Orientări

Orientările nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulament

Versiunea 3.0

4 iunie 2019

Adoptat

Istoricul versiunilor

Versiunea 3.0	4 iunie 2019	Includerea anexei 2 (versiunea 2.0 a anexei 2 adoptată la 4 iunie 2019 în urma consultării publice)
Versiunea 2.1	9 aprilie 2019	Adoptarea unei rectificări a orientărilor (punctul 45)
Versiunea 2.0	23 ianuarie 2019	Adoptarea orientărilor în urma consultării publice – la aceeași dată la care anexa 2 (versiunea 1.0) a fost adoptată spre consultare publică
Versiunea 1.0	25 mai 2018	Adoptarea orientărilor spre consultare publică

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”),

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

având în vedere articolele 12 și 22 din Regulamentul său de Procedură din 25 mai 2018,

în urma analizării rezultatelor consultării publice privind orientările, care a avut loc în perioada 30 mai 2018 - 12 iulie 2018, și a consultării publice privind anexa 2, care a avut loc în perioada 15 februarie - 29 martie 2019, conform articolului 70 alineatul (4) din RGPD,

ADOPTĂ URMĂTOARELE ORIENTĂRI

1 INTRODUCERE

1. Regulamentul General privind Protecția Datelor [Regulamentul (UE) 2016/679, „RGPD” sau „regulamentul”] asigură un cadru modernizat, de responsabilizare și de respectare a drepturilor fundamentale pentru protecția datelor în Europa. Elementul central al acestui nou cadru îl reprezintă o gamă de măsuri care facilitează respectarea dispozițiilor RGPD. Acestea includ cerințe obligatorii în circumstanțe specifice (inclusiv numirea unor responsabili cu protecția datelor și realizarea unor evaluări ale impactului asupra protecției datelor) și măsuri voluntare, cum ar fi codurile de conduită și mecanismele de certificare.
2. Înainte de adoptarea RGPD, Grupul de Lucru instituit prin articolul 29 a stabilit faptul că certificarea ar putea să joace un rol important în cadrul de responsabilizare pentru protecția datelor1. Pentru ca certificarea să furnizeze dovezi fiabile cu privire la respectarea protecției datelor, ar trebui să existe norme clare care să stabilească cerințele pentru acordarea certificării2. Articolul 42 din RGPD asigură temeiul juridic pentru elaborarea acestor norme.
3. Articolul 42 alineatul (1) din RGPD prevede că:

   „Statele membre, autoritățile de supraveghere, Comitetul [European pentru Protecția Datelor] și Comisia Europeană încurajează, în special la nivelul Uniunii, instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest

[1] Grupul de Lucru instituit prin articolul 29, Avizul 3/2010 privind principiul responsabilității, WP 173, 13 iulie 2010, punctele 69-71.
[2] Grupul de Lucru instituit prin articolul 29, Avizul 3/2010 privind principiul responsabilității (WP 173), punctul 69.

domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezentul regulament. Sunt luate în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii."

4. Mecanismele de certificare3 pot îmbunătăți transparența pentru persoanele vizate, dar și în relațiile business-to-business, de exemplu între operatori și persoanele împuternicite de către operatori. Considerentul 100 din RGPD prevede că instituirea de mecanisme de certificare poate îmbunătăți transparența și conformitatea cu regulamentul și poate permite persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante4.

5. RGPD nu introduce un drept sau o obligație de certificare pentru operatori și persoanele împuternicite de către operatori; conform articolului 42 alineatul (3), certificarea este un proces voluntar pentru a ajuta la demonstrarea conformității cu RGPD. Statele membre și autoritățile de supraveghere sunt invitate să încurajeze instituirea de mecanisme de certificare și vor stabili implicarea părților interesate în procesele de certificare și ciclul de viață.

6. În plus, aderarea la mecanisme de certificare aprobate este un factor pe care autoritățile de supraveghere trebuie să îl considere ca un factor agravant sau atenuant atunci când decid să impună o amendă administrativă sau când decid cu privire la cuantumul amenzii [articolul 83 alineatul (2) litera (j)]5.

1.1 Domeniul de aplicare al orientărilor

7. Domeniul de aplicare al prezentelor orientări este limitat; acestea nu constituie un manual de procedură pentru certificare în conformitate cu RGPD. Obiectivul principal al prezentelor orientări este de a identifica cerințele și criteriile generale care pot fi relevante pentru toate tipurile de mecanisme de certificare emise în conformitate cu articolele 42 și 43 din RGPD. În acest scop, orientările:

    - explorează argumentele pentru certificare ca instrument de responsabilizare;
    - explică noțiunile-cheie ale dispozițiilor privind certificarea de la articolele 42 și 43; și
    - explică domeniul de aplicare a ceea ce se poate certifica în conformitate cu articolele 42 și 43, precum și scopul certificării;
    - fac posibil ca rezultatul certificării să fie semnificativ, lipsit de ambiguitate, cât mai reproductibil posibil și comparabil, indiferent de organismul de certificare (comparabilitate).

[3] În prezentele orientări se face trimitere la mecanismele de certificare și la sigiliile și mărcile în domeniul protecției datelor în mod colectiv ca „mecanisme de certificare", a se vedea secțiunea 1.3.2.
[4] Considerentul 100 prevede că, „pentru a se îmbunătăți transparența și conformitatea cu [regulamentul], ar trebui să se încurajeze instituirea de mecanisme de certificare [...] care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante".
[5] A se vedea documentul Grupului de Lucru instituit prin articolul 29, Orientări privind aplicarea și stabilirea unor amenzi administrative în sensul Regulamentului nr. 2016/679 (WP 253).

8. RGPD prevede o serie de mijloace prin care statele membre și autoritățile de supraveghere să pună în aplicare articolele 42 și 43. Orientările oferă consiliere privind interpretarea și punerea în aplicare a dispozițiilor articolelor 42 și 43 și vor ajuta statele membre, autoritățile de supraveghere și organismele naționale de acreditare să stabilească o abordare mai coerentă și armonizată pentru punerea în aplicare a mecanismelor de certificare în conformitate cu RGPD.

9. Consilierea cuprinsă în orientări va fi relevantă pentru:

   - autoritățile de supraveghere competente și Comitetul European pentru Protecția Datelor („Comitetul European pentru Protecția Datelor") la aprobarea criteriilor de certificare conform articolului 42 alineatul (5), articolului 58 alineatul (3) litera (f) și articolului 70 alineatul (1) litera (o);

   - organismele de certificare la elaborarea și revizuirea criteriilor de certificare înainte de cererea de aprobare depusă la autoritatea de supraveghere competentă, conform articolului 42 alineatul (5);

   - Comitetul European pentru Protecția Datelor la aprobarea Sigiliului European privind Protecția Datelor, conform articolului 42 alineatul (5) și articolului 70 alineatul (1) litera (o);

   - autoritățile de supraveghere la elaborarea criteriilor de certificare proprii;

   - Comisia Europeană, care este împuternicită să adopte acte delegate în scopul specificării cerințelor care trebuie luate în considerare pentru mecanismele de certificare, conform articolului 43 alineatul (8);

   - Comitetul European pentru Protecția Datelor atunci când furnizează Comisiei Europene un aviz privind cerințele de certificare în conformitate cu articolul 70 alineatul (1) litera (q) și cu articolul 43 alineatul (8);

   - organismele naționale de acreditare, care vor trebui să țină seama de criteriile de certificare în vederea acreditării organismelor de certificare în conformitate cu EN-ISO/IEC 17065/2012, precum și de cerințele suplimentare în conformitate cu articolul 43; și

   - operatorii și persoanele împuternicite de către operatori la definirea propriei strategii de conformitate cu RGPD și la luarea în considerare a certificării ca mijloc de demonstrare a conformității.

10. Comitetul European pentru Protecția Datelor va publica orientări separate pentru a aborda identificarea criteriilor de aprobare a mecanismelor de certificare ca instrumente de transfer în țările terțe sau către organizații internaționale în conformitate cu articolul 42 alineatul (2).

1.2 Scopul certificării conform RGPD

11. Articolul 42 alineatul (1) prevede că vor fi instituite mecanisme de certificare „care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezentul regulament".

12. RGPD ilustrează contextul în care mecanismele de certificare aprobate pot fi utilizate ca element de demonstrare a respectării obligațiilor operatorilor și persoanelor împuternicite de către operatori cu privire la:

    - punerea în aplicare și demonstrarea măsurilor tehnice și organizatorice adecvate, menționate la articolul 24 alineatele (1) și (3), articolul 25 și articolul 32 alineatele (1) și (3);
    - garanțiile suficiente (oferite de persoana împuternicită de către operator pentru operator), menționate la alineatele (1), și (oferite de a doua persoană împuternicită pentru persoana împuternicită de către operator), menționate la alineatul (4), conform articolului 28 alineatul (5).

