Avizul 15/2020 privind proiectul de decizie al autorităților de supraveghere competente din Germania 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.

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

(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 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 și specifică cerințele ISO 17065, ceea 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. Autoritățile de supraveghere germane de la nivelul federației și al landurilor (denumite în continuare „AS DE") i-au transmis CEPD proiectul de cerințe de acreditare în temeiul articolului 43 alineatul (1) litera (b). Dosarul a fost considerat complet la 13 februarie 2020. Organismul național de acreditare din Germania (ONA), DAkkS, va efectua acreditarea organismelor de certificare în conformitate cu criteriile de certificare prevăzute de RGPD. Aceasta înseamnă că ONA va utiliza cerințele ISO 17065 și cerințele suplimentare stabilite de AS DE, după ce acestea sunt aprobate de AS DE, în urma avizului comitetului privind proiectul de cerințe, pentru a acredita organismele de certificare.

2. Conform articolului 10 alineatul (2) din Regulamentul de procedură al comitetului, din cauza complexității chestiunii în discuție, președintele a decis 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 DE au decis să recurgă la acreditarea comună de către organismul lor național de acreditare (ONA), DAkkS, și AS competentă pentru emiterea acreditării, după ce au compilat cerințele suplimentare în conformitate cu orientările, care ar trebui utilizate la emiterea acreditării.

4. Această evaluare a cerințelor suplimentare de acreditare a AS DE 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 autoritățile de supraveghere astfel încât să permită aplicarea lor practică și coerentă, în concordanță cu contextul în care își desfășoară activitatea autoritățile de supraveghere.

6. Comitetul recunoaște că, având în vedere expertiza lor, organismele naționale de acreditare și autoritățile de supraveghere competente, când este cazul, 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 necesar să sublinieze că, în cazul în care sunt stabilite cerințe suplimentare, acestea ar trebui 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 va face referire la textul documentului respectiv în prezentul aviz. În consecință, comitetul a decis să indice anumite secțiuni ale standardului ISO, dacă este cazul, 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 DE, acest lucru înseamnă că comitetul nu are observații de formulat și nu solicită AS DE să ia măsuri suplimentare.

9. Prezentul aviz nu vizează elementele înaintate de AS DE 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 evaluarea coerentă a următoarelor aspecte:

a. abordarea tuturor domeniilor-cheie evidențiate în anexa la orientări și examinarea oricăror abateri 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. tratarea în mod transparent a plângerilor privind încălcări ale certificării.

10. Având în vedere că:

b. 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;

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

d. 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;

e. 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);

f. 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;

g. 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

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, se publică în formatul pe care autoritatea de supraveghere îl consideră adecvat.

2.2.2 TERMENI ȘI DEFINIȚII

12. Comitetul remarcă faptul că capitolul 3 („Definiții”) din proiectul de cerințe de acreditare al AS DE definește ce tipuri de sisteme de certificare sunt permise, specificând că acestea trebuie să îndeplinească cerințele DIN EN ISO/IEC 17065. În acest sens, trebuie semnalat că secțiunile 5.1 și 5.2 din Orientările CEPD definesc deja ce anume poate fi certificat în temeiul RGPD în mod cuprinzător. Prin urmare, comitetul recunoaște că intenția AS DE este de a nu limita ceea ce se specifică în orientări și că afirmațiile cuprinse în capitolul 3 din proiectul de cerințe de acreditare al AS DE trebuie să fie considerate aplicabile în contextul acestor cerințe de acreditare.

2.2.3 OBSERVAȚII GENERALE

13. Comitetul remarcă faptul că secțiunea „Note generale” din proiectul de cerințe de acreditare al AS DE se referă la „autorizarea” criteriilor de certificare de către CEPD „în conformitate cu articolul 63 și articolul 64 alineatul (1) litera (c) din RGPD”. Comitetul remarcă faptul că RGPD nu conferă CEPD competența de a „autoriza” criterii de certificare. Cu toate acestea, conform articolelor sus-menționate, CEPD poate aproba criterii de certificare. Prin urmare, comitetul recomandă AS DE să elimine trimiterea la „autorizarea de către CEPD”, pentru ca proiectul să corespundă formulării din RGPD.

