Avizul Comitetului (Articolul 64)

Avizul 14/2020 privind proiectul de decizie al autorității de supraveghere competente din Irlanda privind aprobarea cerințelor de acreditare a unui organism de certificare, în conformitate cu articolul 43 alineatul (3) (RGPD)

Adoptat la 25 mai 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 Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018,[1]

având în vedere articolele 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. În conformitate cu articolul 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 temeiul articolului 43. Prin urmare, scopul prezentului aviz este 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 1 la Orientările nr. 4/2018 ale Comitetului european pentru protecția datelor (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) În legătură cu articolul 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.

3) Deși cerințele de acreditare fac obiectul mecanismului pentru asigurarea coerenței, aceasta nu înseamnă că cerințele ar trebui 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 nr. 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 nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în

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

conformitate cu articolele 42 și 43 din Regulamentul 2016/679" vor servi drept ghid 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) din RGPD. În comparație cu obligațiile referitoare la acreditarea organismelor de certificare de către organismele naționale de acreditare, articolul 43 din RGPD 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 stabilite de o autoritate de supraveghere în temeiul articolului 43 alineatul (1) litera (b) din RGPD. CEPD remarcă faptul că articolul 43 alineatul (2) literele (a)-(e) din RGPD reflectă și specifică cerințele ISO 17065, fapt ce va contribui la asigurarea coerenței.[2]

6) Avizul CEPD se adoptă în temeiul articolului 64 alineatul (1) litera (c), alineatele (3) și (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 Irlanda (denumită în continuare „AS IE") și-a prezentat la CEPD proiectul de cerințe de acreditare în conformitate cu articolul 43 alineatul (1) litera (b). Dosarul a fost considerat complet la 13 februarie 2020. Organismul național de acreditare din Irlanda va efectua acreditarea organismelor de certificare în conformitate cu criteriile de certificare prevăzute de RGPD. Aceasta înseamnă că Organismul național de acreditare din Irlanda va utiliza cerințele ISO 17065 și cerințele suplimentare stabilite de AS IE, după aprobarea acestora de AS IE, în urma unui aviz al comitetului privind proiectele de cerințe, pentru a acredita organismele de certificare.

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

[2] Orientările nr. 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor, punctul 39. Disponibil la adresa: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_ro

2 EVALUARE

2.1 Raționamentul general al Comitetul european pentru protecția datelor cu privire la proiectul de decizie înaintat

3. 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, pentru a-i permite unui organism național de acreditare sau unei autorități de supraveghere, conform articolului 43 alineatul (1) din RGPD, să acrediteze un 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 AS IE a decis să recurgă la organismul său național de acreditare (ONA) pentru emiterea acreditării, după ce a compilat cerințele suplimentare în conformitate cu orientările, care ar trebui utilizate de ONA la emiterea acreditării.

4. Această evaluare a cerințelor suplimentare de acreditare a AS IE are ca scop examinarea variațiilor (completări sau eliminări) din orientări și, în special, din anexa 1 la acestea. În plus, avizul CEPD se concentrează, de asemenea, pe toate aspectele care pot avea un impact asupra unei abordări coerente în ceea ce privește acreditarea organismelor de certificare.

5. Trebuie menționat că scopul orientărilor privind acreditarea organismelor de certificare este de a oferi asistență autorităților de supraveghere și de a defini, totodată, cerințele lor de acreditare. 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.

6. Comitetul recunoaște că, având în vedere expertiza lor, organismele naționale de acreditare ar trebui să beneficieze de libertate de decizie atunci când definesc anumite dispoziții specifice în cadrul cerințelor de acreditare aplicabile. Cu toate acestea, comitetul consideră că este necesar să sublinieze că, în cazul în care sunt stabilite cerințe suplimentare, acestea trebuie definite astfel încât să permită aplicarea și revizuirea lor practică și coerentă, după cum este necesar.

7. Comitetul constată că standardele ISO, în special ISO 17065, fac obiectul drepturilor de proprietate intelectuală și, prin urmare, nu vor face referire la textul documentului aferent din prezentul aviz. În consecință, comitetul a decis, după caz, să indice anumite secțiuni ale standardului ISO, fără să reproducă, totuși, textul.

8. În cele din urmă, comitetul a efectuat propria evaluare în conformitate cu structura prevăzută în anexa 1 la orientări (denumită în continuare „anexa”). În cazul în care prezentul aviz nu conține nicio mențiune cu privire la o anumită secțiune din proiectul de cerințe de acreditare al AS IE, acest lucru înseamnă că comitetul nu formulează observații și nu solicită AS IE să ia măsuri suplimentare.