13. Deoarece această certificare nu demonstrează conformitatea în sine și prin sine, ci mai degrabă formează un element care poate fi utilizat pentru a demonstra conformitatea, certificarea ar trebui să se realizeze în mod transparent. Demonstrarea conformității necesită documente justificative, mai exact rapoarte scrise, care nu numai că repetă, ci și descriu modul în care sunt îndeplinite criteriile și, dacă acestea nu sunt îndeplinite inițial, descriu corecțiile și acțiunile corective și pertinența acestora, prezentând astfel motivele pentru acordarea și menținerea certificării. Acest lucru include prezentarea deciziei individuale pentru acordarea, reînnoirea sau retragerea unui certificat. Demonstrarea conformității ar trebui să prezinte motivele, argumentele și dovezile care rezultă din aplicarea criteriilor, precum și concluziile, deciziile sau deducerile desprinse din faptele sau premisele colectate pe parcursul certificării.

1.3 Noțiuni-cheie

14. Următoarea secțiune explorează noțiunile-cheie prevăzute la articolele 42 și 43. Această analiză dezvoltă o înțelegere a termenilor de bază și a domeniului de aplicare al certificării conform RGPD.

1.3.1 Interpretarea „certificării”

15. RGPD nu definește „certificarea”. Organizația Internațională de Standardizare (ISO) oferă o definiție universală a certificării ca fiind „furnizarea de către un organism independent a unei asigurări scrise (un certificat) privind faptul că produsul, serviciul sau sistemul în cauză îndeplinește cerințele specifice.” De asemenea, certificarea este cunoscută ca o „evaluare a conformității efectuată de o terță parte”, iar organismele de certificare pot fi numite, de asemenea, „organisme de evaluare a conformității”. În EN-ISO/IEC 17000:2004 - Evaluarea conformității - Vocabular și principii generale (la care face trimitere ISO17065) - certificarea este definită după cum urmează: „atestarea efectuată de o terță parte [...] în legătură cu produse, procese și servicii”.

16. Atestarea este „emiterea unei declarații, pe baza unei decizii care urmează unei revizuiri, conform căreia s-a demonstrat îndeplinirea cerințelor specificate” (secțiunea 5.2, ISO 17000:2004).

17. În contextul certificării conform articolelor 42 și 43 din RGPD, certificarea face trimitere la atestarea efectuată de o terță parte în legătură cu operațiunile de prelucrare realizate de operatori și persoanele împuternicite de către operatori.

1.3.2 Mecanisme de certificare, sigilii și mărci

18. RGPD nu definește „mecanismele de certificare, sigiliile și mărcile" – și utilizează acești termeni în mod colectiv. Certificatul este o declarație de conformitate. Sigiliul sau marca poate fi utilizat/utilizată pentru a ilustra finalizarea cu succes a procedurii de certificare. Sigiliul sau marca se referă în mod obișnuit la un logo sau un simbol a cărui prezență (pe lângă certificat) indică faptul că obiectul certificării a fost evaluat în mod independent în cadrul unei proceduri de certificare și că este în conformitate cu cerințele specifice, prevăzute în documentele normative, cum ar fi regulamente, standarde sau specificații tehnice. Aceste cerințe în contextul certificării conform RGPD sunt stabilite în cadrul cerințelor suplimentare care completează normele pentru acreditarea organismelor de certificare prevăzute în EN-ISO/IEC 17065/2012, precum și criteriile de certificare aprobate de autoritatea de supraveghere competentă sau de Comitet. Conform RGPD, certificatul, sigiliul sau marca poate fi emis/emisă numai în urma unei evaluări independente a dovezilor de către un organism de certificare acreditat sau de către o autoritate de supraveghere competentă, care prevede faptul că au fost îndeplinite criteriile de certificare.

19. Tabelul oferă un exemplu generic al unui proces de certificare.

Depunerea cererii de către operator sau persoana împuternicită de către operator	Verificare oficială de către organismul de certificare	Evaluare Preevaluare	Evaluare Evaluarea obiectivului evaluării	Evaluare Validarea rezultatelor	Informarea autorității de supraveghere competente	Certificare	Monitorizare	Reînnoirea certificării
Descrierea obiectivului evaluării este lipsită de ambiguitate și completă, incluzând interfețele?	Descrierea obiectivului evaluării poate fi acceptată?	Care sunt criteriile aplicabile?	Obiectivul evaluării îndeplinește criteriile?	Toate criteriile relevante specificate reflectă obiectivul evaluării?	Au fost furnizate motivele pentru acordarea sau retragerea certificării?	Se poate acorda certificatul?	Obiectivul evaluării îndeplinește în continuare criteriile?	Prelucrarea îndeplinește în continuare criteriile de certificare?
Se poate acorda accesul la activitățile de prelucrare din obiectivul evaluării?	Toate documentele sunt complete și actualizate?	Care sunt metodele de evaluare aplicabile?	Documentarea obiectivului evaluării este corectă?	Evaluarea a fost documentată suficient?		Rapoartele sunt pregătite pentru a fi publicate?	Certificatul/sigiliul /marca de garanție este utilizat(ă) în mod corect?	Domeniile de dezvoltare au fost abordate în mod satisfăcător?
Articolul 42 alineatul (6)	Articolul 43 alineatul (4)	Articolul 43 alineatul (4)	Articolul 42 alineatul (5), Articolul 43 alineatul (4)	Articolul 43 alineatul (4)	Articolul 43 alineatul (1), articolul 43 alineatul (5)	Articolul 43 alineatul (1); Articolul 42 alineatul (7)	Articolul 42 alineatul (7)	Articolul 42 alineatul (7)

2 ROLUL AUTORITĂȚILOR DE SUPRAVEGHERE

20. Articolul 42 alineatul (5) prevede că certificarea se emite de către un organism de certificare acreditat sau de către o autoritate de supraveghere competentă. RGPD nu prevede că emiterea certificărilor este o sarcină obligatorie a autorităților de supraveghere. În schimb, RGPD permite o serie de modele diferite. De exemplu, autoritatea de supraveghere poate decide să aleagă una sau mai multe dintre următoarele opțiuni:

    - să emită ea însăși certificarea, cu respectarea propriului său sistem de certificare;
    - să emită ea însăși certificarea, cu respectarea propriului său sistem de certificare, dar să delege total sau parțial procesul de evaluare către terțe părți;
    - să își creeze propriul sistem de certificare și să încredințeze procedura de certificare organismelor de certificare, care emit certificarea; și
    - să încurajeze piața să elaboreze mecanisme de certificare.

21. De asemenea, autoritatea de supraveghere va trebui să își ia rolul în considerare în lumina deciziilor adoptate la nivel național cu privire la mecanismele de acreditare – în special dacă autoritatea de supraveghere însăși este împuternicită să acrediteze organismele de certificare conform articolului 43 alineatul (1) din RGPD. Astfel, fiecare autoritate de supraveghere va stabili ce abordare să adopte pentru a urmări intenția amplă a certificării conform RGPD. Acest lucru se va stabili nu numai în contextul sarcinilor și al competențelor prevăzute la articolele 57 și 58, ci și al considerării certificării ca factor de care trebuie să se țină seama la stabilirea amenzilor administrative și, în termeni mai generali, ca mijloc de demonstrare a conformității.

2.1 Autoritatea de supraveghere ca organism de certificare

22. În cazul în care autoritatea de supraveghere alege să efectueze o certificare, aceasta va trebui să își evalueze rolul cu atenție în ceea ce privește sarcinile care îi sunt atribuite conform RGPD. Rolul său ar trebui să fie transparent în exercitarea funcțiilor sale. Acesta va trebui să ia în considerare în special separația puterilor referitoare la investigații și aplicarea legii pentru a evita orice conflict de interese potențial.

23. Atunci când acționează în calitate de organism de certificare, autoritatea de supraveghere va trebui să asigure instituirea adecvată a unui mecanism de certificare și să își elaboreze propriile criterii de certificare sau să adopte alte criterii de certificare. În plus, fiecare autoritate de supraveghere care emite certificări are sarcina de a le revizui periodic [articolul 57 alineatul (1) litera (o)] și competența de a le retrage în cazul în care cerințele pentru certificare nu sunt sau nu mai sunt îndeplinite [articolul 58 alineatul (2) litera (h)]. Pentru a îndeplini aceste cerințe, este util să se instituie o procedură de certificare și cerințe referitoare la proces și, cu excepția unor dispoziții contrare, de exemplu, în legislația națională, să se stabilească un acord aplicabil legal pentru realizarea de activități de certificare cu organizația individuală solicitantă. Ar trebui să se asigure faptul că acest acord de certificare obligă solicitantul să îndeplinească cel puțin criteriile de certificare, inclusiv demersurile necesare pentru efectuarea evaluării, monitorizarea respectării criteriilor și

revizuirea periodică, inclusiv accesul la informații și/sau sediu, documentarea și publicarea rapoartelor și a rezultatelor și investigarea plângerilor. În plus, se preconizează că o autoritate de supraveghere va respecta cerințele din orientările pentru acreditarea organismelor de certificare pe lângă cerințele prevăzute la articolul 43 alineatul (2).

