Avizul 5/2020 privind proiectul de decizie al autorității de supraveghere competente din Luxemburg privind aprobarea cerințelor de acreditare a unui organism de certificare, în conformitate cu articolul 43 alineatul (3) (RGPD)

Adoptat la 29 ianuarie 2020

Adoptat

Cuprins

Comitetul European pentru Protecția Datelor,

având în vedere articolul 63, articolul 64 alineatul (1) litera (c), articolul 64 alineatele (3)-(8) și articolul 43 alineatul (3) 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 articolul 51 alineatul (1) litera (b) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (denumită în continuare „Directiva privind protecția datelor în scopul asigurării respectării legii"),

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

având în vedere articolele 10 și 22 din Regulamentul său de Procedură din 25 mai 2018,

întrucât:

(1) Rolul principal al Comitetului este de a asigura aplicarea coerentă a Regulamentului (UE) 2016/679 (denumit în continuare „RGDP") în întreg Spațiul Economic European. Conform articolului 64 alineatul (1) din RGPD, Comitetul emite un aviz în cazul în care o autoritate de supraveghere intenționează să aprobe cerințele de acreditare a organismelor de certificare în conformitate cu articolul 43. Prin urmare, scopul prezentului aviz este, prin urmare, de a crea o abordare armonizată în ceea ce privește cerințele pe care o autoritate de supraveghere pentru protecția datelor sau organismul național de acreditare le va aplica pentru acreditarea unui organism de certificare. Chiar dacă nu impune un set unic de cerințe de acreditare, RGPD promovează coerența. Comitetul încearcă să atingă acest obiectiv în avizele sale în primul rând prin încurajarea autorităților de supraveghere să-și elaboreze cerințele de acreditare respectând structura prevăzută în anexa la Orientările CEPD privind acreditarea organismelor de certificare și, în al doilea rând, prin examinarea lor folosind un model pus la dispoziție de CEPD, care permite evaluarea comparativă a cerințelor (în conformitate cu ISO 17065 și cu Orientările CEPD privind acreditarea organismelor de certificare).

(2) Conform articolului 43 din RGPD, autoritățile de supraveghere competente adoptă cerințele de acreditare. Acestea aplică totuși mecanismul pentru asigurarea coerenței, pentru a permite consolidarea încrederii în mecanismul de certificare, în special prin stabilirea unui nivel ridicat al cerințelor.

[1] Trimiterile la „Uniune" din prezentul aviz trebuie înțelese ca trimiteri la „SEE".

(3) Deși cerințele de acreditare fac obiectul mecanismului pentru asigurarea coerenței, asta nu înseamnă că cerințele trebuie să fie identice. Autoritățile de supraveghere competente dispun de o marjă de apreciere în ceea ce privește contextul național sau regional și trebuie să respecte legislația locală. Obiectivul avizului CEPD nu este de a obține un set unic de cerințe ale UE, ci de a evita lipsa semnificativă de coerență care poate afecta, de exemplu încrederea în independența sau expertiza organismelor de certificare acreditate.

(4) „Orientările 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor (2016/679)" (denumite în continuare „orientările") și „Orientările 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul 2016/679" vor servi drept elemente comune în contextul mecanismului pentru asigurarea coerenței.

(5) Dacă un stat membru prevede că organismele de certificare urmează să fie acreditate de autoritatea de supraveghere, aceasta ar trebui 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. Pentru a contribui la o abordare armonizată a acreditării, cerințele 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). CEPD remarcă faptul că articolul 43 alineatul (2) literele (a)-(e) reflectă cerințele ISO 17065, fapt care va contribui la asigurarea coerenței.[2]

(6) Avizul CEPD se adoptă în temeiul articolului 64 alineatul (1) litera (c), alineatele (3)-(8) din RGPD, coroborat cu articolul 10 alineatul (2) din Regulamentul de Procedură al CEPD, în termen de opt săptămâni de la prima zi lucrătoare după ce președintele și autoritatea de supraveghere competentă hotărăsc că dosarul este complet. Prin decizia președintelui, această perioadă poate fi prelungită cu șase săptămâni, în funcție de complexitatea chestiunii.

ADOPTĂ URMĂTORUL AVIZ:

1 EXPUNEREA SUMARĂ A FAPTELOR

1. Autoritatea de supraveghere din Luxemburg a prezentat CEPD proiectul său de cerințe de acreditare în conformitate cu articolul 43 alineatul (1) litera (a). În urma unei decizii potrivit căreia dosarul a fost considerat complet, acesta a fost publicat la 25 octombrie 2019. Autoritatea de supraveghere din Luxemburg va efectua acreditarea organismelor de certificare în conformitate cu criteriile de certificare prevăzute de RGPD.