9. Prezentul aviz nu vizează elementele înaintate de AS IE 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 fie în conformitate cu 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 Comitetului european pentru protecția datelor] potrivit cărora cerințele de acreditare prevăd evaluarea coerentă a următoarelor aspecte:

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

2) independența organismului de certificare;

3) conflictele de interese ale organismului de certificare;

4) expertiza organismului de certificare;

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

6) procedurile pentru emiterea, revizuirea periodică și retragerea certificării prevăzute de RGPD; și

7) gestionarea transparentă a reclamațiilor cu privire la încălcările certificării.

10. 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 decide 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);

e. 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;

f. anexa 1 la Orientările privind acreditarea certificării prevede sugestii de cerințe pe care trebuie să le redacteze o autoritate de supraveghere pentru protecția datelor și care se aplică pe durata acreditării unui organism de certificare de către organismul național de acreditare;

comitetul consideră că:

2.2.1 PREFAȚĂ (Secțiunea 0 a proiectului de cerințe de acreditare al AS IE)

11. Comitetul recunoaște faptul că termenii de cooperare, care reglementează legătura dintre un organism național de acreditare și autoritatea sa de supraveghere pentru protecția datelor, nu constituie o cerință de acreditare a organismelor de certificare în sine. Cu toate acestea, din motive de exhaustivitate și transparență, comitetul consideră că aceste condiții de cooperare, acolo unde există, sunt publicate în formatul pe care autoritatea de supraveghere îl consideră adecvat.

2.2.2 TERMENI ȘI DEFINIȚII

12. Comitetul constată că trimiterea la orientările privind acreditarea ca „WP 261" nu este actualizată. CEPD a adoptat Orientările nr. 4/2018 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul general privind protecția datelor (2016/679). Prin urmare, comitetul încurajează autoritatea de supraveghere din Irlanda să modifice formularea și să facă referire la Orientările nr. 4/2018.

2.2.3 OBSERVAȚII GENERALE

13. Comitetul constată că proiectul de cerințe al autorității de supraveghere din Irlanda se referă în mod repetat la „autoritatea de supraveghere competentă". Întrucât autoritatea de supraveghere competentă în acest caz este AS IE, comitetul încurajează AS IE să înlocuiască trimiterea cu „DPC" sau cu „AS IE", pentru a evita confuziile.

14. Comitetul recunoaște că proiectul de cerințe al AS IE cuprinde o secțiune referitoare la termeni și definiții. Cu toate acestea, unii termeni nu sunt folosiți în mod constant în întreg documentul (de exemplu, „obiect de evaluare" și „ToE"). Pentru a evita orice confuzie, comitetul încurajează AS IE să utilizeze o terminologie coerentă în proiectul de cerințe.

2.2.4 CERINȚE GENERALE DE ACREDITARE (Secțiunea 4 din proiectul de cerințe de acreditare)

15. În ceea ce privește clauza 7 din subsecțiunea 4.1.2 din proiectul de cerințe de acreditare al AS IE, comitetul consideră că formularea este puțin neclară în ceea ce privește persoanele cărora le sunt furnizate motivele pentru aprobarea certificării. În plus, trimiterea la „facilitarea" registrului este, de asemenea, neclară. Prin urmare, comitetul încurajează AS IE să o reformuleze astfel încât să ofere mai multă claritate.

2.2.5 CERINȚE STRUCTURALE (Secțiunea 5 din proiectul de cerințe de acreditare)

16. Comitetul observă că proiectul de cerințe de acreditare al AS IE face referire la numirea „unei persoane cu vechime în funcție relevantă în ceea ce privește responsabilitatea de a supraveghea respectarea protecției datelor și guvernanța informațiilor." Trimiterea la vechimea în funcție relevantă trebuie clarificată în ceea ce privește experiența și sfera de aplicare a autorității. În plus, funcțiile acestei persoane par a fi similare cu cele ale unui responsabil cu protecția datelor. Comitetul încurajează AS IE să stabilească în mod clar funcțiile acestei persoane și să specifice experiența relevantă.