2.2 Sarcini suplimentare ale autorității de supraveghere cu privire la certificare

24. În statele membre în care activează organismele de certificare, autoritatea de supraveghere, indiferent care sunt propriile sale activități, are competența și sarcina:

    - de a evalua criteriile unui sistem de certificare și de a adopta un proiect de decizie [articolul 42 alineatul (5)];
    - de a comunica proiectul de decizie Comitetului atunci când intenționează să aprobe criteriile pentru certificare [articolul 64 alineatul (1) litera (c) și articolul 64 alineatul (7)] și de a lua în considerare avizul Comitetului [articolul 64 alineatul (1) litera (c) și articolul 70 alineatul (1) litera (t)];
    - de a aproba criteriile pentru certificare [articolul 58 alineatul (3) litera (f)] înainte ca acreditarea și certificarea să poată avea loc [articolul 42 alineatul (5) și articolul 43 alineatul (2) litera (b)];
    - de a publica criteriile de certificare [articolul 43 alineatul (6)];
    - de a acționa în calitate de autoritate competentă pentru sistemele de certificare la nivelul UE, care pot rezulta într-un sigiliu european privind protecția datelor aprobat de Comitetul European pentru Protecția Datelor [articolul 42 alineatul (5) și articolul 70 alineatul (1) litera (o)]; și
    - de a obliga un organism de certificare (a) să nu emită certificarea sau (b) să retragă certificarea în cazul în care cerințele de certificare (procedurile sau criteriile de certificare) nu sunt sau nu mai sunt îndeplinite [articolul 58 alineatul (2) litera (h)].

25. RGPD îi atribuie autorității de supraveghere sarcina de a aproba criteriile de certificare, dar nu și de a elabora criteriile. Pentru a aproba criteriile de certificare conform articolului 42 alineatul (5), autoritatea de supraveghere ar trebui să înțeleagă în mod clar la ce să se aștepte, în special în ceea ce privește domeniul de aplicare și conținutul, pentru demonstrarea conformității cu RGPD și cu privire la sarcina sa de a monitoriza și a asigura aplicarea regulamentului. Anexa oferă îndrumări pentru a asigura o abordare armonizată la evaluarea criteriilor în scopul aprobării.

26. Articolul 43 alineatul (1) obligă organismele de certificare să își informeze autoritatea de supraveghere înainte de a emite sau a reînnoi certificări, pentru a permite autorității de supraveghere competente să își exercite competențele corective prevăzute la articolul 58 alineatul (2) litera (h). De asemenea, articolul 43 alineatul (5) obligă organismelor de certificare să transmită autorităților de supraveghere competente motivele acordării sau retragerii certificării solicitate. Deși RGPD permite autorităților de supraveghere să stabilească modul în care să primească, să recunoască, să revizuiască și să trateze aceste

informații din punct de vedere operațional (de exemplu, acest lucru ar putea include soluții tehnologice pentru a permite raportarea de către organismele de certificare), se pot institui procese și criterii de prelucrare a informațiilor și a rapoartelor furnizate cu privire la fiecare proiect de certificare de succes de către organismul de certificare în conformitate cu articolul 43 alineatul (1). Pe baza acestor informații, autoritatea de supraveghere își poate exercita competența de a obliga organismul de certificare să retragă sau să nu emită o certificare [articolul 58 alineatul (2) litera (h)] și să monitorizeze și să asigure aplicarea cerințelor și a criteriilor de certificare conform RGPD [articolul 57 alineatul (1) litera (a) și articolul 58 alineatul (2) litera (h)]. Acest lucru va sprijini o abordare armonizată și comparabilitatea în cadrul certificării de către diferite organisme de certificare și faptul că informațiile privind stadiul certificării unei organizații sunt cunoscute de către autoritățile de supraveghere.

3 ROLUL ORGANISMULUI DE CERTIFICARE

27. Rolul organismului de certificare este de a emite, a revizui, a reînnoi și a retrage certificări [articolul 42 alineatele (5) și (7)] pe baza unui mecanism de certificare și a unor criterii aprobate [articolul 43 alineatul (1)]. Pentru acest lucru, este necesar ca organismul de certificare sau titularul unui sistem de certificare să stabilească și să instituie criterii de certificare și proceduri de certificare, inclusiv proceduri pentru monitorizarea respectării, revizuirii, tratării plângerilor și a retragerii. Criteriile de certificare sunt revizuite ca parte a procesului de acreditare, în care se iau în considerare normele și procedurile conform cărora sunt emise certificările, sigiliile sau mărcile [articolul 43 alineatul (2) litera (c)].

28. Este necesară existența unui mecanism de certificare și a unor criterii de certificare pentru ca organismul de certificare să obțină acreditarea conform articolului 43. Un impact major asupra activității unui organism de certificare rezultă din domeniul de aplicare și tipul criteriilor de certificare, care afectează procedurile de certificare și viceversa. Criteriile specifice pot impune, de exemplu, metode de evaluare specifice, cum ar fi verificările la fața locului și revizuirea codurilor. Aceste proceduri sunt obligatorii pentru acreditare și sunt explicate în mod suplimentar în orientările privind acreditarea.

29. RGPD obligă organismul de certificare să transmită informații autorităților de supraveghere, în special cu privire la certificările individuale, iar aceste informații sunt necesare pentru a monitoriza aplicarea mecanismului de certificare [articolul 42 alineatul (7), articolul 43 alineatul (5), articolul 58 alineatul (2) litera (h)].

4 APROBAREA CRITERIILOR DE CERTIFICARE

30. Criteriile de certificare fac parte integrantă din orice mecanism de certificare. Prin urmare, RGPD prevede aprobarea criteriilor de certificare ale unui mecanism de certificare de către autoritatea de supraveghere competentă [articolul 42 alineatul (5) și articolul 43 alineatul (2) litera (b)]. Or, în cazul Sigiliului European privind Protecția Datelor, criteriile de certificare sunt aprobate de Comitetul European pentru Protecția Datelor [articolul 42 alineatul (5) și

articolul 70 alineatul (1) litera (o)]. Ambele posibilități de aprobare a criteriilor de certificare sunt explicate mai jos.

31. Comitetul European pentru Protecția Datelor recunoaște următoarele scopuri pentru aprobarea criteriilor de certificare:

    - reflectarea adecvată a cerințelor și a principiilor privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal prevăzută în Regulamentul (UE) 2016/679; și
    - contribuirea la aplicarea coerentă a RGPD.

32. Aprobarea se acordă cu condiția ca cerința prevăzută în RGPD ca mecanismul de certificare să permită operatorilor și persoanelor împuternicite de către operatori să demonstreze conformitatea cu RGPD să fie reflectată pe deplin în criteriile de certificare.

4.1 Aprobarea criteriilor de către autoritatea de supraveghere competentă

33. Criteriile de certificare trebuie să fie aprobate de către autoritatea de supraveghere competentă înaintea sau în timpul procesului de acreditare pentru organismul de certificare. De asemenea, aprobarea este necesară pentru sistemele sau seturile de criterii actualizate sau suplimentare prevăzute în ISO 17065 de către același organism de certificare, înainte ca acesta să utilizeze mecanismele de certificare modificate [articolul 42 alineatul (5) și articolul 43 alineatul (2) litera (b)]. Autoritățile de supraveghere tratează toate cererile de aprobare a criteriilor de certificare într-o manieră echitabilă și nediscriminatorie, conform procedurii disponibile public, care specifică ce condiții generale trebuie să fie îndeplinite și descrie procesul de aprobare.

34. Organismul de certificare poate să emită o certificare într-un anumit stat membru numai în conformitate cu criteriile aprobate de autoritatea de supraveghere din acel stat membru. Cu alte cuvinte, criteriile de certificare trebuie să fie aprobate de către autoritatea de supraveghere competentă din statul membru în care organismul de certificare intenționează să ofere certificare și să obțină acreditarea. A se vedea secțiunea de mai jos pentru sisteme de certificare la nivelul UE.

4.2 Aprobarea criteriilor de către Comitetul European pentru Protecția Datelor pentru Sigiliul European privind Protecția Datelor

35. De asemenea, organismul de certificare poate să emită o certificare în conformitate cu criteriile aprobate de Comitetul European pentru Protecția Datelor pentru un Sigiliu European privind Protecția Datelor. Criteriile de certificare aprobate de Comitetul European pentru Protecția Datelor conform articolului 63 pot rezulta într-un Sigiliu European privind Protecția Datelor [articolul 42 alineatul (5)]. În lumina convențiilor existente privind certificarea și acreditarea, Comitetul European pentru Protecția Datelor recunoaște că este de dorit să se evite fragmentarea pieței certificării în domeniul protecției datelor. Acesta observă că articolul 42 alineatul (1) prevede că statele membre, autoritățile de supraveghere,

Comitetul și Comisia încurajează instituirea mecanismelor de certificare, în special la nivelul Uniunii.

4.2.1 Cerere de aprobare

36. Cererea pentru aprobarea criteriilor conform articolului 42 alineatul (5) și articolului 70 alineatul (1) litera (o) de către Comitetul European pentru Protecția Datelor trebuie să fie depusă prin intermediul unei autorități de supraveghere competente și ar trebui să specifice intenția titularului sistemului, a candidatului sau a organismului de certificare acreditat de a oferi criteriile în cadrul unui mecanism de certificare adresat operatorilor și persoanelor împuternicite de către operatori din toate statele membre. Autoritatea de supraveghere competentă va pune proiectul la dispoziția Comitetului European pentru Protecția Datelor atunci când consideră că criteriile ar putea fi aprobate de Comitetul European pentru Protecția Datelor.

