivului). Persoana fizică sau juridică care exercită o astfel de influență asupra prelucrării datelor cu caracter personal participă astfel la stabilirea scopurilor și a mijloacelor prelucrării respective în conformitate cu definiția de la articolul 4 punctul (7) din RGPD.[15]

36. Operatorul trebuie să decidă atât cu privire la scop, cât și cu privire la mijloacele de prelucrare astfel cum se descrie mai jos. Prin urmare, operatorul nu se poate limita doar la stabilirea scopului. Acesta trebuie să ia decizii și în ceea ce privește mijloacele de prelucrare. În schimb, partea care acționează ca persoană împuternicită de operator nu poate determina niciodată scopul prelucrării.

37. În practică, în cazul în care un operator angajează o persoană împuternicită de operator pentru a realiza prelucrarea în numele său, acest fapt înseamnă adesea că persoana împuternicită de operator este în măsură să ia anumite decizii proprii cu privire la modul de realizare a prelucrării. CEPD recunoaște că poate exista o anumită marjă de manevră pentru persoana împuternicită de operator în ceea ce privește posibilitatea de a lua, de asemenea, unele decizii în legătură cu prelucrarea. Din această perspectivă, este necesar să se ofere orientări cu privire la **nivelul de influență** asupra „scopului” și „mijlocului” ar trebui să implice calificarea unei entități ca operator și în ce măsură o persoană împuternicită de operator poate lua propriile decizii.

38. Când o entitate stabilește clar scopurile și mijloacele, atribuind altei entități activități de prelucrare care echivalează cu executarea instrucțiunilor detaliate ale acesteia, situația este simplă și nu există nicio îndoială că cea de a doua entitate trebuie să fie considerată persoană împuternicită de operator, în timp ce prima entitate este operatorul.

Mijloace esențiale și mijloace neesențiale

39. Întrebarea este unde să se stabilească linia de demarcație între deciziile care sunt rezervate operatorului și deciziile care pot fi lăsate la aprecierea persoanei împuternicite de operator. Deciziile privind scopul prelucrării cad întotdeauna, în mod clar, în competența operatorului.

40. În ceea ce privește stabilirea mijloacelor, se poate face o distincție între mijloacele esențiale și mijloacele neesențiale. „Mijloacele esențiale” sunt rezervate în mod tradițional și inerent pentru operator. Deși mijloacele neesențiale pot fi, de asemenea, determinate de către persoana împuternicită de operator, mijloacele esențiale trebuie să fie determinate de către operator. „Mijloacele esențiale” sunt mijloacele care sunt strâns legate de scopul și domeniul de aplicare al prelucrării, precum tipul de date cu caracter personal care sunt prelucrate („*ce date trebuie prelucrate*?”), durata prelucrării („*cât timp se prelucrează acestea?*”), categoriile de destinatari („*cine are acces la acestea?*”) și categoriile de persoane vizate („*ale cui date cu caracter personal sunt prelucrate?*”). Împreună cu scopul prelucrării, mijloacele esențiale sunt, de asemenea, strâns legate de întrebarea dacă prelucrarea este legală, necesară și proporțională. „Mijloacele neesențiale” vizează aspecte mai practice ale implementării, precum alegerea unui anumit tip de hardware sau software sau măsurile de securitate detaliate care pot fi lăsate la aprecierea persoanei împuternicite de operator.

[14] A se vedea și concluziile avocatului general Bot în cauza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, punctul 46).

[15] Hotărârea pronunțată în cauza *Martorii lui Iehova*, C-25/17, ECLI:EU:C:2018:551, punctul 68.

Exemplu: Administrarea salariilor

Angajatorul A angajează o altă întreprindere pentru a administra plata salariilor angajaților săi. Angajatorul A oferă instrucțiuni clare cu privire la cine trebuie plătit, ce sume, până la ce dată, la ce bancă, cât timp se stochează datele, ce date trebuie divulgate autorității fiscale etc. În acest caz, prelucrarea datelor se realizează pentru ca întreprinderea A să plătească salariile angajaților săi, iar administratorul salariilor nu poate utiliza datele în vreun scop propriu. Modul în care administratorul salariilor trebuie să realizeze prelucrarea este definit în esență clar și limitativ. Cu toate acestea, administratorul salariilor poate decide cu privire la anumite aspecte detaliate legate de prelucrare, precum ce software să utilizeze, cum să distribuie accesul în cadrul organizației sale etc. Acest fapt nu modifică rolul acestuia de persoană împuternicită de operator, atât timp cât administratorul nu încalcă sau nu depășește instrucțiunile date de întreprinderea A.

Exemplu: Plăți bancare

Ca parte a instrucțiunilor angajatorului A, administratorul salariilor transmite informații băncii B, astfel încât aceasta să poată realiza plata efectivă către salariații angajatorului A. Această activitate include prelucrarea datelor cu caracter personal de către banca B pe care aceasta o realizează în scopul desfășurării activității bancare. În cadrul acestei activități, banca decide, independent de angajatorul A, cu privire la datele care trebuie prelucrate pentru furnizarea serviciului, cât timp trebuie stocate datele etc. Angajatorul A nu poate avea nicio influență asupra scopului și mijloacelor de prelucrare a datelor de către banca B. Prin urmare, banca B trebuie considerată operator pentru această prelucrare, iar transmiterea datelor cu caracter personal de la administratorul salariilor trebuie considerată divulgare de informații între doi operatori, de la angajatorul A la banca B.

Exemplu: Contabili

De asemenea, angajatorul A angajează întreprinderea de contabilitate C pentru a realiza audituri ale contabilității acesteia și, prin urmare, transferă date privind tranzacțiile financiare (inclusiv date cu caracter personal) către C. Întreprinderea de contabilitate C prelucrează aceste date în absența instrucțiunilor detaliate de la partea A. Întreprinderea de contabilitate C decide unilateral, în conformitate cu dispozițiile legale care reglementează sarcinile activităților de audit realizate de C, că datele pe care le colectează vor fi prelucrate numai în scopul auditării A și stabilește ce date trebuie să dețină, ce categorii de persoane trebuie înregistrate, cât timp se păstrează datele și ce mijloace tehnice trebuie să utilizeze. În aceste condiții, întreprinderea de contabilitate C trebuie considerată un operator separat atunci când furnizează servicii de audit pentru A. Totuși, această evaluare poate fi diferită în funcție de nivelul instrucțiunilor primite din partea A. În situația în care legea nu prevede obligații specifice pentru întreprinderea de contabilitate și întreprinderea client furnizează instrucțiuni foarte detaliate cu privire la prelucrare, întreprinderea de contabilitate ar acționa într-adevăr ca persoană împuternicită de operator. Se poate face o distincție între situația în care prelucrarea are loc - în conformitate cu legile care reglementează această profesie - ca parte a activității de bază a întreprinderii de contabilitate și cea în care prelucrarea este o sarcină auxiliară, mai limitată, care este realizată ca parte a activității întreprinderii client.

Exemplu: Servicii de găzduire

Angajatorul A angajează serviciul de găzduire H pentru a stoca date criptate pe serverele serviciului de găzduire H. Serviciul de găzduire H nu stabilește dacă datele pe care le găzduiește sunt date cu caracter

personal și nici nu prelucrează date în alt mod decât stocându-le pe serverele proprii. Deoarece stocarea este un exemplu de activitate de prelucrare a datelor cu caracter personal, serviciul de găzduire H prelucrează date cu caracter personal în numele angajatorului A și este, prin urmare, o persoană împuternicită de operator. Angajatorul A trebuie să furnizeze instrucțiunile necesare pentru serviciul de găzduire H și trebuie încheiat un acord de prelucrare a datelor în conformitate cu articolul 28, prin care să i se impună serviciului de găzduire H să implementeze măsuri de securitate tehnice și organizatorice. Serviciul de găzduire H trebuie să acorde asistență angajatorului A pentru a asigura că sunt luate măsurile de securitate necesare și să îl notifice în cazul oricărei încălcări a securității datelor cu caracter personal.

41. Chiar dacă deciziile privind mijloacele neesențiale pot fi lăsate la aprecierea persoanei împuternicite de operator, operatorul trebuie să continue să stipuleze anumite elemente în acordul privind persoana împuternicită de operator, precum în legătură cu cerința de securitate, de exemplu, instrucțiunea de a lua toate măsurile necesare în temeiul articolului 32 din RGPD. Acordul trebuie să prevadă, de asemenea, că persoana împuternicită de operator acordă asistență operatorului pentru a asigura respectarea articolului 32, de exemplu. În orice caz, operatorul rămâne responsabil de punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru a asigura și a fi în măsură să demonstreze că prelucrarea este efectuată în conformitate cu regulamentul (articolul 24). Astfel, operatorul trebuie să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile la adresa drepturilor și a libertăților persoanelor fizice. Din acest motiv, operatorul trebuie să fie pe deplin informat cu privire la mijloacele utilizate astfel încât să fie în măsură să ia o decizie în cunoștință de cauză în acest sens. Pentru ca operatorul să fie în măsură să demonstreze legalitatea prelucrării, se recomandă documentarea cel puțin a măsurilor tehnice și organizatorice necesare în contract sau în alt instrument obligatoriu din punct de vedere juridic încheiat între operator și persoana împuternicită de operator.

Exemplu: Centru de intermediere telefonică (call centre)

Întreprinderea X decide să externalizeze o parte din serviciul relații cu clienții către un centru de intermediere telefonică. Centrul de intermediere telefonică primește date identificabile cu privire la achizițiile făcute de clienți, precum și date de contact. Centrul de intermediere telefonică își utilizează software-ul și infrastructura informatică pentru a gestiona datele cu caracter personal referitoare la clienții întreprinderii X. Întreprinderea X semnează un acord privind persoana împuternicită de operator cu furnizorul serviciilor de centru de intermediere telefonică, în conformitate cu articolul 28 din RGPD, după ce a stabilit că măsurile tehnice și organizatorice de securitate propuse de centrul de intermediere telefonică sunt adecvate pentru riscurile în cauză și că centrul de intermediere telefonică va prelucra datele cu caracter personal doar în scopurile întreprinderii X și în conformitate cu instrucțiunile acesteia. Întreprinderea X nu furnizează centrului de intermediere telefonică instrucțiuni suplimentare cu privire la software-ul specific de utilizat și nici instrucțiuni detaliate cu privire la măsurile specifice de securitate de pus în aplicare. În acest exemplu, întreprinderea X rămâne operator, chiar dacă centrul de intermediere telefonică a stabilit anumite mijloace neesențiale de prelucrare.

2.1.5 „Prelucrare a datelor cu caracter personal”

42. Scopurile și mijloacele stabilite de operator trebuie să se refere la „prelucrarea datelor cu caracter personal”. Articolul 4 punctul (2) din RGPD definește prelucrarea datelor cu caracter personal ca „*orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal*”. În consecință, conceptul de operator poate fi legat fie de o singură operațiune de prelucrare, fie de un set de operațiuni. În practică, acest fapt poate însemna că controlul

exercitat de o anumită entitate se poate extinde la întreaga prelucrare în cauză, dar poate fi limitat și la o anumită etapă de prelucrare.[16]

43. În practică, prelucrarea datelor cu caracter personal care implică mai mulți actori poate fi împărțită în mai multe operațiuni de prelucrare mai mici pentru care fiecare actor ar putea fi considerat ca stabilind individual scopul și mijloacele. Pe de altă parte, o secvență sau un set de operațiuni de prelucrare care implică mai mulți actori poate avea loc, de asemenea, în același (aceleași) scop (scopuri), caz în care este posibil ca prelucrarea să implice unul sau mai mulți operatori asociați. Cu alte cuvinte, este posibil ca, la „nivel micro", diferitele operațiuni de prelucrare de-a lungul lanțului de prelucrare să apară ca fiind deconectate, deoarece fiecare dintre ele poate avea un scop diferit. Cu toate acestea, este necesar să se verifice de două ori dacă, la „nivel macro", aceste operațiuni de prelucrare nu trebuie considerate un „set de operațiuni" care urmăresc un scop comun utilizând mijloace definite în comun.

44. Orice persoană care decide să prelucreze date trebuie să ia în considerare dacă acestea includ date cu caracter personal și, în caz afirmativ, care sunt obligațiile care decurg din RGPD. Un actor va fi considerat „operator" chiar dacă nu vizează în mod deliberat date cu caracter personal ca atare sau dacă a evaluat în mod eronat că nu prelucrează date cu caracter personal.

45. Nu este necesar ca operatorul să aibă efectiv acces la datele care sunt în curs de prelucrare.[17] Persoana care externalizează o activitate de prelucrare și, astfel, are o influență determinantă asupra scopului și mijloacelor (esențiale) de prelucrare (de exemplu, prin ajustarea parametrilor unui serviciu astfel încât să influențeze ce date cu caracter personal trebuie prelucrate) trebuie considerată operator chiar dacă nu va avea niciodată acces efectiv la date.

Exemplu: Cercetarea de piață 1

Întreprinderea ABC dorește să înțeleagă ce tipuri de consumatori este cel mai probabil să fie interesați de produsele sale și contractează un furnizor de servicii, XYZ, pentru a obține informații relevante.

Întreprinderea ABC oferă instrucțiuni întreprinderii XYZ cu privire la tipul de informații de care este interesată pentru aceasta și furnizează o listă de întrebări care trebuie adresate celor care participă la cercetarea de piață.

Întreprinderea ABC primește doar informații statistice (de exemplu, identificarea tendințelor de consum pe regiune) de la XYZ și nu are acces la datele cu caracter personal ca atare. Cu toate acestea, întreprinderea ABC a decis că prelucrarea trebuie să aibă loc, prelucrarea este efectuată în scopul și pentru activitatea acesteia și a furnizat întreprinderii XYZ instrucțiuni detaliate cu privire la informațiile care trebuie colectate. Prin urmare, întreprinderea ABC trebuie considerată în continuare operator în ceea ce privește prelucrarea datelor cu caracter personal care are loc pentru a furniza informațiile pe care le-a solicitat. XYZ poate prelucra datele doar în scopul stabilit de întreprinderea ABC și în conformitate cu instrucțiunile detaliate ale acesteia și, prin urmare, trebuie considerat persoană împuternicită de operator.

[16] Hotărârea pronunțată în cauza *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, punctul 74: „*Rezultă, astfel cum a arătat [...] domnul avocat general, că o persoană fizică sau juridică poate fi operator, în sensul articolului 2, litera (d) din Directiva 95/46, împreună cu alții numai în privința operațiunilor care implică prelucrarea de date cu caracter personal cărora le stabilește în comun scopurile sau mijloacele. În schimb [...], această persoană fizică sau juridică nu poate fi considerată operator, în sensul dispoziției menționate, în privința unor operațiuni anterioare sau ulterioare din lanțul de prelucrare cărora nu le stabilește nici scopurile, nici mijloacele.*"

[17] Hotărârea pronunțată în cauza *Wirtschaftsakademie*, C-201/16, ECLI:EU:C:2018:388, punctul 38.

Exemplu: Cercetare de piață 2

Întreprinderea ABC dorește să înțeleagă ce tipuri de consumatori ar putea fi cei mai interesați de produsele sale. Furnizorul de servicii XYZ este o agenție de cercetare de piață care a colectat informații cu privire la interesele consumatorilor printr-o serie de chestionare care se referă la o gamă largă de produse și servicii. Furnizorul de servicii XYZ a cules și a analizat aceste date în mod independent, în conformitate cu metodologia proprie, fără a primi instrucțiuni de la întreprinderea ABC. Pentru a răspunde solicitării întreprinderii ABC, furnizorul de servicii XYZ va genera informații statistice, dar procedează astfel fără a primi instrucțiuni suplimentare cu privire la ce date cu caracter personal trebuie prelucrate sau la modul de prelucrare a acestora pentru a genera aceste statistici. În acest exemplu, furnizorul de servicii XYZ acționează în calitate de operator unic, prelucrând date cu caracter personal în scopuri de cercetare de piață, determinând în mod autonom mijloacele în acest sens. Întreprinderea ABC nu are niciun rol sau responsabilitate speciale în temeiul legislației privind protecția datelor în legătură cu aceste activități de prelucrare, deoarece întreprinderea ABC primește statistici anonimizate și nu este implicată în stabilirea scopurilor și a mijloacelor de prelucrare.

3 DEFINIȚIA OPERATORILOR ASOCIAȚI

3.1 Definiția operatorilor asociați

46. Calificarea ca operatori asociați poate apărea atunci când mai multe părți sunt implicate în prelucrare.

47. Deși conceptul nu este nou și a existat deja în Directiva 95/46/CE, articolul 26 din RGPD introduce norme specifice pentru operatorii asociați și stabilește un cadru care să reglementeze relația dintre aceștia. În plus, în hotărârile pronunțate recent, Curtea de Justiție a Uniunii Europene (CJUE) a contribuit cu clarificări la acest concept și la implicațiile acestuia.[18]

48. Astfel cum se detaliază suplimentar în secțiunea 2 din partea a II-a, calificarea operatorilor asociați va avea în principal consecințe în ceea ce privește alocarea obligațiilor pentru respectarea normelor de protecție a datelor și în special în ceea ce privește drepturile persoanelor fizice.

49. Din această perspectivă, secțiunea următoare vizează să furnizeze orientări cu privire la conceptul de operatori asociați în conformitate cu RGPD și cu jurisprudența CJUE pentru a ajuta entitățile să stabilească situațiile în care acestea ar putea acționa ca operatori asociați și pune conceptul în practică.

3.2 Existența controlului comun

3.2.1 Aspecte generale

50. Definiția operatorului de la articolul 4 punctul (7) din RGPD constituie punctul de plecare pentru stabilirea controlului comun. Aspectele din prezenta secțiune se referă, astfel, direct, la aspectele din

[18] A se vedea în special *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein împotriva Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu împotriva Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG împotriva Verbraucherzentrale NRW eV (*C-40/17). Trebuie remarcat faptul că, deși aceste hotărâri au fost pronunțate de CJUE cu privire la interpretarea conceptului de operatori asociați în temeiul Directivei 95/46/CE, acestea rămân valabile în contextul RGPD, având în vedere că elementele care determină acest concept în temeiul RGPD rămân aceleași ca în temeiul directivei.

secțiunea privind conceptul de operator, pe care le completează. În consecință, evaluarea controlului comun trebuie să reflecte evaluarea controlului „unic” elaborată mai sus.