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

14. În ceea ce privește cerința responsabilității juridice (secțiunea 4.1 din proiectul de cerințe de acreditare al AS DE), comitetul remarcă faptul că, în documentul justificativ, AS DE explică că se așteaptă de la un organism de certificare să dețină proceduri actualizate și, prin urmare, nu este necesar să se adauge cerințe suplimentare în această privință. Cu toate acestea, comitetul consideră că această așteptare nu obligă organismele de certificare să dețină astfel de proceduri. Potrivit celor stabilite în secțiunea 4.1.1 din anexa la orientări, organismele de certificare trebuie să dispună de proceduri actualizate care demonstrează conformitatea cu responsabilitățile juridice stabilite în condițiile de acreditare. În plus, organismul de certificare trebuie să poată demonstra existența unor proceduri și măsuri conforme cu RGPD în mod specific pentru controlul și gestionarea datelor cu caracter personal ale organizației-client ca parte a procesului de certificare. Prin urmare, comitetul recomandă AS DE să modifice proiectul de cerințe, pentru ca acesta să corespundă orientărilor.

15. În ceea ce privește subsecțiunea 4.1.2.2 din proiectul de cerințe de acreditare al AS DE („acordul de certificare”), comitetul remarcă faptul că proiectul de cerințe de acreditare al AS DE nu include obligația de a asigura transparență deplină pentru AS competentă în ceea ce privește procedura de certificare, inclusiv aspectele confidențiale din perspectivă contractuală. În plus, nu există nicio referire la obligația solicitantului de a oferi organismului de certificare acces la activitățile de prelucrare. Prin urmare, comitetul recomandă AS DE să includă obligațiile sus-menționate în proiectul lor.

16. Comitetul constată că trimiterea explicită la sarcinile și la competențele autorității de supraveghere competente (a treia liniuță din secțiunea 4.1.2 din anexă) nu este inclusă în subsecțiunea 4.1.2.2 din

proiectul de cerințe de acreditare al AS DE. Comitetul consideră că această trimitere trebuie să fie adăugată în proiectul de cerințe și, prin urmare, recomandă AS DE să modifice proiectul în consecință.

17. În plus, proiectul de cerințe al AS DE cu privire la acordul de certificare nu include obligația de a permite organismului de certificare să publice toate informațiile necesare pentru acordarea certificării în temeiul articolului 42 alineatul (8) și al articolului 43 alineatul (5) din RGPD (a șaptea liniuță din secțiunea 4.1.2 din anexă). Deși obligația respectivă este inclusă în secțiunea dedicată gestionării procesului din proiectul de cerințe de acreditare al AS DE, comitetul consideră că aceasta trebuie să facă parte din acordul de certificare, pentru a-i consolida caracterul obligatoriu. Astfel, comitetul recomandă AS DE să includă obligația sus-menționată ca parte a elementelor acordului de certificare.

18. Conform anexei, solicitantul trebuie 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 (liniuța a zecea din secțiunea 4.1.2 din anexă). Cu toate acestea, în proiectul de cerințe de acreditare al AS DE, a șasea liniuță din subsecțiunea 4.1.2.2 include doar obligația de a informa organismul de certificare cu privire la modificările semnificative legate de situația sa efectivă sau juridică, însă nu menționează în mod explicit produsele, procesele și serviciile. Comitetul recomandă AS DE să includă o astfel de trimitere, conform anexei.

19. În ceea ce privește subsecțiunea 4.2.7 din proiectul de cerințe de acreditare al AS DE („gestionarea imparțialității"), comitetul recomandă consolidarea criteriilor aplicabile organismelor de certificare care aparțin unei entități juridice separate sau sunt controlate de aceasta, astfel încât să se ia în considerare faptul că orice tip de relație economică dintre organismul de certificare și entitatea juridică, în funcție de caracteristicile sale, poate să afecteze imparțialitatea activităților sale de certificare.