37. Instituția la care trebuie depusă cererea pentru aprobarea criteriilor se va alege în funcție de sediul titularilor sistemului de certificare sau al organismelor de certificare.

38. În cazul în care un organism de certificare depune o cerere, acest lucru ar avea loc în mod normal în cadrul procesului de solicitare a acreditării sau în cazul în care acesta este acreditat deja fie de către autoritatea de supraveghere competentă, fie de către organismul național de acreditare din statul său membru. În cazul în care organismul de certificare este acreditat deja pentru un mecanism de certificare conform RGPD, acest lucru poate contribui la simplificarea procesului de aprobare.

4.2.2 Criterii pentru Sigiliul European privind Protecția Datelor

39. Comitetul European pentru Protecția Datelor va coordona procesul de evaluare și va aproba criteriile pentru Sigiliul European privind Protecția Datelor astfel cum s-a solicitat. Evaluarea va aborda domenii precum: domeniul de aplicare al criteriilor și capacitatea de a servi ca certificare comună. În cazul în care criteriile sunt aprobate de Comitetul European pentru Protecția Datelor, se preconizează că autoritatea de supraveghere competentă pentru sediul din UE al organismului de certificare va fi cea care va soluționa plângerile cu privire la mecanism și va informa celelalte autorități de supraveghere. De asemenea, această autoritate de supraveghere este competentă să adopte măsuri împotriva organismului de certificare. Dacă este cazul, autoritatea de supraveghere competentă va notifica celelalte autorități de supraveghere și Comitetul European pentru Protecția Datelor.

40. Criteriile de certificare care vizează o certificare comună fac obiectul unor cereri la nivelul UE și ar trebui să prevadă un mecanism specific pentru abordarea acestor cereri. Mecanismele europene de certificare trebuie să fie destinate utilizării în toate statele membre. În temeiul articolului 42 alineatul (5), mecanismul pentru un Sigiliu European privind Protecția Datelor, precum și criteriile acestuia trebuie să fie adaptabile astfel încât să ia în considerare regulamentele naționale specifice sectorului, dacă este cazul, de exemplu, pentru prelucrarea datelor în școli, și să prevadă o aplicare la nivel european.

41. Exemplu: O școală internațională care oferă școlarizare persoanelor vizate din Uniune are sediul în statul membru „A”. Școala dorește să certifice procesul de înscrieri online printr-un sistem de certificare la nivelul UE, pentru a obține un Sigiliu European privind Protecția Datelor. Această școală dorește să solicite certificarea operațiunilor de prelucrare oferită de un organism de certificare cu sediul în statul membru „B” pe baza unui Sigiliu European privind Protecția Datelor. Criteriile pentru sigiliu, concepute și documentate în cadrul mecanismului relevant, trebuie să poată lua în considerare regulamentele pentru școli aplicabile în statul membru „A”. De asemenea, criteriile ar trebui să prevadă ca procesul de înscriere online al școlii să ofere informații și să ia în considerare cerințele aplicabile de protecție a datelor din statul membru în cauză, care pot fi diferite în alte state membre. Un exemplu îl constituie seturile de date cu caracter personal care trebuie să fie prezentate în scopul înscrierilor, cum ar fi notele sau rezultatele testelor din grădiniță, perioadele de păstrare diferite, colectarea sau prelucrarea datelor financiare sau biometrice, alte limitări ale prelucrării.

    - Criteriile la nivel înalt pentru aprobarea unui mecanism pentru Sigiliul European privind Protecția Datelor includ:
        - criteriile aprobate de Comitet;
        - aplicarea în cadrul jurisdicțiilor care reflectă locul în care există cerințe legale naționale adecvate și regulamente specifice sectorului;
        -
    - criterii armonizate care pot fi adaptate pentru a reflecta cerințele naționale;
        - descrierea mecanismului de certificare, specificând:
        - acordurile de certificare, care recunosc cerințele paneuropene;
        - procedurile pentru a asigura și a oferi soluții pentru diversitatea la nivel național și pentru a asigura faptul că sigiliul contribuie la demonstrarea conformității cu RGPD; și
        - limba rapoartelor adresate tuturor autorităților de supraveghere afectate.

42. De asemenea, anexa conține orientări privind criteriile pentru Sigiliul European privind Protecția Datelor.

4.2.3 Rolul acreditării

43. Astfel cum se observă la punctul 4.2.1, atunci când criteriile sunt identificate ca fiind adecvate pentru certificarea comună și au fost aprobate ca atare de către Comitet conform articolului 42 alineatul (5), organismele de certificare pot fi acreditate să efectueze certificarea în conformitate cu aceste criterii la nivelul Uniunii.

44. Sistemele care urmează să fie oferite doar în anumite state membre nu sunt candidate pentru sigiliile europene. Acreditarea pentru domeniul de aplicare al unui Sigiliu European

privind Protecția Datelor necesită acreditarea în statul membru în care își are sediul organismul de certificare ce intenționează să utilizeze sistemul în cauză, și anume care este responsabil pentru emiterea certificărilor și gestionarea activităților de certificare ale entităților și filialelor sale din alte state membre. În cazul în care alte sedii sau birouri gestionează și efectuează certificări în mod autonom, pentru fiecare dintre aceste sedii sau birouri va fi necesară o acreditare separată în statul membru în care se află acestea. Cu alte cuvinte, acreditarea este necesară numai în statul membru în care se află sediul organismului de certificare atunci când doar sediile emit certificate. În schimb, atunci când și alte sedii ale organismului de certificare emit certificate, aceste sedii trebuie, de asemenea, să fie acreditate.

45. Prin urmare, dacă un organism de certificare nu a fost acreditat să emită certificări conform Sigiliului European privind Protecția Datelor, atunci criteriile aprobate de Comitetul European pentru Protecția Datelor nu pot fi utilizate iar sigiliul nu poate fi oferit.

5 ELABORAREA CRITERIILOR DE CERTIFICARE

46. RGPD a instituit un cadru pentru elaborarea criteriilor de certificare. Întrucât cerințele fundamentale privind procedura de certificare sunt abordate în articolele 42 și 43, care prevăd, în același timp, criterii esențiale pentru procedurile de certificare, fundamentul pentru criteriile de certificare trebuie să provină din principiile și normele prevăzute în RGPD și să contribuie la asigurarea faptului că acestea sunt îndeplinite.

47. Elaborarea criteriilor de certificare ar trebui să se axeze pe posibilitatea de verificare, semnificația și caracterul adecvat al criteriilor de certificare pentru a demonstra conformitatea cu regulamentul. Criteriile de certificare ar trebui să fie formulate astfel încât să fie clare și inteligibile și să permită aplicarea practică.

48. La elaborarea criteriilor de certificare, se iau în considerare, dacă este cazul, următoarele aspecte legate de conformitate, în sprijinul evaluării operațiunii de prelucrare, printre altele:

- legalitatea prelucrării în conformitate cu articolul 6;
- principiile prelucrării datelor în conformitate cu articolul 5;
- drepturile persoanelor vizate în conformitate cu articolele 12-23;
- obligația de notificare a încălcării securității datelor cu caracter personal în conformitate cu articolul 33;
- obligația de a asigura protecția datelor începând cu momentul conceperii și în mod implicit, în conformitate cu articolul 25;
- dacă a fost efectuată o evaluare a impactului asupra protecției datelor, în conformitate cu articolul 35 alineatul (7) litera (d), dacă este cazul; și
- măsurile tehnice și organizatorice instituite în conformitate cu articolul 32.

49. Măsura în care aceste considerente sunt reflectate în criterii poate varia în funcție de domeniul de aplicare al certificării, care poate include tipul operațiunii/operațiunilor de prelucrare și domeniul (de exemplu, sectorul sănătății) de certificare.

5.1 Ce se poate certifica în conformitate cu RGPD?

50. Comitetul European pentru Protecția Datelor consideră că RGPD oferă un domeniul amplu de aplicare pentru ceea ce se poate certifica în conformitate cu RGPD, atât timp când se pune accentul pe sprijinirea demonstrării conformității cu acest regulament a operațiunilor de prelucrare efectuate de operatori și de persoanele împuternicite de către operatori [articolul 42 alineatul (1)].

51. La evaluarea unei operațiuni de prelucrare trebuie să se ia în considerare următoarele trei componente principale, dacă este cazul:

    1. datele cu caracter personal (domeniul de aplicare material al RGPD);
    2. sistemele tehnice - infrastructura, precum hardware-ul și software-ul, utilizate pentru prelucrarea datelor cu caracter personal; și
    3. procesele și procedurile legate de operațiunea/operațiunile de prelucrare.