51. Articolul 26 din RGPD, care reflectă definiția din articolul 4 punctul (7) din RGPD prevede că *„în cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați.”* În sens general, există control comun cu privire la o activitate specifică de prelucrare atunci când părți diferite stabilesc *în comun* scopul și mijloacele acestei activități de prelucrare. Prin urmare, evaluarea existenței operatorilor asociați necesită analiza dacă stabilirea scopurilor și a mijloacelor care caracterizează un operator este decisă de mai multe părți. „În comun” trebuie interpretat ca însemnând „împreună cu” sau „nu individual”, sub diferite forme și combinații, astfel cum se explică în continuare.

52. Evaluarea controlului comun trebuie efectuată pe baza unei analize mai degrabă factuale decât formale a influenței reale asupra scopurilor și mijloacelor de prelucrare. Toate acordurile existente sau preconizate trebuie verificate în funcție de circumstanțele factuale referitoare la relația dintre părți. Un criteriu pur formal nu ar fi suficient cel puțin din două motive: în unele cazuri, ar lipsi desemnarea formală a unui operator asociat, prevăzută, de exemplu, prin lege sau într-un contract; în alte cazuri, este posibil ca desemnarea formală să nu reflecte realitatea aranjamentelor, prin atribuirea formală a rolului de operator unei entități care, în realitate, nu este în măsură să „stabilească” scopurile și mijloacele de prelucrare.

53. Nu toate prelucrările care implică mai multe entități duc la un control comun. Criteriul general pentru existența controlului comun este **participarea comună a două sau mai multe entități la stabilirea scopurilor și a mijloacelor** unei operațiuni de prelucrare. Mai concret, participarea comună trebuie să includă stabilirea scopurilor, pe de o parte, și stabilirea mijloacelor, de cealaltă parte. În cazul în care fiecare dintre aceste elemente este stabilit de toate entitățile în cauză, acestea trebuie considerate operatori asociați ai prelucrării respective.

3.2.2 Evaluarea participării comune

54. Participarea comună la stabilirea scopurilor și mijloacelor implică faptul că mai multe entități influențează în mod decisiv dacă și cum are loc prelucrarea. În practică, participarea comună poate lua mai multe forme diferite. De exemplu, participarea comună se poate concretiza sub forma unei **decizii comune** luate de două sau mai multe entități sau poate decurge din **decizii convergente** luate de două sau mai multe entități cu privire la scopurile și mijloacele esențiale.

55. Participarea comună prin intermediul unei *decizii comune* înseamnă a decide împreună și implică intenția comună în conformitate cu sensul cel mai răspândit al termenului „în comun” menționat în articolul 26 din RGPD.

Situația participării comune prin *decizii convergente* decurge în special din jurisprudența CJUE privind conceptul de operatori asociați. Deciziile pot fi considerate convergente în ceea ce privește scopurile și mijloacele **dacă se completează reciproc și dacă sunt necesare pentru ca prelucrarea să aibă loc astfel încât să aibă un impact tangibil asupra stabilirii scopurilor și mijloacelor prelucrării**. Trebuie subliniat faptul că noțiunea de decizii convergente trebuie luată în considerare în legătură cu scopurile și mijloacele prelucrării, dar nu și cu alte aspecte ale relației comerciale dintre părți.[19] Ca atare, un criteriu important pentru identificarea deciziilor convergente în acest context **este dacă prelucrarea nu ar fi posibilă fără participarea ambelor părți la scopuri și mijloace în sensul că prelucrările de către**

[19] Într-adevăr, toate acordurile comerciale implică decizii convergente ca parte a procesului prin care se ajunge la acord.

fiecare parte sunt inseparabile, adică sunt legate între ele în mod indisolubil. Cu toate acestea, situația operatorilor asociați care acționează pe baza unor decizii convergente trebuie să fie diferențiată de cazul unei persoane împuternicite de operator, întrucât aceasta din urmă, deși participă la efectuarea unei prelucrări, nu prelucrează datele în scopuri proprii, ci efectuează prelucrarea în numele operatorului.

56. Faptul că una dintre părți nu are acces la datele cu caracter personal prelucrate nu este suficient pentru a exclude controlul comun.[20] De exemplu, în cauza *Martorii lui Iehova*, CJUE a considerat că o comunitate religioasă trebuie considerată operator, împreună cu membrii săi care asigură activitatea de predicare, în ceea ce privește prelucrarea datelor cu caracter personal efectuată de aceasta în contextul activității de predicare din casă în casă.[21] CJUE a considerat că nu era necesar ca comunitatea să aibă acces la datele în cauză sau să stabilească faptul că respectiva comunitate a oferit membrilor săi orientări sau instrucțiuni scrise în legătură cu prelucrarea datelor.[22] Comunitatea a participat la stabilirea scopurilor și a mijloacelor prin organizarea și coordonarea activităților membrilor acesteia, ceea ce a contribuit la realizarea obiectivului comunității Martorilor lui Iehova.[23] În plus, comunitatea avea cunoștință la nivel general de faptul că o astfel de prelucrare este efectuată pentru răspândirea credinței acesteia.[24]

57. De asemenea, este important să se sublinieze, astfel cum a clarificat CJUE, că o entitate va fi considerată operator asociat cu cealaltă parte (celelalte părți) doar în ceea ce privește operațiunile pentru care stabilește, împreună cu cealaltă parte (celelalte părți), mijloacele și scopurile aceleiași operațiuni de prelucrare a datelor, în special în cazul deciziilor convergente. În cazul în care una dintre aceste entități decide singură scopurile și mijloacele operațiunilor care sunt anterioare sau ulterioare în lanțul de prelucrare, entitatea respectivă trebuie considerată ca unicul operator în ceea ce privește această operațiune anterioară sau ulterioară.[25]

58. Existența răspunderii comune nu implică în mod necesar răspunderea egală a diferiților operatori implicați în prelucrarea datelor cu caracter personal. Dimpotrivă, CJUE a clarificat faptul că operatorii respectivi pot fi implicați în etape diferite ale prelucrării respective și în grade diferite, astfel încât nivelul de răspundere al fiecăruia dintre ei trebuie să fie evaluat în ceea ce privește toate circumstanțele relevante ale cazului respectiv.

3.2.2.1 Scop (scopuri) stabilit (stabilite) în comun

59. Controlul comun există în cazul în care entitățile implicate în aceeași operațiune de prelucrare efectuează prelucrarea în scopuri stabilite în comun. Acesta va fi cazul entităților implicate care prelucrează datele în aceleași scopuri sau în scopuri comune.

60. În plus, atunci când entitățile nu au același scop pentru prelucrare, controlul comun poate fi stabilit, de asemenea, în conformitate cu jurisprudența CJUE, atunci când entitățile implicate urmăresc scopuri strâns legate între ele sau care sunt complementare. Este cazul, de exemplu, în care există un beneficiu reciproc care rezultă din aceeași operațiune de prelucrare, cu condiția ca fiecare dintre entitățile implicate să participe la stabilirea scopurilor și mijloacelor pentru operațiunea relevantă de prelucrare.

---

[20] Hotărârea pronunțată în cauza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punctul 38.
[21] Hotărârea pronunțată în cauza *Martorii lui Iehova*, C-25/17, ECLI:EU:C:2018:551, punctul 75.
[22] Ibid.
[23] Ibid., punctul 71.
[24] Ibid.
[25] Hotărârea pronunțată în cauza *Fashion ID*, C-40/17, ECLI:EU:2018:1039, punctul 74 „*În schimb și fără a aduce atingere unei eventuale răspunderi civile prevăzute de dreptul național în această privință, această persoană fizică sau juridică nu poate fi considerată operator, în sensul dispoziției menționate, în privința unor operațiuni anterioare sau ulterioare din lanțul de prelucrare cărora nu le stabilește nici scopurile, nici mijloacele*”.

Cu toate acestea, noțiunea de beneficiu reciproc nu este decisivă și poate fi doar un indiciu. În hotărârea pronunțată în cauza *Fashion ID*, de exemplu, CJUE a clarificat faptul că un operator de site web participă la stabilirea scopurilor (și a mijloacelor) prelucrării prin inserarea unui modul social pe un site web pentru a optimiza publicitatea produselor proprii făcându-le mai vizibile pe rețelele de socializare. CJUE a considerat că operațiunile de prelucrare în cauză au fost efectuate atât în interesele economice al operatorului site-ului web, cât și ale furnizorului modulului social.[26]

61. De asemenea, astfel cum a subliniat CJUE în hotărârea pronunțată în cauza *Wirtschaftsakademie*, prelucrarea datelor cu caracter personal prin intermediul statisticilor referitoare la vizitatorii unei pagini pentru fani este menită să permită Facebook să își îmbunătățească sistemul de publicitate transmis prin intermediul rețelei proprii și să permită administratorului paginii pentru fani să obțină statistici pentru a gestiona promovarea activității proprii.[27] Fiecare entitate în acest caz își urmărește propriul interes, însă ambele părți participă la stabilirea scopurilor (și a mijloacelor) de prelucrare a datelor cu caracter personal în ceea ce privește vizitatorii paginii pentru fani.[28]

62. În acest sens, este important de subliniat că simpla existență a unui beneficiu reciproc (de exemplu comercial) care decurge dintr-o activitate de prelucrare nu dă naștere unui control comun. În cazul în care entitatea implicată în prelucrare nu urmărește un scop (scopuri) propriu (proprii) în legătură cu activitatea de prelucrare, ci este doar plătită pentru serviciile prestate, aceasta acționează mai degrabă ca persoană împuternicită de operator decât ca operator asociat.

3.2.2.2 Mijloace stabilite în comun

63. Pentru controlul comun este, de asemenea, necesar ca două sau mai multe entități să fi exercitat o influență asupra mijloacelor de prelucrare. Acest fapt nu înseamnă că, pentru a exista control comun, fiecare entitate implicată trebuie să stabilească toate mijloacele în toate situațiile. Într-adevăr, astfel cum a clarificat CJUE, entități diferite pot fi implicate în etape diferite ale prelucrării respective și în grade diferite. Prin urmare, operatori asociați diferiți pot defini mijloacele de prelucrare într-o măsură diferită, în funcție de cine este efectiv în măsură să procedeze astfel.

64. De asemenea, este posibil ca una dintre entitățile implicate să furnizeze mijloacele de prelucrare și să le pună la dispoziție pentru activități de prelucrare a datelor cu caracter personal efectuate de alte entități. Entitatea care decide să utilizeze aceste mijloace, astfel încât datele cu caracter personal să poată fi prelucrate într-un anumit scop, participă, de asemenea, la stabilirea mijloacelor de prelucrare.

65. Acest scenariu poate apărea în special în cazul platformelor, al instrumentelor standardizate sau al altor infrastructuri care permit părților să prelucreze aceleași date cu caracter personal și care au fost configurate într-un anumit mod de una dintre părți pentru a fi utilizate de alte părți care pot decide, de asemenea, cum să le configureze.[29] Utilizarea unui sistem tehnic deja existent nu exclude controlul comun atunci când utilizatorii sistemului pot decide cu privire la prelucrarea datelor cu caracter personal care va fi efectuată în acest context.

66. Ca exemplu în acest sens, CJUE a statuat, în cauza *Wirtschaftsakademie* că administratorul unei pagini pentru fani găzduite pe Facebook, prin definirea parametrilor pe baza audienței țintă a acesteia și a obiectivelor de gestionare și de promovare a activităților sale, trebuie considerat ca participând la

[26] Hotărârea pronunțată în cauza *Fashion ID,* C-40/17, ECLI:EU:2018:1039, punctul 80.
[27] Hotărârea pronunțată în cauza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punctul 34.
[28] Hotărârea pronunțată în cauza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punctul 39.
[29] Furnizorul sistemului poate fi un operator asociat dacă sunt îndeplinite criteriile menționate mai sus, și anume dacă furnizorul participă la stabilirea scopurilor și mijloacelor. În caz contrar, furnizorul trebuie considerat persoană împuternicită de operator.

stabilirea mijloacelor de prelucrare a datelor cu caracter personal referitoare la vizitatorii paginii sale pentru fani.

67. Mai mult, alegerea făcută de o entitate de a utiliza în scopuri proprii un instrument sau un alt sistem dezvoltat de o altă entitate, care permite prelucrarea datelor cu caracter personal, va constitui probabil o decizie comună cu privire la mijloacele respectivei prelucrări de către entitățile respective. Acest lucru rezultă din cauza Fashion ID, în care CJUE a concluzionat că, prin inserarea pe site-ul său web a butonului „îmi place" al Facebook pus la dispoziția operatorilor de site-uri web de către Facebook, Fashion ID a exercitat o influență decisivă cu privire la operațiunile care implică colectarea și transmiterea datelor cu caracter personal ale vizitatorilor site-ului său web către Facebook și, prin urmare, a stabilit împreună cu Facebook mijloacele acestei prelucrări.[30]

68. Este important de subliniat că **utilizarea unui sistem sau a unei infrastructuri comune de prelucrare nu va conduce, în toate cazurile, la calificarea părților implicate ca operatori asociați,** în special în cazul în care prelucrarea pe care aceștia o efectuează este separabilă și ar putea fi efectuată de o parte fără intervenția celeilalte sau în cazul în care furnizorul este o persoană împuternicită de operator în absența oricărui scop propriu (simpla existență a unui beneficiu comercial pentru părțile implicate nu este suficientă pentru a fi calificată drept unul dintre scopurile prelucrării).

Exemplu: Agenție de turism

O agenție de turism trimite datele cu caracter personal ale clienților săi la compania aeriană și la un lanț de hoteluri, în vederea efectuării rezervărilor pentru un pachet de servicii de călătorie. Compania aeriană și hotelul confirmă disponibilitatea locurilor și a camerelor solicitate. Agenția de turism emite documentele de călătorie și cupoanele pentru clienții săi. Fiecare dintre actori prelucrează datele pentru efectuarea propriilor lor activități, utilizând propriile lor mijloace. În această situație, agenția de turism, compania aeriană și hotelul sunt trei operatori de date diferiți care prelucrează date în scopuri proprii și separate și nu există control comun.

Agenția de turism, lanțul hotelier și compania aeriană decid ulterior să participe împreună la configurarea unei platforme comune online pentru scopul comun de a furniza oferte de pachete de servicii de călătorie. Aceștia convin asupra mijloacelor esențiale care trebuie utilizate, cum ar fi datele care vor fi stocate, modul în care vor fi alocate și confirmate rezervările și cine poate avea acces la informațiile stocate. În plus, aceștia decid să facă schimb de date referitoare la clienții proprii pentru a desfășura acțiuni comune de marketing. În acest caz, agenția de turism, compania aeriană și lanțul hotelier stabilesc împreună motivul și modul în care sunt prelucrate datele cu caracter personal ale clienților respectivi și, prin urmare, vor fi operatori asociați în ceea ce privește operațiunile de prelucrare legate de platforma comună de rezervare online și de acțiunile comune de marketing. Cu toate acestea, fiecare entitate ar urma să își păstreze controlul exclusiv în ceea ce privește alte activități de prelucrare în afara platformei comune online.

Exemplu: Proiect de cercetare realizat de institute

Mai multe institute de cercetare decid să participe la un proiect comun specific de cercetare și să utilizeze în acest scop platforma existentă a unuia dintre institutele implicate în proiect. Fiecare institut încarcă pe platformă date cu caracter personal pe care le deține deja în scopul cercetării comune și utilizează datele furnizate de ceilalți prin intermediul platformei pentru desfășurarea cercetării. În

[30] Hotărârea pronunțată în cauza Fashion ID, C-40/17, ECLI:EU:2018:1039, punctele 77-79.

acest caz, toate institutele se califică drept operatori asociați pentru prelucrarea datelor cu caracter personal realizată prin stocarea și dezvăluirea informațiilor de pe această platformă deoarece au decis împreună scopul prelucrării și mijloacele care vor fi utilizate (platforma existentă). Cu toate acestea, fiecare institut este un operator separat pentru orice altă prelucrare care poate fi efectuată în afara platformei în scopurile lor respective.

Exemplu: Operațiune de marketing

Întreprinderile A și B au lansat produsul C sub marcă comună și doresc să organizeze un eveniment de promovare a acestui produs. În acest scop, ele decid să facă schimb de date din bazele lor de date respective referitoare la clienți și clienții potențiali și să hotărască în ceea ce privește lista invitaților la eveniment pe această bază. De asemenea, convin asupra modalităților de trimitere a invitațiilor la eveniment, asupra modului de colectare a feedbackului în cursul evenimentului și asupra acțiunilor de marketing ulterioare. Întreprinderile A și B pot fi considerate operatori asociați pentru prelucrarea datelor cu caracter personal referitoare la organizarea evenimentului promoțional deoarece decid împreună cu privire la scopul definit în comun și mijloacele esențiale de prelucrare a datelor în acest context.

Exemplu: Studii clinice[31]

Un furnizor de servicii medicale (cercetătorul) și o universitate (sponsorul) decid să lanseze împreună un studiu clinic cu același scop. Aceștia colaborează la redactarea protocolului studiului [și anume, scopul, metodologia/conceptul studiului, datele care trebuie colectate, criteriile de excludere/includere a subiecților, reutilizarea bazei de date (dacă este cazul) etc.]. Aceștia pot fi considerați ca operatori asociați pentru acest studiu clinic deoarece stabilesc împreună și convin asupra aceluiași scop și asupra mijloacelor esențiale de prelucrare. Colectarea datelor cu caracter personal din fișa medicală a pacientului în scop de cercetare trebuie diferențiată de stocarea și utilizarea acelorași date în scop de asistență medicală a pacientului, pentru care furnizorul de servicii medicale continuă să fie operatorul.

În cazul în care cercetătorul nu participă la redactarea protocolului (acesta pur și simplu acceptă protocolul elaborat deja de sponsor) și protocolul este conceput doar de către sponsor, cercetătorul trebuie să fie considerat persoană împuternicită de operator iar sponsorul operator pentru acest studiu clinic.

Exemplu: Recrutarea de personal

Întreprinderea X ajută întreprinderea Y să recruteze personal nou cu ajutorul celebrului său serviciu cu valoare adăugată, „global matchz”. Întreprinderea X caută candidații potriviți atât printre CV-urile primite direct de întreprinderea Y, cât și printre cele pe care le are deja în baza de date proprie. Această bază de date este creată și gestionată de întreprinderea X pe cont propriu. Astfel, se asigură faptul că întreprinderea X îmbunătățește corelarea dintre ofertele de locuri de muncă și persoanele aflate în căutarea unui loc de muncă, sporindu-și astfel veniturile. Chiar dacă nu au luat o decizie în mod formal împreună, întreprinderile X și Y participă împreună la prelucrare cu scopul de a găsi candidați potriviți pe baza unor decizii convergente: decizia de a crea și gestiona serviciul „global matchz” pentru

[31] CEPD intenționează să ofere orientări suplimentare în legătură cu studiile clinice în contextul viitoarelor sale orientări privind prelucrarea datelor cu caracter personal în scopuri medicale și de cercetare științifică.

