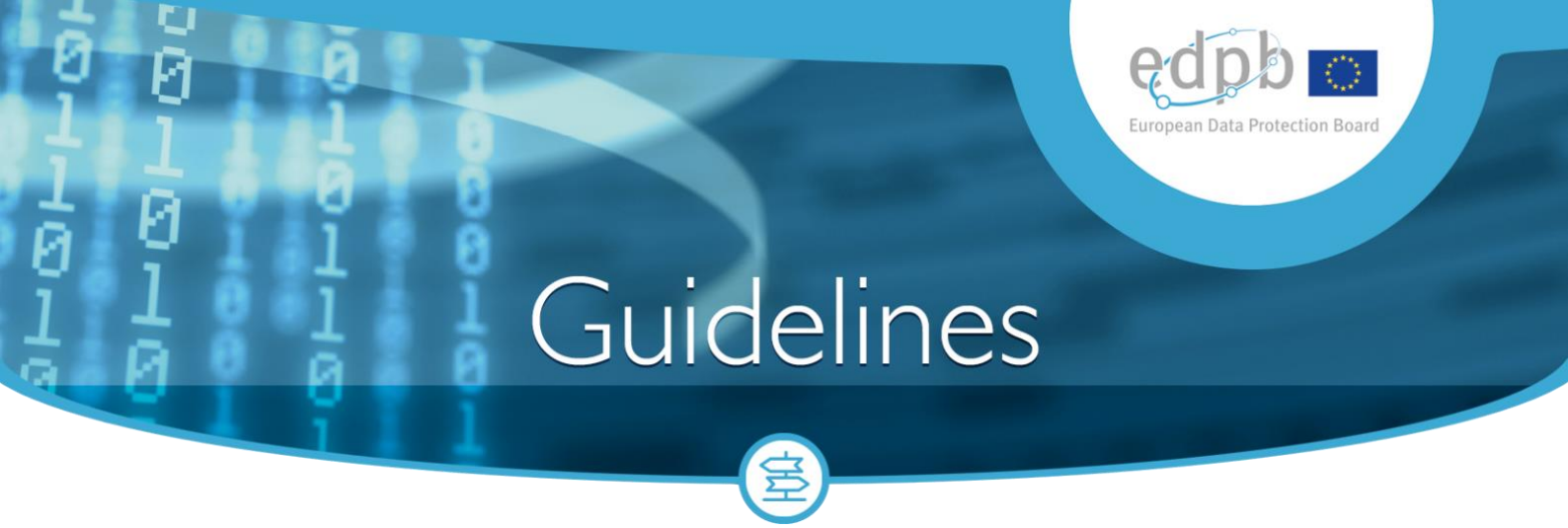

Orientări

Orientările nr. 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor (2016/679)

Versiunea 3.0

4 iunie 2019

Adoptat

Istoricul versiunilor

Versiunea 3.0	4 iunie 2019	Includerea anexei 1 (versiunea 2.0 a anexei 1, adoptată la 4 iunie 2019, ulterior consultării publice)
Versiunea 2.0	4 decembrie 2018	Adoptarea orientărilor în urma consultării publice – În aceeași zi a fost adoptată anexa 1 (versiunea 1.0) în vederea consultării publice
Versiunea 1.0	6 februarie 2018	Adoptarea orientărilor de către Grupul de lucru „Articolul 29” (versiunea pentru consultarea publică). Această versiune a fost susținută de Comitetul european pentru protecția datelor la data de 25 mai 2018

Cuprins

Comitetul European pentru Protecția Datelor,

Având în vedere articolul 70 alineatul (1) litera (e) din Regulamentul 2016/679/UE 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,

După analiza rezultatelor consultării publice referitoare la orientări care a avut loc în februarie 2018 și la anexă care a avut loc în perioada 14 decembrie 2018 – 1 februarie 2019, în conformitate cu articolul 70 alineatul (4) din RGPD,

ADOPTĂ URMĂTOARELE ORIENTĂRI

1 INTRODUCERE

1. Regulamentul General privind Protecția Datelor [Regulamentul (UE) 2016/679] (denumit în continuare „RGPD"), care intră în vigoare la 25 mai 2018, asigură un cadru modernizat, responsabil și bazat pe respectarea drepturilor fundamentale în domeniul protecției datelor în Europa. O serie de măsuri menite să faciliteze respectarea dispozițiilor RGPD sunt esențiale pentru acest nou cadru. Acestea includ cerințe obligatorii în circumstanțe specifice (inclusiv numirea responsabililor cu protecția datelor și efectuarea de evaluări ale impactului asupra protecției datelor), precum și măsuri voluntare, cum ar fi codurile de conduită și mecanismele de certificare.

2. În cadrul instituirii mecanismelor de certificare și a sigiliilor și mărcilor din domeniul protecției datelor, articolul 43 alineatul (1) din RGPD impune statelor membre să se asigure că organismele de certificare care emit certificarea în temeiul articolului 42 alineatul (1) sunt acreditate fie de autoritatea de supraveghere competentă, fie de organismul național de acreditare, fie de ambele entități. Dacă acreditarea este efectuată de organismul național de acreditare în conformitate cu ISO/IEC 17065/2012, cerințele suplimentare stabilite de autoritatea de supraveghere competentă trebuie, de asemenea, aplicate.

3. Mecanismele de certificare pertinente pot îmbunătăți conformitatea cu RGPD și transparența pentru persoanele vizate și în relațiile *business-to-business* (B2B), de exemplu între operatori și persoanele împuternicite de către operatori. Operatorii și persoanele împuternicite de către operatori vor beneficia de un certificat emis de o parte terță independentă, cu scopul de a demonstra conformitatea operațiunilor lor de prelucrare[1].

[1] Considerentul 100 din RGPD prevede că instituirea mecanismelor de certificare poate îmbunătăți transparența și conformitatea cu regulamentul și poate permite persoanelor vizate să evalueze nivelul de protecție a datelor aferent produselor și serviciilor relevante.

4. În acest context, Comitetul European pentru Protecția Datelor recunoaște că este necesar să ofere orientări cu privire la acreditare. Valoarea aparte și scopul acreditării constau în faptul că oferă o declarație oficială privind competența organismelor de certificare, care permite generarea încrederii în mecanismul de certificare.

5. Scopul orientărilor este de a oferi îndrumări privind interpretarea și punerea în aplicare a dispozițiilor articolului 43 din RGPD. În special, acestea au scopul de a ajuta statele membre, autoritățile de supraveghere și organismele naționale de acreditare să instituie o bază de referință coerentă și armonizată pentru acreditarea organismelor de certificare care emit certificarea în conformitate cu RGPD.

2 DOMENIUL DE APLICARE AL ORIENTĂRILOR

6. Prezentele orientări:

- stabilește scopul acreditării în contextul RGPD;
- explică căile disponibile pentru acreditarea organismelor de certificare în conformitate cu articolul 43 alineatul (1) și identifică aspectele-cheie care trebuie luate în considerare;
- oferă un cadru pentru stabilirea unor cerințe suplimentare de acreditare atunci când acreditarea este gestionată de organismul național de acreditare; și
- oferă un cadru pentru stabilirea cerințelor de acreditare, atunci când acreditarea este gestionată de autoritatea de supraveghere.