52. Fiecare componentă utilizată în operațiunile de prelucrare trebuie să facă obiectul unei evaluări conform criteriilor stabilite. Pot avea influență cel puțin patru factori semnificativi diferiți: 1) organizarea și structura juridică a operatorului sau a persoanei împuternicite de către operator; 2) departamentul, mediul și persoanele implicate în operațiunea/operațiunile de prelucrare; 3) descrierea tehnică a elementelor care trebuie evaluate; și, în final, 4) infrastructura IT care sprijină operațiunea de prelucrare, inclusiv sistemele de operare, sistemele virtuale, bazele de date, sistemele de autentificare și de autorizare, routerele și firewall-urile, sistemele de stocare, infrastructura de comunicații sau accesul la internet și măsurile tehnice conexe.

53. Toate cele trei componente principale sunt relevante pentru elaborarea procedurilor și a criteriilor de certificare. În funcție de obiectul certificării, măsura în care acestea sunt luate în considerare poate varia. De exemplu, în unele cazuri, unele componente pot fi ignorate dacă se consideră că nu sunt relevante pentru obiectul certificării.

54. Pentru a aduce precizări suplimentare referitoare la ceea ce se poate certifica în conformitate cu RGPD, RGPD conține orientări suplimentare. Rezultă din articolul 42 alineatul (7) că certificările conform RGPD trebuie să fie emise numai pentru operatorii și persoanele împuternicite de către operatori ceea ce, de exemplu, exclude certificarea responsabililor cu protecția datelor. Articolul 43 alineatul (1) litera (b) face trimitere la ISO 17065 care prevede acreditarea organismelor de certificare ce evaluează conformitatea produselor, a serviciilor și a proceselor. O operațiune de prelucrare sau o serie de operațiuni poate rezulta într-un produs sau serviciu din terminologia ISO 17065 și astfel poate face obiectul certificării. De exemplu, prelucrarea datelor angajaților în scopul plății salariului sau al gestionării concediilor reprezintă o serie de operațiuni în sensul RGPD și poate rezulta într-un produs, proces sau serviciu din terminologia ISO.

55. Pe baza acestor considerente, Comitetul European pentru Protecția Datelor consideră că domeniul de aplicare al certificării conform RGPD este îndreptat către operațiunile de prelucrare sau seturile de operațiuni. Acestea pot cuprinde procesele de guvernanță în sensul măsurilor organizatorice, așadar ca părți integrante ale operațiunii de prelucrare (de exemplu, procesul de guvernanță instituit pentru soluționarea plângerilor ca parte a prelucrării datelor angajaților în scopul plății salariului).

56. Pentru a evalua conformitatea operațiunii de prelucrare cu criteriile de certificare, trebuie să se prevadă un caz de utilizare. De exemplu, conformitatea utilizării infrastructurii tehnice implementate în operațiunea de prelucrare depinde de categoriile de date pe care aceasta este concepută să le prelucreze. Măsurile organizatorice depind de categoriile și volumul de date și de infrastructura tehnică utilizată pentru prelucrare, ținând seama de natura, domeniul de aplicare, conținutul și scopurile prelucrării, precum și de riscurile privind drepturile și libertățile persoanelor vizate.

57. În plus, trebuie reținut faptul că aplicațiile IT pot să fie foarte diferite, chiar dacă servesc acelorași scopuri de prelucrare. Prin urmare, trebuie să se țină seama de acest lucru atunci când se definește domeniul de aplicare al mecanismelor de certificare și când se elaborează criteriile de certificare, și anume domeniul de aplicare al certificării și criteriile ar trebui să fie suficient de stricte încât să excludă aplicațiile IT concepute în mod diferit.

5.2 Stabilirea obiectului certificării

58. Domeniul de aplicare al unui mecanism de certificare trebuie să se distingă de obiect - denumit și obiectivul evaluării - în proiectele de certificare individuale din cadrul unui mecanism de certificare. Un mecanism de certificare își poate defini domeniul de aplicare fie în termeni generali, fie în legătură cu un tip sau un domeniu specific al operațiunilor de prelucrare și, astfel, poate să identifice deja obiectele certificării care intră în domeniul de aplicare al mecanismului de certificare (de exemplu, asigurarea stocării și a protecției datelor cu caracter personal conținute într-un seif digital). În orice moment, poate avea loc o evaluare fiabilă, semnificativă a conformității numai dacă obiectul individual al unui proiect de certificare este descris cu exactitate. Trebuie să se descrie în mod clar ce operațiuni de prelucrare sunt incluse în obiectul de certificare și apoi componentele principale, și anume datele, procesele și infrastructura tehnică ce vor fi evaluate și cele care nu vor fi evaluate. În acest sens, întotdeauna trebuie să fie luate în considerare și descrise interfețele cu alte procese. În mod clar, ceea ce nu se cunoaște nu poate face parte din evaluare și, astfel nu se poate certifica. În orice caz, obiectul individual al certificării trebuie să fie semnificativ cu privire la mesajul sau cererea transmisă cu privire la/prin certificare și nu ar trebui să inducă în eroare utilizatorul, clientul sau consumatorul.

59. [Exemplul 1]

    O bancă le oferă clienților săi un site web pentru servicii bancare electronice. În cadrul acestui serviciu, există posibilitatea de a efectua transferuri, de a cumpăra acțiuni, de a iniția ordine de plată programate și de a gestiona contul. În cadrul unui mecanism de certificare în domeniul protecției datelor, cu un domeniu de aplicare general, pe baza unor criterii generale, banca dorește să certifice următoarele:

a) conectarea securizată

Conectarea securizată este o operațiune de prelucrare care este ușor de înțeles de către utilizatorul final și care este relevantă din perspectiva protecției datelor, deoarece joacă un rol important în asigurarea securității datelor cu caracter personal implicate. Prin urmare, această operațiune de prelucrare este necesară pentru conectarea securizată și, astfel, poate constitui un obiectiv semnificativ al evaluării dacă certificatul specifică în mod clar că doar operațiunea de prelucrare a conectării este certificată.

b) Dezvoltarea web front-end

Deși dezvoltarea web front-end poate fi relevantă din perspectiva protecției datelor, aceasta nu este ușor de înțeles de către utilizatorul final și, prin urmare, nu poate fi un obiectiv semnificativ al evaluării. În plus, nu este clar pentru utilizator ce servicii de pe site-ul web și, astfel, ce operațiuni de prelucrare sunt acoperite de certificare.

c) Serviciile bancare electronice

Dezvoltarea web front-end împreună cu dezvoltarea back-end sunt operațiuni de prelucrare oferite în cadrul serviciului bancar electronic, care pot fi semnificative pentru utilizator. În acest context, ambele trebuie să fie incluse în obiectivul evaluării, în timp ce operațiunile de prelucrare care nu sunt legate în mod direct de prestarea serviciului bancar electronic, cum ar fi operațiunile de prelucrare în scopul prevenirii spălării banilor, pot fi excluse din obiectivul evaluării.

Cu toate acestea, serviciile bancare electronice oferite de bancă prin intermediul site-ului său web pot să includă, de asemenea, alte servicii care, în schimb, necesită propriile operațiuni de prelucrare. În acest context, alte servicii pot să includă, de exemplu, oferirea unui produs de asigurare. Deoarece acest serviciu suplimentar nu are legătură directă cu scopul de a oferi servicii bancare electronice, acesta poate fi exclus din obiectivul evaluării. Dacă acest serviciu suplimentar (asigurarea) este exclus din obiectivul evaluării, interfețele pentru acest serviciu integrate pe site-ul web fac parte din obiectivul evaluării și, prin urmare, trebuie să fie descrise pentru a se face o distincție clară între servicii. O astfel de descriere este necesară pentru a identifica și a evalua posibilele fluxuri de date dintre cele două servicii.

60. [Exemplul 2]

O bancă le oferă clienților săi un serviciu care le permite să regrupeze informațiile legate de diferite conturi și cărți de credit de la mai multe bănci (agregarea conturilor). Banca dorește să își certifice acest serviciu conform RGPD. Autoritatea de supraveghere competentă a aprobat o serie specifică de criterii de certificare care se axează pe acest tip de activitate. Domeniul de aplicare al mecanismului de certificare abordează doar următoarele aspecte legate de conformitate:

- autentificarea utilizatorului; și
- mijloacele acceptabile de a obține datele care urmează să fie agregate de la alte bănci/servicii.

Deoarece domeniul de aplicare al acestui mecanism de certificare definește în sine obiectivul evaluării, nu este posibil să se restrângă obiectivul evaluării în mod semnificativ conform domeniului de aplicare propus și să se certifice doar caracteristici specifice sau o singură activitate de prelucrare. În acest scenariu, un obiectiv al evaluării trebuie să fie egal cu un domeniu de aplicare specific.

5.3 Metodele și metodologia de evaluare

61. O evaluare a conformității pentru a contribui la demonstrarea conformității operațiunilor de prelucrare necesită identificarea și stabilirea metodelor și a metodologiei de evaluare. Contează dacă informațiile pentru evaluare sunt colectate doar din documentație (care nu ar fi suficientă în sine) sau dacă acestea sunt colectate în mod activ la fața locului sau prin acces direct sau indirect. Modul în care sunt colectate informațiile are consecințe pentru semnificația certificării și, prin urmare, ar trebui să fie definit și descris.

