DECIZIE nr. 20 din 24 iunie 2021 privind aprobarea Cerinţelor suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679

Având în vedere prevederile art. 42 alin. (1) din Regulamentul (UE) **2016/679** privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei **95/46/CE**, denumit în continuare *Regulamentul general privind protecţia datelor*,

ţinând cont de prevederile art. 43 din Regulamentul general privind protecţia datelor, referitoare la organismele de certificare, prin care se dispune că statele membre se asigură că organismele de certificare pot fi acreditate de organismul naţional de acreditare desemnat în conformitate cu Regulamentul (CE) nr. **765/2008** al Parlamentului European şi al Consiliului de stabilire a cerinţelor de acreditare şi de supraveghere a pieţei în ceea ce priveşte comercializarea produselor şi de abrogare a Regulamentului (CEE) nr. **339/93**, în conformitate cu standardul EN-ISO/IEC 17065/2012 şi cu cerinţele suplimentare stabilite de Autoritatea naţională de supraveghere, competentă potrivit art. 55 sau 56 din Regulamentul general privind protecţia datelor,

având în vedere calitatea oficială a Asociaţiei de Acreditare din România - RENAR de organism naţional de acreditare, în temeiul Regulamentului (CE) nr. **765/2008**, al Ordonanţei Guvernului nr. **23/2009** privind activitatea de acreditare a organismelor de evaluare a conformităţii, aprobată cu modificări prin Legea nr. **256/2011**, precum şi al Legii nr. **190/2018** privind măsuri de punere în aplicare a Regulamentului (UE) **2016/679** al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei **95/46/CE** (Regulamentul general privind protecţia datelor), cu modificările ulterioare,

în considerarea Standardului european EN-ISO/IEC 17065/2012 (Standardul român SR EN ISO/CEI 17065:2013 este identic cu Standardul european EN-ISO/IEC 17065/2012 şi are acelaşi statut ca şi versiunile oficiale, fiind publicat cu permisiunea Organizaţiei Comune Europene de Standardizare),

având în vedere documentul emis de Comitetul european pentru protecţia datelor intitulat "Orientările nr. 1/2018 privind certificarea şi identificarea criteriilor de certificare în conformitate cu articolele 42 şi 43 din Regulamentul general privind protecţia datelor", versiunea 3.0 din 4 iunie 2019,

ţinând cont de faptul că organismul de certificare din România - RENAR a fost consultat de Autoritatea naţională de supraveghere cu privire la proiectul de document conţinând Cerinţele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**,

ţinând cont de art. 64 alin. (1) lit. c) din Regulamentul general privind protecţia datelor, potrivit căruia Comitetul european pentru protecţia datelor emite un aviz de fiecare dată când o autoritate de supraveghere competentă intenţionează să aprobe cerinţe pentru acreditarea unui organism de certificare în conformitate cu art. 43 alin. (3) sau a criteriilor de certificare menţionate la art. 42 alin. (5) din Regulamentul general privind protecţia datelor,

luând în considerare Avizul nr. 13 din 23 martie 2021 al Comitetului european pentru protecţia datelor privind proiectul de "Cerinţe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**", întocmit de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter

Personal,
în baza Notei Direcţiei juridice şi comunicare nr. 125 din 7.08.2020 cu privire la proiectul de Decizie privind "Cerinţele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**",
în temeiul prevederilor art. 3 alin. (5) şi (6) şi ale art. 10 alin. (1) lit. a) şi b) din Legea nr. **102/2005** privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, precum şi ale art. 6 alin. (2) lit. b) din **Regulamentul de organizare şi funcţionare a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal**, aprobat prin Hotărârea Biroului permanent al Senatului nr. **16/2005**, cu modificările şi completările ulterioare,
preşedintele Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal emite prezenta decizie.

Art. 1

Se aprobă Cerinţele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**, prevăzute în anexa care face parte integrantă din prezenta decizie.

Art. 2

Prezenta decizie intră în vigoare la data publicării în Monitorul Oficial al României, Partea I.