[2] Punctul 39 din Orientări: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_ro.pdf

2. Conform articolului 10 alineatul (2) din Regulamentul de Procedură al Comitetului, din cauza complexității chestiunii în discuție, președintele a hotărât să prelungească perioada inițială de adoptare de opt săptămâni cu încă șase săptămâni.

2 EVALUARE

2.1 Raționamentul general al CEPD cu privire la proiectul de cerințe de acreditare înaintat

Scopul prezentului aviz este de a evalua cerințele de acreditare elaborate de o autoritate de supraveghere, fie în legătură cu ISO 17065, fie ca un set complet de cerințe, cu scopul de a permite unui organism național de acreditare sau unei autorități de supraveghere, în conformitate cu articolul 43 alineatul (1) din RGPD, să ofere acreditarea unui organism de certificare responsabil cu eliberarea și reînnoirea certificării în conformitate cu articolul 42 din RGPD. Acest lucru nu aduce atingere sarcinilor și competențelor autorității de supraveghere competente. În acest caz specific, Comitetul constată că, în conformitate cu legislația națională, autorității de supraveghere din Luxemburg îi revine responsabilitatea de a efectua acreditarea organismelor de certificare. În acest scop, autoritatea de supraveghere din Luxemburg a elaborat un set de cerințe speciale pentru acreditarea organismelor de certificare în coroborare cu un set de criterii de certificare care urmează să fie aprobate oficial.

Evaluarea cerințelor de acreditare are ca scop examinarea variațiilor (completări sau eliminări) din orientări și în special din anexă. În plus, avizul CEPD se concentrează, de asemenea, pe toate aspectele care pot afecta o abordare coerentă în ceea ce privește acreditarea organismelor de certificare.

Trebuie menționat că scopul Orientărilor privind acreditarea organismelor de certificare este de a oferi asistență autorităților de supraveghere și de a defini, totodată, cerințele de acreditare ale acestora. Anexa la orientări nu constituie cerințe de acreditare ca atare. Prin urmare, cerințele de acreditare pentru organismele de certificare trebuie definite de autoritatea de supraveghere într-un mod care să permită aplicarea lor practică și coerentă, în concordanță cu contextul în care își desfășoară activitatea autoritatea de supraveghere.

Comitetul și-a efectuat evaluarea în conformitate cu structura prevăzută în anexa 1 la orientări. În cazul în care prezentul aviz nu conține nicio mențiune despre o anumită secțiune din proiectul de cerințe de acreditare al autorității de supraveghere din Luxemburg, acest lucru înseamnă că comitetul nu formulează observații și nu solicită autorității de supraveghere din Luxemburg să ia măsuri suplimentare. Comitetul constată că autoritatea de supraveghere din Luxemburg a furnizat informații menite să faciliteze evaluarea proiectului de cerințe de acreditare. Avizul comitetului se referă însă numai la proiectele de cerințe de acreditare.

În plus, prezentul aviz nu vizează elementele înaintate de autoritatea de supraveghere din Luxemburg care nu se încadrează în domeniul de aplicare al articolului 43 alineatul (2) din RGPD, precum trimiterile la legislația națională. Cu toate acestea, Comitetul remarcă faptul că legislația națională trebuie să se conformeze RGPD atunci când acest lucru se impune.

2.2 Principalele puncte pe care trebuie să se concentreze evaluarea [articolul 43 alineatul (2) din RGPD și anexa 1 la Orientările CEPD] potrivit cărora cerințele de acreditare prevăd ca următoarele aspecte să fie evaluate într-un mod coerent:

a. abordarea tuturor domeniilor-cheie, astfel cum se subliniază în anexa la orientări și ținând seama de orice abatere de la anexă;

b. independența organismului de certificare;

c. conflictele de interese ale organismului de certificare;

d. expertiza organismului de certificare;

e. măsurile de salvgardare adecvate menite să asigure faptul că criteriile de certificare din RGPD sunt aplicate corespunzător de organismul de certificare;

f. procedurile pentru emiterea, revizuirea periodică și retragerea certificării prevăzute de RGPD; și

g. gestionarea transparentă a reclamațiilor cu privire la încălcările certificării.