20. În ceea ce privește secțiunea 4.6 din proiectul de cerințe de acreditare al AS DE („informații publice"), comitetul remarcă faptul că nu există nicio trimitere la publicarea tuturor versiunilor criteriilor aprobate și a procedurilor de certificare. Prin urmare, comitetul încurajează AS DE să modifice proiectul de cerințe de acreditare pentru a face explicit faptul că publicarea include toate versiunile criteriilor aprobate și procedurile de certificare. În plus, comitetul remarcă faptul că al doilea punct din secțiunea 4.6 afirmă că „sistemele de certificare folosite de organismul de certificare criteriile aprobate în conformitate cu articolul 42 alineatul (5) din RGPD, care specifică durata de aplicare autorizată, *trebuie să fie în general publicate*." Pentru a evita orice ambiguitate, comitetul încurajează AS DE să elimine sintagma „în general" și să includă un „și" între „organismul de certificare" și „criteriile aprobate".

2.2.5 CERINȚE PRIVIND RESURSELE (capitolul 6 din proiectul de cerințe de acreditare)

21. În ceea ce privește cerințele de expertiză și, în special, subsecțiunea 6.1.2.1 din proiectul de cerințe de acreditare al AS DE („competențele în domeniul resurselor umane"), comitetul remarcă faptul că, la cunoștințele necesare în domeniile enumerate, nu se specifică faptul că aceste cunoștințe trebuie să fie relevante și adecvate. Pentru a asigura coerența cu nivelul de expertiză solicitat în anexă, comitetul recomandă AS DE să alinieze formularea cu orientările, impunând cunoștințe relevante și adecvate.

22. În plus, comitetul remarcă faptul că cerințele pentru personalul cu expertiză tehnică responsabil de luarea deciziilor includ cel puțin 7 ani de experiență profesională sau 5 ani de experiență profesională în protecția datelor tehnice, în funcție de nivelul de pregătire, în timp ce personalul responsabil de evaluări trebuie să aibă 4 ani de experiență profesională sau 2 ani de experiență profesională în protecția datelor tehnice și experiență în procedura de testare, în funcție de nivelul de pregătire. În mod similar, personalul cu expertiză juridică responsabil de luarea deciziilor trebuie să aibă cel puțin 5 ani de experiență profesională în dreptul privind protecția datelor, în timp ce personalul responsabil de evaluări trebuie să aibă cel puțin 2 ani de experiență în dreptul privind protecția datelor și în procedurile de audit. Comitetul constată că numărul minim necesar de ani de experiență profesională pentru personalul responsabil de luarea deciziilor și cel pentru personalul responsabil de evaluări diferă semnificativ. În acest sens, comitetul consideră că cerințele de competență pentru evaluatori și factorii de decizie trebuie să fie adaptate ținându-se cont de sarcinile diferite pe care le îndeplinesc, nu de numărul de ani de experiență. Comitetul consideră că evaluatorii trebuie să aibă expertiză și experiență profesională mai specializate în domeniul procedurilor tehnice (de exemplu, audituri și certificări), în timp ce factorii decizionali trebuie să aibă expertiză și experiență profesională mai generale și mai cuprinzătoare în domeniul protecției datelor. Având în vedere acest lucru, comitetul încurajează AS DE să pună un accent mai mare pe cunoștințe și/sau experiență de bază diferite pentru evaluatori și factorii decizionali și să reducă divergențele între anii de experiență necesari pentru aceștia.

23. În plus, comitetul consideră că cunoașterea sistemelor de management relevante pentru domeniul de certificare trebuie să fie extinsă la ISO/IEC 27701:2019 - Tehnici de securitate - Extensie a ISO/IEC 27001 și ISO/IEC 27002 pentru gestionarea informațiilor privind confidențialitatea - Cerințe și orientări și încurajează AS DE să includă aceste trimiteri.

24. În final, în ceea ce privește cerințele în materie de educație pentru personalul tehnic, comitetul consideră lista disciplinelor este deja adaptată expertizei tehnice impuse de anexă. Prin urmare, comitetul încurajează AS DE să elimine trimiterea la „științe naturale” din lista de discipline în ceea ce privește educația universitară a personalului tehnic.