întreprinderea X și decizia întreprinderii Y de a îmbogăți baza de date cu CV-urile pe care le primește direct. Astfel de decizii se completează reciproc, nu se pot separa și sunt necesare pentru ca prelucrarea operațiunii de identificare a candidaților potriviți să aibă loc. Prin urmare, în acest caz special, aceste entități trebuie considerate operatori asociați pentru această prelucrare. Cu toate acestea, întreprinderea X este unicul operator al prelucrării necesare pentru gestionarea bazei sale de date, iar întreprinderea Y este unicul operator al prelucrării ulterioare a angajării în scopuri proprii (organizarea de interviuri, încheierea contractului și gestionarea datelor de resurse umane).

Exemplu: Analiza datelor cu caracter personal privind sănătatea

Întreprinderea ABC, dezvoltatorul unei aplicații de monitorizare a tensiunii arteriale, și întreprinderea XYZ, un furnizor de aplicații pentru profesioniștii din domeniul medical, doresc să examineze modul în care modificările tensiunii arteriale pot contribui la prognozarea anumitor boli. Întreprinderile decid să creeze un proiect comun și să se adreseze spitalului DEF pentru a-l invita să se implice.

Datele cu caracter personal care vor fi prelucrate în cadrul acestui proiect constau în date cu caracter personal pe care întreprinderea ABC, spitalul DEF și întreprinderea XYZ le prelucrează separat în calitate de operatori individuali. Decizia de a prelucra aceste date pentru a evalua modificările tensiunii arteriale este luată în comun de către cei trei actori. Întreprinderea ABC, spitalul DEF și întreprinderea XYZ au stabilit în comun scopurile prelucrării. Întreprinderea XYZ ia inițiativa de a propune mijloacele esențiale de prelucrare. Atât întreprinderea ABC, cât și spitalul DEF acceptă aceste mijloace esențiale după ce s-au implicat inclusiv în dezvoltarea unor caracteristici ale aplicației astfel încât rezultatele să poată fi utilizate în mod suficient de către ei. Cele trei organizații convin astfel asupra unui scop comun pentru prelucrare, care este evaluarea modului în care modificările tensiunii arteriale pot contribui la prognozarea anumitor boli. După finalizarea cercetării, întreprinderea ABC, spitalul DEF și întreprinderea XYZ pot beneficia de evaluare prin utilizarea rezultatelor în activitățile proprii. Pentru toate aceste motive, entitățile se califică drept operatori asociați pentru această prelucrare comună specifică.

În cazul în care întreprinderea XYZ ar fi solicitată pur și simplu de către ceilalți să efectueze această evaluare fără a avea un scop propriu și ar fi prelucrat pur și simplu date în numele celorlalți, întreprinderea XYZ s-ar califica ca persoană împuternicită de operator chiar dacă i s-ar fi atribuit stabilirea mijloacelor neesențiale.

3.2.3 Situații în care nu există control comun

69. Faptul că mai mulți actori sunt implicați în aceeași prelucrare nu înseamnă că aceștia acționează în mod necesar ca operatori asociați ai acestei prelucrări. Nu toate tipurile de parteneriate, cooperări sau colaborări implică calificarea ca operatori asociați, întrucât această calificare necesită o analiză individuală a fiecărei prelucrări vizate și a rolului exact al fiecărei entități în ceea ce privește fiecare prelucrare. Cazurile de mai jos reprezintă exemple neexhaustive de situații în care nu există control comun.

70. De exemplu, schimbul acelorași date sau al aceluiași set de date între două entități fără scopuri stabilite în comun sau mijloace de prelucrare stabilite în comun trebuie considerat o transmitere de date între operatori diferiți.

Exemplu: Transmiterea datelor despre angajați către autoritatea fiscală

O întreprindere colectează și prelucrează datele cu caracter personal ale angajaților săi în scopul gestionării salariilor, a asigurărilor de sănătate etc. Conform legii, întreprinderea are obligația să transmită autorității fiscale toate datele despre salarii, în vederea consolidării controlului fiscal.

În acest caz, chiar dacă atât întreprinderea, cât și autoritatea fiscală prelucrează aceleași date privind salariile, lipsa unor scopuri și mijloace stabilite în comun cu privire la această prelucrare a datelor va duce la calificarea celor două entități ca doi operatori de date separați.

71. Controlul comun poate fi, de asemenea, exclus în situația în care mai multe entități utilizează o bază de date comună sau o infrastructură comună, în cazul în care fiecare entitate stabilește în mod independent scopurile proprii.

Exemplu: Operațiuni de marketing într-un grup de întreprinderi care utilizează o bază de date comună:

Un grup de întreprinderi utilizează aceeași bază de date pentru gestionarea clienților și a clienților potențiali. Această bază de date este găzduită pe serverele întreprinderii-mamă, care, prin urmare, este o persoană împuternicită de întreprinderi în ceea ce privește stocarea datelor. Fiecare entitate a grupului introduce datele propriilor clienți și ale potențialilor clienți și prelucrează aceste date exclusiv în scopuri proprii. De asemenea, fiecare entitate decide în mod independent cu privire la accesul, perioadele de păstrare, rectificarea sau ștergerea datelor cu caracter personal ale clienților și ale clienților săi potențiali. Acestea nu pot accesa sau utiliza datele celeilalte. Simplul fapt că aceste întreprinderi utilizează o bază de date comună nu implică, în sine, un control comun. În aceste circumstanțe, fiecare întreprindere este, astfel, un operator separat.

Exemplu: Operatori independenți care utilizează o infrastructură comună

Întreprinderea XYZ găzduiește o bază de date și o pune la dispoziția altor întreprinderi pentru a prelucra și găzdui a datelor cu caracter personal cu privire la angajații lor. Întreprinderea XYZ este o persoană împuternicită de operator în ceea ce privește prelucrarea și stocarea datelor angajaților altor întreprinderi, deoarece aceste operațiuni sunt efectuate în numele și în conformitate cu instrucțiunile acestor întreprinderi. În plus, celelalte întreprinderi prelucrează datele fără nicio implicare din partea întreprinderii XYZ și în scopuri pe care întreprinderea XYZ nu le împărtășește deloc.

72. De asemenea, pot exista situații în care actori diferiți prelucrează succesiv aceleași date cu caracter personal într-un lanț de operațiuni, fiecare dintre acești actori având un scop independent și mijloace independente în partea lor din lanțul de prelucrare. În absența participării comune la stabilirea scopurilor și mijloacelor aceleiași operațiuni de prelucrare sau ale aceluiași set de operațiuni, controlul comun trebuie să fie exclus, iar actorii diferiți trebuie considerați operatori independenți succesivi.

Exemplu: Analiză statistică pentru o sarcină de interes public

Autoritatea publică (autoritatea A) are sarcina legală de a efectua analize și statistici relevante cu privire la evoluția ratei de ocupare a forței de muncă din țara respectivă. În acest scop, multe alte entități publice au obligația legală de a divulga autorității A date specifice. Autoritatea A decide să utilizeze un sistem specific pentru prelucrarea datelor, inclusiv colectarea acestora. Acest fapt înseamnă, de asemenea, că celelalte unități sunt obligate să utilizeze sistemul pentru a divulga datele pe care le dețin. În acest caz, fără a aduce atingere atribuirii de roluri prin lege, autoritatea A va fi singurul operator al prelucrării în scopul analizei și al statisticilor privind rata de ocupare a forței de muncă prelucrată în sistem, deoarece autoritatea A stabilește scopul prelucrării și a decis modul în care

va fi organizată prelucrarea. Desigur, celelalte entități publice, ca operatori pentru activitățile proprii de prelucrare, sunt responsabile de asigurarea exactității datelor pe care le-au prelucrat anterior și pe care le divulgă ulterior autorității A.

4 DEFINIȚIA PERSOANEI ÎMPUTERNICITE DE OPERATOR

73. Persoana împuternicită de operator este definită la articolul 4 punctul (8) ca persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului. Similar definiției operatorului, definiția persoanei împuternicite de operator se referă la o gamă largă de actori - aceasta poate fi „*persoana fizică sau juridică, autoritatea publică, agenția sau alt organism*”. Acest fapt înseamnă că, în principiu, nu există nicio limitare cu privire la tipul de actor care ar putea să își asume rolul de persoană împuternicită de operator. Ar putea fi o organizație, dar ar putea fi și o persoană fizică.

74. RGPD stabilește obligații direct aplicabile în mod specific persoanelor împuternicite de operatori, astfel cum se specifică suplimentar în partea II secțiunea 1 din prezentele orientări. O persoană împuternicită de operator poate fi considerată răspunzătoare sau amendată în caz de nerespectare a acestor obligații sau în cazul în care acționează în afara sau contrar instrucțiunilor legale ale operatorului sau în contradicție cu acestea.

75. Prelucrarea datelor cu caracter personal poate implica mai multe persoane împuternicite de operatori. De exemplu, un operator poate alege el însuși să angajeze în mod direct mai multe persoane împuternicite de operator, prin implicarea mai multor persoane împuternicite de operator în diferite etape ale prelucrării (mai multe persoane împuternicite de operator). Un operator ar putea decide, de asemenea, să angajeze o persoană împuternicită de operator care, la rândul său — cu autorizarea operatorului — angajează una sau mai multe persoane împuternicite de operator [„subcontractant (subcontractanți)”]. Activitatea de prelucrare atribuită persoanei împuternicite de operator poate fi limitată la o sarcină sau la un context foarte specific sau poate fi mai generală și extinsă.

76. Există două condiții elementare pentru a fi calificat ca persoană împuternicită de operator:

    a) existența ca *entitate separată* în raport cu operatorul și

    b) prelucrarea datelor cu caracter personal *în numele operatorului*.

77. *O entitate separată* înseamnă că operatorul decide să delege toate sau o parte din activitățile de prelucrare unei organizații externe. În cadrul unui grup de întreprinderi, o întreprindere poate fi persoană împuternicită de operator pentru o altă întreprindere care acționează ca operator, întrucât ambele întreprinderi sunt entități separate. Pe de altă parte, un departament din cadrul unei întreprinderi nu poate fi o persoană împuternicită de operator pentru un alt departament din cadrul aceleiași entități.

78. În cazul în care operatorul decide să prelucreze el însuși datele, utilizând propriile resurse în cadrul organizației sale, de exemplu prin intermediul personalului propriu, aceasta nu este o situație în care persoana împuternicită de operator este implicată. Angajații și celelalte persoane care acționează sub autoritatea directă a operatorului, precum personalul angajat temporar, nu trebuie considerate persoane împuternicite de operator, deoarece prelucrează date cu caracter personal ca parte a entității operatorului. În conformitate cu articolul 29, aceștia sunt, de asemenea, obligați să respecte instrucțiunile operatorului.

79. *Prelucrarea datelor cu caracter personal în numele operatorului* necesită în primul rând ca entitatea separată să prelucreze datele cu caracter personal în beneficiul operatorului. La articolul (4) punctul (2), prelucrarea este definită ca un concept care include o gamă largă de operațiuni, care variază de la colectare, stocare și consultare, la utilizare, diseminare sau punere la dispoziție în orice alt mod și distrugere. Conceptul de „prelucrare" este descris anterior, în detaliu, la punctul 2.1.5.

80. În al doilea rând, prelucrarea trebuie efectuată în numele unui operator, dar altfel decât sub autoritatea sau controlul direct al acestuia. Luarea de măsuri „în numele" înseamnă deservirea intereselor altei persoane și reamintește de conceptul juridic de „delegare". În cazul legislației privind protecția datelor, persoanei împuternicite de operator i se solicită să pună în practică instrucțiunile transmise de operator cel puțin cu privire la scopul prelucrării și elementele esențiale ale mijloacelor. Legalitatea prelucrării în conformitate cu articolul 6 și, dacă este relevant, cu articolul 9 din regulament va decurge din activitatea operatorului iar persoana împuternicită de operator trebuie să prelucreze datele doar în conformitate cu instrucțiunile operatorului. Cu toate acestea, astfel cum este descris mai sus, instrucțiunile operatorului pot lăsa o anumită marjă de apreciere cu privire la modul în care pot fi deservite cel mai bine interesele operatorului, permițând persoanei împuternicite de operator să aleagă cele mai adecvate mijloace tehnice și organizatorice.[32]

81. Luarea de măsuri „în numele" înseamnă, de asemenea, că persoana împuternicită de operator nu poate efectua prelucrarea în scopuri proprii. Astfel cum se prevede la articolul 28 alineatul (10), o persoană împuternicită de operator încalcă RGPD dacă nu respectă instrucțiunile operatorului și începe să-și stabilească propriile scopuri și mijloace de prelucrare. Persoana împuternicită de operator va fi considerată operator cu privire la respectiva prelucrare și poate face obiectul sancțiunilor pentru nerespectarea instrucțiunilor operatorului.

Exemplu: Furnizor de servicii desemnat persoană împuternicită de operator, dar care acționează ca operator

Furnizorul de servicii MarketinZ oferă servicii de publicitate promoțională și de marketing direct pentru diferite întreprinderi. Întreprinderea GoodProductZ încheie un contract cu MarketinZ, conform căruia aceasta din urmă furnizează publicitate comercială pentru clienții GoodProductZ și este prezentată ca persoană împuternicită de operator. Cu toate acestea, MarketinZ decide să utilizeze baza de date de clienți a GoodProducts și în alte scopuri decât publicitatea pentru GoodProducts, cum ar fi dezvoltarea propriei activități comerciale. Decizia de a adăuga un scop suplimentar la cel pentru care au fost transferate datele cu caracter personal transformă MarketinZ într-un operator pentru acest set de operațiuni de prelucrare, iar prelucrarea acestora în acest scop ar constitui o încălcare a RGPD.

82. CEPD reamintește că nu orice furnizor de servicii care prelucrează date cu caracter personal pe parcursul furnizării unui serviciu este o „persoană împuternicită de operator" în sensul RGPD. Rolul unei persoane împuternicite de operator nu decurge din natura unei entități care prelucrează date, ci din activitățile concrete ale acesteia într-un context specific. Cu alte cuvinte, aceeași entitate poate avea în același timp rolul de operator pentru anumite operațiuni de prelucrare și rolul de persoană împuternicită de operator pentru altele, iar calificarea acesteia ca operator sau persoană împuternicită de operator trebuie evaluată în raport cu seturi de date sau operațiuni specifice. Natura serviciului va stabili dacă activitatea de prelucrare este echivalentă cu prelucrarea datelor cu caracter personal în numele operatorului în sensul RGPD. În practică, în cazul în care serviciul furnizat nu vizează în mod specific prelucrarea datelor cu caracter personal sau în cazul în care o astfel de prelucrare nu constituie un element-cheie al serviciului, furnizorul de servicii poate fi în măsură să stabilească în mod

[32] A se vedea partea I, punctul 2.1.4, unde se descrie distincția între mijloacele esențiale și cele neesențiale.

independent scopurile și mijloacele de prelucrare respective, necesare pentru furnizarea serviciului. În această situație, furnizorul de servicii trebuie considerat un operator separat, și nu o persoană împuternicită de operator.[33] Cu toate acestea, este necesară o analiză individuală, de la caz la caz, pentru a stabili gradul de influență pe care fiecare entitate îl are efectiv în stabilirea scopurilor și mijloacelor de prelucrare.

Exemplu: Serviciu de taximetrie

Un serviciu de taximetrie oferă o platformă digitală care permite întreprinderilor să rezerve un taxi pentru a transporta angajați sau invitați la și de la aeroport. Atunci când rezervă un taxi, întreprinderea ABC specifică numele angajatului care trebuie să fie preluat de la aeroport, astfel încât șoferul să poată confirma identitatea angajatului în momentul preluării. În acest caz, serviciul de taximetrie prelucrează datele cu caracter personal ale angajatului ca parte a serviciului său către întreprinderea ABC, dar această prelucrare nu este obiectivul serviciului. Serviciul de taximetrie a conceput platforma de rezervare online ca parte a dezvoltării activității sale comerciale pentru a furniza servicii de transport, fără a primi nicio instrucțiune de la întreprinderea ABC. De asemenea, serviciul de taximetrie stabilește în mod independent categoriile de date pe care le colectează și cât timp le reține. Prin urmare, serviciul de taximetrie acționează ca operator de sine stătător, fără a aduce atingere faptului că prelucrarea are loc în urma unei cereri a întreprinderii ABC pentru serviciile acestuia.

83. CEPD menționează că un furnizor de servicii poate continua să acționeze ca persoană împuternicită de operator chiar dacă prelucrarea datelor cu caracter personal nu este obiectul principal sau primordial al serviciului, cu condiția ca clientul serviciului să continue să stabilească scopurile și mijloacele de prelucrare în practică. Atunci când analizează dacă să atribuie sau nu prelucrarea datelor cu caracter personal unui anumit furnizor de servicii, operatorii trebuie să evalueze cu atenție dacă furnizorul de servicii în cauză le permite să exercite un grad suficient de control, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile potențiale pentru persoanele vizate.

Exemplu: Centru de intermediere telefonică (call centre)

Întreprinderea X își externalizează serviciul suport clienți către întreprinderea Y, care oferă un centru de intermediere telefonică pentru a-i ajuta pe clienții întreprinderii X răspunzând la întrebările acestora. Serviciul de suport clienți înseamnă că întreprinderea Y trebuie să aibă acces la baza de date cu clienții întreprinderii X. Întreprinderea Y poate accesa date doar pentru a oferi serviciul achiziționat de întreprinderea X și nu poate prelucra date în alte scopuri decât cele declarate de întreprinderea X. Întreprinderea Y trebuie considerată persoană împuternicită de operator, iar un acord privind persoana împuternicită de operator trebuie încheiat între întreprinderile X și Y.

Exemplu: Serviciu IT general

Întreprinderea Z angajează un furnizor de servicii IT pentru asistență tehnică IT pentru sistemele proprii, care includ un volum mare de date cu caracter personal. Accesul la datele cu caracter personal nu constituie obiectul principal al serviciului de suport, dar accesul sistematic la datele cu caracter personal al furnizorului de servicii IT este inevitabil pentru prestarea serviciului. Prin urmare,

[33] A se vedea, de asemenea, considerentul 81 din RGPD, care se referă la atribuirea de „activități de prelucrare unei persoane împuternicite de operator", indicând faptul că această activitate de prelucrare este o parte importantă a deciziei operatorului de a solicita unei persoane împuternicite de operator să prelucreze date cu caracter personal în numele său.