3. Având în vedere că:

a. articolul 43 alineatul (2) din RGPD prevede lista domeniilor de acreditare pe care un organism de certificare trebuie să le abordeze pentru a fi acreditat;

b. articolul 43 alineatul (3) din RGPD prevede că cerințele de acreditare a organismelor de certificare se aprobă de autoritatea de supraveghere competentă;

c. articolul 57 alineatul (1) literele (p) și (q) din RGPD prevăd că o autoritate de supraveghere competentă trebuie să elaboreze și să publice cerințele de acreditare a organismelor de certificare și poate hotărî să efectueze chiar ea acreditarea organismelor de certificare;

d. articolul 64 alineatul (1) litera (c) din RGPD prevede că Comitetul emite un aviz în cazul în care o autoritate de supraveghere intenționează să aprobe cerințele de acreditare pentru un organism de certificare în conformitate cu articolul 43 alineatul (3).

comitetul consideră că:

2.2.1 OBSERVAȚII GENERALE

4. Comitetul constată că proiectul de cerințe de acreditare nu respectă complet structura prevăzută în anexa 1 la orientări. De exemplu, lipsesc secțiunile privind „domeniul de aplicare” și „termenii și definițiile”. În această privință, Comitetul constată că unii termeni nu sunt folosiți consecvent în întreg documentul, de exemplu termenii „client” și „solicitant”. Pentru a evita confuziile, când este posibil, termenii folosiți ar trebui armonizați cu orientările și definițiile din anexă și utilizați consecvent. Prin urmare, în scopul de a facilita evaluarea, Comitetul încurajează autoritatea de supraveghere din Luxemburg să respecte structura din anexa 1 [la orientări] în proiectul de cerințe de acreditare și să adauge secțiunile care lipsesc.

5. Comitetul observă că, în întreg documentul, există mai multe trimiteri la cerințele „acestui mecanism de certificare” (de exemplu cerința 4.6.4) sau la organismele de certificare care sunt acreditate „în conformitate cu (...) mecanismul de certificare” (de exemplu cerința 2.2.2). Trimiterea la mecanismul de certificare pare a fi o problemă legată de redactare. Comitetul încurajează, așadar, autoritatea de

supraveghere din Luxemburg să redacteze trimiterile astfel încât să menționeze că organismele de certificare sunt acreditate pe baza cerințelor aprobate de autoritatea de supraveghere.

6. Într-o notă similară, trimiterea la „cerințele prevăzute în acest mecanism de certificare”, utilizate în întreg documentul (de exemplu cerința 1.1.1.2), produce confuzie. O trimitere mai adecvată ar putea fi „criteriile stabilite în mecanismul de certificare”. Astfel, Comitetul încurajează autoritatea de supraveghere din Luxemburg să clarifice toate trimiterile la „mecanismul de certificare” din întreg documentul.

7. Comitetul remarcă faptul că mai multe cerințe (de exemplu, 3.2.1.1 și 4.1.2) se referă la „standardele internaționale relevante”, la „standardul relevant” sau la „standardul specificat”. Nu există însă o definiție a acestor standarde și, prin urmare, nu este clar care sunt standardele la care se face referire. Astfel, Comitetul recomandă autorității de supraveghere din Luxemburg să precizeze semnificația acestor standarde. Acest lucru ar putea fi realizat, de exemplu, în secțiunile „domeniu de aplicare” sau „termeni și definiții”.

2.2.2 CERINȚE GENERALE DE ACREDITARE

8. Comitetul constată că cerința 1.1.1.1 a autorității de supraveghere din Luxemburg se referă la alt standard („ISAE 3000”), pe care CEPD nu l-a evaluat. Prin urmare, Comitetul recomandă autorității de supraveghere din Luxemburg să precizeze că cerințele nu pot fi anulate de niciun standard extern, cum este ISAE 3000.

9. Comitetul constată că cerințele prevăzute în secțiunea 1.6 nu includ obligația organismului de certificare de a publica și de a facilita punerea la dispoziția publicului a tuturor versiunilor cerințelor aprobate și a tuturor procedurilor de certificare, după cum se prevede în anexa la orientări (secțiunea 4.6). Comitetul constată că autoritatea de supraveghere din Luxemburg ar putea fi deținătorul sistemului de certificare, cu toate acestea, Comitetul consideră că ar fi util să se adauge o trimitere adecvată pentru a se asigura faptul că criteriile sunt actualizate și ușor accesibile direct prin organismul de certificare. În acest sens, comitetul consideră că, prin faptul că informațiile sunt puse la dispoziție doar la cerere, așa cum prevede cerința 1.6.1, autoritatea de supraveghere din Luxemburg stabilește o cerință mai strictă decât anexa, care stabilește că informațiile trebuie să fie ușor accesibile publicului. Prin urmare, Comitetul recomandă autorității de supraveghere din Luxemburg să modifice cerința pentru a include obligația organismului de certificare de a face ușor accesibile publicului toate versiunile cerințelor aprobate și toate procedurile de certificare, conform anexei la orientări.