-****-

Preşedintele Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal,
Ancuţa Gianina Opre

ANEXĂ: CERINŢELE SUPLIMENTARE pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679

CAPITOLUL I: Introducere

Regulamentul (UE) **2016/679** privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei **95/46/CE** (Regulamentul general privind protecţia datelor) prevede că statele membre, autorităţile de supraveghere, comitetul şi Comisia Europeană încurajează instituirea de mecanisme de certificare în domeniul protecţiei datelor, precum şi de sigilii şi mărci în acest domeniu, care să permită demonstrarea faptului că operaţiunile de prelucrare efectuate de operatori şi de persoanele împuternicite de operatori respectă această reglementare, luându-se în considerare necesităţile specifice ale microîntreprinderilor, ale întreprinderilor mici şi mijlocii.

Corelat cu aceste prevederi, art. 43 din Regulamentul (UE) **2016/679** dispune că statele membre se asigură că organismele de certificare pot fi acreditate de organismul naţional de acreditare desemnat în conformitate cu Regulamentul (CE) nr. **765/2008** al Parlamentului European şi al Consiliului, în conformitate cu standardul EN-ISO/IEC 17065/2012 şi cu cerinţele suplimentare stabilite de autoritatea naţională de supraveghere.

La nivelul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare *ANSPDCP*) a fost elaborat prezentul document care conţine "Cerinţe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**".

La întocmirea documentului conţinând cerinţele suplimentare au fost luate în considerare o serie de documente, printre care şi cerinţele EN-ISO/IEC 17065/2012 şi Ghidul nr. 1/2018 privind certificarea şi identificarea criteriilor de certificare, document adoptat de Comitetul european pentru protecţia datelor.

Standardul european EN-ISO/IEC 17065/2012 este identic cu standardul român SR EN ISO/CEI 17065:2013.

SR EN ISO/CEI 17065:2013 reprezintă versiunea română a textului în limba engleză a standardului european EN-ISO/IEC 17065/2012 care a fost tradus de ASRO (Organismul naţional de standardizare din România), are acelaşi statut ca versiunile oficiale şi a fost publicat cu permisiunea CEN (Organizaţia Comună Europeană de Standardizare).

De asemenea, având în vedere calitatea oficială a Asociaţiei de Acreditare din România - RENAR de organism naţional de acreditare, în temeiul Regulamentului (CE) nr. **765/2008** şi al Ordonanţei Guvernului nr. **23/2009** privind activitatea de acreditare a organismelor de evaluare a conformităţii, aprobată cu modificări prin Legea nr. **256/2011**, acesta a fost consultat cu privire la conţinutul documentului intitulat "Cerinţe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) **2016/679**".

CAPITOLUL II: Scopul

Acest document conţine cerinţe suplimentare la EN-ISO/IEC 17065/2012 pentru evaluarea competenţei, funcţionării consecvente şi imparţialităţii organismelor de certificare a protecţiei datelor.

Domeniul de aplicare al EN-ISO/IEC 17065/2012 se aplică în conformitate cu Regulamentul (UE) **2016/679**. Orientările privind acreditarea şi certificarea oferă informaţii suplimentare. Domeniul de aplicare al unui mecanism de certificare (de exemplu, certificarea operaţiunilor de prelucrare a serviciilor cloud) va fi luat în considerare în evaluarea de către RENAR şi ANSPDCP în timpul procesului de acreditare, în special în ceea ce priveşte criteriile, expertiza şi metodologia de evaluare. Domeniul larg de aplicare al EN-ISO/IEC 17065/2012 care acoperă produsele, procesele şi serviciile nu trebuie să diminueze sau să înlocuiască cerinţele Regulamentului (UE) **2016/679**, de exemplu, un mecanism de guvernanţă nu poate fi singurul element al unui mecanism de certificare, deoarece certificarea trebuie să includă prelucrarea datelor cu caracter personal, adică operaţiunile de prelucrare. În conformitate cu art. 42 alin. (1) din Regulamentul (UE) **2016/679**, certificarea se aplică numai operaţiunilor de prelucrare ale operatorilor şi ale persoanelor împuternicite de operatori.