întreprinderea Z concluzionează că furnizorul de servicii IT — fiind o întreprindere separată și, în mod inevitabil, solicitată să prelucreze date cu caracter personal, chiar dacă acesta nu este obiectivul principal al serviciului — trebuie să fie considerat persoană împuternicită de operator. Prin urmare, se încheie un acord privind persoana împuternicită de operator cu furnizorul de servicii IT.

Exemplu: Consultant IT care rezolvă o problemă de software

Întreprinderea ABC angajează un specialist IT de la o altă întreprindere pentru a rezolva o problemă cu un software utilizat de întreprinderea ABC. Consultantul IT nu este angajat să prelucreze date cu caracter personal, iar întreprinderea ABC stabilește că orice acces la datele cu caracter personal va fi pur și simplu accidental și, prin urmare, foarte limitat în practică. Prin urmare, ABC concluzionează că specialistul IT nu este o persoană împuternicită de operator (și nici un operator de sine stătător) și că întreprinderea ABC va lua măsurile adecvate în conformitate cu articolul 32 din RGPD pentru a împiedica consultantul IT să prelucreze date cu caracter personal în mod neautorizat.

84. Astfel cum s-a menționat mai sus, nimic nu împiedică persoana împuternicită de operator să ofere un serviciu definit în prealabil, însă operatorul trebuie să ia decizia finală de a aproba în mod activ modul în care se efectuează prelucrarea, cel puțin în ceea ce privește mijloacele esențiale de prelucrare. Astfel cum s-a menționat mai sus, o persoană împuternicită de operator are o marjă de manevră în ceea ce privește mijloacele neesențiale, a se vedea mai sus la punctul 2.1.4.

Exemplu: Furnizor de servicii cloud

O municipalitate a decis să utilizeze un furnizor de servicii cloud pentru a prelucra informații în cadrul serviciilor sale școlare și educaționale. Serviciul cloud oferă servicii de mesagerie, videoconferințe, stocare de documente, gestionarea calendarului, procesare de texte etc. și va implica prelucrarea datelor cu caracter personal referitoare la elevi și profesori. Furnizorul de servicii cloud a oferit un serviciu standardizat prestat la nivel mondial. Cu toate acestea, municipalitatea trebuie să se asigure că acordul în vigoare respectă articolul 28 alineatul (3) din RGPD, că datele cu caracter personal al căror operator este aceasta sunt prelucrate exclusiv în scopurile municipalității. De asemenea, aceasta trebuie să se asigure că furnizorul de servicii cloud respectă instrucțiunile sale specifice privind perioadele de stocare, ștergerea datelor etc., indiferent de ceea ce este oferit în general în cadrul serviciului standardizat.

5 DEFINIȚIA PĂRȚII TERȚE/A DESTINATARULUI

85. Regulamentul nu definește doar conceptele de operator și de persoană împuternicită de operator, ci și conceptele de destinatar și parte terță. Spre deosebire de conceptele de operator și persoană împuternicită de operator, regulamentul nu prevede obligații sau responsabilități specifice pentru destinatari și părți terțe. Se poate spune că acestea sunt concepte relative în sensul că descriu o relație cu un operator sau o persoană împuternicită de operator dintr-o perspectivă specifică, de exemplu un operator sau o persoană împuternicită de operator divulgă date unui destinatar. Un destinatar al datelor cu caracter personal și o parte terță pot fi considerați simultan ca fiind operator sau persoană împuternicită de operator din alte perspective. De exemplu, entitățile care vor fi considerate destinatari sau părți terțe dintr-o perspectivă sunt operatori pentru prelucrarea pentru care acestea stabilesc scopul și mijloacele.

Partea terță

86. Articolul 4 punctul (10) definește o „*parte terță*" ca o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât

- persoana vizată,
- operatorul,
- persoană împuternicită de operator și
- persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

87. Definiția corespunde, în general, definiției anterioare a „*terțului*" din Directiva 95/46/CE.

88. Deși termenii „*date cu caracter personal*", „*persoană vizată*", „*operator*" și „*persoană împuternicită de operator*" sunt definiți în regulament, conceptul „*[persoanele] care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal*" nu este definit. Cu toate acestea, în general, acest concept se înțelege ca făcând referire la persoanele care aparțin entității juridice a operatorului sau a persoanei împuternicite de operator (un angajat sau un rol foarte comparabil cu cel al angajaților, de exemplu, personal interimar furnizat prin intermediul unei agenții pentru ocuparea temporară a forței de muncă), dar numai în măsura în care aceste persoane sunt autorizate să prelucreze date cu caracter personal. Un angajat etc. care obține acces la datele pe care nu este autorizat să le acceseze și în alte scopuri decât cele ale angajatorului nu se încadrează în această categorie. În schimb, acest angajat trebuie considerat parte terță în ceea ce privește prelucrarea efectuată de angajator. În măsura în care angajatul prelucrează date cu caracter personal în scopuri proprii, distincte de cele ale angajatorului său, acesta va fi considerat operator și își asumă toate consecințele și răspunderile care decurg în raport cu prelucrarea datelor cu caracter personal.[34]

89. Prin urmare, partea terță se referă la o persoană care, în situația specifică în cauză, nu este o persoană vizată, un operator, o persoană împuternicită de operator sau un angajat. De exemplu, operatorul poate angaja o persoană împuternicită de operator și să o instructeze să transfere date cu caracter personal unei părți terțe. Această parte terță va fi apoi considerată operator de sine stătător pentru prelucrarea pe care o efectuează în scopuri proprii. Trebuie remarcat faptul că, în cadrul unui grup de întreprinderi, întreprinderea diferită de operator sau de persoana împuternicită de operator este o parte terță, chiar dacă face parte din același grup din care face parte întreprinderea care acționează ca operator sau persoană împuternicită de operator.

Exemplu: Servicii de curățenie

Întreprinderea A încheie un contract cu o întreprindere de servicii de curățenie pentru curățarea birourilor acesteia. Agenții de curățenie nu trebuie să acceseze sau să prelucreze în alt mod date cu caracter personal. Chiar dacă aceștia pot intra în contact ocazional cu astfel de date atunci când se deplasează prin birou, își pot îndeplini sarcina fără a accesa date și li se interzice prin contract să acceseze sau să prelucreze în alt mod date cu caracter personal pe care întreprinderea A le păstrează ca operator. Agenții de curățenie nu sunt angajați ai întreprinderii A și nici nu sunt considerați ca fiind sub directa autoritate a întreprinderii respective. Nu există nicio intenție de a angaja întreprinderea de servicii de curățenie sau pe angajații acesteia pentru prelucrarea datelor cu caracter personal în

[34] Cu toate acestea, angajatorul (ca operator inițial) ar putea avea în continuare o anumită răspundere în cazul în care noua prelucrare are loc din cauza lipsei unor măsuri de securitate adecvate.

numele întreprinderii A. Prin urmare, întreprinderea de servicii de curățenie și angajații acesteia trebuie să fie considerați ca parte terță, iar operatorul trebuie să se asigure că există măsuri de securitate adecvate pentru a preveni accesul acestora la date și pentru a stabili o obligație de confidențialitate în cazul în care aceștia ar putea intra în contact accidental cu date cu caracter personal.

Exemplu: Grupuri de întreprinderi - întreprindere-mamă și filiale

Întreprinderile X și Y fac parte din grupul Z. Ambele întreprinderi X și Y prelucrează date cu privire la respectivii lor angajați în scopul administrării. La un moment dat, întreprinderea-mamă ZZ decide să solicite date privind angajații de la toate filialele pentru a pregăti statistici la nivel de grup. Atunci când transferă date de la întreprinderile X și Y către întreprinderea ZZ, aceasta din urmă trebuie considerată o parte terță, indiferent dacă toate întreprinderile fac parte din același grup. Întreprinderea ZZ va fi considerată operator pentru efectuarea prelucrării datelor în scopuri statistice.

Destinatarul

90. Articolul 4 punctul (9) definește „*destinatarul*" ca persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice nu trebuie considerate destinatari atunci când primesc date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern (de exemplu, autorități fiscale și vamale, unități de investigații financiare etc.)[35]

91. Definiția corespunde, în general, definiției anterioare a termenului „*destinatar*" din Directiva 95/46/CE.

92. Definiția cuprinde orice persoană căreia îi sunt transmise date cu caracter personal, indiferent dacă este sau nu o parte terță. De exemplu, atunci când un operator transmite date cu caracter personal unei alte entități, fie unei persoane împuternicite de operator, fie unei părți terțe, această entitate este un destinatar. Destinatarul terț este considerat operator pentru orice prelucrare pe care o efectuează în scopuri proprii după primirea datelor.

Exemplu: Divulgarea datelor între întreprinderi

Agenția de turism ExploreMore organizează călătorii la cererea clienților săi individuali ai acesteia. În cadrul acestui serviciu, agenția de turism transmite datele cu caracter personal ale clienților către companii aeriene, hoteluri și organizatori de excursii pentru ca aceste entități să își poată presta serviciile respective. ExploreMore, hotelurile, companiile aeriene și furnizorii de excursii trebuie considerați fiecare operatori pentru prelucrarea pe care o efectuează în cadrul serviciilor respective. Nu există nicio relație operator-persoană împuternicită de operator. Cu toate acestea, companiile aeriene, hotelurile și furnizorii de excursii trebuie considerați destinatari atunci când primesc datele cu caracter personal de la ExploreMore.

[35] A se vedea, de asemenea, considerentul 31 din RGPD.

PARTEA II — CONSECINȚELE ATRIBUIRII UNOR ROLURI DIFERITE

1 RELAȚIA DINTRE OPERATOR ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

93. O nouă caracteristică distinctă a RGPD este reprezentată de dispozițiile care impun obligații direct persoanelor împuternicite de operator. De exemplu, o persoană împuternicită de operator trebuie să se asigure că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea [articolul 28 alineatul (3); persoana împuternicită de operator trebuie să păstreze o evidență a tuturor categoriilor de activități de prelucrare [articolul 30 alineatul (2)] și să implementeze măsuri tehnice și organizatorice adecvate (articolul 32). De asemenea, persoana împuternicită de operator trebuie să desemneze un responsabil cu protecția datelor în anumite condiții (articolul 37) și are obligația să înștiințeze operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal [articolul 33 alineatul (2)]. În plus, normele privind transferurile de date către țări terțe (capitolul V) se aplică atât persoanelor împuternicite de operator, cât și operatorilor. În acest sens, CEPD consideră că articolul 28 alineatul (3) din RGPD, deși indică un conținut specific pentru contractul necesar dintre operator și persoana împuternicită de operator, impune obligații directe persoanelor împuternicite de operator, inclusiv obligația de a asista operatorul în asigurarea respectării normelor.[36]

1.1 Alegerea persoanei împuternicite de operator

94. Operatorul are **obligația de a utiliza „doar persoane împuternicite care oferă garanții suficiente** pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate", astfel încât prelucrarea să respecte cerințele RGPD — inclusiv pentru securitatea prelucrării — și să asigure protecția drepturilor persoanelor vizate.[37] Prin urmare, operatorul este responsabil de evaluarea caracterului suficient al garanțiilor oferite de persoana împuternicită de operator și trebuie să fie în măsură să demonstreze că a luat în considerare în mod serios toate elementele prevăzute în RGPD.

95. Garanțiile „oferite" de persoana împuternicită de operator sunt cele pe care persoana împuternicită de operator este în măsură să **le demonstreze spre satisfacția operatorului**, întrucât acestea sunt singurele care pot fi luate în considerare efectiv de către operator atunci când evaluează respectarea obligațiilor sale. Adesea, acest fapt va necesita un schimb de documente relevante (de exemplu, politica de confidențialitate, condițiile de utilizare, evidența activităților de prelucrare, politica de gestionare a evidențelor, politica de securitate a informațiilor, rapoartele auditurilor externe privind protecția datelor, certificările internaționale recunoscute, precum seria ISO 27000).

96. Evaluarea de către operator a măsurii în care garanțiile sunt suficiente este o formă de evaluare a riscurilor, care va depinde în mare măsură de tipul de prelucrare atribuită persoanei împuternicite de operator și trebuie efectuată în fiecare caz individual, ținând seama de natura, domeniul de aplicare, contextul și de scopurile prelucrării, precum și de riscurile la adresa drepturilor și libertăților persoanelor fizice. În consecință, CEPD nu poate furniza o listă exhaustivă a documentelor sau a acțiunilor pe care persoana împuternicită de operator trebuie să le prezinte sau să le demonstreze în

[36] De exemplu, persoana împuternicită de operator trebuie să acorde asistență operatorului, atunci când este necesar și la cerere, în asigurarea respectării obligațiilor legate de evaluări ale impactului asupra protecției datelor (considerentul 95 din RGPD). Acest lucru trebuie să se reflecte în contractul dintre operator și persoana împuternicită de operator în temeiul articolul 28 alineatul (3) litera (f) din RGPD.
[37] Articolul 28 alineatul (1) și considerentul 81 din RGPD.

orice scenariu dat, deoarece acest fapt depinde în mare măsură de circumstanțele specifice ale prelucrării.

97. Următoarele elemente[38] trebuie avute în vedere de către operator pentru a evalua dacă garanțiile sunt suficiente: **cunoștințele de specialitate** ale persoanei împuternicite de operator (de exemplu expertiză tehnică cu privire la măsurile de securitate și încălcări ale securității datelor); **fiabilitatea** persoanei împuternicite de operator; **resursele** persoanei împuternicite de operator. De asemenea, reputația persoanei împuternicite de operator pe piață poate fi un factor relevant care trebuie luat în considerare de operatori.

98. În plus, aderarea la un cod de conduită aprobat sau la un mecanism de certificare poate fi utilizată drept element care poate demonstra garanții suficiente.[39] Prin urmare, persoanelor împuternicite de către operator li se recomandă să informeze operatorul cu privire la această circumstanță, precum și cu privire la orice modificare a condițiilor respective.

99. Obligația de a utiliza doar persoanele împuternicite de operator „care oferă garanții suficiente" prevăzută la articolul 28 alineatul (1) din RGPD este o obligație continuă. Aceasta nu se încheie în momentul în care operatorul și persoana împuternicită de către operator încheie un contract sau un alt act juridic. Mai degrabă, la intervale corespunzătoare, operatorul trebuie să verifice garanțiile persoanei împuternicite de operator, inclusiv prin audituri și inspecții, după caz.[40]

1.2 Forma contractului sau a altui act juridic

100. Orice prelucrare a datelor cu caracter personal de către o persoană împuternicită de operator trebuie să fie reglementată de un contract sau de un alt act juridic încheiat în temeiul dreptului UE sau al dreptului intern între operator și persoana împuternicită de operator, astfel cum se prevede la articolul 28 alineatul (3) din RGPD.

101. Un astfel de act juridic trebuie să fie încheiat **în scris, inclusiv în format electronic**.[41] Prin urmare, acordurile nescrise (indiferent de gradul lor de aprofundare sau de eficacitate) nu pot fi considerate suficiente pentru a îndeplini cerințele prevăzute la articolul 28 din RGPD. Pentru a evita orice dificultăți în demonstrarea faptului că contractul sau alt act juridic produce efecte, CEPD recomandă să se asigure că semnăturile necesare sunt incluse în actul juridic, în conformitate cu legislația aplicabilă (de exemplu, dreptul contractelor).

102. În plus, contractul sau un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern trebuie să fie **obligatoriu pentru persoana împuternicită de operator** în ceea ce privește operatorul, și anume trebuie să stabilească obligații pentru persoana împuternicită de operator care sunt obligatorii în temeiul dreptului UE sau al dreptului intern. De asemenea, acesta trebuie să stabilească obligațiile operatorului. În majoritatea cazurilor, va exista un contract, dar regulamentul se referă și la „alt act juridic", cum ar fi o lege națională (primară sau secundară) sau un alt instrument juridic. În cazul în care actul juridic nu include întregul conținut minim necesar, acesta trebuie completat cu un contract sau cu un alt act juridic care include elementele lipsă.

[38] Considerentul 81 din RGPD.
[39] Articolul 28 alineatul (5) și considerentul 81 din RGPD.
[40] A se vedea, de asemenea, articolul 28 alineatul (3) litera (h) din RGPD.
[41] a se vedea articolul 28 alineatul (9) din RGPD.

103. Întrucât regulamentul stabilește o obligație clară de încheiere a unui contract scris, în cazul în care nu este în vigoare niciun alt act juridic relevant, absența acestuia constituie o încălcare a RGPD.[42] Atât operatorul, cât și persoana împuternicită de operator au responsabilitatea de a se asigura că există un contract sau un alt act juridic care reglementează prelucrarea.[43] Sub rezerva dispozițiilor articolul 83 din RGPD, autoritatea de supraveghere competentă va putea să aplice o amendă administrativă atât operatorului, cât și persoanei împuternicite de operator, ținând seama de circumstanțele fiecărui caz în parte. Contractele care au fost încheiate înainte de data aplicării RGPD ar fi trebuit să fie actualizate în temeiul articolului 28 alineatul (3). Absența unei astfel de actualizări, pentru a alinia un contract existent anterior la cerințele RGPD, constituie o încălcare a articolul 28 alineatul (3).

Un contract scris în temeiul articolul 28 alineatul (3) din RGPD poate fi inserat într-un contract mai cuprinzător, cum ar fi un acord privind nivelul serviciilor. Pentru a facilita demonstrarea conformității cu RGPD, CEPD recomandă ca elementele contractului care vizează aplicarea dispozițiilor articolului 28 din RGPD să fie clar identificate ca atare într-un singur loc (de exemplu, într-o anexă).

104. Pentru a respecta obligația de a încheia un contract, **operatorul și persoana împuternicită de operator pot alege să își negocieze propriul contract**, inclusiv toate elementele obligatorii, **sau să se bazeze, integral sau parțial, pe clauze contractuale standard în legătură cu obligațiile prevăzute la articolul 28**.[44]

105. Un set de clauze contractuale standard (CCS) poate fi adoptat alternativ de Comisie[45] sau de o autoritate de supraveghere, în conformitate cu mecanismul pentru asigurarea coerenței.[46] Aceste

[42] Cu toate acestea, prezența (sau lipsa) unui acord scris nu are o influență decisivă pentru existența unei relații de tipul operator și persoana împuternicită de operator. În cazul în care există motive să se considere că acest contract nu corespunde realității în ceea ce privește controlul efectiv, pe baza unei analize factuale a circumstanțelor care caracterizează relația dintre părți și modalitatea de prelucrare a datelor cu caracter personal, acordul poate fi înlăturat. Pe de altă parte, în lipsa unui acord scris privind prelucrarea, s-ar putea considera că există totuși o relație de tipul operator și persoana împuternicită de operator. Acest fapt ar implica, cu toate acestea, o încălcare a articolul 28 alineatul (3) din RGPD. În plus, în anumite circumstanțe, lipsa unei definiții clare a relației dintre operator și persoana împuternicită de operator poate ridica problema lipsei temeiului juridic pe care trebuie să se bazeze fiecare prelucrare, de exemplu în ceea ce privește comunicarea datelor dintre operator și persoana împuternicită de operator.