2.2.6 CERINȚE PRIVIND PROCESELE (capitolul 7 din proiectul de cerințe de acreditare)

25. Comitetul remarcă faptul că capitolul 7 din proiectul de cerințe de acreditare al AS DE face câteva trimiteri la „criteriile sale” (de exemplu în secțiunile 7.4, 7.6, 7.11 și 7.13.). Pentru a evita orice ambiguități, comitetul încurajează AS DE să clarifice sensul termenului respectiv, de exemplu prin adăugarea unei explicații în anexa 1 (Glosar).

26. Cu privire la secțiunea 7.1 din proiectul de cerințe de acreditare al AS DE („informații generale”), comitetul remarcă faptul că nu există nicio trimitere explicită la obligația organismului de certificare de a respecta cerințele suplimentare. Deși această obligație ar putea fi dedusă din textul proiectului de cerințe, comitetul consideră că trebuie să se includă o trimitere explicită la obligația sus-menționată. Prin urmare, comitetul recomandă AS DE să modifice proiectul în consecință.

27. Comitetul constată că proiectul de cerințe suplimentare al AS DE nu conține nicio trimitere la utilizarea unui sigiliu european aprobat privind protecția datelor, conform secțiunii 7.1.2 din anexă.

Comitetul consideră că această trimitere trebuie să fie inclusă, mai ales luând în considerare faptul că acreditarea unui organism de certificare care acordă sigilii europene privind protecția datelor poate fi necesară în fiecare dintre statele membre în care organismul de certificare își are sediul.[3] Prin urmare, comitetul recomandă AS DE să includă trimiterea sus-menționată. De exemplu, proiectul de cerințe ar putea să specifice următoarele: *„AS competentă este notificată înainte ca un organism de certificare să înceapă să utilizeze un sigiliu european aprobat privind protecția datelor într-un nou stat membru dintr-un birou satelit".*

28. Comitetul constată că, în secțiunea 7.2 („cererea"), proiectul de cerințe de acreditare al AS DE prevede situația în care se recurge la utilizarea unor persoane împuternicite de operator pentru a efectua operațiuni de prelucrare a datelor, conform anexei la orientări. Cu toate acestea, comitetul remarcă faptul că, atunci când se recurge la utilizarea unor persoane împuternicite de operator, cererea trebuie să conțină contractul (contractele) relevant(e) dintre operatori și persoanele împuternicite de operatori, conform celor specificate în anexă. Prin urmare, comitetul recomandă AS DE să alinieze formularea la orientări, incluzând trimiteri la contractul (contractele) dintre operatori și persoanele împuternicite de operatori. În plus, comitetul încurajează AS DE să ia în considerare dacă, în acest caz, trebuie menționată o trimitere la operatori asociați și la acordurile specifice dintre aceștia.

29. Comitetul remarcă faptul că secțiunea 7.2 din proiectul de cerințe de acreditare al AS DE menționează că „operatorul de date și persoana împuternicită de operator au dreptul de a solicita certificarea." Posibilitatea ca persoanele împuternicite de operatori să solicite certificarea va depinde de sistemul de certificare specific. Prin urmare, pentru a evita confuziile, comitetul încurajează AS DE să elimine trimiterile de mai sus sau să clarifice că posibilitatea ca persoanele împuternicite de operatori să fie certificate va depinde de sfera de aplicare a sistemului de certificare.

30. În ceea ce privește secțiunea 7.3 din proiectul de cerințe de acreditare al AS DE („cererile de evaluare"), comitetul remarcă faptul că proiectul de cerințe de acreditare al AS DE afirmă că „metodele de evaluare planificate sunt specificate contractual [...]". Pentru a clarifica faptul că aceasta este o cerință, comitetul încurajează AS DE să redacteze din nou primul paragraf, pentru a clarifica faptul că metodele de evaluare trebuie să fie incluse în acordul de certificare - respectiv să redacteze din nou cerința ca fiind „metodele de evaluare planificate trebuie să fie specificate contractual [...]". În plus, comitetul încurajează AS DE să înlocuiască trimiterea la secțiunea 7.3.1.b din ISO 17065 cu secțiunea 7.3 din ISO 17065, pentru a alinia formularea cu anexa. De asemenea, comitetul observă că al patrulea punct se referă la competențele tehnice și juridice adecvate. Din motive de claritate, comitetul încurajează AS DE să adauge „în domeniul protecției datelor".