    Procedurile pentru emiterea și revizuirea periodică a certificărilor ar trebui să includă specificații pentru a identifica nivelul adecvat de evaluare (profunzime sau granularitate) pentru îndeplinirea criteriilor de certificare și ar trebui să includă:

    - furnizarea de informații cu privire la metodele de evaluare aplicate și constatările colectate, de exemplu în timpul auditurilor la fața locului sau din documente, precum și specificarea acestora;
    - furnizarea de metode de evaluare axate pe operațiunile de prelucrare (date, sisteme, procese), precum și a scopului prelucrării;
    - asigurarea identificării categoriilor de date, a necesităților în materie de protecție și a implicării sau a neimplicării persoanelor împuternicite de către operatori sau a terțelor părți;
    - asigurarea identificării rolurilor și a existenței unui mecanism de control al accesului, definit în jurul rolurilor și al responsabilităților.

62. Profunzimea evaluării are impact asupra semnificației și valorii certificării. Prin reducerea profunzimii evaluării în scopuri pragmatice sau pentru a reduce costurile, semnificația certificării în domeniul protecției datelor se va diminua. Pe de altă parte, deciziile privind granularitatea evaluării pot depăși capacitățile financiare ale solicitantului și adesea și capacitatea evaluatorilor și a auditorilor. În scopul demonstrării conformității, este posibil să nu fie esențial întotdeauna să se ajungă la o analiză extrem de detaliată a sistemelor IT utilizate pentru ca aceasta să rămână semnificativă.

5.4 Documentarea evaluării

63. Documentarea certificării ar trebui să fie amănunțită și cuprinzătoare. Lipsa documentării înseamnă că nu poate avea loc o evaluare adecvată. Funcția esențială a documentării certificării este aceea că asigură transparență în procesul de evaluare în cadrul mecanismului de certificare. Documentarea oferă răspunsuri la întrebări referitoare la cerințele stabilite de lege. Mecanismele de certificare ar trebui să prevadă o metodologie standardizată de

documentare. După aceea, evaluarea va permite compararea documentării certificării cu starea actuală la fața locului și cu criteriile de certificare.

64. O documentare cuprinzătoare a ceea ce a fost certificat și a metodologiei utilizate servește la asigurarea transparenței. Conform articolului 43 alineatul (2) litera (c), mecanismele de certificare ar trebui să stabilească proceduri care să permită revizuirea certificărilor. Pentru a permite autorității de supraveghere să evalueze dacă și în ce măsură se poate recunoaște certificarea în cadrul investigațiilor oficiale, o documentare detaliată poate fi mijlocul cel mai adecvat de comunicare. Prin urmare, documentarea efectuată în timpul evaluării ar trebui să se concentreze pe trei aspecte principale:

    - consecvența și coerența metodelor de evaluare executate;
    - metodele de evaluare orientate către demonstrarea conformității obiectului de certificare cu criteriile de certificare și, astfel, cu regulamentul; și
    - dacă rezultatele evaluării au fost validate de un organism de certificare independent și imparțial.

5.5 Documentarea rezultatelor

65. Considerentul 100 oferă informații privind obiectivele urmărite prin introducerea certificării.

„Pentru a se îmbunătăți transparența și conformitatea cu prezentul regulament, ar trebui să se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.”

66. Pentru a se îmbunătăți transparența, documentarea și comunicarea rezultatelor joacă un rol important. Organismele de certificare care utilizează mecanismele de certificare, sigiliile sau mărcile orientate către persoanele vizate (în rolurile lor de consumatori sau clienți) ar trebui să furnizeze informații ușor accesibile, inteligibile și semnificative cu privire la operațiunea/operațiunile de prelucrare certificată/certificate. Informațiile publice ar trebui să includă cel puțin:

    - descrierea obiectivului evaluării;
    - trimiteri la criteriile aprobate, aplicate obiectivului specific al evaluării;
    - metodologia pentru evaluarea criteriilor (evaluare la fața locului, documentare etc.); și
    - durata valabilității certificatului; și
    - ar trebui să permită comparabilitatea rezultatelor pentru autoritățile de supraveghere și public.

6 ORIENTĂRI PENTRU DEFINIREA CRITERIILOR DE CERTIFICARE

67. Criteriile de certificare fac parte integrantă din mecanismul de certificare. Procedura de certificare include cerințele privind modul și măsura în care are loc evaluarea, cine efectuează evaluarea, precum și granularitatea evaluării care are loc în cadrul proiectelor de certificare individuale referitoare la un obiect sau obiectiv specific al evaluării. Criteriile de certificare prevăd cerințele nominale în conformitate cu care este evaluată operațiunea efectivă de prelucrare definită în obiectivul evaluării. Aceste orientări pentru definirea criteriilor de certificare oferă consiliere generală care va facilita evaluarea criteriilor de certificare în scopul aprobării.

    - La aprobarea sau definirea criteriilor de certificare ar trebui să se țină seama de următoarele considerente generale. Criteriile de certificare ar trebui:
    - să fie uniforme și verificabile;
    - să poată fi auditate pentru a facilita evaluarea operațiunilor de prelucrare conform RGPD, specificând, în special, obiectivele și orientările în materie de punere în aplicare pentru realizarea acelor obiective;
    - să fie relevante cu privire la publicul vizat [de exemplu, B2B și business-to-customer (B2C)];
    - să ia în considerare și, dacă este cazul, să fie interoperabile cu alte standarde (cum ar fi standardele ISO, standardele de la nivel național); și
    - să fie flexibile și adaptabile pentru a fi aplicate unor tipuri și dimensiuni diferite de organizații, inclusiv microîntreprinderilor și întreprinderilor mici și mijlocii în conformitate cu articolul 42 alineatul (1) și pentru abordarea bazată pe riscuri în conformitate cu considerentul (77).

68. O întreprindere locală mică, precum un comerciant cu amănuntul, va desfășura de obicei operațiuni de prelucrare mai puțin complexe decât un comerciant cu amănuntul multinațional mare. Deși cerințele pentru legalitatea operațiunilor de prelucrare sunt aceleași, trebuie să se țină seama de domeniul de aplicare al prelucrării datelor și de complexitatea acesteia; prin urmare, este necesar ca mecanismele de certificare și criteriile acestora să fie adaptabile în funcție de activitatea de prelucrare în cauză.

6.1 Standardele existente

69. Organismele de certificare vor trebui să ia în considerare modul în care criteriile specifice țin seama de instrumentele relevante existente, cum ar fi codurile de conduită, de standardele tehnice sau de inițiativele de reglementare și legale naționale. În mod ideal, criteriile vor fi interoperabile cu standardele existente, care pot ajuta un operator sau o persoană împuternicită de către operator să își îndeplinească obligațiile conform RGPD. Cu toate acestea, deși standardele din industrie se axează adesea pe protecția și securitatea organizației împotriva amenințărilor, RGPD are drept scop protejarea drepturilor

fundamentale ale persoanelor fizice. Această perspectivă diferită trebuie să fie luată în considerare la elaborarea criteriilor sau la aprobarea criteriilor sau a mecanismelor de certificare pe baza standardelor din industrie.

6.2 Definirea criteriilor

70. Criteriile de certificare trebuie să corespundă declarației de certificare (mesaj sau cerere) a unui mecanism sau sistem de certificare și să corespundă așteptărilor pe care acesta le generează. Denumirea unui mecanism de certificare poate să identifice deja domeniul de aplicare și va avea consecințe pentru stabilirea criteriilor.

71. [Exemplul 3]

    Un mecanism denumit „HealthPrivacyMark” ar trebui să își limiteze domeniul de aplicare la sectorul sănătății. Denumirea sigiliului generează așteptarea că cerințele privind protecția datelor în legătură cu datele medicale au fost examinate. În consecință, criteriile acestui mecanism trebuie să fie adecvate pentru a evalua cerințele privind protecția datelor în acest sector.

72. [Exemplul 4]

    Un mecanism care se referă la certificarea operațiunilor de prelucrare care cuprinde sistemele de guvernanță în ceea ce privește prelucrarea datelor ar trebui să identifice criteriile care permit recunoașterea și evaluarea proceselor de guvernanță și măsurile sale tehnice și organizatorice de sprijin.

73. [Exemplul 5]

    Criteriile pentru un mecanism care se referă la cloud computing trebuie să ia în considerare cerințele tehnice speciale necesare pentru utilizarea serviciilor cloud. De exemplu, dacă serverele se află în afara UE, criteriile trebuie să ia în considerare condițiile stabilite la capitolul V din RGPD cu privire la transferurile de date către țări terțe.

74. Criteriile concepute pentru a fi adecvate diferitelor obiective ale evaluării din diferite sectoare și/sau state membre ar trebui: să permită aplicarea pentru diferite scenarii; să permită identificarea măsurilor adecvate pentru a fi adecvate operațiunilor de prelucrare mici, medii sau mari și să reflecte riscurile de probabilitate și gravitate diferite privind drepturile și libertățile persoanelor fizice în conformitate cu RGPD. Prin urmare, procedurile de certificare (de exemplu, pentru documentare, testare sau metoda și profunzimea evaluării) care completează criteriile trebuie să răspundă acestor nevoi, să permită și să dispună de norme, de exemplu pentru aplicarea criteriilor relevante în proiectele de certificare individuale. Criteriile trebuie să faciliteze evaluarea furnizării unor garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate.