CAPITOLUL III: Definiţii

În contextul prezentului document se aplică termenii şi definiţiile din îndrumările privind acreditarea (Orientările Comitetului european pentru protecţia datelor 4/2018) şi certificarea (Orientările Comitetului european pentru protecţia datelor 1/2018), iar acestea au întâietate faţă de definiţiile oferite de standardul EN-ISO/IEC 17065/2012.

Pentru a facilita o înţelegere comună, principalele definiţii sunt prezentate mai jos:

- *certificare*: evaluarea şi atestarea imparţială efectuate de o parte terţă conform căreia îndeplinirea criteriilor de certificare a fost demonstrată în contextul certificării în conformitate cu art. 42 şi 43 din Regulamentul (UE) **2016/679** cu privire la operaţiunile de prelucrare de către operatori şi persoanele împuternicite de operatori;
- *acreditare*: atestarea terţilor legată de activităţile unui organism de evaluare a conformităţii care transmite o demonstraţie formală a competenţei sale de a efectua certificarea în conformitate cu art. 42 şi 43 din Regulamentul (UE) **2016/679**. Acesta este rezultatul procesului de evaluare pentru un organism de certificare de succes (ca parte a procesului de acreditare);
- *organism de certificare*: organisme terţe de evaluare a conformităţii care operează scheme de certificare;
- *criterii de certificare*: criteriile pe baza cărora se realizează o certificare pentru o anumită schemă de certificare;
- *schema de certificare*: un sistem de certificare legat de anumite produse, procese şi

servicii cărora li se aplică aceleaşi cerinţe, norme şi proceduri. Aceasta include în principal criteriile de certificare şi metodologia de evaluare;
- *mecanism de certificare*: sistemul prin care un operator sau o persoană împuternicită de operator devine certificat/ă. Este un sistem de certificare aprobat, care este disponibil solicitantului cu un set de proceduri existente. Este un serviciu furnizat de un organism de certificare acreditat pe baza criteriilor aprobate şi a metodologiei de evaluare;
- *obiectivul evaluării (target of evaluation - ToE)*: obiectul certificării. În cazul certificării, acestea vor fi operaţiunile de prelucrare relevante pe care operatorul sau persoana împuternicită de operator le aplică pentru a fi evaluate şi certificate;
- *solicitant*: organizaţia care a solicitat certificarea operaţiunilor sale de prelucrare;
- *client*: organizaţia care a fost certificată.

CAPITOLUL IV: Cerinţe generale privind acreditarea

SECŢIUNEA 1: 4.1. Aspecte legale şi contractuale

(1) 4.1.1. Responsabilitate legală

Un organism de certificare trebuie să poată demonstra (în-orice moment) Asociaţiei de Acreditare din România - RENAR că dispune de proceduri actualizate care demonstrează conformitatea cu responsabilităţile juridice stabilite în condiţiile de acreditare, inclusiv cerinţele suplimentare referitoare la aplicarea Regulamentului (UE) **2016/679**. Trebuie reţinut faptul că, întrucât organismul de certificare este el însuşi un operator de date/o persoană împuternicită de către un operator, acesta trebuie să poată demonstra existenţa unor proceduri şi măsuri conforme cu Regulamentul (UE) **2016/679**, în mod specific pentru controlul şi prelucrarea datelor cu caracter personal ale organizaţiei-client ca parte a procesului de certificare.

ANSPDCP poate decide să adauge alte cerinţe şi proceduri pentru a verifica dacă organismele de certificare respectă dispoziţiile Regulamentului (UE) **2016/679** înainte de acreditare.