[43] Articolul 28 alineatul (3) nu se aplică doar operatorilor. În situația în care doar persoana împuternicită de operator face obiectul domeniului de aplicare teritorială a RGPD, obligația ar trebui să fie direct aplicabilă doar persoanei împuternicite de operator; a se vedea, de asemenea, Orientările CEPD nr. 3/2018 privind domeniul de aplicare teritorial al RGPD, p. 12.

[44] Articolul 28 alineatul (6) din RGPD. CEPD reamintește că clauzele contractuale standard în sensul respectării articolul 28 din RGPD nu sunt aceleași cu clauzele contractuale standard menționate la articolul 46 alineatul (2). În timp ce primul articol prevede și clarifică modul în care dispozițiile alineatelor (3) și (4) ale articolului 28 vor fi îndeplinite, al doilea articol oferă garanții adecvate în cazul transferului de date cu caracter personal către o țară terță sau o organizație internațională în absența unei decizii privind caracterul adecvat al nivelului de protecție în temeiul articolul 45 alineatul (3).

[45] Articolul 28 alineatul (7) din RGPD. Articolul 28 alineatul (7) din RGPD. Articolul 28 alineatul (7) din RGPD. Articolul 28 alineatul (7) din RGPD. A se vedea Avizul comun nr. 1/2021 al CEPD-AEPD privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori: https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_ro.pdf

[46] Articolul 28 alineatul (8) din RGPD. Registrul deciziilor luate de autoritățile de supraveghere și de instanțe cu privire la aspecte tratate în cadrul mecanismului pentru asigurarea coerenței, inclusiv clauzele contractuale standard în sensul respectării articolului 28 din RGPD, poate fi accesat aici: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_ro.

clauze pot face parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul articolelor 42 sau 43.[47]

106. CEPD dorește să clarifice faptul că operatorii și persoanele împuternicite de operatori nu au nicio obligație de a încheia un contract pe baza CCS și nici nu este neapărat ca acesta să fie preferat la negocierea unui contract individual. Ambele opțiuni sunt viabile în sensul respectării legislației privind protecția datelor, în funcție de circumstanțele specifice, atât timp cât îndeplinesc cerințele prevăzute la articolul 28 alineatul (3).

107. În cazul în care părțile doresc să beneficieze de clauzele contractuale standard, clauzele de protecție a datelor din acordul lor trebuie să fie aceleași cu cele ale CCS. CCS vor lăsa adesea unele spații libere care trebuie completate sau opțiuni care urmează să fie selectate de către părți. De asemenea, astfel cum s-a menționat mai sus, CCS vor fi, în general, inserate într-un acord mai amplu care descrie obiectul contractului, condițiile financiare ale acestuia și alte clauze convenite: părțile vor putea adăuga clauze suplimentare (de exemplu, legea aplicabilă și jurisdicția) atât timp cât acestea nu contrazic, direct sau indirect, CCS[48] și nu subminează protecția conferită de RGPD și de dreptul UE sau dreptul intern în materie de protecție a datelor.

108. Contractele dintre operatori și persoanele împuternicite de operatori pot fi uneori redactate unilateral de una dintre părți. Identitatea părții sau a părților care redactează contractul poate depinde de mai mulți factori, inclusiv de poziția părților pe piață și de puterea contractuală a acestora, de expertiza lor tehnică, precum și de accesul la servicii juridice. De exemplu, unii furnizori de servicii au tendința să stabilească clauze și condiții standard, care includ acorduri privind prelucrarea datelor.

109. Un acord între operator și persoana împuternicită de operator trebuie să respecte cerințele articolul 28 din RGPD pentru a asigura că persoana împuternicită de operator prelucrează date cu caracter personal cu respectarea RGPD. Orice astfel de acord trebuie să țină seama de responsabilitățile specifice ale operatorilor și ale persoanelor împuternicite de operatori. Deși articolul 28 prevede o listă de puncte care trebuie abordate în orice contract care reglementează relația dintre operatori și persoanele împuternicite de operatori, acesta permite negocieri între părțile la astfel de contracte. În unele situații, un operator sau o persoană împuternicită de operator poate avea o putere de negociere mai redusă de personalizare a acordului privind protecția datelor. Invocarea clauzelor contractuale standard adoptate în temeiul articolul 28 [alineatele (7) și (8)] poate contribui la reechilibrarea pozițiilor de negociere și la asigurarea faptului că contractele respectă RGPD.

110. Deoarece contractul și condițiile sale comerciale detaliate sunt elaborate de furnizorul de servicii și nu de către operator, nu este problematic în sine și nu constituie, în sine, un temei suficient pentru a concluziona că furnizorul de servicii trebuie să fie considerat operator. De asemenea, dezechilibrul

[47] Articolul 28 alineatul (6) din RGPD.

[48] CEPD reamintește că același grad de flexibilitate este permis atunci când părțile aleg să utilizeze CCS ca garanție adecvată pentru transferurile către țări terțe în temeiul articolul 46 alineatul (2) litera (c) sau al articolul 46 alineatul (2) litera (d) din RGPD. Considerentul 109 din RGPD clarifică faptul că: „*Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu trebuie să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori trebuie să fie încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție*".

dintre puterea contractuală a unui mic operator de date în raport cu furnizorii mari de servicii nu trebuie considerat ca o justificare pentru ca operatorul să accepte clauze și condiții contractuale care nu respectă legislația privind protecția datelor și nici nu poate scuti operatorul de obligațiile acestuia în materie de protecție a datelor. Operatorul trebuie să evalueze condițiile și, în măsura în care le acceptă în mod liber și utilizează serviciul, a acceptat, de asemenea, întreaga responsabilitate pentru respectarea RGPD. Orice modificare propusă de o persoană împuternicită de operator a acordurilor privind prelucrarea datelor incluse în clauzele și condițiile standard trebuie să fie notificată direct operatorului și aprobată de acesta, ținând seama de marja de manevră de care dispune persoana împuternicită de operator în ceea ce privește elementele neesențiale ale mijloacelor (vezi punctele 40-41 de mai sus). Simpla publicare a acestor modificări pe site-ul web al persoanei împuternicite de operator nu înseamnă respectarea articolului 28.

1.3 Conținutul contractului sau al altui act juridic

111. Înainte de analizarea fiecăreia dintre cerințele detaliate prevăzute în RGPD cu privire la conținutul contractului sau al altui act juridic, sunt necesare câteva observații generale.

112. Deși elementele prevăzute la articolul 28 din regulament constituie conținutul de bază al acestuia, contractul trebuie să fie o modalitate prin care operatorul și persoana împuternicită de operator să clarifice suplimentar modul în care aceste elemente principale vor fi puse în aplicare cu instrucțiuni detaliate. Prin urmare, **acordul privind prelucrarea nu trebuie să reia dispozițiile RGPD pur și simplu**: mai curând, trebuie să includă informații mai specifice, concrete cu privire la modul în care se vor îndeplini cerințele și ce nivel de securitate este necesar pentru prelucrarea datelor cu caracter personal care fac obiectul acordului privind prelucrarea. Departe de a fi un exercițiu proforma, negocierea și stipularea contractului sunt o șansă de a preciza detalii cu privire la prelucrare.[49] Într-adevăr, „protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator [...] necesită o atribuire clară a responsabilităților” în temeiul RGPD.[50]

113. În același timp, contractul trebuie **să țină seama de *„sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate”***.[51] În general, contractul dintre părți trebuie să fie redactat în conformitate cu activitatea specifică de prelucrare a datelor. De exemplu, nu este necesar să se impună măsuri de protecție și proceduri deosebit de stricte unei persoane împuternicite de operator să efectueze o activitate de prelucrare, din care rezultă doar riscuri minore: deși fiecare persoană împuternicită de operator trebuie să respecte cerințele stipulate în regulament, măsurile și procedurile trebuie personalizate conform situației specifice. În orice caz, contractul trebuie să cuprindă toate elementele de la articolul 28 alineatul (3). În același timp, contractul trebuie să conțină anumite elemente care pot contribui la înțelegerea de către persoana împuternicită de operator a riscurilor la adresa drepturilor și libertăților persoanelor vizate care decurg din prelucrare: deoarece activitatea este efectuată în numele operatorului, adesea operatorul înțelege mai bine riscurile pe care le implică prelucrarea, întrucât operatorul este conștient de circumstanțele în care este introdusă prelucrarea.

[49] A se vedea, de asemenea, Avizul CEPD nr. 14/2019 privind proiectul de clauze contractuale standard înaintat de AS din Danemarca [articolul 28 alineatul (8) din RGPD], p. 5.
[50] Considerentul 79 din RGPD.
[51] Considerentul 81 din RGPD.

114. În ceea ce privește **conținutul necesar al contractului** sau al altui act juridic, CEPD interpretează articolul 28 alineatul (3) în sensul că acesta trebuie să stabilească:

- **obiectul** prelucrării (de exemplu, înregistrările de supraveghere video ale persoanelor care intră și ies dintr-un complex de înaltă securitate). Deși obiectul prelucrării este un concept larg, acesta trebuie formulat cu suficiente specificații, astfel încât să fie clar care este obiectul principal al prelucrării;
- **durata**[52] prelucrării: trebuie să se specifice perioada exactă de timp sau criteriile utilizate pentru determinarea acesteia; de exemplu, s-ar putea face referire la durata acordului privind prelucrarea;
- **natura** prelucrării: tipul de operațiuni efectuate ca parte a prelucrării (de exemplu: „filmare", „înregistrare", „arhivare de imagini",...) **și scopul** prelucrării (de exemplu: depistarea pătrunderii neautorizate). Această descriere trebuie să fie cât mai cuprinzătoare posibil, în funcție de activitatea specifică de prelucrare, pentru a permite părților externe (de exemplu, autorităților de supraveghere) să înțeleagă conținutul și riscurile prelucrării atribuite persoanei împuternicite de operator;
- **tipul de date cu caracter personal**: acest fapt trebuie specificat cât mai detaliat posibil (de exemplu: imagini video ale unor persoane care intră și ies din complex). Nu ar fi adecvat să se precizeze doar că este vorba despre „date cu caracter personal în temeiul articolul 4 punctul (1) din RGPD" sau despre „categorii speciale de date cu caracter personal în temeiul articolul 9". În cazul unor categorii speciale de date, contractul sau actul juridic trebuie să stipuleze cel puțin tipurile de date vizate, de exemplu „informații privind fișe medicale" sau „informații privind apartenența persoanei vizate la un sindicat";
- **categorii de persoane vizate**: și aici trebuie indicat într-un mod destul de specific (de exemplu: „vizitatori", „angajați", servicii de livrare etc.);
- **obligațiile și drepturile operatorului**: drepturile operatorului sunt abordate suplimentar în secțiunile următoare (de exemplu, în ceea ce privește dreptul operatorului de a efectua inspecții și audituri). În ceea ce privește obligațiile operatorului, printre exemple se include obligația operatorului de a furniza persoanei împuternicite de acesta datele menționate în contract, de a furniza și de a documenta orice instrucțiune care are impact asupra prelucrării datelor de către persoana împuternicită de operator, de a asigura, înainte și pe tot parcursul prelucrării, respectarea de către persoana împuternicită de operator a obligațiilor prevăzute în RGPD, de a supraveghea prelucrarea, inclusiv prin efectuarea de audituri și inspecții la persoana împuternicită de operator.

115. Deși RGPD enumeră elemente care trebuie întotdeauna incluse în acord, ar putea fi necesară includerea altor informații relevante, în funcție de context și de riscurile prelucrării, precum și de orice cerință relevantă suplimentară.

[52] Durata prelucrării nu este neapărat echivalentă cu durata acordului (pot exista obligații legale de păstrare a datelor pe durate mai lungi sau mai scurte).

1.3.1 Persoana împuternicită de operator trebuie să prelucreze datele doar pe baza unor instrucțiuni documentate din partea operatorului [articolul 28 alineatul (3) litera (a) din RGPD].

116. Necesitatea de a preciza această obligație decurge din faptul că persoana împuternicită de operator prelucrează datele în numele operatorului. Operatorii trebuie să pună la dispoziția persoanelor împuternicite de operatori instrucțiuni legate de fiecare activitate de prelucrare. Aceste instrucțiuni pot include prelucrarea permisă și inacceptabilă a datelor cu caracter personal, proceduri mai detaliate, modalități de securizare a datelor etc. Persoana împuternicită de operator nu trebuie să depășească instrucțiunile operatorului. Cu toate acestea, este posibil ca persoana împuternicită de operator să sugereze elemente care, dacă sunt acceptate de operator, devin parte a instrucțiunilor date.

117. Atunci când o persoană împuternicită de operator prelucrează date nerespectând sau depășind instrucțiunile operatorului, iar acest fapt echivalează cu o decizie de stabilire a scopurilor și mijloacelor prelucrării, persoana împuternicită de operator își va încălca obligațiile și va fi chiar considerată operator în ceea ce privește această prelucrare în conformitate cu articolul 28 alineatul (10) (vezi subsecțiunea 1.5 de mai jos[53]).

118. Instrucțiunile emise de operator trebuie să fie **documentate**. În acest scop, se recomandă includerea unei proceduri și a unui model pentru furnizarea de instrucțiuni mai amănunțite într-o anexă la contract sau la alt act juridic. Alternativ, instrucțiunile pot fi furnizate sub orice formă scrisă (de exemplu, e-mail), precum și în orice altă formă documentată, atât timp cât este posibil să se țină evidențe ale acestor instrucțiuni. În orice caz, pentru a evita orice dificultăți în a demonstra că instrucțiunile operatorului au fost documentate în mod corespunzător, CEPD recomandă păstrarea acestor instrucțiuni împreună cu contractul sau cu alte acte juridice.

119. Obligația persoanei împuternicite de operator de a se abține de la orice activitate de prelucrare care nu se bazează pe instrucțiunile operatorului se aplică, de asemenea, **transferurilor** de date cu caracter personal către o țară terță sau către o organizație internațională. Contractul trebuie să precizeze cerințele pentru transferurile către țări terțe sau către organizații internaționale, ținând seama de dispozițiile capitolului V din RGPD.

120. CEPD recomandă ca operatorul să acorde atenția cuvenită acestui punct specific, în special atunci când persoana împuternicită de operator va delega unele activități de prelucrare altor persoane împuternicite de operator și atunci când persoana împuternicită de operator are diviziuni sau unități situate în țări terțe. În cazul în care instrucțiunile operatorului nu permit transferurile sau divulgările către țări terțe, persoanei împuternicite de operator nu i se va permite să atribuie prelucrarea unui subcontractant dintr-o țară terță și nici să obțină prelucrarea datelor în una dintre diviziile sale din afara UE.

121. O persoană împuternicită de operator poate prelucra date altfel decât pe baza unor instrucțiuni documentate ale operatorului atunci când **persoana împuternicită de operator este obligată să prelucreze și/sau să transfere date cu caracter personal în temeiul dreptului UE sau al dreptului intern care se aplică persoanei împuternicite de operator**. Această dispoziție evidențiază în plus importanța negocierii și a redactării cu atenție a acordurilor privind prelucrarea datelor, deoarece, de exemplu, ar putea fi necesar ca oricare dintre părți să solicite consultanță juridică cu privire la existența unei astfel de cerințe legale. Trebuie procedat astfel în timp util, deoarece persoana împuternicită de

[53] A se vedea partea II subsecțiunea 1.5 („Persoana împuternicită de operator stabilește scopurile și mijloacele de prelucrare”).

operator are obligația de a informa operatorul cu privire la această cerință înainte de a începe prelucrarea. Doar în cazul în care aceeași lege (a UE sau a unui stat membru) interzice persoanei împuternicite de operator să informeze operatorul din „motive importante de interes public", nu există o astfel de obligație de informare. În orice caz, orice transfer sau divulgare poate avea loc numai dacă este autorizat(ă) de dreptul Uniunii, inclusiv în conformitate cu articolul 48 din RGPD.

1.3.2 Persoana împuternicită de operator trebuie să se asigure că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate [articolul 28 alineatul (3) litera (b) din RGPD].

122. Contractul trebuie să precizeze că persoana împuternicită de operator trebuie să se asigure că orice persoană căreia i se permite să prelucreze datele cu caracter personal se angajează să respecte confidențialitatea. Acest lucru se poate întâmpla fie prin intermediul unui acord contractual specific, fie ca urmare a obligațiilor statutare deja existente.

123. Conceptul cuprinzător de „persoane autorizate să prelucreze datele cu caracter personal" include angajații și lucrătorii temporari. În general, persoana împuternicită de operator trebuie să pună datele cu caracter personal doar la dispoziția angajaților care au efectiv nevoie de acestea pentru a efectua sarcinile pentru care persoana împuternicită de operator a fost angajată de operator.

124. Angajamentul sau obligația de confidențialitate trebuie să fie „adecvată", adică trebuie să interzică efectiv persoanei autorizate să divulge orice informații confidențiale fără autorizare și trebuie să fie suficient de cuprinzătoare pentru a cuprinde toate datele cu caracter personal prelucrate în numele operatorului, precum și condițiile în care sunt prelucrate datele cu caracter personal.

1.3.3 Persoana împuternicită de operator trebuie să ia toate măsurile necesare în temeiul articolul 32 [articolul 28 alineatul (3) litera (c) din RGPD].

125. Potrivit articolului 32, operatorul și persoana împuternicită de operator trebuie să pună în aplicare măsuri tehnice și organizatorice de securitate adecvate. Deși această obligație este deja impusă direct persoanei împuternicite de operator ale cărei operațiuni de prelucrare țin de domeniul de aplicare al RGPD, obligația de a lua toate măsurile necesare în temeiul articolului 32 trebuie totuși să se reflecte în contractul privind activitățile de prelucrare atribuite de operator.