10. Comitetul constată că cerința 1.2.4 se referă la „procesul certificat”. Comitetul consideră că s-ar putea folosi o formulare mai exactă, în concordanță cu orientările, de exemplu „operațiuni/activități de prelucrare certificate”. Aceasta prevede un domeniul de aplicare mai extins al certificării, așa cum se prevede în RGPD. Prin urmare, Comitetul încurajează autoritatea de supraveghere din Luxemburg să modifice proiectul de cerințe în mod corespunzător.

2.2.3 CERINȚE PRIVIND RESURSELE

11. Comitetul constată că cerința 3.1.1.2 pare repetitivă și neclară, devenind ambiguă din cauza terminologiei diferite utilizate. De exemplu, formularea celui de al treilea paragraf prevede că partenerul de angajament ia decizia de adecvare doar pe baza criteriilor sale. Comitetul recomandă autorității de supraveghere din Luxemburg să revizuiască formularea pentru a face cerința mai clară și mai inteligibilă, folosind o terminologie consecventă.

2.2.4 CERINȚE PRIVIND PROCESUL

12. Comitetul observă că cerința 4.2.1 oferă câteva exemple de informații necesare. Cu toate acestea, primele două exemple prezentate ar trebui să constituie în sine o cerință, în conformitate cu secțiunea 7.2 din anexa 1 la orientări. Prin urmare, Comitetul încurajează autoritatea de supraveghere din Luxemburg să modifice formularea și să includă ca cerințe exemplele menționate anterior.

13. În ceea ce privește secțiunea 4.4 (Evaluarea) referitor la cerințele de acreditare ale autorității de supraveghere din Luxemburg, Comitetul consideră că cerințele de acreditare ar trebui să includă obligația organismului de certificare de a se asigura că au fost elaborate metode de evaluare și că metodele de evaluare menționate, descrise în mecanismul de certificare, sunt standardizate și se aplică la nivel general. În acest fel s-ar asigura folosirea de metode de evaluare comparabile pentru obiective de evaluare comparabile. Orice abatere de la aceste metode de evaluare trebuie justificată de organismul de certificare. Prin urmare, Comitetul recomandă autorității de supraveghere din Luxemburg să modifice proiectul pentru a include obligația menționată anterior, care îi revine organismului de certificare.

14. În plus, Comitetul ia notă de faptul că cerința 4.4.2 prevede că, deși externalizarea nu este permisă, organismul de certificare poate apela la experți externi pentru domenii specifice. În acest sens, este important să se precizeze că organismul de certificare va avea în continuare responsabilitatea de a lua deciziile, chiar dacă apelează la experți externi. Prin urmare, Comitetul recomandă autorității de supraveghere din Luxemburg să modifice formularea cerinței 4.4.2 în consecință.

15. Comitetul observă că secțiunea 4.7 din cerințele de acreditare ale autorității de supraveghere din Luxemburg („documentația de certificare”) nu abordează cerința din anexă privind documentarea perioadei de supraveghere (secțiunea 7.9). Prin urmare, Comitetul încurajează autoritatea de supraveghere din Luxemburg să includă perioada de monitorizare în secțiunea 7.9 privind supravegherea.

16. În ceea ce privește secțiunea 4.8 („registrul activităților de prelucrare certificate”) din cerințele de acreditare ale autorității de supraveghere din Luxemburg, cerința 4.8.1 prevede că informațiile vor fi furnizate publicului „la cerere”. Comitetul consideră că obligația de transparență prevăzută în secțiunea 7.8 din anexa 1 ar fi îndeplinită mai eficient dacă organismul de certificare ar pune la dispoziție informațiile în mod proactiv. Prin urmare, Comitetul recomandă autorității de supraveghere din Luxemburg să modifice proiectul pentru a asigura faptul că organismul de certificare pune la dispoziția publicului informațiile menționate în secțiunea 7.8 din anexa 1 la orientări.

17. Comitetul constată că secțiunea 4.8 are o rubrică dedicată supravegherii, care nu conține nicio cerință. Comitetul recomandă autorității de supraveghere din Luxemburg să precizeze cum se va efectua monitorizarea.