(2) 4.1.2. Acord de certificare

În plus faţă de cerinţele prevăzute în EN-ISO/IEC 17065/2012, organismul de certificare trebuie să demonstreze că acordul său de certificare (contractul dintre organismul de certificare şi client):

1. impune solicitantului să respecte întotdeauna atât cerinţele de certificare generale în sensul pct. 4.1.2.2 lit. (a) din EN-ISO/IEC 17065/2012, cât şi criteriile aprobate de ANSPDCP sau de Comitetul european pentru protecţia datelor, în conformitate cu art. 43 alin. (2) lit. (b) şi art. 42 alin. (5) din Regulamentul (UE) **2016/679**;

2. impune solicitantului să asigure transparenţa deplină pentru ANSPDCP în ceea ce priveşte procedura de certificare, inclusiv aspectele confidenţiale din perspectivă contractuală legate de respectarea protecţiei datelor, în temeiul art. 42 alin. (7) şi al art. 58 alin. (1) lit. (c) din Regulamentul (UE) **2016/679**;

3. nu reduce responsabilitatea solicitantului în ceea ce priveşte respectarea Regulamentului (UE) **2016/679** şi nu aduce atingere sarcinilor şi competenţelor ANSPDCP, în conformitate cu art. 42 alin. (5) din Regulamentul (UE) **2016/679**;

4. impune solicitantului să furnizeze organismului de certificare toate informaţiile şi să permită acestuia accesul la activităţile sale de prelucrare necesare pentru desfăşurarea procedurii de certificare, în temeiul art. 42 alin. (6) din Regulamentul (UE) **2016/679**;

5. impune solicitantului să respecte termenele-limită şi procedurile aplicabile. Acordul de certificare trebuie să stipuleze că termenele-limită şi procedurile care rezultă, de exemplu, din programul de certificare sau din alte reglementări trebuie să fie respectate şi asumate;

6. stabileşte regulile privind validitatea, reînnoirea şi retragerea certificării, în

conformitate cu art. 42 alin. (7) şi art. 43 alin. (4) din Regulamentul (UE) **2016/679**, inclusiv normele care stabilesc intervalele adecvate pentru reevaluare sau examinare (regularitate), în conformitate cu art. 42 alin. (7) din Regulamentul (UE) **2016/679**;

7. permite organismului de certificare să publice toate informaţiile necesare pentru acordarea sau retragerea certificării, în temeiul art. 42 alin. (8) şi al art. 43 alin. (5) din Regulamentul (UE) **2016/679**;

8. include norme privind măsurile de precauţie necesare pentru investigarea reclamaţiilor; conţine, de asemenea, declaraţii explicite privind structura şi procedura pentru gestionarea reclamaţiilor, în conformitate cu art. 43 alin. (2) lit. (d) din Regulamentul (UE) **2016/679**;

9. stabileşte consecinţele pentru clientul organismului de certificare în cazul în care acreditarea organismului de certificare a fost suspendată sau retrasă şi acest lucru are impact asupra clientului, precum şi paşii care trebuie luaţi;

10. impune solicitantului să informeze organismul de certificare în eventualitatea unor modificări semnificative legate de situaţia sa de fapt sau juridică şi în privinţa produselor, proceselor şi serviciilor sale vizate de certificare.

(3) 4.1.3. Utilizarea sigiliilor şi mărcilor în domeniul protecţiei datelor

Certificatele, sigiliile şi mărcile se utilizează numai în conformitate cu art. 42 şi 43 din Regulamentul (UE) **2016/679** şi cu îndrumările privind acreditarea şi certificarea.

O copie a sigiliului/mărcii/logoului va fi furnizată ANSPDCP.

SECŢIUNEA 2: 4.2. Managementul imparţialităţii

Organismul de acreditare (RENAR) asigură că, în plus faţă de cerinţa de la pct. 4.2. din EN-ISO/IEC 17065/2012,

1. organismul de certificare respectă cerinţele suplimentare ale ANSPDCP [în temeiul art. 43 alin. (1) lit. (b) din Regulamentul (UE) **2016/679**]:

a) în conformitate cu art. 43 alin. (2) lit. (a) din Regulamentul (UE) **2016/679**, oferă dovezi separate ale independenţei sale. Aceasta se aplică îndeosebi dovezilor referitoare la finanţarea organismului de certificare în măsura în care aceasta are legătură cu asigurarea imparţialităţii;

b) sarcinile şi obligaţiile sale nu conduc la un conflict de interese în temeiul art. 43 alin. (2) lit. (e) din Regulamentul (UE) **2016/679**;

2. organismul de certificare nu are o legătură relevantă cu clientul pe care îl evaluează, spre exemplu organismul de certificare nu ar trebui să aparţină aceluiaşi grup de companii şi nici nu ar trebui controlat în vreun fel de clientul pe care îl evaluează.