2.2.6 CERINȚE PRIVIND RESURSELE (Secțiunea 6 din proiectul de cerințe de acreditare)

17. În ceea ce privește personalul organismului de certificare (subsecțiunea 6.1), comitetul constată că cerințele pentru personalul cu expertiză tehnică în materie de responsabilitate în luarea deciziilor includ cel puțin 5 ani de experiență profesională legată de obiectul certificării, în timp ce personalul responsabil cu evaluările trebuie să aibă minimum doi ani de experiență profesională. În mod similar, personalul cu expertiză juridică în luarea deciziilor trebuie să aibă cel puțin 5 ani de experiență profesională, în timp ce personalul responsabil cu evaluările trebuie să aibă cel puțin 2 ani de experiență. Comitetul constată că numărul minim necesar de ani de experiență profesională pentru personalul responsabil cu luarea deciziilor și cel pentru personalul responsabil cu evaluările diferă semnificativ. În acest sens, comitetul consideră că accentul ar trebui pus mai curând pe diferitele tipuri de expertiză decât pe numărul de ani de experiență profesională. În opinia comitetului, evaluatorii trebuie să aibă o expertiză mai specializată și o experiență profesională în materie de proceduri tehnice (de exemplu, audituri și certificări), în timp ce factorii decizionali trebuie să aibă expertiză și experiență profesională mai generale și mai cuprinzătoare în materie de protecție a datelor. Având în vedere acest lucru, comitetul încurajează AS IE să pună un accent mai mare pe diferitele cunoștințe și/sau experiență de bază pentru evaluatori și factorii decizionali și să reducă divergențele între anii de experiență necesari pentru aceștia.

2.2.7 CERINȚE PRIVIND PROCESELE (Secțiunea 7 din proiectul de cerințe de acreditare)

18. În ceea ce privește subsecțiunea 7.10 din proiectul de cerințe de acreditare ale AS IE („Modificări care afectează certificarea”), comitetul observă că nu există nicio referire la procedurile de modificare care trebuie convenite, în conformitate cu secțiunea 7.10 din anexă. Comitetul încurajează AS IE să includă o astfel de trimitere și să menționeze o parte din procedurile care ar putea fi puse în aplicare (de exemplu, perioadele de tranziție, procesul aprobărilor cu autoritatea de supraveghere competentă...). În plus, comitetul consideră că modificările în ceea ce privește stadiul actual al tehnologiei sunt, de asemenea, relevante și ar putea afecta certificarea. Prin urmare, comitetul încurajează AS IE să includă această posibilitate pe lista modificărilor care afectează certificarea. În cele din urmă, comitetul salută includerea încălcărilor de date cu caracter personal și a încălcărilor RGPD pe lista modificărilor care pot afecta certificarea. Cu toate acestea, pentru a asigura claritatea, comitetul încurajează AS IE să specifice că încălcările de date sau încălcările RGPD sunt luate în considerare numai în măsura în care au legătură cu certificarea.

19. În ceea ce privește modificările care afectează certificarea (subsecțiunea 7.10 din proiectul de cerințe al AS IE) și, în special, al cincilea punct informativ, comitetul constată că AS IE se referă la „deciziile obligatorii aplicabile ale Comitetului european pentru protecția datelor” și, de asemenea, la articolul 39 din Regulamentul de procedură al CEPD, care conține „toate documentele finale adoptate de CEPD”. Pentru a asigura o înțelegere clară a ceea ce înseamnă „deciziile Comitetului european pentru protecția datelor”, comitetul încurajează AS IE să clarifice trimiterea. Un exemplu ar putea fi trimiterea la „documentele adoptate de Comitetul european pentru protecția datelor”.

20. Comitetul observă că subsecțiunea 7.11 din proiectul de cerințe al AS IE (încetarea, limitarea, suspendarea sau retragerea certificării) nu conține obligația organismului de certificare de a accepta deciziile și ordinele din partea AS IE de a retrage sau de a nu elibera certificarea unui solicitant dacă cerințele pentru certificare nu sunt îndeplinite sau nu mai sunt îndeplinite. Prin urmare, comitetul recomandă AS IE să includă o astfel de obligație.

3 CONCLUZII/RECOMANDĂRI

21. Proiectul de cerințe de acreditare al autorității de supraveghere din Irlanda poate duce la aplicarea incoerentă a acreditării organismelor de certificare și trebuie făcute următoarele modificări:

22. În ceea ce privește „cerințele privind procesul”, comitetul recomandă AS IE:

1) să includă în subsecțiunea 7.11 obligația organismului de certificare de a accepta deciziile și ordinele din partea AS IE de a retrage sau de a nu elibera certificarea unui solicitant dacă cerințele de certificare nu sunt îndeplinite sau încetează să mai fie îndeplinite.

4 OBSERVAȚII FINALE

23. Prezentul aviz se adresează AS IE și va fi publicat în temeiul articolului 64 alineatul (5) litera (b) din RGPD.

24. Conform articolului 64 alineatele (7) și (8) din RGPD, AS IE îi comunică 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, furnizează proiectul de listă modificat sau, dacă nu intenționează să urmeze avizul comitetului, oferă motivele relevante pentru care nu dorește să urmeze acest aviz, integral sau parțial.

25. AS IE comunică comitetului decizia finală pentru a o include în registrul deciziilor care au făcut obiectul mecanismului pentru asigurarea coerenței, în temeiul articolului 70 alineatul (1) litera (y) din RGPD.

Pentru Comitetul european pentru protecția datelor

Președinte

(Andrea Jelinek)