18. În ceea ce privește încetarea, reducerea, suspendarea sau retragerea certificării (subsecțiunea 4.10), Comitetul constată că nu există nicio referire la obligația organismului de certificare de a accepta deciziile și ordinele din partea autorității de supraveghere competente de a retrage sau de a nu elibera certificarea unui client (solicitant) dacă cerințele de certificare nu sunt îndeplinite sau încetează să mai fie îndeplinite. Această obligație este prevăzută la articolul 58 alineatul (2) litera (h) din RGPD, precum și în secțiunea 7.11 din anexa 1. Prin urmare, Comitetul recomandă autorității de

supraveghere din Luxemburg să modifice cerințele de acreditare specificând normele privind retragerea, încetarea, reducerea sau suspendarea certificării.

19. Comitetul constată că secțiunea 9 din anexă care are rubrici generale nu conține cerințe. De exemplu, secțiunea 9.3.4 privind suspendarea sau retragerea acreditării nu este inclusă aici. Acestea sunt rubrici importante care oferă trimiteri încrucișate la secțiunile relevante sau la cerințele care sunt adăugate. Comitetul încurajează autoritatea de supraveghere din Luxemburg să precizeze unde sunt acoperite cerințele.

3 CONCLUZII/RECOMANDĂRI

20. Proiectul de cerințe de acreditare al autorității de supraveghere din Luxemburg poate să ducă la aplicarea incoerentă a acreditării organismelor de certificare și trebuie făcute următoarele modificări:

21. Ca observații generale, Comitetul recomandă autorității de supraveghere din Luxemburg:

    1. să precizeze semnificația cuvântului „standard”, menționat în mai multe cerințe (de exemplu, 3.2.1.1 și 4.1.2). Acest lucru ar putea fi realizat, de exemplu, în secțiunile „domeniu de aplicare” sau „termeni și definiții”.

22. În ceea ce privește „cerințele generale de acreditare”, Comitetul recomandă autorității de supraveghere din Luxemburg:

    1. să precizeze că cerințele nu pot fi anulate de niciun standard extern, cum ar fi ISAE 3000;

    2. să modifice cerința din secțiunea 1.6 pentru a include obligația organismului de certificare de a publica și de a face ușor accesibile publicului toate versiunile criteriilor aprobate și toate procedurile de certificare, conform anexei la orientări.

23. În ceea ce privește „cerințele privind resursele”, Comitetul recomandă autorității de supraveghere din Luxemburg:

    1. să reformuleze cerința 3.1.1.2 pentru a o face mai clară și mai ușor de înțeles, folosind o terminologie consecventă.

24. În ceea ce privește „cerințele privind procesul”, Comitetul recomandă autorității de supraveghere din Luxemburg:

    1. să modifice secțiunea 4.4 a proiectului de cerințe pentru a include obligația organismului de certificare de a se asigura că metodele de evaluare au fost elaborate și că metodele de evaluare descrise în mecanismul de certificare, sunt standardizate și se aplică la nivel general. Orice abatere de la metodele de evaluare trebuie justificată de organismul de certificare;

    2. să modifice formularea cerinței 4.4.2 pentru menționa clar că organismul de certificare va avea în continuare responsabilitatea de a lua deciziile, chiar dacă apelează la experți externi;

    3. să modifice secțiunea 4.8 din proiectul său de cerințe de acreditare pentru a preciza că organismul de certificare va pune la dispoziția publicului informațiile menționate în secțiunea 7.8 din anexa 1 la orientări;

4. să precizeze în secțiunea 4.8 modul de desfășurare a monitorizării;

5. să modifice subsecțiunea 4.10 pentru a specifica normele referitoare la retragerea, încetarea, reducerea sau suspendarea certificării.

4 OBSERVAȚII FINALE

25. Prezentul aviz se adresează autorității de supraveghere din Luxemburg și va fi publicat în temeiul articolului 64 alineatul (5) litera (b) din RGPD.

26. Conform articolului 64 alineatele (7) și (8) din RGPD, autoritatea de supraveghere îi va comunica președintelui pe cale electronică în termen de două săptămâni de la primirea avizului, dacă își va păstra sau își va modifica proiectul de listă. În aceeași perioadă, va furniza proiectul de listă modificat sau, dacă nu intenționează să urmeze avizul comitetului, va oferi motivele relevante pentru care nu dorește să urmeze acest aviz, integral sau parțial.

Pentru Comitetul European pentru Protecția Datelor

Președinte

(Andrea Jelinek)