SECŢIUNEA 3: 4.3. Răspundere juridică şi finanţare

În plus faţă de cerinţa de la pct. 4.3.1 din EN-ISO/IEC 17065/2012, organismul de acreditare (RENAR) asigură periodic că organismul de certificare dispune de măsuri adecvate (de exemplu, asigurare sau rezerve) pentru a-şi acoperi obligaţiile în regiunile geografice în care operează.

Organismul de certificare trebuie să îşi demonstreze stabilitatea şi independenţa financiară. Organismul de certificare trebuie să aibă o asigurare de răspundere civilă adecvată domeniului de activitate. Valoarea asigurării de răspundere civilă trebuie să fie stabilită pe baza rezultatelor evaluării riscurilor care decurg din activităţile sale.

SECŢIUNEA 4: 4.4. Condiţii nediscriminatorii

Se aplică cerinţele EN-ISO/IEC 17065/2012.

SECŢIUNEA 5: 4.5. Confidenţialitate

Se aplică cerinţele EN-ISO/IEC 17065/2012.

SECŢIUNEA 6: 4.6. Informaţii disponibile public

În plus faţă de cerinţa de la pct. 4.6 din EN-ISO/IEC 17065/2012, organismul de acreditare (RENAR) solicită organismului de certificare să asigure cel puţin ca:

1. toate versiunile (actuale şi anterioare) ale criteriilor aprobate utilizate în sensul art. 42 alin. (5) din Regulamentul (UE) **2016/679** să fie publicate şi uşor de accesat de către public, la fel ca toate procedurile de certificare care indică, în general, perioada respectivă de validitate. Forma de publicare trebuie să fie adecvată pentru a informa publicul într-un mod cât mai cuprinzător. Acest lucru este de obicei garantat prin formularul electronic;

2. informaţiile privind procedurile de soluţionare a reclamaţiilor şi căile de atac să fie puse la dispoziţia publicului în temeiul art. 43 alin. (2) lit. (d) din Regulamentul (UE) **2016/679**. În acelaşi timp, această obligaţie de publicare nu se referă numai la incidente specifice, ci şi la structura şi procedura de gestionare a reclamaţiilor de către organismul de certificare. Informaţiile care sunt făcute publice se referă doar la statistici sau alte tipuri de informaţii anonimizate.

CAPITOLUL V: Cerinţe referitoare la structură

SECŢIUNEA 1: 5.1. Structura organizaţională şi managementul de cel mai înalt nivel

Se aplică cerinţele EN-ISO/IEC 17065/2012.

SECŢIUNEA 2: 5.2. Mecanismul pentru asigurarea imparţialităţii

În plus, potrivit cap. 5.2 (capitolele 5.1.1 şi 5.2) din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să demonstreze ANSPDCP, în cadrul procedurii de acreditare, faptul că mecanismul de asigurare a independenţei îndeplineşte cerinţele art. 43 alin. (2) lit. (a) şi (e) din Regulamentul (UE) **2016/679** şi că sarcinile şi obligaţiile sale nu conduc la un conflict de interese. Independenţa înseamnă că organismul de certificare în cauză poate acţiona fără instrucţiuni şi presiuni, iar stabilitatea financiară este asigurată.