6.3 Durata de viață a criteriilor de certificare

75. Chiar dacă criteriile de certificare trebuie să fie fiabile în timp, acestea nu ar trebui să fie greu de schimbat. Criteriile de certificare fac obiectul revizuirii, de exemplu în cazul în care:

    - cadrul juridic este modificat;
    - termenele și dispozițiile sunt interpretate prin hotărâri ale Curții de Justiție a Uniunii Europene; sau
    - stadiul actual al tehnologiei a evoluat.

Pentru Comitetul European pentru Protecția Datelor,

Președinte

(Andrea Jelinek)

ANEXA 1: SARCINILE ȘI COMPETENȚELE AUTORITĂȚILOR DE SUPRAVEGHERE ÎN LEGĂTURĂ CU CERTIFICAREA ÎN CONFORMITATE CU RGPD

	Dispoziții	Cerințe
Sarcini	Articolul 43 alineatul (6)	Obligă autoritatea de supraveghere să publice criteriile menționate la articolul 42 alineatul (5) într-o formă ușor de accesat și să le transmită Comitetului.
	Articolul 57 alineatul (1) litera (n)	Obligă autoritatea de supraveghere să aprobe criteriile de certificare conform articolului 42 alineatul (5).
	Articolul 57 alineatul (1) litera (o)	Prevede că, acolo unde este cazul (și anume, în cazul în care emite certificarea), aceasta să efectueze o revizuire periodică a certificărilor acordate, în conformitate cu articolul 42 alineatul (7).
	Articolul 64 alineatul (1) litera (c)	Obligă autoritatea de supraveghere să comunice proiectul de decizie Comitetului, atunci când vizează aprobarea criteriilor pentru certificare menționate la articolul 42 alineatul (5).
Competențe	Articolul 58 alineatul (1) litera (c)	Prevede că autoritatea de supraveghere are competența de a efectua revizuiri ale certificării în temeiul articolului 42 alineatul (7).
	Articolul 58 alineatul (2) litera (h)	Prevede că autoritatea de supraveghere are competența de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare sau de a obliga organismul de certificare să nu elibereze o certificare.
	Articolul 58 alineatul (3) litera (e)	Prevede că autoritatea de supraveghere are competența de a acredita organismele de certificare
	Articolul 58 alineatul (3) litera (f)	Prevede că autoritatea de supraveghere are competența de a emite certificări și de a aproba criterii de certificare.

ANEXA 2:

1 INTRODUCERE

Anexa 2 oferă orientări pentru revizuirea și evaluarea criteriilor de certificare în conformitate cu articolul 42 alineatul (5). Aceasta identifică temele pe care autoritățile de supraveghere a protecției datelor și Comitetul European pentru Protecția Datelor le vor lua în considerare și le vor aplica în scopul aprobării criteriilor de certificare ale unui mecanism de certificare. Întrebările ar trebui avute în vedere de către organismele de certificare și titularii sistemelor care doresc să elaboreze și să prezinte criterii spre aprobare. Lista nu este exhaustivă, ci prezintă temele minime care trebuie avute în vedere. Nu vor fi aplicabile toate întrebările; acestea ar trebui însă avute în vedere la elaborarea criteriilor și ar putea fi necesar să se prezinte motivele pentru care criteriile nu acoperă anumite aspecte. Unele întrebări apar de mai multe ori, întrucât sunt formulate din perspective diferite. Prezentele orientări trebuie avute în vedere în conformitate cu cerințele juridice prevăzute de RGPD și, după caz, de legislația națională.

2 DOMENIUL DE APLICARE AL MECANISMULUI DE CERTIFICARE ȘI OBIECTIVUL EVALUĂRII

a. Domeniul de aplicare al mecanismului de certificare (pentru care vor fi utilizate criteriile privind protecția datelor) este clar descris?

b. Domeniul de aplicare al mecanismului de certificare este semnificativ pentru publicul țintă și neechivoc?

- *Exemplu: Un „sigiliu de societate de încredere” sugerează că au fost auditate activitățile de prelucrare ale întregii întreprinderi, deși în realitate numai anumite operațiuni de prelucrare, de exemplu procesul de plată online, fac obiectul certificării. Prin urmare, domeniul de aplicare este înșelător.*

c. Domeniul de aplicare al mecanismului de certificare reflectă toate aspectele relevante ale operațiunilor de prelucrare?

- *Exemplu: O „marcă privind confidențialitatea în domeniul sănătății” trebuie să includă toate datele de evaluare referitoare la sănătate pentru a îndeplini cerințele în conformitate cu articolul 9.*

d. Domeniul de aplicare al mecanismului de certificare permite o certificare semnificativă a protecției datelor având în vedere natura, conținutul și nivelul de risc al operațiunilor de prelucrare aferente?

- *Exemplu: Domeniul de aplicare al mecanismului de certificare nu este semnificativ pentru persoanele vizate în cazul în care acesta acoperă numai anumite aspecte ale operațiunilor de prelucrare, cum ar fi colectarea datelor, dar nu și alte operațiuni de prelucrare, cum ar fi prelucrarea în scopul creării de profiluri de publicitate sau gestionarea drepturilor persoanelor vizate.*

e. Domeniul de aplicare al mecanismului de certificare acoperă prelucrarea datelor cu caracter personal în țara din care provine cererea sau acoperă prelucrarea și/sau transferurile transfrontaliere?

f. Criteriile de certificare descriu în mod suficient modul în care trebuie definit obiectivul evaluării?

- *Exemplu: Un „sigiliu privind confidențialitatea" al cărui domeniu de aplicare general cere numai „specificarea prelucrării care face obiectul certificării" nu ar oferi orientări suficient de clare privind modul de a stabili și de a descrie obiectivul evaluării.*
- *Exemplu: În cazul unui domeniu de aplicare (specific), „sigiliul privind confidențialitatea pentru seifuri" referitor la stocarea securizată, ar trebui descris în mod detaliat care sunt cerințele pentru a îndeplini criteriile acestui domeniu de aplicare, de exemplu definirea seifului, cerințele sistemului, măsurile tehnice și organizatorice obligatorii. În acest caz, domeniul de aplicare poate defini în mod clar obiectivul evaluării.*

(1) Criteriile prevăd ca obiectivul evaluării să includă identificarea tuturor operațiunilor de prelucrare relevante, ilustrarea fluxurilor de date și o definire a sferei de aplicare a obiectivului evaluării?

- *Exemplu: Un mecanism de certificare oferă certificarea operațiunilor de prelucrare efectuate de operatori în temeiul RGPD fără a aduce precizări suplimentare privind sfera de aplicare (domeniul de aplicare general). Criteriile aplicate de mecanism prevăd ca operatorul solicitant să stabilească operațiunea de prelucrare vizată (obiectivul evaluării) din punctul de vedere al tipurilor de date, al sistemelor și al proceselor utilizate.*

(2) Criteriile prevăd ca solicitantul să precizeze când începe și când se încheie prelucrarea care face obiectul evaluării? Criteriile prevăd ca obiectivul evaluării să includă interfețele atunci când operațiunile de prelucrare interdependente nu sunt incluse ca parte a obiectivului evaluării? Acest lucru este justificat în mod satisfăcător?

- *Exemplu: Un obiectiv al evaluării care descrie în detaliu operațiunile de prelucrare ale unui serviciu oferit online, inclusiv înregistrarea utilizatorilor, furnizarea serviciilor, facturarea, înregistrarea adreselor IP, interfețele pentru utilizatori și părți terțe, dar nu și locul în care se află serverele (deși descrie acordurile privind procesarea și măsurile tehnice și organizatorice).*

g. Criteriile garantează că obiectivele (individuale ale) evaluării pot fi înțelese de publicul-țintă, inclusiv de persoanele vizate, după caz?

3 CERINȚE GENERALE

a. Sunt identificați, explicați și descriși toți termenii relevanți utilizați în catalogul de criterii (și anume, setul complet de criterii de certificare)?

b. Sunt identificate toate referințele normative?

c. Criteriile includ definirea responsabilităților, a procedurilor și a prelucrării în materie de protecție a datelor care sunt acoperite de domeniul de aplicare al mecanismului de certificare?

4 OPERAȚIUNILE DE PRELUCRARE, ARTICOLUL 42 ALINEATUL (1)

În ceea ce privește domeniul de aplicare al mecanismului de certificare (general sau specific), criteriile abordează toate componentele relevante ale operațiunilor de prelucrare (date, sisteme și procese)?

a. În ceea ce privește obiectivul evaluării, criteriile prevăd identificarea temeiurilor juridice valabile pentru prelucrare?

b. În ceea ce privește obiectivul evaluării, criteriile recunosc etapele relevante ale prelucrării și întregul ciclu de viață al datelor, inclusiv ștergerea și/sau anonimizarea?

c. În ceea ce privește obiectivul evaluării, criteriile prevăd portabilitatea datelor?

d. În ceea ce privește obiectivul evaluării, criteriile permit identificarea și luarea în considerare a tipurilor speciale de operațiuni de prelucrare, de exemplu procesul decizional automatizat sau crearea de profiluri?

e. În ceea ce privește obiectivul evaluării, criteriile permit identificarea categoriilor speciale de date?

f. Criteriile permit și prevăd evaluarea riscului asociat operațiunilor de prelucrare individuale și a necesității de a proteja drepturile și libertățile persoanelor vizate?

g. Criteriile permit și prevăd luarea în considerare în mod corespunzător a riscurilor la adresa drepturilor și libertăților persoanelor fizice?