126. Astfel cum s-a indicat anterior, contractul de prelucrare nu trebuie să reia pur și simplu dispozițiile din RGPD. Contractul trebuie să includă sau să facă trimitere la informații privind măsurile de securitate care trebuie adoptate**, obligația persoanei împuternicite de operator să obțină aprobarea operatorului înainte de a efectua modificări**, precum și la o revizuire periodică a măsurilor de securitate, astfel încât să se asigure caracterul adecvat al acestora în ceea ce privește riscurile, care pot evolua în timp. Gradul de detaliere a informațiilor privind măsurile de securitate care trebuie incluse în contract trebuie să fie suficient pentru a permite operatorului să evalueze caracterul adecvat al măsurilor în temeiul articolul 32 alineatul (1) din RGPD. În plus, descrierea este, de asemenea, necesară pentru a permite operatorului să își respecte obligația de responsabilitate în temeiul articolului 5 alineatul (2) și al articolului 24 din RGPD în ceea ce privește măsurile de securitate impuse persoanei împuternicite de operator. O obligație corespunzătoare a persoanei împuternicite de operator de a ajuta operatorul și de a pune la dispoziție toate informațiile necesare pentru a demonstra respectarea obligațiilor poate fi dedusă din articolul 28 alineatul (3) literele (f) și (h) din RGPD.

127. Nivelul instrucțiunilor furnizate de operator persoanei împuternicite de operator cu privire la măsurile care trebuie puse în aplicare va depinde de circumstanțele specifice. În unele cazuri, operatorul poate

furniza o descriere clară și detaliată a măsurilor de securitate care trebuie puse în aplicare. În alte cazuri, operatorul poate descrie obiectivele de securitate minime care trebuie îndeplinite, solicitând în același timp persoanei împuternicite de operator să propună punerea în aplicare a unor măsuri de securitate specifice. În orice caz, operatorul trebuie să furnizeze persoanei împuternicite de operator o descriere a activităților de prelucrare și a obiectivelor de securitate (pe baza evaluării riscurilor efectuate de operator), precum și să aprobe măsurile propuse de persoana împuternicită de operator. Acest aspect ar putea fi inclus într-o anexă la contract. Operatorul își exercită competența decizională cu privire la principalele caracteristici ale măsurilor de securitate, fie prin enumerarea explicită a măsurilor, fie prin aprobarea celor propuse de persoana împuternicită de operator.

1.3.4 Persoana împuternicită de operator trebuie să respecte condițiile menționate la articolul 28 alineatele (2) și (4) pentru angajarea unei alte persoane împuternicite de operator [articolul 28 alineatul (3) litera (d) din RGPD].

128. Acordul trebuie să precizeze că persoana împuternicită de operator nu poate angaja o altă persoană împuternicită de operator fără autorizația scrisă prealabilă a operatorului, precum și dacă această autorizație trebuie să fie specifică sau generală. În cazul unei autorizații generale, persoana împuternicită de operator trebuie să informeze operatorul cu privire la orice modificare a subcontractanților în temeiul unei autorizații scrise și să ofere operatorului posibilitatea de a formula obiecții. Se recomandă ca în contract să se stabilească procesul în acest sens. Trebuie remarcat faptul că obligația persoanei împuternicite de operator de a-l informa pe acesta cu privire la orice schimbare a subcontractanților implică faptul că persoana împuternicită de operator indică sau semnalează în mod activ astfel de modificări către operator.[54] De asemenea, în cazul în care este necesară o autorizație specifică, contractul trebuie să stabilească procesul de obținere a unei astfel de autorizații.

129. În cazul în care persoana împuternicită de operator angajează o altă persoană împuternicită de operator, trebuie să se încheie un contract între ele, care impune aceleași obligații în materie de protecție a datelor ca cele impuse persoanei împuternicite de operator inițiale sau aceste obligații trebuie impuse printr-un alt act juridic în temeiul dreptului Uniunii sau al dreptului intern (vezi, punctul de mai jos 160). Aceasta include obligația în temeiul articolului 28 alineatul (3) litera (h) de a permite desfășurarea auditurilor realizate de operator sau de un alt auditor mandatat și de a contribui la acestea.[55] Persoana împuternicită de operator este răspunzătoare față de operator pentru respectarea de către celelalte persoane împuternicite de operator a obligațiilor în materie de protecție a datelor (pentru detalii suplimentare privind conținutul recomandat al acordului, vezi subsecțiunea 1.6 de mai jos[56]).

1.3.5 Persoana împuternicită de operator trebuie să acorde asistență operatorului la îndeplinirea obligației acestuia de a răspunde cererilor de exercitare a drepturilor persoanei vizate [articolul 28 alineatul (3) litera (e) din RGPD].

130. Deși asigură că cererile persoanelor vizate sunt prelucrate de operator, contractul trebuie să stipuleze că persoana împuternicită de operator are obligația de a acorda asistență „prin măsuri tehnice și

[54] În schimb, în acest sens, de exemplu, nu este suficient ca persoana împuternicită de operator să-i furnizeze operatorului doar un acces generalizat la o listă a subcontractanților, care ar putea fi actualizată periodic, fără a indica operatorului fiecare subcontractant nou avut în vedere. Cu alte cuvinte, persoana împuternicită de operator trebuie să informeze în mod activ operatorul cu privire la orice modificare a listei (și anume, în special cu privire la fiecare subcontractant nou avut în vedere).

[55] A se vedea, de asemenea, Avizul nr. 14/2019 al CEPD privind proiectul de clauze contractuale standard înaintat de AS din Danemarca [articolul 28 alineatul (8) din RGPD], adoptat la 9 iulie 2019, punctul 44.

[56] A se vedea partea II subsecțiunea 1.6 („Subcontractanți”).

organizatorice adecvate, în măsura în care acest lucru este posibil". Natura acestei asistențe poate varia foarte mult, „ținând seama de natura prelucrării" și în funcție de tipul de activitate încredințată persoanei împuternicite de operator. Detaliile privind asistența care urmează să fie acordată de către persoana împuternicită de operator trebuie incluse în contract sau într-o anexă la acesta.

131. Deși asistența poate consta pur și simplu în transmiterea promptă a oricărei cereri primite și/sau în a permite operatorului să extragă și să gestioneze în mod direct datele cu caracter personal relevante, în anumite circumstanțe, persoanei împuternicite de operator i se vor atribui sarcini tehnice mai specifice, în special atunci când este în măsură să extragă și să gestioneze datele cu caracter personal.

132. Este esențial să se rețină faptul că, deși gestionarea practică a cererilor individuale poate fi externalizată către persoana împuternicită de operator, operatorul este responsabil de răspunsul la aceste cereri. Prin urmare, operatorul trebuie să evalueze dacă cererile persoanelor vizate sunt admisibile și/sau dacă cerințele stabilite prin RGPD sunt îndeplinite, fie pentru fiecare caz în parte, fie prin instrucțiuni clare furnizate persoanei împuternicite de operator în contract înainte de începerea prelucrării. De asemenea, termenele stabilite în capitolul III nu pot fi prelungite de operator pe baza faptului că informațiile necesare trebuie furnizate de persoana împuternicită de operator.

1.3.6 Persoana împuternicită de operator trebuie să acorde asistență operatorului pentru ca acesta să asigure respectarea obligațiilor prevăzute la articolele 32-36 [articolul 28 alineatul (3) litera (f) din RGPD].

133. Contractul trebuie să evite pur și simplu reluarea acestor obligații de asistență: **acordul trebuie să conțină detalii cu privire la modul în care i se solicită persoanei împuternicite de operator să-l ajute pe acesta să îndeplinească obligațiile enumerate**. De exemplu, pot fi adăugate proceduri și formulare la anexele la acord, permițându-i persoanei împuternicite de operator să-i furnizeze operatorului toate informațiile necesare.

134. Tipul și gradul de asistență care urmează să fie acordată de persoana împuternicită de operator pot varia foarte mult *„ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator".* Operatorul trebuie să informeze în mod adecvat persoana împuternicită de operator cu privire la riscul pe care îl implică prelucrarea și cu privire la orice altă circumstanță care poate ajuta persoana împuternicită de operator să își îndeplinească obligațiile.

135. În ceea ce privește obligațiile specifice, persoana împuternicită de operator are, în primul rând, obligația de a acorda asistență operatorul în îndeplinirea obligației de a adopta măsuri tehnice și organizatorice adecvate pentru a asigura securitatea prelucrării.[57] Deși acest lucru se poate suprapune, într-o anumită măsură, cu cerința ca persoana împuternicită de operator să adopte măsuri de securitate adecvate, în cazul în care operațiunile de prelucrare ale persoanei împuternicite de operator intră în domeniul de aplicare al RGPD, acestea rămân două obligații distincte, deoarece una se referă la propriile măsuri ale persoanei împuternicite de operator, iar cealaltă se referă la cele ale operatorului.

136. În al doilea rând, persoana împuternicită de operator trebuie să acorde asistență operatorului la îndeplinirea obligației de notificare a încălcării securității datelor cu caracter personal către autoritatea de supraveghere și către persoanele vizate. Persoana împuternicită de operator trebuie să notifice operatorul ori de câte ori descoperă o încălcare a securității datelor cu caracter personal care afectează echipamentele/sistemele IT ale persoanei împuternicite de operator sau ale subcontractantului și să ajute operatorul să obțină informațiile care trebuie menționate în raportul către autoritatea de

[57] Articolul 32 din RGPD.

supraveghere.[58] RGPD prevede că operatorul trebuie să notifice o încălcare fără întârzieri nejustificate, pentru a reduce la minimum prejudiciul suferit de persoanele fizice și pentru a crește la maximum posibilitatea de a remedia încălcarea într-un mod adecvat. Astfel, notificarea operatorului de către persoana împuternicită de operator trebuie să aibă loc, de asemenea, fără întârzieri nejustificate.[59] În funcție de caracteristicile specifice ale prelucrării atribuite persoanei împuternicite de operator, ar putea fi oportun ca părțile să includă în contract un interval de timp specific (de exemplu, un număr de ore) în care persoana împuternicită de operator trebuie să notifice operatorul, precum și punctul de contact pentru astfel de notificări, modalitatea și conținutul minim așteptat de operator.[60] Acordul contractual dintre operator și persoana împuternicită de operator poate include, de asemenea, autorizația și cerința ca persoana împuternicită de operator să notifice direct o încălcare a securității datelor în conformitate cu articolele 33 și 34, răspunderea juridică pentru notificare revenindu-i însă operatorului.[61] În cazul în care persoana împuternicită de operator notifică o încălcare a securității datelor direct autorității de supraveghere și informează persoanele vizate în conformitate cu articolele 33 și 34, persoana împuternicită de operator trebuie, de asemenea, să informeze operatorul și să-i furnizeze copii ale notificării și ale informațiilor adresate persoanelor vizate.

137. În plus, persoana împuternicită de operator trebuie, de asemenea, să acorde asistență operatorului la efectuarea evaluărilor impactului asupra protecției datelor atunci când este necesar și la consultarea autorității de supraveghere atunci când se constată că există un risc mare care nu poate fi diminuat.

138. Obligația de asistență nu constă într-un transfer de responsabilitate, întrucât aceste obligații îi revin operatorului. De exemplu, deși evaluarea impactului asupra protecției datelor poate fi efectuată în practică de către o persoană împuternicită de operator, operatorul rămâne răspunzător pentru obligația de a efectua evaluarea[62] iar persoana împuternicită de operator este obligată doar să acorde asistență operatorului „dacă este necesar și la cerere.”[63] Ca urmare, operatorul este cel care trebuie să aibă inițiativa de a realiza evaluarea impactului asupra protecției datelor și nu persoana împuternicită de operator.

1.3.7 La încetarea activităților de prelucrare, persoana împuternicită de operator trebuie, la alegerea operatorului, să șteargă sau să returneze operatorului toate datele cu caracter personal și să șteargă copiile existente [articolul 28 alineatul (3) litera (g) din RGPD].

139. Clauzele contractuale au scopul să asigure faptul că datele cu caracter personal fac obiectul unei protecții adecvate după încheierea „furnizării serviciilor legate de prelucrare”: prin urmare, operatorul trebuie să decidă ce trebuie să facă persoana împuternicită de operator cu privire la datele cu caracter personal.

[58] Articolul 33 alineatul (3) din RGPD.
[59] Pentru mai multe informații, a se vedea Orientările privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP250rev.01, 6 februarie 2018, p. 13-14.
[60] A se vedea, de asemenea, Avizul nr. 14/2019 al CEPD privind proiectul de clauze contractuale standard înaintat de AS din Danemarca [articolul 28 alineatul (8) din RGPD], adoptat la 9 iulie 2019, punctul 40.
[61] Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP250rev.01, 6 februarie 2018, p. 14.
[62] Grupul de lucru Articolul 29 privind protecția datelor, Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679, WP 248 rev.01, p. 14.
[63] Considerentul 95 din RGPD.

140. Operatorul poate decide la început dacă datele cu caracter personal trebuie șterse sau returnate precizând acest aspect în contract, printr-o comunicare scrisă transmisă în timp util persoanei împuternicite de operator. Contractul sau alt act juridic trebuie să reflecte posibilitatea operatorului de date de a schimba alegerea făcută înainte de încetarea furnizării serviciilor legate de prelucrare. Contractul trebuie să precizeze procesul de furnizare a acestor instrucțiuni.

141. În cazul în care operatorul alege ca datele cu caracter personal să fie șterse, persoana împuternicită de operator trebuie să se asigure că ștergerea se efectuează în condiții de siguranță, inclusiv în sensul respectării articolului 32 din RGPD. Persoana împuternicită de operator trebuie să confirme operatorului că ștergerea a fost finalizată într-un termen convenit și într-un mod convenit.

142. Persoana împuternicită de operator trebuie să șteargă toate copiile existente ale datelor, cu excepția cazului în care dreptul UE sau dreptul intern prevăd o stocare suplimentară. În cazul în care persoana împuternicită de operator sau operatorul are cunoștință de orice astfel de cerință legală, aceasta (acesta) trebuie să informeze cealaltă parte cât mai curând posibil.

1.3.8 Persoana împuternicită de operator trebuie să pună la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la articolul 28 și să permită și să contribuie la audituri, inclusiv inspecții, desfășurate de operator sau de un alt auditor mandatat de operator [articolul 28 alineatul (3) litera (h) din RGPD].

143. Contractul trebuie să conțină detalii cu privire la frecvența și circulația informațiilor dintre persoana împuternicită de operator și operator, astfel încât operatorul să fie pe deplin informat cu privire la detaliile prelucrării care sunt relevante pentru a demonstra respectarea obligațiilor prevăzute la articolul 28 din RGPD. De exemplu, părțile relevante din evidențele activităților de prelucrare ale persoanei împuternicite de operator pot fi puse la dispoziția operatorului. Persoana împuternicită de operator trebuie să furnizeze toate informațiile cu privire la modul în care se va desfășura activitatea de prelucrare în numele operatorului. Aceste informații trebuie să includă informații privind funcționarea sistemelor utilizate, măsuri de securitate, modul în care sunt îndeplinite cerințele privind păstrarea datelor, localizarea datelor, transferurile de date, persoanele care au acces la date și care sunt destinatarii datelor, subcontractanții utilizați etc.

144. În contract trebuie prevăzute, de asemenea, detalii suplimentare cu privire la competența de a efectua și la obligația de a contribui la inspecții și audituri desfășurate de operator sau de un alt auditor mandatat de operator.

RGPD precizează că inspecțiile și auditurile sunt desfășurate de operator sau de o parte terță mandatată de acesta. Scopul unui astfel de audit este să asigure că operatorul deține toate informațiile privind activitatea de prelucrare efectuată în numele său și garanțiile furnizate de persoana împuternicită de operator. Persoana împuternicită de operator poate sugera alegerea unui anumit auditor, dar decizia finală trebuie lăsată la aprecierea operatorului, în conformitate cu articolul 28 alineatul (3) litera (h) din RGPD.[64] În plus, chiar și în cazul în care inspecția este efectuată de un auditor propus de persoana împuternicită de operator, operatorul își păstrează dreptul de a contesta domeniul de aplicare, metodologia și rezultatele inspecției.[65]

[64] A se vedea Avizul comun nr. 1/2021 al CEPD — AEPD privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori, punctul 43.
[65] A se vedea Avizul nr. 14/2019 privind proiectul de clauze contractuale standard înaintat de AS din Danemarca [articolul 28 alineatul (8) din RGPD], punctul 43.

Părțile trebuie să coopereze cu bună credință și să evalueze dacă și când este necesar să se efectueze audituri la sediul persoanei împuternicite de operator, precum și ce tip de audit sau inspecție (la distanță/la fața locului/în alt mod, pentru a colecta informațiile necesare) ar fi necesar(ă) și adecvat(ă) în cazul respectiv, ținând seama, de asemenea, de preocupările legate de securitate; decizia finală în acest sens trebuie luată de operator. În urma rezultatelor inspecției, operatorul trebuie să fie în măsură să solicite persoanei împuternicite de operator să ia măsuri ulterioare, de exemplu pentru a remedia deficiențele și lacunele identificate.[66] De asemenea, trebuie stabilite proceduri specifice privind inspecția desfășurată de persoana împuternicită de operator și de operator la sediul subcontractanților (vezi subsecțiunea 1.6 de mai jos[67]).

145. Chestiunea privind împărțirea cheltuielilor între operator și persoana împuternicită de operator în ceea ce privește auditurile nu este reglementată în RGPD și face obiectul unor considerații de ordin comercial. Cu toate acestea, potrivit articolului 28 alineatul (3) litera (h), contractul trebuie să includă obligația persoanei împuternicite de operator de a pune la dispoziția acestuia toate informațiile necesare și obligația de a permite și de a contribui la audituri, inclusiv inspecții, desfășurate de operator sau alt auditor mandatat de operator. În practică, aceasta înseamnă că părțile nu trebuie să introducă în contract clauze care prevăd plata unor cheltuieli sau onorarii care ar fi în mod clar disproporționate sau excesive, având astfel un efect de descurajare asupra uneia dintre părți. Astfel de clauze ar implica într-adevăr faptul că drepturile și obligațiile prevăzute la articolul 28 alineatul (3) litera (h) nu ar fi niciodată exercitate în practică și ar deveni pur teoretice chiar dacă acestea sunt parte integrantă din garanțiile privind protecția datelor prevăzute la articolul 28 din RGPD.

1.4 Instrucțiuni care încalcă legislația privind protecția datelor

146. În conformitate cu articolul 28 alineatul (3), persoana împuternicită de operator trebuie să informeze imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă RGPD sau alte dispoziții ale Uniunii sau ale statelor membre privind protecția datelor.

147. Într-adevăr, persoana împuternicită de operator are obligația de a respecta instrucțiunile operatorului, dar are și o obligație generală de a respecta legea. O instrucțiune care încalcă legislația privind protecția datelor pare să creeze un conflict între cele două obligații menționate anterior.

148. După ce este informat că una dintre instrucțiunile sale poate încălca legislația privind protecția datelor, operatorul va trebui să evalueze situația și să stabilească dacă instrucțiunea încalcă efectiv legislația privind protecția datelor.