CAPITOLUL VI: Cerinţe referitoare la resurse

SECŢIUNEA 1: 6.1. Personalul organismului de certificare

(1) În plus faţă de cerinţa din capitolul 6 al EN-ISO/IEC 17065/2012, organismul de acreditare (RENAR) se asigură, pentru fiecare organism de certificare, că personalul acestuia:

1. deţine expertiză adecvată şi continuă demonstrată (cunoştinţe şi experienţă) în ceea ce priveşte protecţia datelor, în temeiul art. 43 alin. (1) din Regulamentul (UE) **2016/679**;

2. dispune de independenţă şi expertiză continuă în legătură cu obiectul certificării, în temeiul art. 43 alin. (2) lit. (a) din Regulamentul (UE) **2016/679**, şi nu se află în conflict de interese, în temeiul art. 43 alin. (2) lit. (e) din Regulamentul (UE) **2016/679**;

3. se angajează să respecte criteriile menţionate la art. 42 alin. (5), în temeiul art. 43 alin. (2) lit. (b) din Regulamentul (UE) **2016/679**;

4. dispune de cunoştinţe şi experienţă relevante şi adecvate în ceea ce priveşte aplicarea legislaţiei în materie de protecţie a datelor;

5. dispune de cunoştinţe şi experienţă relevante şi adecvate în ceea ce priveşte măsurile tehnice şi organizatorice relevante de protecţie a datelor;

6. poate demonstra că deţine experienţă în domeniile menţionate în cerinţele suplimentare prevăzute la subpct. 1, 4 şi 5.

(2) În cazul personalului care deţine expertiză tehnică:

- trebuie să aibă o calificare într-un domeniu relevant de expertiză tehnică cel puţin la nivelul 6 CEC[1] sau un titlu protejat recunoscut (de exemplu, dovada experienţei, contractele anterioare, atestarea de către angajatorii anteriori) în profesia reglementată relevantă sau deţine experienţă profesională semnificativă;

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

- personalul responsabil de deciziile de certificare trebuie să aibă experienţă profesională semnificativă în identificarea şi punerea în aplicare a măsurilor de protecţie a datelor; aceasta poate fi dovedită cu documente referitoare la calificări profesionale adecvate, cursuri etc., care să ateste calificările sau competenţele necesare, în măsura în care sunt relevante;
- personalul responsabil de evaluări trebuie să deţină şi să demonstreze cel puţin doi ani de experienţă profesională în protecţia datelor, precum şi cunoştinţe tehnice şi experienţă în ceea ce priveşte proceduri similare (de exemplu, certificări/audituri, dovada experienţei, contractele anterioare, atestarea de către angajatorii anteriori); acestea pot fi dovedite cu documente referitoare la calificări profesionale adecvate, cursuri etc., care să ateste calificările sau competenţele necesare, în măsura în care sunt relevante.

Personalul trebuie să demonstreze că îşi menţine cunoştinţele specifice domeniului (competenţele tehnice şi de audit) printr-o dezvoltare profesională continuă.

(3) În cazul personalului care deţine expertiză juridică:

- trebuie să aibă studii juridice în cadrul unei universităţi din UE sau al unei universităţi recunoscute de stat, pe o perioadă de cel puţin opt semestre, inclusiv diplomă de master (LL. M. - A Master of Laws degree) sau echivalentul acesteia ori experienţă profesională semnificativă;
- personalul responsabil de deciziile de certificare trebuie să deţină şi să demonstreze o experienţă profesională semnificativă în domeniul privind protecţia datelor; aceasta poate fi dovedită cu documente referitoare la calificări profesionale adecvate, cursuri etc., care să ateste calificările sau competenţele necesare;
- personalul responsabil de evaluări trebuie să demonstreze cel puţin doi ani de experienţă profesională în domeniul privind protecţia datelor şi cunoştinţe şi experienţă în ceea ce priveşte procedurile comparabile (de exemplu, certificări/audituri, dovada experienţei, contractele anterioare, atestarea de către angajatorii anteriori); acestea pot fi dovedite cu documente referitoare la calificări profesionale adecvate, cursuri etc., care să ateste calificările sau competenţele necesare.