…

5 LEGALITATEA PRELUCRĂRII

a. Criteriile prevăd verificarea legalității prelucrării pentru operațiunile de prelucrare individuale în ceea ce privește scopul și necesitatea prelucrării?

b. Criteriile impun verificarea tuturor cerințelor unui temei juridic pentru operațiunile de prelucrare individuală?

6 PRINCIPII, ARTICOLUL 5

a. Criteriile abordează în mod adecvat toate principiile de protecție a datelor în conformitate cu articolul 5?

b. Criteriile prevăd demonstrarea reducerii la minimum a datelor pentru fiecare obiectiv individual al evaluării?

…

7 OBLIGAȚIILE GENERALE ALE OPERATORILOR ȘI ALE PERSOANELOR ÎMPUTERNICITE DE CĂTRE OPERATORI

a. Criteriile prevăd demonstrarea existenței unor acorduri contractuale între operatori și persoanele împuternicite de către aceștia?

b. Acordurile dintre operatori și persoanele împuternicite de aceștia sunt supuse evaluării?

c. Criteriile reflectă obligațiile operatorului în conformitate cu capitolul IV?

d. Criteriile prevăd prezentarea de dovezi cu privire la revizuirea și actualizarea măsurilor tehnice și organizatorice luate de operator în conformitate cu articolul 24 alineatul (1)?

e. Criteriile verifică dacă organizația a evaluat necesitatea de a numi un responsabil cu protecția datelor, astfel cum se prevede la articolul 37? Dacă este cazul, responsabilul cu protecția datelor îndeplinește cerințele de la articolele 37-39?

f. Criteriile verifică dacă este prevăzută obligația de a păstra evidențe ale activităților de prelucrare în conformitate cu articolul 30 alineatul (5) și dacă acestea îndeplinesc cerințele de la articolul 30?

8 DREPTURILE PERSOANELOR VIZATE

a. Criteriile abordează în mod adecvat dreptul persoanei vizate la informare și prevăd luarea de măsuri în acest sens?

b. Criteriile prevăd ca persoanele vizate să beneficieze de un acces adecvat sau chiar mai extins la datele lor, inclusiv în ceea ce privește portabilitatea datelor?

c. Criteriile prevăd adoptarea de măsuri care să ofere posibilitatea de a interveni în operațiunile de prelucrare pentru a asigura respectarea drepturilor persoanelor vizate și pentru a permite corectarea, ștergerea sau restricționarea?

…

9 RISCURI PENTRU DREPTURILE ȘI LIBERTĂȚILE PERSOANELOR FIZICE

a. Criteriile permit și prevăd evaluarea riscului la adresa drepturilor și libertăților persoanelor fizice?

b. Criteriile oferă sau prevăd o metodologie recunoscută de evaluare a riscurilor? Dacă este cazul, aceasta este proporțională?

c. Criteriile permit și prevăd evaluarea impactului operațiunilor de prelucrare avute în vedere la adresa drepturilor și libertăților persoanelor fizice?

d. Criteriile prevăd consultarea prealabilă cu privire la riscurile rămase care nu au putut fi atenuate, pe baza rezultatelor evaluării impactului asupra protecției datelor?

10 MĂSURI TEHNICE ȘI ORGANIZATORICE CARE GARANTEAZĂ PROTECȚIA

a. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice care să asigure confidențialitatea operațiunilor de prelucrare?

b. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice care să asigure integritatea operațiunilor de prelucrare?

c. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice care să asigure disponibilitatea operațiunilor de prelucrare?

d. Criteriile prevăd aplicarea unor măsuri care să asigure transparența operațiunilor de prelucrare în ceea ce privește:

e. responsabilitatea?

f. drepturile persoanelor vizate?

g. evaluarea operațiunilor de prelucrare individuale, de exemplu pentru transparența algoritmică?

h. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice care garantează respectarea drepturilor persoanelor vizate, de exemplu capacitatea de a furniza informații sau portabilitatea datelor?

i. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice care asigură capacitatea de a interveni în operațiunile de prelucrare pentru a asigura respectarea drepturilor persoanelor vizate și pentru a permite corectarea, ștergerea sau restricționarea?

j. Criteriile prevăd aplicarea unor măsuri care asigură capacitatea de a interveni în operațiunile de prelucrare pentru a corecta sau a verifica sistemul sau procesul?

k. Criteriile prevăd aplicarea unor măsuri tehnice și organizatorice pentru a asigura reducerea la minimum a datelor, de exemplu disocierea sau separarea datelor de persoana vizată, anonimizarea sau pseudonimizarea sau izolarea sistemelor de date?

l. Criteriile prevăd măsuri tehnice pentru a pune în aplicare protecția implicită a datelor?

m. Criteriile prevăd măsuri tehnice și organizatorice pentru a pune în aplicare protecția datelor începând cu momentul conceperii, de exemplu un sistem de gestionare a protecției datelor care să demonstreze, să informeze, să controleze și să asigure respectarea cerințelor privind protecția datelor?

n. Criteriile prevăd măsuri tehnice și organizatorice pentru a asigura formarea și sensibilizarea periodică a personalului care are acces permanent sau regulat la datele cu caracter personal?

o. Criteriile prevăd revizuirea măsurilor?

p. Criteriile prevăd autoevaluarea/auditul intern?

q. Criteriile prevăd luarea unor măsuri pentru a se asigura faptul că obligațiile de notificare a încălcării securității datelor cu caracter personal sunt îndeplinite la timp și în mod corespunzător?

r. Criteriile prevăd existența și verificarea procedurilor de gestionare a incidentelor?

s. Criteriile prevăd monitorizarea aspectelor în evoluție legate de confidențialitate și de tehnologie, precum și actualizarea sistemului atunci când este necesar?

…

11 ALTE CARACTERISTICI SPECIALE FAVORABILE PROTECȚIEI DATELOR

a. Criteriile prevăd punerea în aplicare a unor tehnici de consolidare a protecției datelor? Aceasta ar putea include criterii privind consolidarea protecției datelor prin eliminarea sau reducerea datelor cu caracter personal și/sau a riscului pentru protecția datelor.

- *Exemplu: Criteriile care prevăd o capacitate consolidată de disociere prin intermediul unei gestionări a identității axate pe utilizator, precum mecanismele ABC (attribute-based credentials), în locul gestionării identității axate pe organizație, ar reflecta o tehnică de consolidare a protecției datelor.*

b. Criteriile prevăd punerea în aplicare a unor mecanisme consolidate de control de către persoanele vizate, care să faciliteze autodeterminarea și libertatea de alegere?

…

12 CRITERII ÎN SCOPUL DE A DEMONSTRA EXISTENȚA UNOR GARANȚII ADECVATE PENTRU TRANSFERUL DE DATE CU CARACTER PERSONAL

Criteriile vor fi abordate în viitoarele orientări privind articolul 42 alineatul (2).

13 CRITERII SUPLIMENTARE PENTRU UN SIGILIU EUROPEAN PRIVIND PROTECȚIA DATELOR

a. Criteriile au în vedere acoperirea tuturor statelor membre?

b. Criteriile permit să se ia în considerare legislația sau scenariile din statele membre în materie de protecție a datelor?

c. Criteriile prevăd evaluarea obiectivului individual al evaluării în ceea ce privește dispozițiile specifice sectorului ale legislației din statele membre în materie de protecție a datelor?

d. Criteriile prevăd ca operatorul sau persoana împuternicită de către operator să le furnizeze persoanelor vizate și părților interesate informații în limbile statelor membre privind

e. Prelucrarea/obiectivele evaluării?

f. Documentația prelucrării/obiectivului evaluării?

g. Rezultatele evaluării?

…

14 EVALUAREA GENERALĂ A CRITERIILOR

a. Criteriile acoperă în întregime domeniul de aplicare al mecanismului de certificare (sunt cuprinzătoare), astfel încât garanțiile oferite să fie suficiente pentru a se putea avea încredere în certificare?

- *Exemplu: În cazul în care mecanismul de certificare se referă la operațiuni de prelucrare în domeniul sănătății, ar trebui să se garanteze un nivel ridicat de protecție a datelor prin definirea unor criterii care să asigure, de exemplu, o evaluare aprofundată și aplicarea principiilor de confidențialitate începând cu momentul conceperii și în mod implicit.*

b. Criteriile sunt proporționale cu dimensiunea operațiunii de prelucrare care face obiectul mecanismului de certificare, cu sensibilitatea informațiilor și cu riscul asociat prelucrării?

c. Se estimează că aceste criterii vor îmbunătăți respectarea protecției datelor de către operatori și persoanele împuternicite de aceștia?

d. Persoanele vizate vor beneficia de o consolidare a drepturilor lor de informare, inclusiv faptul că li se vor explica rezultatele dorite?