31. Comitetul observă că secțiunea 7.4 din proiectul de cerințe de acreditare al AS DE („metode de evaluare") nu include obligația organismului de certificare de a descrie suficiente metode de evaluare pentru a evalua conformitatea operațiunii (operațiunilor) de prelucrare cu criteriile de certificare. Comitetul recomandă AS DE să modifice proiectul de cerințe, pentru ca acesta să includă această trimitere. De exemplu, s-ar putea adăuga următorul text: *„Organismul de certificare se asigură că mecanismele utilizate pentru acordarea certificării descriu suficiente metode de evaluare pentru a evalua conformitatea operațiunii (operațiunilor) de prelucrare cu criteriile de certificare."* În

[3] În acest sens, a se vedea Orientările nr. 1/2018, punctul 44.

plus, în ceea ce privește primul domeniu care face obiectul acestor metode de evaluare, comitetul consideră că necesitatea și proporționalitatea se evaluează și în raport cu persoanele vizate în cauză, dacă este necesar. În final, comitetul remarcă faptul că nu există nicio trimitere la documentarea metodelor și a constatărilor. Prin urmare, comitetul încurajează AS DE să modifice proiectul și să includă aceste trimiteri în mod explicit.

32. În ceea ce privește certificările existente (secțiunea 7.4 din proiectul de cerințe de acreditare al AS DE), comitetul consideră că a patra liniuță de la pagina 13 generează confuzie, deoarece este neclar care este legătura dintre perioada de valabilitate a certificării actuale și cea a certificării anterioare și modul în care acestea s-ar corela între ele. De asemenea, nu pare admisibil să se conteste validitatea certificării emise anterior de un alt organism de certificare acreditat. Pe scurt, ar fi necesară o clarificare în acest paragraf în ceea ce privește mențiunea privind relația dintre diferitele elemente. Comitetul recomandă AS DE să modifice proiectul, în special clarificând că durata valabilității certificării în temeiul RGPD nu trebuie să depindă de valabilitatea altor tipuri de certificări.

33. În ceea ce privește secțiunea 7.5 („apreciere”) din proiectul de cerințe de acreditare al AS DE, comitetul încurajează AS DE să modifice titlul secțiunii în „examinare”.

34. Cu privire la modificările care afectează certificarea (secțiunea 7.10 din proiectul de cerințe de acreditare al AS DE), comitetul remarcă faptul că proiectul de cerințe de acreditare al AS DE stabilește că „clientul este informat în timp util cu privire la modificările aduse cadrului juridic care îl afectează”. Ținând cont de necesitatea de a menține imparțialitatea organismului de certificare, comitetul încurajează AS DE să reformuleze propoziția, pentru a clarifica faptul că se pun la dispoziția clientului în timp util informații cu caracter general privind modificările care ar putea să-l afecteze. În plus, pentru a asigura o înțelegere clară a ceea ce înseamnă „decizii ale Comitetului european pentru protecția datelor”, comitetul încurajează AS DE să clarifice trimiterea. Un exemplu ar putea fi trimiterea la „documentele adoptate de Comitetul european pentru protecția datelor”.

35. Comitetul observă că secțiunea 7.11 din proiectul de cerințe de acreditare al AS DE („încetarea, restricționarea, suspendarea sau retragerea certificării”) nu conține obligația organismului de certificare de a accepta deciziile și ordinele din partea AS DE de a retrage sau de a nu elibera certificarea unui solicitant dacă cerințele pentru certificare nu sunt sau nu mai sunt îndeplinite. Prin urmare, comitetul recomandă AS DE să includă o astfel de obligație. În plus, comitetul încurajează AS DE să înlocuiască termenul „restricționare” cu „reducere” în titlul secțiunii, conform anexei la orientări.

2.2.7 ALTE CERINȚE SUPLIMENTARE

36. Referitor la subsecțiunea 8.11.3 din proiectul de cerințe de acreditare al AS DE („gestionarea plângerilor”), comitetul încurajează AS DE să înlocuiască trimiterea la „plângeri justificate” cu „plângeri fondate”, pentru a asigura mai multă claritate.