149. CEPD recomandă părților să negocieze și să convină prin contract asupra consecințelor notificării unei instrucțiuni care încalcă legislația, trimise de persoana împuternicită de operator, și în cazul lipsei de acțiune din partea operatorului în acest context. Un exemplu ar fi introducerea unei clauze privind rezilierea contractului în cazul în care operatorul continuă să ofere o instrucțiune ilegală. Un alt exemplu ar fi o clauză privind posibilitatea ca persoana împuternicită de operator să suspende punerea în aplicare a instrucțiunii afectate până când operatorul își confirmă, modifică sau retrage instrucțiunea[68].

[66] A se vedea Avizul nr. 14/2019 privind proiectul de clauze contractuale standard înaintat de AS din Danemarca [articolul 28 alineatul (8) din RGPD], punctul 43.
[67] A se vedea partea II subsecțiunea 1.6 („Subcontractanți”).
[68] A se vedea Avizul comun nr. 1/2021 al CEPD — AEPD privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori, punctul 39.

1.5 Persoana împuternicită de operator stabilește scopurile și mijloacele de prelucrare

150. În cazul în care persoana împuternicită de operator încalcă regulamentul prin stabilirea scopurilor și mijloacelor de prelucrare, aceasta este considerată un operator în ceea ce privește prelucrarea respectivă [articolul 28 alineatul (10) din RGPD].

1.6 Subcontractanți

151. Activitățile de prelucrare a datelor sunt adesea efectuate de un număr mare de actori, iar lanțurile de subcontractare devin din ce în ce mai complexe. RGPD introduce obligații specifice care se declanșează atunci când un subcontractant intenționează să angajeze un alt actor, adăugând astfel o altă verigă în lanț, prin atribuirea de activități care necesită prelucrarea datelor cu caracter personal. Analiza dacă furnizorul de servicii acționează ca subcontractant trebuie efectuată în conformitate cu cele descrise anterior în legătură cu conceptul de persoană împuternicită de operator (vezi punctul anterior 83).

152. Deși lanțul poate fi destul de lung, operatorul își păstrează rolul central în stabilirea scopului și mijloacelor de prelucrare. Articolul 28 alineatul (2) din RGPD prevede că persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului (inclusiv în format electronic). În cazul unei autorizații generale scrise, persoana împuternicită de operator trebuie să informeze operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări. În ambele cazuri, persoana împuternicită de operator trebuie să obțină autorizația scrisă a operatorului înainte ca orice prelucrare a datelor cu caracter personal să fie atribuită subcontractantului. Pentru a desfășura evaluarea și pentru a lua decizia dacă să autorizeze subcontractarea, operatorului de date va trebui să primească o listă a subcontractanților preconizați (care include în cazul fiecăruia: sediile acestora, ce acțiuni vor întreprinde și dovada garanțiilor care au fost puse în aplicare) de la persoana împuternicită de operator.[69]

153. Autorizația scrisă prealabilă poate fi specifică, și anume, se poate referi la un subcontractant specific pentru o activitate specifică de prelucrare și la un moment specific, sau generală. Acest fapt trebuie precizat în contract sau într-un alt act juridic care reglementează prelucrarea.

154. În cazurile în care operatorul decide să accepte anumiți subcontractanți în momentul semnării contractului, trebuie inclusă în contract sau într-o anexă la acesta o listă a subcontractanților aprobați. Lista trebuie ulterior actualizată, în conformitate cu autorizația generală sau specifică acordată de operator.

155. În cazul în care operatorul alege să acorde o **autorizație specifică**, trebuie să precizeze în scris la ce subcontractant și la ce activitate de prelucrare se referă. Orice modificare ulterioară va trebui să fie autorizată ulterior de către operator înainte de a fi pusă în aplicare. În cazul în care nu se răspunde la cererea de autorizare specifică a persoanei împuternicite de operator în termenul stabilit, aceasta trebuie să fie considerată respinsă. Operatorul trebuie să ia decizia de a acorda sau de a refuza autorizația, ținând seama de obligația de a utiliza numai persoane împuternicite de operator care oferă „garanții suficiente” (vezi subsecțiunea 1.1 de mai sus[70]).

[69] Aceste informații sunt necesare pentru ca operatorul să poată respecta principiul responsabilității prevăzut la articolul 24 și dispozițiile de la articolul 28 alineatul (1), de la articolul 32 și de la capitolul V din RGPD.
[70] A se vedea partea II — subsecțiunea 1.1 („Alegerea persoanei împuternicite de operator”).

156. Alternativ, operatorul poate acorda o **autorizație generală** pentru utilizarea subcontractanților (în contract, inclusiv o listă cu astfel de subcontractanți într-o anexă la acesta), care trebuie completată cu criterii care să orienteze alegerea persoanei împuternicite de operator (de exemplu, garanții în ceea ce privește măsurile tehnice și organizatorice, cunoștințele de specialitate, fiabilitatea și resursele).[71] În acest scenariu, persoana împuternicită de operator trebuie să informeze operatorul în timp util cu privire la orice adăugare sau înlocuire preconizată a subcontractantului (subcontractanților), astfel încât să ofere operatorului posibilitatea de a formula obiecții.

157. Prin urmare, principala diferență dintre autorizația specifică și scenariile de autorizare generală constă în modul în care este interpretată lipsa de răspuns din partea operatorului: în cazul autorizației generale, dacă operatorul nu formulează obiecții în termenul stabilit, acest fapt poate fi interpretat ca autorizare.

158. În ambele scenarii, contractul trebuie să includă detalii cu privire la termenul pentru aprobarea sau formularea de obiecții din partea operatorului și cu privire la modul în care părțile intenționează să comunice cu privire la acest subiect (de exemplu, modele). Acest termen trebuie să fie rezonabil, având în vedere tipul de prelucrare, complexitatea activităților atribuite persoanei împuternicite de operator (și subcontractanților) și relația dintre părți. În plus, contractul trebuie să includă detalii cu privire la etapele practice ca urmare a formulării de obiecții de către operator (de exemplu, prin specificarea termenului în care operatorul și persoana împuternicită de operator trebuie să decidă dacă încetează prelucrarea).

159. Indiferent de criteriile sugerate de operator pentru a alege furnizorii, persoana împuternicită de operator rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor subcontractanților [articolul 28 alineatul (4) din RGPD]. Prin urmare, persoana împuternicită de operator trebuie să se asigure că propune subcontractanți care furnizează garanții suficiente.

160. În plus, atunci când o persoană împuternicită de operator intenționează să angajeze un subcontractant (autorizat), aceasta trebuie să încheie un contract cu subcontractantul, care să impună aceleași obligații ca cele impuse primei persoane împuternicite de operator de către operator sau obligațiile trebuie să fie impuse prin alt act juridic în temeiul dreptului UE sau dreptului intern. Întregul lanț de activități de prelucrare trebuie să fie reglementat prin acorduri scrise. Impunerea „acelorași" obligații trebuie interpretată într-o manieră mai mult funcțională decât formală: nu este necesar ca în contract să se includă exact aceleași cuvinte ca cele utilizate în contractul dintre operator și persoana împuternicită de operator, ci trebuie să se asigure că obligațiile sunt aceleași în ceea ce privește substanța. Aceasta înseamnă, de asemenea, că, în cazul în care persoana împuternicită de operator atribuie subcontractantului o parte specifică de prelucrare, căreia nu i se pot aplica unele obligații, aceste obligații nu trebuie incluse „în mod implicit" în contractul cu subcontractantul, deoarece acest fapt ar genera doar incertitudine. De exemplu, în legătură cu asistența acordată pentru obligațiile legate de încălcarea securității datelor, un subcontractant ar putea notifica direct operatorului o încălcare a securității datelor dacă cele trei părți sunt de acord. Cu toate acestea, în cazul unei astfel de notificări directe, persoana împuternicită de operator trebuie să fie informată și să obțină o copie a notificării.

[71] Această obligație a operatorului decurge din principiul responsabilității prevăzut la articolul 24 și din obligația de a respecta dispozițiile de la articolul 28 alineatul (1), de la articolul 32 și de la capitolul V din RGPD.

2 CONSECINȚELE CONTROLULUI COMUN

2.1 Stabilirea în mod transparent a responsabilităților fiecărui operator asociat în ceea ce privește respectarea obligațiilor în temeiul RGPD

161. Articolul 26 alineatul (1) din RGPD prevede că operatorii asociați stabilesc și convin în mod transparent asupra responsabilităților fiecăruia în ceea ce privește respectarea obligațiilor în temeiul regulamentului.

162. Prin urmare, operatorii asociați trebuie să stabilească „ce face fiecare", stabilind între ei cine va trebui să îndeplinească sarcinile pentru a se asigura că prelucrarea respectă obligațiile aplicabile în temeiul RGPD în ceea ce privește prelucrarea comună vizată. Cu alte cuvinte, trebuie să efectueze o distribuire a responsabilităților în scopul respectării obligațiilor, astfel cum rezultă din utilizarea termenului „*fiecăruia*" de la articolul 26 alineatul (1). Acest lucru nu exclude posibilitatea ca dreptul Uniunii sau dreptul intern să prevadă deja anumite responsabilități pentru fiecare operator asociat. În acest caz, acordul privind operatorul asociat trebuie să abordeze, de asemenea, orice responsabilități suplimentare necesare pentru a asigura conformitatea cu RGPD care nu sunt abordate în dispozițiile legale.[72]

163. Obiectivul acestor norme este de a garanta că, în cazul în care sunt implicați mai mulți actori, în special în medii complexe de prelucrare a datelor, responsabilitatea pentru respectarea normelor de protecție a datelor este atribuită fără echivoc pentru a se evita reducerea protecției datelor cu caracter personal sau faptul că un conflict negativ de competențe ar putea duce la lacune prin care unele obligații să nu fie respectate de către niciuna părțile implicate în prelucrare. În acest context, trebuie clarificat faptul că toate responsabilitățile trebuie să fie atribuite în funcție de circumstanțele factuale pentru a se ajunge la un acord operativ. CEPD observă că există situații în care influența unui operator asociat și influența factuală a acestuia complică obținerea unui acord. Totuși, aceste circumstanțe nu exclud controlul comun și nu pot contribui la scutirea niciunei părți de obligațiile care îi revin în temeiul RGPD.

164. Mai precis, articolul 26 alineatul (1) precizează că stabilirea responsabilităților fiecăruia (și anume sarcinile) în scopul respectării obligațiilor în temeiul RGPD trebuie să fie efectuată de operatorii asociați „*în special"* în ceea ce privește exercitarea drepturilor persoanei vizate și obligațiile de a furniza informațiile menționate la articolele 13 și 14, cu excepția cazului și în măsura în care responsabilitățile corespunzătoare fiecărui operator sunt stabilite de dreptul Uniunii sau de dreptul intern care se aplică operatorilor.

165. Din această dispoziție reiese clar că operatorii asociați trebuie să definească cine va fi responsabil cu răspunsul la cereri atunci când persoanele vizate își exercită drepturile acordate prin RGPD și de a le furniza informații, astfel cum se prevede la articolele 13 și 14 din RGPD. Acest aspect se referă doar la definirea părții din cadrul relației interne a acestora care este obligată să răspundă la cererile persoanelor vizate. . Indiferent de orice astfel de acorduri, persoana vizată poate contacta pe oricare dintre operatorii asociați în conformitate cu articolul 26 alineatul (3) din RGPD. Cu toate acestea, utilizarea termenului „*în special*" indică faptul că obligațiile care fac obiectul atribuirii responsabilităților în sensul respectării obligațiilor de către fiecare parte implicată, astfel cum se menționează în această dispoziție, nu sunt exhaustive. Rezultă că atribuirea responsabilităților între

[72] „În orice caz, acordul privind operatorul asociat ar trebui să abordeze în mod cuprinzător toate responsabilitățile operatorilor asociați, inclusiv pe cele care ar fi putut fi deja prevăzute în dreptul UE sau dreptul intern relevant și fără a aduce atingere obligației operatorilor asociați de a pune la dispoziție esența acordului privind operatorul asociat în conformitate cu articolul 26 alineatul (2) din RGPD."

operatorii asociați în scopul respectării obligațiilor nu se limitează la temele menționate la articolul 26 alineatul (1), ci se extinde la alte obligații ale operatorului în temeiul RGPD. Într-adevăr, operatorii asociați trebuie să se asigure că întreaga prelucrare comună respectă pe deplin RGPD.

166. Din această perspectivă, măsurile în scopul respectării obligațiilor și obligațiile aferente de care operatorii asociați trebuie să țină seama atunci când stabilesc responsabilitățile fiecăruia, în plus față de cele menționate în mod specific la articolul 26 alineatul (1), includ, printre altele, fără limitare:

- Punerea în aplicare a principiilor generale de protecție a datelor (articolul 5)
- Legalitatea prelucrării[73] (articolul 6)
- Măsuri de securitate (articolul 32)
- Notificarea autorității de supraveghere și a persoanei vizate în cazul unei încălcări a securității datelor cu caracter personal[74] (articolele 33 și 34)
- Evaluările impactului asupra protecției datelor (articolele 35 și 36)[75]
- Utilizarea unei persoane împuternicite de operator (articolul 28)
- Transferurile de date către țări terțe (capitolul V)
- Organizarea contactelor cu persoanele vizate și cu autoritățile de supraveghere

167. Alte teme care ar putea fi luate în considerare în funcție de prelucrarea în cauză și de intenția părților sunt, de exemplu, limitările privind utilizarea datelor cu caracter personal în alt scop de către unul dintre operatorii asociați. În acest sens, ambii operatori au întotdeauna obligația de a se asigura că au amândoi un temei juridic pentru prelucrare. Uneori, în contextul controlului în comun, un operator pune la dispoziția celuilalt datele cu caracter personal. În ceea ce privește responsabilitatea, fiecare operator are datoria de a se asigura că datele nu sunt prelucrate ulterior într-un mod incompatibil cu scopurile pentru care au fost colectate inițial de către operatorul care a pus datele la dispoziție.[76]

168. Operatorii asociați pot avea un anumit grad de flexibilitate în ceea ce privește distribuirea și repartizarea obligațiilor între ei, atât timp cât asigură respectarea deplină a RGPD în ceea ce privește

[73] Deși RGPD nu împiedică operatorii asociați să utilizeze un temei juridic diferit pentru operațiunile de prelucrare diferite efectuate, se recomandă utilizarea, ori de câte ori este posibil, a aceluiași temei juridic pentru un anumit scop.

[74] A se vedea, de asemenea, Orientările CEPD privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP250.rev.01, care prevăd că la controlul comun se include „*stabilirea părții care va avea responsabilitatea pentru asigurarea respectării obligațiilor prevăzute la articolele 33 și 34. GL29 recomandă ca mecanismele contractuale dintre operatorii asociați să includă dispoziții care stabilesc operatorul care va prelua sarcina sau va fi responsabil pentru asigurarea respectării obligațiilor de notificare a încălcării prevăzute în RGPD.*" (p. 13).

[75] A se vedea, de asemenea, Orientările CEPD privind evaluarea impactului asupra protecției datelor, WP248.rev.01, care prevăd următoarele: *„Atunci când operațiunea de prelucrare implică operatori asociați, aceștia trebuie să definească obligațiile lor respective în mod exact. DPIA a acestora trebuie să stabilească partea care este responsabilă pentru diferitele măsuri concepute pentru a trata riscurile și pentru a proteja drepturile și libertățile fundamentale ale persoanelor vizate. Fiecare operator de date trebuie să își exprime necesitățile și să facă schimb de informații utile fără a compromite secretele (de exemplu, protecția secretelor comerciale, proprietatea intelectuală, informații comerciale confidențiale) sau fără a dezvălui vulnerabilitățile*." (p. 7).

[76] Fiecare divulgare de către un operator necesită o bază legală și o evaluare a compatibilității, indiferent dacă destinatarul este un operator separat sau un operator asociat. Cu alte cuvinte, existența unei relații de tipul operatori asociați nu înseamnă în mod automat că operatorul asociat care primește datele poate, de asemenea, să prelucreze în mod legal datele în scopuri suplimentare care depășesc domeniul de aplicare al controlului comun.

prelucrarea în cauză. Repartizarea trebuie să țină seama de factori precum cine este competent și în poziția să asigure efectiv drepturile persoanei vizate, precum și să respecte obligațiile relevante în temeiul RGPD. CEPD recomandă documentarea factorilor relevanți și analiza internă efectuată pentru repartizarea diferitelor obligații. Această analiză face parte din documentația în temeiul principiului responsabilității.

169. Nu este necesar ca obligațiile să fie repartizate în mod egal între operatorii asociați. În acest sens, CJUE a statuat recent că *„existența unei responsabilități comune nu înseamnă în mod necesar o răspundere echivalentă a diferitor operatori vizați de o prelucrare a datelor cu caracter personal.”*”.[77] Cu toate acestea, pot exista cazuri în care nu toate obligațiile pot fi repartizate și operatorii asociați pot fi nevoiți să respecte aceleași cerințe care decurg din RGPD, ținând seama de natura și contextul prelucrării în comun. De exemplu, operatorii asociați care utilizează instrumente sau sisteme comune de prelucrare a datelor trebuie să asigure, în special, respectarea principiului limitării scopului și să pună în aplicare măsuri adecvate pentru a asigura securitatea datelor cu caracter personal prelucrate cu ajutorul instrumentelor comune.

170. Un alt exemplu este cerința ca fiecare operator asociat să păstreze o evidență a activităților de prelucrare sau să desemneze un responsabil cu protecția datelor (RPD) în cazul în care sunt îndeplinite condițiile prevăzute la articolul 37 alineatul (1). Aceste cerințe nu au legătură cu prelucrarea comună, ci li se aplică în calitate de operatori.

2.2 Atribuirea responsabilităților trebuie să se facă printr-un acord

2.2.1 Forma acordului

171. Articolul 26 alineatul (1) din RGPD introduce o nouă obligație pentru operatorii asociați, aceea de a-și stabili responsabilitățile proprii *„prin intermediul unui acord între ei*”. RGPD nu specifică forma juridică a acestui acord. Prin urmare, operatorii asociați sunt liberi să convină asupra formei acordului.

172. În plus, acordul privind atribuirea responsabilităților este obligatoriu pentru fiecare dintre operatorii asociați. Părțile convin și se angajează *reciproc* să fie responsabile fiecare de respectarea obligațiilor stipulate în acord ca responsabilitate proprie.