7. Orientările nu constituie un manual de procedură pentru acreditarea organismelor de certificare în conformitate cu RGPD. Nu elaborează un nou standard tehnic pentru acreditarea organismelor de certificare în scopul RGPD.

8. Orientările se adresează:

- statelor membre care trebuie să se asigure că organismele de certificare sunt acreditate de autoritatea de supraveghere și/sau de organismul național de acreditare;
- organismelor naționale de acreditare care desfășoară acreditarea organismelor de certificare în temeiul articolului 43 alineatul (1) litera (b);
- autorității de supraveghere competente care precizează „cerințele suplimentare” față de cele ale standardului ISO/IEC 17065/2012[2] în cazul în care acreditarea este efectuată de organismul național de acreditare în temeiul articolului 43 alineatul (1) litera (b);
- Comitetului european pentru protecția datelor, atunci când emite un aviz și aprobă cerințele de acreditare ale autorității de supraveghere competente în temeiul articolului 43 alineatul (3), al articolului 70 alineatul (1) litera (p) și al articolului 64 alineatul (1) litera (c);

[2] Organizația Internațională de Standardizare: Evaluarea conformității — Cerințe pentru organisme care certifică produse, procese și servicii.

- autorității de supraveghere competente care precizează cerințele de acreditare în cazul în care acreditarea este efectuată de autoritatea de supraveghere în temeiul articolului 43 alineatul (1) litera (a);

- altor părți interesate, cum ar fi organisme de certificare potențiale sau proprietari ai unor sisteme de certificare, care asigură criterii și proceduri de certificare[3].

9. Definiții

10. Următoarele definiții urmăresc să promoveze o înțelegere comună a elementelor de bază ale procesului de acreditare. Acestea trebuie considerate puncte de referință și nu au pretenția de a fi incontestabile. Aceste definiții se bazează pe cadrele de reglementare și pe standardele existente, în special pe dispozițiile relevante ale RGPD și ale standardului ISO/IEC 17065/2012.

11. În sensul prezentelor orientări, se aplică următoarele definiții:

12. „*acreditare*" a organismelor de certificare, vezi secțiunea 3 privind interpretarea acreditării în sensul articolului 43 din RGPD;

13. „*cerințe suplimentare*" înseamnă cerințele stabilite de autoritatea de supraveghere care este competentă și în raport cu care se efectuează acreditarea[4];

14. „*certificare*" înseamnă evaluarea și atestarea imparțială, efectuată de o parte terță[5], care arată că îndeplinirea criteriilor de certificare a fost demonstrată;

15. „*organism de certificare*" înseamnă un organism terț de evaluare[6] a conformității[7] care operează un mecanism de certificare[8];

16. „*schemă de certificare*" înseamnă un sistem de certificare legat de anumite produse, procese și servicii cărora li se aplică aceleași cerințe, norme și proceduri specifice[9];

---

[3] Proprietarul sistemului este o organizație identificabilă care a stabilit criterii și cerințe de certificare în raport cu care trebuie evaluată conformitatea. Acreditarea este asigurată de organizația care efectuează evaluări [articolul 43 alineatul (4)] în raport cu cerințele sistemului de certificare și emite certificatele (și anume, organismul de certificare, cunoscut și sub denumirea de organism de evaluare a conformității). Organizația care efectuează evaluările poate fi aceeași organizație care a elaborat și deține sistemul, dar pot exista acorduri în care o organizație deține sistemul, iar o alta (sau mai multe altele) efectuează evaluările.

[4] Articolul 43 alineatele (1), (3) și (6).

[5] De remarcat că, în conformitate cu ISO 17000, atestarea de către o parte terță (certificarea) este „aplicabilă tuturor obiectelor supuse evaluării conformității" (5.5) „cu excepția organismelor de evaluare a conformității propriu-zise, cărora le este aplicabilă acreditarea" [5.6].

[6] Activitatea de evaluare a conformității de către o parte terță este efectuată de o organizație independentă de persoana sau organizația care furnizează obiectul și de interesele utilizatorilor asupra obiectului respectiv, vezi ISO 17000, punctul 2.4.

[7] Vezi ISO 17000, punctul 2.5: „organism care efectuează servicii de evaluare a conformității"; ISO 17011: „organism care efectuează servicii de evaluare a conformității și care poate face obiectul acreditării"; ISO 17065, punctul 3.12.

[8] Articolul 42 alineatul (1), articolul 42 alineatul (5) din RGPD.

[9] Vezi punctul 3.9 coroborat cu anexa B la ISO 17065.

17. „criterii” sau criterii de certificare înseamnă criteriile pe baza cărora se face certificarea (evaluarea conformității)[10];

18. „organism național de acreditare” înseamnă unicul organism dintr-un stat membru desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului care realizează acreditarea dispunând de autoritatea conferită de statul respectiv[11].

3 INTERPRETAREA „ACREDITĂRII” ÎN SENSUL ARTICOLULUI 43 DIN RGPD

19. RGPD nu definește „acreditarea”. Articolul 2 punctul 10 din Regulamentul (CE) nr. 765/2008, care stabilește cerințele generale pentru acreditări, definește acreditarea ca fiind

20. „o atestare de către un organism național de acreditare a faptului că un organism de evaluare a conformității îndeplinește cerințele stabilite prin standarde armonizate, și, după caz, orice alte cerințe suplimentare, inclusiv cele stabilite în cadrul schemelor sectoriale relevante, pentru realizarea activităților specifice de evaluare a conformității”

21. În conformitate cu ISO/IEC 17011

22. „acreditarea se referă la atestarea de către o parte terță, referitoare la un organism de evaluare a conformității, care demonstrează în mod oficial competența acestuia de a îndeplini sarcini specifice de evaluare a conformității.”

23. Articolul 43 alineatul (1) prevede:

24. „Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere competente, prevăzute la articolele 57 și 58, organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor, după ce informează autoritatea de supraveghere pentru a-i permite să își exercite competențele în temeiul articolului 58 alineatul (2) litera (h), emit și reînnoiesc certificarea. Statele membre se asigură că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entități:

    (a) autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56;

    (b) organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului în conformitate cu standardul ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56.”

25. În ceea ce privește RGPD, cerințele de acreditare se vor baza pe:

- ISO/IEC 17065/2012 și „cerințele suplimentare” stabilite de autoritatea de supraveghere care este competentă în conformitate cu articolul 43 alineatul (1) litera (b), dacă acreditarea este efectuată de organismul național de acreditare, și de autoritatea de supraveghere, atunci când efectuează ea însăși acreditarea.

[10] A se vedea articolul 42 alineatul (5).
[11] Vezi articolul 2 punctul 11 din Regulamentul 765/2008/CE.

26. În ambele cazuri, cerințele consolidate trebuie să acopere cerințele menționate la articolul 43 alineatul (2).

27. Comitetul european pentru protecția datelor recunoaște că scopul acreditării este de a furniza o declarație oficială privind competența unui organism pentru a efectua certificarea (activități de evaluare a conformității)[12]. Acreditarea din punctul de vedere al RGPD trebuie înțeleasă ca însemnând următoarele:

28. o atestare[13] de către un organism național de acreditare și/sau de către o autoritate de supraveghere a faptului că un organism de certificare[14] este calificat să efectueze certificarea în temeiul articolelor 42 și 43 din RGPD, ținând cont de standardul ISO/IEC 17065/2012 și de cerințele suplimentare stabilite de autoritatea de supraveghere și sau de Comitet.

4 ACREDITAREA ÎN CONFORMITATE CU ARTICOLUL 43 ALINEATUL (1) DIN RGPD

29. Articolul 43 alineatul (1) recunoaște că există mai multe opțiuni pentru acreditarea organismelor de certificare. RGPD impune autorităților de supraveghere și statelor membre să definească procesul de acreditare a organismelor de certificare. Această secțiune stabilește căile pentru acreditare prevăzute la articolul 43.

4.1 Rolul statelor membre

30. Articolul 43 alineatul (1) impune statelor membre *să se asigure* că organismele de certificare sunt acreditate, dar permite fiecărui stat membru să stabilească cine trebuie să fie responsabil de efectuarea evaluării care duce la acreditare. Pe baza articolului 43 alineatul (1), sunt disponibile trei opțiuni; acreditarea se realizează:

(1) numai de către autoritatea de supraveghere, pe baza propriilor cerințe;

(2) numai de către organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) 765/2008 și pe baza standardului ISO/IEC 17065/2012 și a cerințelor suplimentare stabilite de autoritatea de supraveghere competentă; sau

(3) atât de către autoritatea de supraveghere, cât și de către organismul național de acreditare (și conform cerințelor enumerate la punctul 2 de mai sus).

31. Este de competența fiecărui stat membru să decidă dacă organismul național de acreditare sau autoritatea de supraveghere sau ambele împreună vor efectua aceste activități de acreditare, dar, în orice caz, trebuie să se asigure că sunt furnizate resurse adecvate[15].

4.2 Interacțiunea cu Regulamentul (CE) 765/2008

[12] Vezi considerentul 15 din Regulamentul 765/2008/CE.
[13] Vezi articolul 2 punctul 10 din Regulamentul (CE) 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor.
[14] Vezi definiția termenului „acreditare” conform ISO 17011.
[15] Vezi articolul 4 alineatul (9) din Regulamentul (CE) 765/2008.

32. Comitetul european pentru protecția datelor remarcă faptul că articolul 2 punctul 11 din Regulamentul (CE) nr. 765/2008 definește un organism național de acreditare ca fiind „*singurul* organism dintr-un stat membru care realizează acreditarea dispunând de autoritatea conferită de statul respectiv”.

33. Articolul 2 punctul (11) poate fi considerat incompatibil cu articolul 43 alineatul (1) din RGPD, care permite acreditarea de către un organism diferit de organismul național de acreditare al statului membru. Comitetul european pentru protecția datelor consideră că intenția legislației UE a fost de a deroga de la principiul general conform căruia acreditarea se realizează exclusiv de către autoritatea națională de acreditare, acordând autorităților de supraveghere aceeași competență în ceea ce privește acreditarea organismelor de certificare. Prin urmare, articolul 43 alineatul (1) este *lex specialis* în raport cu articolul 2 punctul 11 din Regulamentul 765/2008.

4.3 Rolul organismului național de acreditare

34. Articolul 43 alineatul (1) litera (b) prevede că organismul național de acreditare acreditează organismele de certificare în conformitate cu standardul ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere competentă.

35. Din motive de claritate, Comitetul european pentru protecția datelor constată că trimiterea specifică la „litera (b) de la alineatul (1)” din articolul 43 alineatul (3) implică faptul că „cerințele respective” indică „cerințele suplimentare” stabilite de autoritatea de supraveghere competentă în temeiul articolului 43 alineatul (1) litera (b) și cerințele prevăzute la articolul 43 alineatul (2).

36. În procesul de acreditare, organismele naționale de acreditare aplică cerințele suplimentare pe care trebuie să le furnizeze autoritățile de supraveghere.

37. Un organism de certificare cu acreditare existentă pe baza ISO/IEC 17065/2012 pentru sistemele de certificare care nu sunt legate de RGPD care dorește să extindă domeniul de aplicare al acreditării sale pentru a acoperi certificarea emisă în conformitate cu RGPD va trebui să îndeplinească cerințele suplimentare stabilite de autoritatea de supraveghere în cazul în care acreditarea este gestionată de organismul național de acreditare. Dacă acreditarea pentru certificare în temeiul RGPD este oferită doar de către autoritatea de supraveghere competentă, un organism de certificare care solicită acreditarea va trebui să îndeplinească cerințele stabilite de autoritatea de supraveghere respectivă.

4.4 Rolul autorității de supraveghere

38. Comitetul european pentru protecția datelor remarcă faptul că articolul 57 alineatul (1) litera (q) prevede că autoritatea de supraveghere *coordonează* procedura de acreditare a unui organism de certificare în conformitate cu articolul 43 ca „sarcină a autorității de supraveghere”, în temeiul articolului 57, iar articolul 58 alineatul (3) litera (e) prevede că autoritatea de supraveghere are competența de autorizare și de consiliere pentru acreditarea organismelor de certificare în conformitate cu articolul 43. Formularea articolului 43 alineatul (1) oferă o anumită flexibilitate, iar funcția de acreditare a autorității de supraveghere trebuie înțeleasă ca fiind o sarcină doar dacă este cazul. Dreptul intern al statelor membre poate fi utilizat pentru a clarifica acest aspect. Cu toate acestea, în procesul de acreditare de către un organism național de acreditare, organismul de certificare are obligația, conform articolului 43 alineatul (2) litera (a), să demonstreze autorității de

supraveghere competente, într-un mod satisfăcător, independența și expertiza în legătură cu obiectul mecanismului de certificare pe care îl oferă.[16]

39. Dacă un stat membru prevede că organismele de certificare urmează să fie acreditate de autoritatea de supraveghere, aceasta trebuie să stabilească cerințe de acreditare, inclusiv cerințele prevăzute la articolul 43 alineatul (2), dar fără a se limita la acestea. În comparație cu obligațiile referitoare la acreditarea organismelor de certificare de către organismele naționale de acreditare, articolul 43 prevede mai puține instrucțiuni cu privire la cerințele de acreditare atunci când autoritatea de supraveghere efectuează ea însăși acreditarea. Pentru a contribui la o abordare armonizată a acreditării, criteriile de acreditare utilizate de autoritatea de supraveghere trebuie să se ghideze după ISO/IEC 17065 și trebuie completate cu cerințele suplimentare pe care le stabilește o autoritate de supraveghere în temeiul articolului 43 alineatul (1) litera (b). Comitetul european pentru protecția datelor remarcă faptul că articolul 43 alineatul (2) literele (a)-(e) reflectă și specifică cerințele ISO 17065, ceea ce va contribui la asigurarea coerenței.

40. Dacă un stat membru prevede că organismele de certificare urmează să fie acreditate de organismele naționale de acreditare, autoritatea de supraveghere trebuie să stabilească cerințe suplimentare care să vină în completarea convențiilor de acreditare existente prevăzute în Regulamentul (CE) 765/2008 (în cazul cărora articolele 3-14 se referă la organizarea și funcționarea acreditării organismelor de evaluare a conformității) și a normelor tehnice care descriu metodele și procedurile organismelor de certificare. Având în vedere cele de mai sus, Regulamentul (CE) 765/2008 oferă îndrumări suplimentare: Articolul 2 punctul 10 definește acreditarea și face trimitere la „standardele armonizate” și la „orice alte cerințe suplimentare, inclusiv cele stabilite în cadrul schemelor sectoriale relevante”. Rezultă că cerințele suplimentare stabilite de autoritatea de supraveghere trebuie să includă cerințe specifice și să se concentreze pe facilitarea evaluării, printre altele, a independenței și a nivelului de competență în domeniul protecției datelor ale organismelor de certificare, de exemplu a capacității acestora de a evalua și a certifica operațiunile de prelucrare a datelor cu caracter personal de către operatori și persoanele împuternicite de către operatori în temeiul articolului 42 alineatul (1). Aceasta include competența necesară pentru sistemele sectoriale și în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor fizice și, în special, dreptul acestora la protecția datelor cu caracter personal[17]. Anexa la prezentele orientări poate oferi informații autorităților de supraveghere competente atunci când stabilesc „cerințele suplimentare” în conformitate cu articolul 43 alineatul (1) litera (b) și cu articolul 43 alineatul (3).

41. Articolul 43 alineatul (6) prevede că „cerințele menționate la alineatul (3) din prezentul articol și criteriile [de certificare] menționate la articolul 42 alineatul (5) se publică de către autoritatea de supraveghere într-o formă ușor de accesat”. Prin urmare, pentru a asigura transparența, se publică toate criteriile și cerințele aprobate de autoritatea de supraveghere. În ceea ce privește calitatea și încrederea în organismele de certificare, ar fi de dorit ca toate cerințele pentru acreditare să fie ușor accesibile publicului.

[16] Cerințele suplimentare stabilite de autoritatea de supraveghere în conformitate cu articolul 43 alineatul (1) litera (b) trebuie să specifice cerințele în materie de independență și de expertiză. Vezi și anexa 1 la orientări.
[17] Vezi articolul 1 alineatul (2) din RGPD.

4.5 Autoritatea de supraveghere care acționează în calitate de organism de certificare

42. Articolul 42 alineatul (5) prevede că o autoritate de supraveghere poate emite certificate, dar RGPD nu impune ca aceasta să fie acreditată pentru a îndeplini cerințele Regulamentului (CE) 765/2008. Comitetul european pentru protecția datelor remarcă faptul că articolul 43 alineatul (1) litera (a) și, în mod specific, articolul 58 alineatul (2) litera (h) și alineatul 3 literele (a), (e) și (f) împuternicesc autoritățile de supraveghere să efectueze atât acreditarea, cât și certificarea și, în același timp, să ofere consiliere și, dacă este cazul, să retragă certificări sau să oblige organismele de certificare să nu elibereze certificări.

43. Pot exista situații în care separarea rolurilor și a sarcinilor de acreditare și de certificare este adecvată sau necesară, de exemplu în cazul în care o autoritate de supraveghere și alte organisme de certificare coexistă într-un stat membru și ambele emit aceeași gamă de certificări. Prin urmare, autoritățile de supraveghere trebuie să ia suficiente măsuri organizatorice pentru a separa sarcinile prevăzute de RGPD pentru a ancora și a facilita mecanismele de certificare, luând în același timp măsuri de precauție pentru a evita conflictele de interese care pot apărea în urma acestor sarcini. În plus, statele membre și autoritățile de supraveghere trebuie să țină seama de nivelul european armonizat la formularea legislației și a procedurilor naționale referitoare la acreditare și certificare, în conformitate cu RGPD.

4.6 Cerințe de acreditare

44. Anexa la prezentele orientări oferă îndrumări cu privire la identificarea cerințelor suplimentare de acreditare. Aceasta identifică dispozițiile relevante din RGPD și sugerează cerințe pe care autoritățile de supraveghere și organismele naționale de acreditare trebuie să le aibă în vedere pentru a asigura respectarea RGPD.

45. Astfel cum s-a stabilit mai sus, în cazul în care organismele de certificare sunt acreditate de organismul național de acreditare în temeiul Regulamentului (CE) 765/2008, standardul relevant pentru acreditare va fi ISO/IEC 17065/2012, completat cu cerințele suplimentare stabilite de autoritatea de supraveghere. Articolul 43 alineatul (2) reflectă dispozițiile generice ale ISO/IEC 17065/2012 în lumina protecției drepturilor fundamentale în temeiul RGPD. Cadrul din anexă utilizează articolul 43 alineatul (2) și standardul ISO/IEC 17065/2012 ca bază pentru identificarea cerințelor și a criteriilor suplimentare referitoare la evaluarea competenței în domeniul protecției datelor a organismelor de certificare și a capacității acestora de a respecta drepturile și libertățile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, astfel cum este consacrată în RGPD. Comitetul european pentru protecția datelor remarcă faptul că acesta se axează în special pe garantarea faptului că organismele de certificare au un nivel adecvat de competență în domeniul protecției datelor, în conformitate cu articolul 43 alineatul (1).

46. Cerințele de acreditare suplimentare stabilite de autoritatea de supraveghere se vor aplica tuturor organismelor de certificare care solicită acreditarea. Organismul de acreditare va evalua dacă organismul de certificare este competent pentru a desfășura activitatea de certificare în conformitate cu cerințele suplimentare și obiectul certificării. Trebuie să existe trimiteri la sectoare sau la domenii specifice de certificare pentru care este acreditat organismul de certificare.

47. Comitetul European pentru Protecția Datelor constată că, în plus față de cerințele ISO/IEC 17065/2012, este necesară și o competență specială în domeniul protecției datelor în cazul în care alte organisme externe, cum ar fi laboratoare sau auditori, efectuează părți sau componente ale activităților de certificare în numele unui organism de certificare acreditat. În aceste cazuri, acreditarea acestor organisme externe în temeiul RGPD nu este posibilă. Cu toate acestea, pentru a se asigura caracterul adecvat al acestor organisme pentru activitatea lor în numele organismelor de certificare acreditate, este necesar ca organismul de certificare acreditat să se asigure că această competență în domeniul protecției datelor solicitată organismului acreditat există și este demonstrată și pentru organismul extern în ceea ce privește activitatea relevantă desfășurată.

48. Cadrul de identificare a cerințelor de acreditare suplimentare prezentate în anexa la prezentele orientări nu constituie un manual de procedură pentru procesul de acreditare realizat de organismul național de acreditare sau de autoritatea de supraveghere. Acesta oferă îndrumări privind structura și metodologia și, prin urmare, un set de instrumente pentru autoritățile de supraveghere în vederea identificării cerințelor suplimentare pentru acreditare.

ANEXA 1

Anexa 1 oferă îndrumări pentru specificarea cerințelor de acreditare „suplimentare” ținând seama de ISO/IEC 17065/2012 și în conformitate cu articolul 43 alineatul (1) litera (b) și articolul 43 alineatul (3) din RGPD.

Prezenta anexă oferă sugestii de cerințe pe care o autoritate de supraveghere în domeniul protecției datelor trebuie să le elaboreze și să le aplice în cadrul acreditării unui organism de certificare de către organismul național de acreditare sau autoritatea de supraveghere competentă[18]. Aceste cerințe suplimentare trebuie comunicate Comitetului European pentru rotecția datelor înainte de aprobare, în conformitate cu articolul 64 alineatul (1) litera (c).

Prezenta anexă trebuie coroborată cu ISO/IEC 17065/2012. Numerele secțiunilor utilizate în prezenta anexă corespund celor utilizate în standardul ISO/IEC 17065/2012. În cazul în care autoritățile de supraveghere realizează acreditarea în temeiul articolului 43 alineatul (1) litera (a), o bună practică ar consta în aplicarea acestei abordări atunci când ea este fezabilă. Aceasta va susține acreditarea armonizată la nivelul UE.

Fără a aduce atingere orientării următoare sau în absența unor orientări cu privire la orice element al ISO/IEC 17065/2012, autoritatea de supraveghere competentă poate formula noi cerințe suplimentare referitoare la elementele respective în cazul în care sunt în conformitate cu dreptul național.

0 PREFIX

[Această secțiune vizează orice Condiții de cooperare convenite, dacă este cazul, între organismul național de acreditare și autoritatea de supraveghere în domeniul protecției datelor, de exemplu care entitate trebuie să fie responsabilă de primirea cererilor sau cum ar trebui organizată recunoașterea criteriilor aprobate ca parte a procesului de acreditare.]

1 DOMENIU DE APLICARE[19]

Domeniul de aplicare al ISO/IEC 17065/2012 se aplică în conformitate cu RGPD. Orientările privind acreditarea și certificarea oferă mai multe informații. Domeniul de aplicare al unui mecanism de certificare (de exemplu, certificarea operațiunilor de prelucrare a serviciilor de cloud) trebuie luat în considerare în evaluarea efectuată de organismul național de acreditare și autoritatea de supraveghere competentă în timpul procesului de acreditare, îndeosebi în ceea ce privește criteriile, expertiza și metodologia de evaluare. Domeniul extins de aplicare al ISO/IEC 17065/2012, care acoperă produse, procese și servicii, nu ar trebui să reducă cerințele prevăzute de RGPD sau să primeze asupra acestora, de exemplu, un mecanism de guvernanță nu poate fi singurul element al unui mecanism de certificare, întrucât certificarea trebuie să includă prelucrarea datelor cu caracter personal, respectiv operațiuni de prelucrare. În temeiul articolului 42 alineatul (1), certificarea în

[18] Pentru informații referitoare la procesul de aprobare pentru criteriile de certificare, a se vedea secțiunea 4 din orientările privind certificarea.
[19] Numerotarea face referire la ISO/IEC 17065/2012.

temeiul RGPD se aplică numai operațiunilor de prelucrare ale operatorilor și persoanelor împuternicite de către operatori.

2 REFERINȚĂ NORMATIVĂ

RGPD are întâietate față de ISO/IEC 17065/2012. În cazul în care în cerințele suplimentare sau la nivelul mecanismului de certificare se face referire la alte standarde ISO, se interpretează că acestea respectă cerințele stabilite în RGPD.

3 TERMENI ȘI DEFINIȚII

În contextul prezentei anexe, se aplică termenii și definițiile din orientările privind acreditarea (WP 261) și certificarea (EDPB 1/2018) și acestea au întâietate față de definițiile din standardul ISO.

4 CERINȚE GENERALE PRIVIND ACREDITAREA

4.1 Aspecte juridice și contractuale

4.1.1 Răspundere juridică

Un organism de certificare ar trebui să poată demonstra (în orice moment) organismului național de acreditare sau autorității de supraveghere competente că dispune de proceduri actualizate care demonstrează conformitatea cu responsabilitățile juridice stabilite în condițiile de acreditare, inclusiv cerințele suplimentare referitoare la aplicarea Regulamentului 2016/679/CE. A se lua notă de faptul că, întrucât organismul de certificare este el însuși un operator de date/o persoană împuternicită de către un operator, acesta trebuie să poată demonstra existența unor proceduri și măsuri conforme cu Regulamentul 2016/679/CE în mod specific pentru controlul și prelucrarea datelor cu caracter personal ale organizației-client ca parte a procesului de certificare.

Autoritatea de supraveghere competentă poate decide să adauge alte cerințe și proceduri pentru a verifica dacă organismele de certificare respectă dispozițiile RGPD înainte de acreditare.

4.1.2 Acordul de certificare („AC”)

Cerințele minime pentru un acord de certificare sunt completate cu cele de mai jos.

Organismul de certificare demonstrează, în plus față de cerințele prevăzute în ISO/IEC 17065/2012, că acordurile sale de certificare:

1. impun solicitantului să respecte întotdeauna atât cerințele de certificare generale în sensul punctului 4.1.2.2 litera (a) din ISO/IEC 17065/2012, cât și criteriile aprobate de autoritatea de supraveghere competentă sau de Comitetul european pentru protecția datelor în conformitate cu articolul 43 alineatul (2) litera (b) și articolul 42 alineatul (5);
2. impun solicitantului să asigure transparența deplină pentru autoritatea de supraveghere competentă în ceea ce privește procedura de certificare, inclusiv aspectele confidențiale din perspectivă contractuală legate de respectarea protecției datelor în temeiul articolului 42 alineatul (7) și al articolului 58 alineatul (1) litera (c);
3. nu reduc responsabilitatea solicitantului în ceea ce privește respectarea Regulamentului 2016/679/CE și nu aduc atingere sarcinilor și competențelor autorităților de supraveghere competente în conformitate cu articolul 42 alineatul (5);

4. impun solicitantului să furnizeze organismului de certificare toate informațiile și să acorde acestuia accesul la activitățile sale de prelucrare necesare pentru desfășurarea procedurii de certificare în temeiul articolului 42 alineatul (6);
5. impun solicitantului să respecte termenele-limită și procedurile aplicabile. Acordul de certificare trebuie să stipuleze că termenele-limită și procedurile care rezultă, de exemplu, din programul de certificare sau din alte reglementări trebuie să fie respectate și asumate;
6. în ceea ce privește punctul 4.1.2.2 litera (c) nr. 1 din ISO/IEC 17065/2012, stabilesc normele privind validitatea, reînnoirea și retragerea în conformitate cu articolul 42 alineatul (7) și articolul 43 alineatul (4), inclusiv normele care stabilesc intervalele adecvate pentru reevaluare sau examinare (regularitate) în conformitate cu articolul 42 alineatul (7);
7. permit organismului de certificare să publice toate informațiile necesare pentru acordarea certificării în temeiul articolului 42 alineatul (8) și al articolului 43 alineatul (5);
8. includ norme privind măsurile de precauție necesare pentru investigarea plângerilor în sensul punctului 4.1.2.2 litera (c) nr. 2 și, în plus, litera (j); conțin, de asemenea, declarații explicite privind structura și procedura pentru gestionarea plângerilor în conformitate cu articolul 43 alineatul (2) litera (d);
9. în plus față de cerințele minime menționate la punctul 4.1.2.2 din ISO/IEC 17065/2012; în cazul în care consecințele retragerii sau suspendării acreditării organismului de certificare au un impact asupra clientului, consecințele pentru client ar trebui, de asemenea, să fie abordate;
10. impun solicitantului să informeze organismul de certificare în eventualitatea unor modificări semnificative legate de situația sa efectivă sau juridică și în privința produselor, proceselor și serviciilor sale vizate de certificare.

4.1.3 Utilizarea sigiliilor și mărcilor în domeniul protecției datelor

Certificatele, sigiliile și mărcile se utilizează numai în conformitate cu articolele 42 și 43 și cu orientările privind acreditarea și certificarea.

4.2 Gestionarea imparțialității

Organismul de acreditare asigură că, în plus față de cerința de la punctul 4.2. din ISO/IEC 17065/2012,

1. organismul de certificare respectă cerințele suplimentare ale autorității de supraveghere competente [în temeiul articolului 43 alineatul (1) litera (b)]
    a. în conformitate cu articolul 43 alineatul (2) litera (a), oferă dovezi separate ale independenței sale. Aceasta se aplică îndeosebi dovezilor referitoare la finanțarea organismului de certificare în măsura în care aceasta are legătură cu asigurarea imparțialității;
    b. sarcinile și obligațiile sale nu conduc la un conflict de interese în temeiul articolului 43 alineatul (2) litera (e);
2. organismul de certificare nu are o legătură relevantă cu clientul pe care îl evaluează.

4.3 Răspundere și finanțare

În plus față de cerința de la punctul 4.3.1 din ISO/IEC 17065/2012, organismul de acreditare asigură periodic că organismul de certificare dispune de măsuri adecvate (de exemplu, asigurare sau rezerve) pentru a-și acoperi obligațiile în regiunile geografice în care operează.

4.4 Condiții nediscriminatorii

Autoritatea de supraveghere poate formula cerințe suplimentare în cazul în care sunt în conformitate cu dreptul național.

4.5 Confidențialitate

Autoritatea de supraveghere poate formula cerințe suplimentare în cazul în care sunt în conformitate cu dreptul național.

4.6 Informații publice

În plus față de cerința de la punctul 4.6 din ISO/IEC 17065/2012, organismul de acreditare solicită organismului de certificare ca cel puțin

1. toate versiunile (actuală și anterioare) ale criteriilor aprobate utilizate în sensul articolului 42 alineatul (5) să fie publicate și ușor de accesat de către public, la fel ca toate procedurile de certificare care indică, în general, perioada respectivă de validitate;
2. informațiile privind procedurile de tratare a plângerilor și căile de atac să fie puse la dispoziția publicului în temeiul articolului 43 alineatul (2) litera (d).

5 CERINȚE STRUCTURALE, ARTICOLUL 43 ALINEATUL (4) [EVALUAREA „ADECVATĂ”]

5.1 Structura organizatorică și personalul de conducere de nivel superior

Autoritatea de supraveghere poate formula cerințe suplimentare.

5.2 Mecanisme de asigurare a imparțialității

Autoritatea de supraveghere poate formula cerințe suplimentare.

6 CERINȚE PRIVIND RESURSELE

6.1 Personalul organismului de certificare

În plus față de cerința din secțiunea 6 a ISO/IEC 17065/2012, organismul de acreditare asigură, pentru fiecare organism de certificare, că personalul acestuia:

1. deține expertiză adecvată și constantă demonstrată (cunoștințe și experiență) în ceea ce privește protecția datelor, în temeiul articolului 43 alineatul (1);
2. dispune de independență și expertiză constantă în legătură cu obiectul certificării, în temeiul articolului 43 alineatul (2) litera (a), și nu se află în conflict de interese, în temeiul articolului 43 alineatul (2) litera (e);
3. se angajează să respecte criteriile menționate la articolul 42 alineatul (5), în temeiul articolului 43 alineatul (2) litera (b);
4. dispune de cunoștințe și experiență relevante și adecvate în ceea ce privește aplicarea legislației în materie de protecție a datelor;
5. dispune de cunoștințe și experiență relevante și adecvate în ceea ce privește măsurile tehnice și organizatorice relevante de protecție a datelor.
6. poate demonstra că deține experiență în domeniile menționate în cerințele suplimentare 6.1.1, 6.1.4 și 6.1.5.

În cazul personalului care deține expertiză tehnică:

- a obținut o calificare într-un domeniu relevant de expertiză tehnică cel puțin la nivelul 6 CEC[20] sau un titlu protejat recunoscut (de exemplu, inginer diplomat) în profesia reglementată relevantă sau deține experiență profesională semnificativă.
- *Personalul responsabil de deciziile de certificare* trebuie să aibă experiență profesională semnificativă în identificarea și punerea în aplicare a măsurilor de protecție a datelor.
- *Personalul responsabil de evaluări* trebuie să dețină experiență profesională în protecția datelor tehnice și cunoștințe și experiență în ceea ce privește procedura comparabilă (de exemplu, certificări/audituri) și să fie înregistrat conform normelor în vigoare.

Personalul trebuie să demonstreze că își menține cunoștințele specifice domeniului în ceea ce privește competențele tehnice și de audit printr-o dezvoltare profesională continuă.

În cazul personalului care deține expertiză juridică:

- studii juridice în cadrul unei universități din UE sau al unei universități recunoscute de stat, pe o perioadă de cel puțin opt semestre, inclusiv diplomă de master (LL.M.) sau echivalentul acesteia ori experiență profesională semnificativă.
- *Personalul responsabil de deciziile de certificare* trebuie să demonstreze o experiență profesională semnificativă în dreptul privind protecția datelor și să fie înregistrat conform normelor în vigoare în statul membru.
- *Personalul responsabil de evaluări* trebuie să demonstreze cel puțin doi ani de experiență profesională în dreptul privind protecția datelor și cunoștințe și experiență în ceea ce privește procedurile comparabile (de exemplu, certificări/audituri) și să fie înregistrat atunci când statul membru prevede această obligație.
    - Personalul trebuie să demonstreze că își menține cunoștințele specifice domeniului în ceea ce privește competențele tehnice și de audit printr-o dezvoltare profesională continuă.

6.2 Resurse pentru evaluare

Autoritatea de supraveghere poate formula cerințe suplimentare în cazul în care sunt în conformitate cu dreptul național.

7 CERINȚE PRIVIND PROCESUL, ARTICOLUL 43 ALINEATUL (2) LITERELE (C), (D)

7.1 Aspecte generale

În plus față de cerința din secțiunea 7.1 din ISO/IEC 17065/2012, organismul de acreditare are obligația de a asigura următoarele:

1. organismele de certificare respectă cerințele suplimentare ale autorității de supraveghere competente [în temeiul articolului 43 alineatul (1) litera (b)] atunci când depun cererea, astfel încât sarcinile și obligațiile să nu conducă la un conflict de interese, în temeiul articolului 43 alineatul (2) litera (b);

[20] A se vedea instrumentul de comparare a cadrelor de calificări la adresa https://ec.europa.eu/ploteus/ro/compare

2. informează autoritățile de supraveghere competente relevante înainte ca un organism de certificare să înceapă să utilizeze un sigiliu european privind protecția datelor într-un stat membru nou, dintr-un birou-satelit.

7.2 Cererea

În plus față de punctul 7.2 din ISO/IEC 17065/2012, trebuie să se impună ca

1. obiectul certificării (ținta evaluării) să fie descris în detaliu în cerere. Aceasta include, de asemenea, interfețe și transferuri către alte sisteme și organizații, protocoale și alte elemente de asigurare;
2. cererea trebuie să specifice dacă se recurge la persoane împuternicite de către operatori și, în cazul în care persoanele împuternicite de către operatori sunt solicitantul însuși, responsabilitățile și sarcinile acestora trebuie descrise, iar cererea trebuie să conțină contractul (contractele) relevant(e) dintre operatori și persoanele împuternicite de către operatori.

7.3 Examinarea cererii

În plus față de punctul 7.3 din ISO/IEC 17065/2012, trebuie să se impună ca:

1. în acordul de certificare să fie prevăzute metode de evaluare obligatorii în ceea ce privește ținta evaluării;
2. evaluarea de la punctul 7.3 litera (e) privind existența unui nivel suficient de expertiză să țină seama atât de expertiza tehnică, cât și de cea juridică în domeniul protecției datelor, în măsura adecvată.

7.4 Evaluare

În plus față de punctul 7.4 din ISO/IEC 17065/2012, mecanismele de certificare trebuie să descrie metode de evaluare suficiente pentru evaluarea conformității operațiunii (operațiunilor) de prelucrare cu criteriile de certificare, inclusiv, de exemplu, după caz:

1. o metodă de evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu scopul lor și persoanele vizate respective;
2. o metodă de evaluare a acoperirii, alcătuirii și evaluării tuturor riscurilor avute în vedere de către operator și persoana împuternicită de către operator în ceea ce privește consecințele juridice în temeiul articolelor 30, 32, 35 și 36 din RGPD, precum și definiția măsurilor tehnice și organizatorice în temeiul articolelor 24, 25 și 32 din RGPD, în măsura în care articolele menționate mai sus se aplică obiectului certificării; și
3. o metodă de evaluare a măsurilor de remediere, inclusiv garanții, elemente de protecție și proceduri, pentru asigurarea protecției datelor cu caracter personal în contextul prelucrării care urmează să fie atribuite obiectului certificării, precum și pentru demonstrarea faptului că cerințele juridice, astfel cum sunt prevăzute în criterii, sunt respectate; și
4. documentarea metodelor și constatărilor.

Organismului de certificare ar trebui să i se impună să asigure că aceste metode de evaluare sunt standardizate și aplicabile în mod general. Aceasta înseamnă că pentru ținte ale evaluării comparabile se utilizează metode de evaluare comparabile. Orice abatere de la această procedură trebuie justificată de organismul de certificare.

În plus față de punctul 7.4.2 din ISO/IEC 17065/2012, ar trebui să se permită ca evaluarea să fie efectuată de experți externi care au fost recunoscuți de organismul de certificare.

În plus față de punctul 7.4.5 din ISO/IEC 17065/2012, ar trebui să se impună ca certificarea protecției datelor în conformitate cu articolele 42 și 43 din RGPD, care acoperă deja o parte din obiectul certificării, să poată fi inclusă într-o certificare curentă. Cu toate acestea, nu va fi suficientă înlocuirea completă a evaluărilor (parțiale). Organismul de certificare are obligația de a verifica respectarea criteriilor. Recunoașterea necesită, în orice caz, disponibilitatea unui raport de evaluare complet sau a informațiilor care să permită o evaluare a activității de certificare anterioare și a rezultatelor acesteia. O declarație de certificare sau atestate de certificare similare nu ar trebui considerate suficiente pentru a înlocui un raport.

În plus față de punctul 7.4.6 din ISO/IEC 17065/2012, ar trebui să se impună ca organismul de certificare să stabilească în detaliu, în cadrul mecanismului său de certificare, modul în care, prin datele solicitate la punctul 7.4.6, clientul (solicitantul certificării) este informat cu privire la neconformitățile din cadrul unui mecanism de certificare. În acest context, ar trebui să se definească cel puțin natura și calendarul acestor date.

În plus față de punctul 7.4.9 din ISO/IEC 17065/2012, ar trebui să se impună ca documentația să fie pusă integral la dispoziția autorității de supraveghere din domeniul protecției datelor, la cerere.

7.5 Examinare

În plus față de punctul 7.5 din ISO/IEC 17065/2012, sunt necesare proceduri de acordare, de examinare periodică și de revocare a certificărilor respective în temeiul articolului 43 alineatele (2) și (3).

7.6 Decizia de certificare

În plus față de punctul 7.6.1 din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să stabilească în detaliu, în cadrul procedurilor sale, modul în care sunt asigurate independența și responsabilitatea cu privire la deciziile de certificare individuale.

7.7 Documentarea certificării

În plus față de punctul 7.7.1 litera (e) din ISO/IEC 17065/2012 și în conformitate cu articolul 42 alineatul (7) din RGPD, ar trebui să se impună ca perioada de validitate a certificărilor să nu depășească trei ani.

În plus față de punctul 7.7.1. litera (e) din ISO/IEC 17065/2012, ar trebui să se impună ca perioada de monitorizare vizată în sensul secțiunii 7.9 să fie, de asemenea, documentată.

În plus față de punctul 7.7.1. litera (f) din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să denumească obiectul certificării în documentația certificării (indicând statutul versiunii sau caracteristici similare, dacă se aplică).

7.8 Repertoriul produselor certificate

În plus față de punctul 7.8 din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să mențină informațiile privind produsele, procesele și serviciile certificate disponibile pe plan intern și pentru public. Organismul de certificare va pune la dispoziția publicului o sinteză a raportului de evaluare. Scopul acestei sinteze este de a contribui la asigurarea transparenței în ceea ce privește elementele certificate și modul în care au fost evaluate. Aceasta va explica aspecte precum:

(a) domeniul de aplicare al certificării și o descriere pertinentă a obiectului certificării (ținta evaluării);

(b) criteriile de certificare respective (inclusiv versiunea sau statutul funcțional);

(c) metodele de evaluare și testele efectuate, precum și

(d) rezultatul (rezultatele).

În plus față de punctul 7.8 din ISO/IEC 17065/2012 și în temeiul articolului 43 alineatul (5) din RGPD, organismul de certificare informează autoritățile de supraveghere competente cu privire la motivele pentru acordarea sau revocarea certificării solicitate.

7.9 Măsuri de supraveghere

În plus față de punctele 7.9.1, 7.9.2 și 7.9.3 din ISO/IEC 17065/2012 și în conformitate cu articolul 43 alineatul (2) litera (c) din RGPD, ar trebui să se impună ca măsurile de monitorizare periodică să fie obligatorii pentru menținerea certificării în perioada de monitorizare.

7.10 Modificări cu impact asupra certificării

În plus față de punctele 7.10.1 și 7.10.2 din EN ISO/IEC 17065/2012, modificările cu impact asupra certificării care trebuie luate în considerare de organismul de certificare includ: modificări ale legislației privind protecția datelor, adoptarea de acte delegate ale Comisiei Europene în conformitate cu articolul 43 alineatele (8) și (9), decizii ale Comitetului european pentru protecția datelor și decizii ale instanțelor judecătorești legate de protecția datelor. Procedurile legate de modificări, care urmează a fi convenite aici, pot include aspecte precum: perioadele de tranziție, procesele de aprobare cu autoritatea de supraveghere competentă, reevaluarea obiectului relevant al certificării și măsuri adecvate de revocare a certificării, în cazul în care operațiunea de prelucrare certificată nu mai respectă criteriile actualizate.

7.11 Încetarea, reducerea, suspendarea sau retragerea certificării

În plus față de capitolul 7.11.1 din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să informeze imediat, în scris, autoritatea de supraveghere competentă și organismul național de acreditare, după caz, cu privire la măsurile adoptate și continuarea, restricționarea, suspendarea și retragerea certificării.

În conformitate cu articolul 58 alineatul (2) litera (h), organismului de certificare i se impune să accepte deciziile și ordinele autorității de supraveghere competente de a retrage sau a nu emite certificarea pentru un client (solicitant) în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite.

7.12 Evidențe

Organismului de certificare ar trebui să i se impună să păstreze toată documentația completă, inteligibilă, actualizată și adecvată pentru a face obiectul unui audit.

7.13 Plângeri și căi de atac, articolul 43 alineatul (2) litera (d)

În plus față de punctul 7.13.1 din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să definească:

(a) cine poate depune plângeri sau prezenta obiecțiuni;

(b) cine le prelucrează la nivelul organismului de certificare;

(c) ce verificări au loc în acest context; și

(d) posibilitățile de consultare de care dispun părțile interesate.

În plus față de punctul 7.13.2 din ISO/IEC 17065/2012, organismului de certificare ar trebui să i se impună să definească:

(a) modul în care trebuie oferită această confirmare și destinatarii vizați ai acesteia;

(b) termenele pentru aceasta; și

(c) procesele care urmează să fie inițiate ulterior.

În plus față de punctul 7.13.1 din ISO/IEC 17065/2012, organismul de certificare trebuie să definească modul în care este asigurată separarea între activitățile de certificare și tratarea căilor de atac și a plângerilor.

8 CERINȚE PRIVIND SISTEMUL DE GESTIONARE

O cerință generală privind sistemul de gestionare în conformitate cu capitolul 8 din ISO/IEC 17065/2012 constă în faptul că punerea în aplicare a tuturor cerințelor din capitolele precedente în sfera de aplicare a mecanismului de certificare de către organismul de certificare acreditat este documentată, evaluată, controlată și monitorizată în mod independent.

Principiul de bază al gestionării este acela de a defini un sistem potrivit căruia obiectivele sale sunt stabilite cu eficacitate și eficiență, în mod specific: punerea în aplicare a serviciilor de certificare – prin intermediul unor specificații adecvate. Aceasta necesită transparența și posibilitatea verificării punerii în aplicare a cerințelor de acreditare de către organismul de certificare și conformitatea permanentă a acestuia.

În acest scop, sistemul de gestionare trebuie să specifice o metodologie care să îndeplinească și să controleze aceste cerințe, în conformitate cu normele privind protecția datelor și în vederea verificării constante a acestora împreună cu organismul acreditat însuși.

Aceste principii de gestionare și punerea lor documentată în aplicare trebuie să fie transparente și să fie publicate de către organismul de certificare acreditat în baza procedurii de acreditare în temeiul articolului 58 și, ulterior, la cererea autorității de supraveghere din domeniul protecției datelor, în orice moment în timpul unei investigații sub forma unor controale privind protecția datelor în temeiul articolului 58 alineatul (1) litera (b) sau a unei examinări a certificărilor emise în conformitate cu articolul 42 alineatul (7) în temeiul articolului 58 alineatul (1) litera (c).

În special, organismul de certificare acreditat trebuie să publice în permanență și în mod continuu certificările efectuate și bazele acestora (sau mecanismele ori schemele de certificare), durata valabilității certificărilor și care sunt cadrele și condițiile aplicabile (considerentul 100).

8.1 Cerințe generale privind sistemul de gestionare

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.2 Documentarea în cadrul sistemului de gestionare

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.3 Controlul documentelor

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.4 Controlul înregistrărilor

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.5 Analiza gestionării

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.6 Audituri interne

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.7 Măsuri corective

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

8.8 Măsuri preventive

Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

9 ALTE CERINȚE SUPLIMENTARE21

9.1 Actualizarea metodelor de evaluare

Organismul de certificare stabilește proceduri pentru ghidarea actualizării metodelor de evaluare, care trebuie aplicate în contextul evaluării prevăzute la punctul 7.4. Actualizarea trebuie să aibă loc pe parcursul modificărilor în ceea ce privește cadrul juridic, riscul (riscurile) relevant(e), nivelul de dezvoltare și costurile de punere în aplicare a măsurilor tehnice și organizatorice.

9.2 Menținerea expertizei

Organismele de certificare stabilesc proceduri pentru a asigura formarea angajaților lor în vederea actualizării competențelor acestora, ținând seama de evoluțiile enumerate la punctul 9.1.

9.3 Responsabilități și competențe

9.3.1 Comunicarea între organismele de certificare și clienții lor

Se instituie proceduri pentru punerea în aplicare a procedurilor și structurilor de comunicare adecvate între organismul de certificare și clientul acestuia. Acestea includ:

1. păstrarea documentației referitoare la sarcini și responsabilități de către organismul de certificare acreditat, în scopul
    a. cererilor de informații sau
    b. pentru a permite contactul în eventualitatea unei plângeri legate de o certificare;
2. menținerea unui proces de solicitare în scopul
    a. informării cu privire la statutul solicitării;
    b. evaluări efectuate de autoritatea de supraveghere competentă cu privire la:
        i. feedback;
        ii. deciziile autorității de supraveghere competente.

[21] Autoritatea de supraveghere competentă poate specifica și adăuga alte cerințe suplimentare dacă sunt în conformitate cu dreptul național.

9.3.2 Documentarea activităților de evaluare

Autoritatea de supraveghere poate formula cerințe suplimentare.

9.3.3 Gestionarea soluționării plângerilor

Se instituie o procedură de soluționare a plângerilor ca parte integrantă a sistemului de gestionare, care pune în aplicare, în mod special, cerințele de la punctele 4.1.2.2 litera (c), 4.1.2.2 litera (j), 4.6 litera (d) și 7.13 din ISO/IEC 17065/2012.

Plângerile și obiecțiunile relevante ar trebui împărtășite cu autoritatea de supraveghere competentă.

9.3.4 Gestionarea retragerilor

Procedurile aplicabile în eventualitatea suspendării sau retragerii acreditării sunt integrate în sistemul de gestionare al organismului de certificare, inclusiv notificările transmise clienților.