3 CONCLUZII/RECOMANDĂRI

37. Proiectul de cerințe de acreditare al autorităților de supraveghere germane de la nivelul federației și al landurilor poate să ducă la aplicarea incoerentă a acreditării organismelor de certificare și trebuie făcute următoarele modificări:

38. În ceea ce privește „observațiile generale”, comitetul recomandă AS DE:

a. să elimine trimiterea la „autorizarea de către CEPD”, pentru ca proiectul să corespundă formulării RGPD.

39. În ceea ce privește „cerințele generale de acreditare”, comitetul recomandă ca AS DE:

b. să modifice cerințele referitoare la răspunderea juridică (subsecțiunea 4.1) pentru a le alinia cu orientările;

c. să modifice subsecțiunea 4.1.2.2 în așa fel încât să includă în acordul de certificare obligația de a asigura transparență deplină pentru AS DE în ceea ce privește procedura de certificare și să ofere organismului de certificare acces la activitățile de prelucrare ale solicitantului;

d. să includă, în subsecțiunea 4.1.2.2, o trimitere explicită la sarcinile și la competențele autorității de supraveghere competente, în conformitate cu anexa;

e. să includă, printre elementele acordului de certificare, obligația de a permite organismului de certificare să publice toate informațiile necesare pentru acordarea certificării în temeiul articolului 42 alineatul (8) și al articolului 43 alineatul (5) din RGPD;

f. să includă o trimitere explicită la „produsele, procesele și serviciile vizate de certificare” la a șasea liniuță din subsecțiunea 4.1.2.2;

g. să consolideze, în subsecțiunea 4.2.7, criteriile aplicabile organismelor de certificare care aparțin unei entități juridice separate sau sunt controlate de aceasta, astfel încât să se ia în considerare faptul că orice tip de relație economică dintre organismul de certificare și entitatea juridică, în funcție de caracteristicile sale, poate să afecteze imparțialitatea activităților sale de certificare.

40. În ceea ce privește „cerințele privind resursele”, comitetul recomandă AS DE:

h. să alinieze formularea din subsecțiunea 6.1.2.1 cu orientările, solicitând cunoștințe relevante și adecvate.

41. În ceea ce privește „cerințele privind procesul”, comitetul recomandă AS DE:

i. să modifice secțiunea 7.1 astfel încât aceasta să conțină o trimitere explicită la obligația organismului de certificare de a respecta cerințele suplimentare;

j. să includă o trimitere la utilizarea unui sigiliu european aprobat privind protecția datelor;

k. să alinieze formularea din secțiunea 7.2 cu orientările, incluzând trimiterea la contractul (contractele) dintre operatori și persoanele împuternicite de operatori;

l. să includă în secțiunea 7.4 obligația organismului de certificare de a descrie suficiente metode de evaluare pentru a evalua conformitatea operațiunii (operațiunilor) de prelucrare cu criteriile de certificare;

m. să clarifice în secțiunea 7.4 că durata valabilității certificării în temeiul RGPD nu trebuie să depindă de valabilitatea altor tipuri de certificări;

n. să includă în secțiunea 7.11 obligația organismului de certificare de a accepta deciziile și ordinele din partea AS DE de a retrage sau de a nu elibera certificarea unui solicitant dacă cerințele de certificare nu mai sunt îndeplinite.

4 OBSERVAȚII FINALE

42. Prezentul aviz se adresează autorităților de supraveghere germane de la nivelul federației și al landurilor și va fi publicat în temeiul articolului 64 alineatul (5) litera (b) din RGPD.

43. Conform articolului 64 alineatele (7) și (8) din RGPD, AS DE îi comunică președintelui pe cale electronică, în termen de două săptămâni de la primirea avizului, dacă vor păstra sau vor modifica proiectul de decizie. În aceeași perioadă, acestea furnizează proiectul de decizie modificat sau, dacă nu intenționează să urmeze avizul comitetului, oferă motivele relevante pentru care nu doresc să urmeze acest aviz, integral sau parțial.

44. AS DE comunică comitetului decizia finală pentru a fi inclusă 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)

Adoptat