173. Prin urmare, din motive de securitate juridică, chiar dacă nu există nicio cerință legală în RGPD privind un contract sau alt act juridic, CEPD recomandă ca acest acord să fie încheiat sub forma unui document obligatoriu, precum un contract sau alt act juridic obligatoriu în temeiul dreptului UE sau al dreptului intern care se aplică operatorilor. Acest fapt ar oferi certitudine și ar putea fi utilizat pentru a demonstra transparență și responsabilitate. Într-adevăr, în cazul nerespectării atribuirii convenite prevăzute în acord, caracterul obligatoriu al acestuia permite unui operator să îl tragă pe celălalt la răspundere pentru ceea ce s-a prevăzut în acord ca fiind responsabilitatea acestuia. De asemenea, în conformitate cu principiul responsabilității, utilizarea unui contract sau a unui alt act juridic va permite operatorilor asociați să demonstreze că respectă obligațiile care le revin în temeiul RGPD.

174. Modul în care responsabilitățile, și anume sarcinile, sunt repartizate fiecărui operator asociat trebuie să fie precizat într-un limbaj clar și simplu în acord.[78] Această cerință este importantă, deoarece asigură

[77] Hotărârea pronunțată în cauza *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, punctul 43.

[78] Astfel cum se menționează în considerentul 79 din RGPD: *„[...] responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator, inclusiv în ceea ce privește monitorizarea de către autoritățile de supraveghere și măsurile adoptate de acestea, necesită o atribuire clară a responsabilităților în temeiul prezentului regulament, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori*”.

securitatea juridică și evită posibilele conflicte nu doar în relația dintre operatorii asociați, ci și față de persoanele vizate și autoritățile de protecție a datelor.

175. Pentru a încadra mai bine atribuirea responsabilităților între părți, CEPD recomandă ca acordul să furnizeze, de asemenea, informații generale privind prelucrarea comună, specificând în special obiectul și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate.

2.2.2 Obligații față de persoanele vizate

176. RGPD prevede mai multe obligații ale operatorilor asociați față de persoanele vizate:

Acordul trebuie să reflecte în mod adecvat rolurile și raporturile corespunzătoare ale operatorilor asociați *față de* persoanele vizate.

177. În completarea celor explicate mai sus în secțiunea 2.1 din prezentele orientări, este important ca operatorii asociați să clarifice în acord rolul fiecăruia, „*în special*” în ceea ce privește exercitarea drepturilor persoanei vizate și obligațiile acestora de a furniza informațiile menționate la articolele 13 și 14. Articolul 26 din RGPD subliniază importanța acestor obligații specifice. Prin urmare, operatorii asociați trebuie să se organizeze și să convină cu privire la cine și în ce mod va furniza informațiile și cu privire la cine și în ce mod va furniza răspunsurile la cererile persoanei vizate. Indiferent de conținutul acordului cu privire la acest aspect specific, persoana vizată poate contacta oricare dintre operatorii asociați pentru a-și exercita drepturile în conformitate cu articolul 26 alineatul (3), astfel cum se explică mai jos.

178. Modul în care sunt organizate aceste obligații în acord trebuie să reflecte „*în mod corespunzător*”, și anume precis, realitatea prelucrări comune respective. De exemplu, dacă doar unul dintre operatorii asociați comunică cu persoanele vizate în scopul prelucrării comune, operatorul respectiv ar putea fi mai în măsură să informeze persoanele vizate și, eventual, să răspundă cererilor acestora.

Esența acestui acord trebuie făcută cunoscută persoanei vizate.

179. Această dispoziție este menită să asigure faptul că persoana vizată cunoaște „*esența acordului*”. De exemplu, trebuie să fie foarte clar pentru o persoană vizată care este operatorul de date care servește ca punct de contact pentru exercitarea drepturilor persoanei vizate (fără a aduce atingere faptului că aceasta își poate exercita drepturile cu privire la și în raport cu fiecare dintre operatorii asociați). Obligația de a face cunoscută persoanelor vizate esența acordului este importantă în cazul controlului comun, pentru ca persoana vizată să știe care sunt responsabilitățile fiecărui operator.

180. RGPD nu specifică ce trebuie să cuprindă conceptul de „*esența acestui acord*”. CEPD recomandă ca esența să cuprindă cel puțin toate elementele informațiilor menționate la articolele 13 și 14 care trebuie să fie deja accesibile persoanei vizate și, pentru fiecare dintre aceste elemente, acordul trebuie să precizeze operatorul asociat responsabil de asigurarea respectării acestor elemente. De asemenea, esența acordului trebuie să indice punctul de contact, dacă acesta este desemnat.

181. Nu este precizat modul în care aceste informații sunt făcute cunoscute persoanei vizate. Contrar altor dispoziții din RGPD [cum ar fi articolul 30 alineatul (4) pentru evidența activităților de prelucrare sau articolul 40 alineatul (11) pentru registrul codurilor de conduită aprobate], articolul 26 nu indică faptul că aceste informații trebuie făcute cunoscute „*la cerere*” și nici puse „*la dispoziția publicului prin mijloace corespunzătoare*”. Prin urmare, operatorii asociați decid modalitatea cea mai eficace de a face cunoscută persoanelor vizate esența acordului (de exemplu, împreună cu informațiile de la articolul 13 sau 14, în politica de confidențialitate sau în urma unei cereri adresate responsabilului cu protecția

datelor, dacă există, sau punctului de contact care ar fi putut fi desemnat). Operatorii asociați trebuie să se asigure fiecare că informațiile sunt furnizate în mod consecvent.

Acordul poate să desemneze un punct de contact pentru persoanele vizate.

182. Articolul 26 alineatul (1) prevede posibilitatea ca operatorii asociați să desemneze în acord un punct de contact pentru persoanele vizate. Această desemnare nu este obligatorie.

183. Informarea cu privire la o modalitate unică de a contacta posibili operatori asociați multipli permite persoanelor vizate să știe pe cine pot contacta cu privire la toate aspectele legate de prelucrarea datelor lor cu caracter personal. În plus, aceasta permite operatorilor asociați multipli să-și coordoneze mai eficient relațiile și comunicările *cu* persoanele vizate.

184. Din aceste motive, pentru a facilita exercitarea drepturilor persoanelor vizate în temeiul RGPD, CEPD recomandă operatorilor asociați să desemneze acest punct de contact.

185. Punctul de contact poate fi responsabilul cu protecția datelor, dacă există, reprezentantul din Uniune (pentru operatorii asociați care nu sunt stabiliți în Uniune) sau orice alt punct de contact de la care pot fi obținute informații.

Indiferent de clauzele acordului, persoanele vizate își pot exercita drepturile cu privire la și în raport cu fiecare dintre operatorii asociați.

186. În temeiul articolul 26 alineatul (3), o persoană vizată nu are obligații în temeiul acordului și își poate exercita drepturile în temeiul RGPD în ceea ce privește și în raport cu fiecare dintre operatorii de date asociați.

187. De exemplu, în cazul operatorilor asociați stabiliți în state membre diferite sau în cazul în care doar unul dintre operatorii asociați este stabilit în Uniune, persoana vizată poate contacta, la alegerea sa, fie operatorul stabilit în statul membru în care își are reședința obișnuită sau locul de muncă, fie operatorul stabilit în altă parte în UE sau în SEE.

188. Chiar dacă acordul și esența acestuia, făcută cunoscută, indică un punct de contact pentru primirea și tratarea tuturor cererilor persoanelor vizate, cu toate acestea, persoanele vizate pot să decidă în alt mod.

189. Prin urmare, este important ca operatorii asociați să organizeze în prealabil în acordul acestora modul în care vor gestiona răspunsurile la cererile pe care le-ar putea primi de la persoanele vizate. În acest sens, se recomandă ca operatorii asociați să comunice celorlalți responsabili sau punctului de contact desemnat cererile primite pentru ca acestea să fie tratate cu eficacitate. Obligarea persoanelor vizate să contacteze punctul de contact desemnat sau operatorul responsabil ar impune persoanei vizate o sarcină excesivă care ar fi contrară obiectivului de a facilita exercitarea drepturilor acesteia în temeiul RGPD.

2.3 Obligații față de autoritățile de protecție a datelor

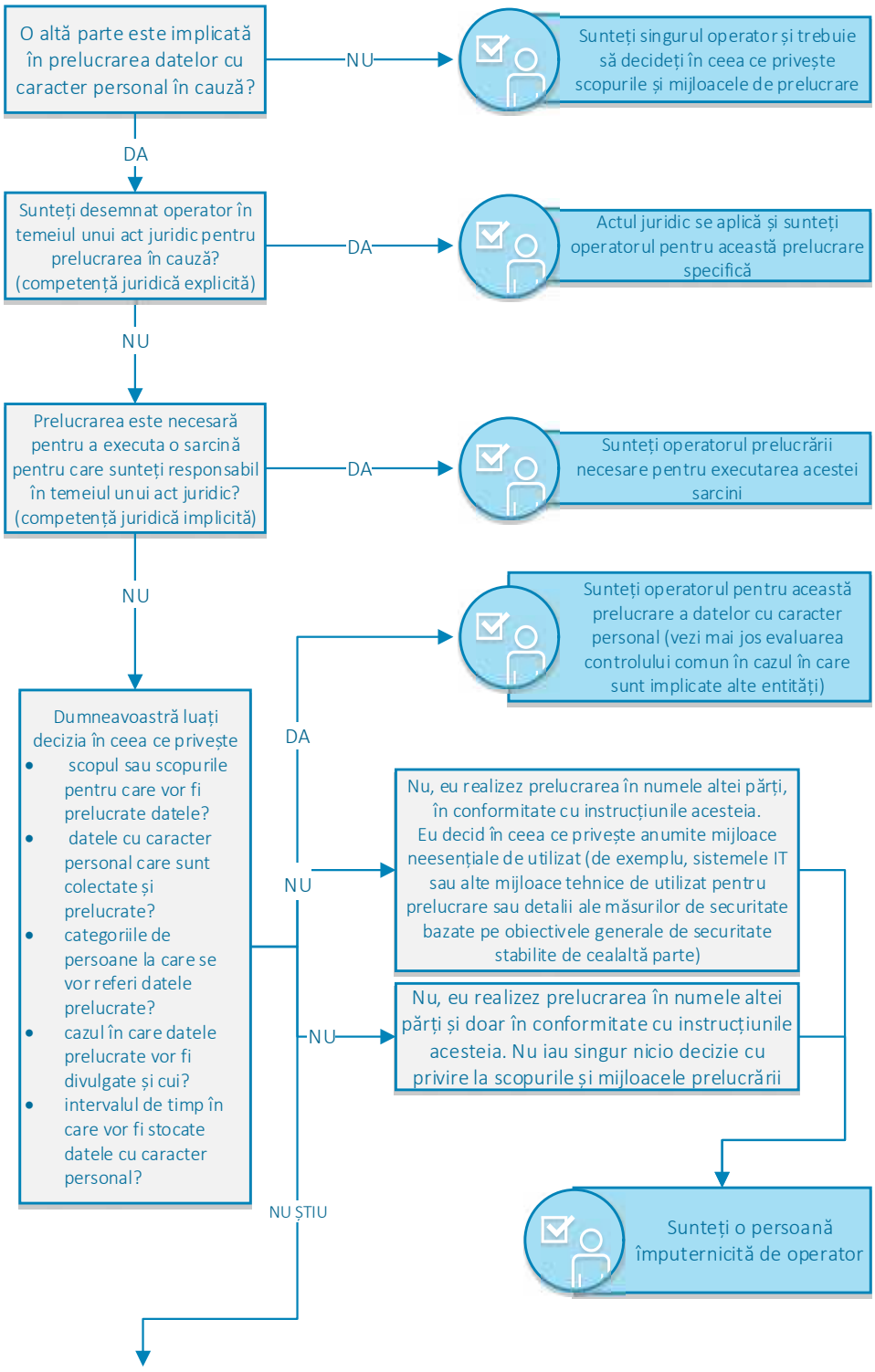
190. Operatorii asociați trebuie să organizeze în cadrul acordului modul în care vor comunica cu autoritățile de supraveghere competente în materie de protecție a datelor. Această comunicare ar putea include o consultare posibilă în temeiul articolul 36 din RGPD, notificarea unei încălcări a securității datelor cu caracter personal, desemnarea unui responsabil cu protecția datelor.

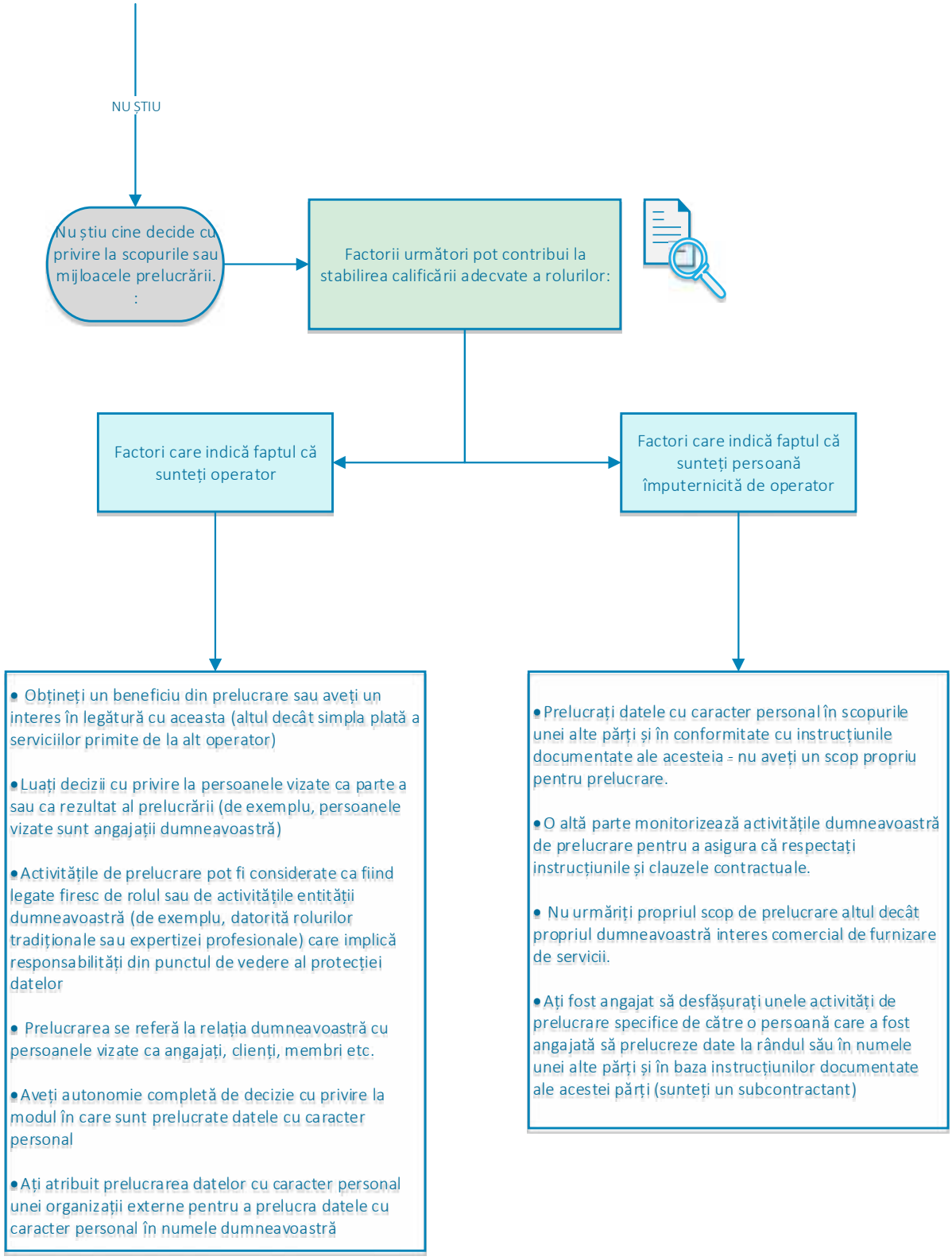
191. Trebuie reamintit faptul că autoritățile de protecție a datelor nu sunt obligate să respecte clauzele acordului nici în ceea ce privește calificarea părților ca operatori asociați, nici în ceea ce privește

punctul de contact desemnat. Prin urmare, autoritățile pot contacta oricare dintre operatorii asociați pentru a-și exercita competențele în temeiul articolul 58 în ceea ce privește prelucrarea comună.

Anexa I – Grafic pentru aplicarea conceptelor de operator, persoană împuternicită de operator și operatori asociați în practică

Notă: pentru a evalua corespunzător rolul fiecărei entități implicate, trebuie identificată mai întâi operațiunea specifică de prelucrare a datelor cu caracter personal în cauză și scopul exact al acesteia. În cazul în care sunt implicate mai multe entități, este necesar să se evalueze dacă scopurile și mijloacele sunt stabilite în comun, ceea ce înseamnă control comun.




NU ȘTIU
Nu știu cine decide cu privire la scopurile sau mijloacele prelucrării. :
Factorii următori pot contribui la stabilirea calificării adecvate a rolurilor:
Factori care indică faptul că sunteți operator
Factori care indică faptul că sunteți persoană împuternicită de operator
• Obțineți un beneficiu din prelucrare sau aveți un interes în legătură cu aceasta (altul decât simpla plată a serviciilor primite de la alt operator)
• Luați decizii cu privire la persoanele vizate ca parte a sau ca rezultat al prelucrării (de exemplu, persoanele vizate sunt angajații dumneavoastră)
• Activitățile de prelucrare pot fi considerate ca fiind legate firesc de rolul sau de activitățile entității dumneavoastră (de exemplu, datorită rolurilor tradiționale sau expertizei profesionale) care implică responsabilități din punctul de vedere al protecției datelor
• Prelucrarea se referă la relația dumneavoastră cu persoanele vizate ca angajați, clienți, membri etc.
• Aveți autonomie completă de decizie cu privire la modul în care sunt prelucrate datele cu caracter personal
• Ați atribuit prelucrarea datelor cu caracter personal unei organizații externe pentru a prelucra datele cu caracter personal în numele dumneavoastră
• Prelucrați datele cu caracter personal în scopurile unei alte părți și în conformitate cu instrucțiunile documentate ale acesteia - nu aveți un scop propriu pentru prelucrare.
• O altă parte monitorizează activitățile dumneavoastră de prelucrare pentru a asigura că respectați instrucțiunile și clauzele contractuale.
• Nu urmăriți propriul scop de prelucrare altul decât propriul dumneavoastră interes comercial de furnizare de servicii.
• Ați fost angajat să desfășurați unele activități de prelucrare specifice de către o persoană care a fost angajată să prelucreze date la rândul său în numele unei alte părți și în baza instrucțiunilor documentate ale acestei părți (sunteți un subcontractant)

Control comun - În cazul în care sunteți operatorul și alte părți sunt implicate în prelucrarea datelor cu caracter personal: