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

Adoptat la 4 decembrie 2018

Cuprins

1 Introducere 3
2 Domeniul de aplicare al ghidului 4
3 Interpretarea „acreditării” în sensul articolului 43 din RGPD 6
4 Acreditarea în conformitate cu articolul 43 alineatul (1) din RGPD 7
4.1 Rolul statelor membre 7
4.2 Interacțiunea cu Regulamentul (CE) 765/2008 7
4.3 Rolul organismului național de acreditare 8
4.4 Rolul autorității de supraveghere 8
4.5 Autoritatea de supraveghere care acționează în calitate de organism de certificare 9
4.6 Cerințe de acreditare 10

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,

ADOPTĂ URMĂTORUL GHID

1 INTRODUCERE

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.

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.

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]

În acest context, Comitetul european pentru protecția datelor recunoaște că este necesar să ofere îndrumări 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.

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

Scopul ghidului 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 GHIDULUI

Prezentul ghid:

- 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.

Ghidul 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.

Ghidul 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].

Definiții

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.

În sensul prezentului ghid, se aplică următoarele definiții:

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

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

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

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

„*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]

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

---

[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 în acel obiect, 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.

[10] Vezi articolul 42 alineatul (5).

„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

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

„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”

În conformitate cu ISO/IEC 17011

„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.”

Articolul 43 alineatul (1) prevede:

„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.”

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.

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

[11] Vezi articolul 2 punctul (11) din Regulamentul 765/2008/CE.

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:

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

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

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 articolul 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 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).

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

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 „*unicul* organism

[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.

dintr-un stat membru care realizează acreditarea dispunând de autoritatea conferită de statul respectiv".

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

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.

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).

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

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

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 temeiul articolul 43 ca „sarcină a autorității de supraveghere", în conformitate cu articolul 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 temeiul articolul 43. Formularea articolului 43 alineatul (1) prevede 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]

[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 ghid.

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, dar fără a se limita la cerințele prevăzute la articolul 43 alineatul (2). 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. În scopul de 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 o autoritate de supraveghere le stabilește în temeiul articolului 43 alineatul (1) litera (b). Comitetul European pentru Protecția Datelor remarcă faptul că articolul 43 alineatul (2) literele (a)-(e) reflectă cerințele ISO 17065, ceea ce va contribui la asigurarea coerenței.

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 capacitatea 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 prezentul ghid 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).

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 accesibilă”. 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.

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

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 Regulamentul (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

[17] Vezi articolul 1 alineatul (2) din RGPD.

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.

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

Anexa la prezentul ghid 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.

Astfel cum s-a stabilit mai sus, în cazul în care organismele de certificare sunt acreditate de organismul național de acreditare în temeiul Regulamentul (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 plus criterii 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).

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.

Comitetul European pentru Protecția Datelor constată că, pe lângă 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 nu este posibilă acreditarea acestor organisme externe în temeiul RGPD. 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.

Cadrul de identificare a cerințelor de acreditare suplimentare prezentate în anexa la prezentul ghid 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.

Pentru Comitetul European pentru Protecția Datelor

Președintele

(Andrea Jelinek)