Personalul trebuie să demonstreze că îşi menţine competenţele specifice domeniului (competenţele tehnice şi/sau juridice), precum şi de audit printr-o formare profesională continuă.

SECŢIUNEA 2: 6.2. Resurse pentru evaluare

Se aplică cerinţele EN-ISO/IEC 17065/2012.

CAPITOLUL VII: Cerinţe referitoare la proces

SECŢIUNEA 1: 7.1. Generalităţi

În plus faţă de cerinţa din capitolul 7.1 din EN-ISO/IEC 17065/2012, organismul de acreditare (RENAR) are obligaţia de a asigura următoarele:

1. organismele de certificare respectă cerinţele suplimentare ale autorităţii de supraveghere competente [în temeiul art. 43 alin. (1) lit. (b) din Regulamentul (UE) **2016/679**] atunci când depun cererea, astfel încât sarcinile şi obligaţiile să nu conducă la un conflict de interese, în temeiul art. 43 alin. (2) lit. (b) din Regulamentul (UE) **2016/679**;

2. informează autorităţile de supraveghere competente relevante înainte ca un organism de certificare să înceapă să utilizeze un sigiliu european privind protecţia datelor într-un stat membru nou dintr-un punct de lucru.

SECŢIUNEA 2: 7.2. Solicitare

În plus faţă de cerinţa de la capitolul 7.2 din EN-ISO/IEC 17065/2012, obiectivul

evaluării (ToE) trebuie să fie descris în detaliu în cerere. Aceasta include, de asemenea, interfeţe şi transferuri către alte sisteme şi organizaţii, protocoale şi alte elemente de asigurare. De asemenea, cererea trebuie să specifice dacă se recurge la persoane împuternicite de către operatori şi, în cazul în care persoanele împuternicite de către operatori au calitatea de solicitant, responsabilităţile şi sarcinile acestora trebuie descrise, iar cererea trebuie să conţină contractul (contractele) relevant(e) dintre operatori şi persoanele împuternicite de către operatori.

În plus, cererea trebuie să specifice dacă operatorii asociaţi sunt implicaţi în prelucrare şi, în cazul în care operatorii asociaţi sunt solicitanţii, responsabilităţile şi sarcinile lor trebuie descrise, iar cererea trebuie să conţină aranjamentele convenite.

Operatorul şi persoana împuternicită de operator au dreptul să solicite certificarea, având în vedere că posibilitatea persoanelor împuternicite de operator de a fi certificate va depinde de domeniul de aplicare al schemei de certificare.

SECŢIUNEA 3: 7.3. Analiza solicitării

În plus faţă de capitolul 7.3 din EN-ISO/IEC 17065/2012, în acordul de certificare trebuie să fie prevăzute metode de evaluare obligatorii în ceea ce priveşte obiectul evaluării şi luând în considerare legea privind protecţia datelor aplicabilă clientului. Totodată, evaluarea de la capitolul 7.3 litera (e) din EN-ISO/IEC 17065/2012 privind existenţa unui nivel suficient de expertiză trebuie să ţină seama atât de expertiza tehnică, cât şi de cea juridică în domeniul protecţiei datelor, în măsura adecvată.

SECŢIUNEA 4: 7.4. Evaluare

(1) În plus faţă de capitolul 7.4 din EN-ISO/IEC 17065/2012, mecanismele de certificare trebuie să descrie metode de evaluare suficiente pentru evaluarea conformităţii operaţiunii (operaţiunilor) de prelucrare cu criteriile de certificare, inclusiv, de exemplu, după caz:

1. o metodă de evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu scopul lor şi persoanele vizate respective;

2. o metodă de evaluare a acoperirii, alcătuirii şi evaluării tuturor riscurilor avute în vedere de către operator şi persoana împuternicită de către operator în ceea ce priveşte consecinţele juridice în temeiul art. 30, 32, 35 şi 36 din Regulamentul (UE) **2016/679**, precum şi definiţia măsurilor tehnice şi organizatorice în temeiul art. 24, 25 şi 32 din Regulamentul (UE) **2016/679**, în măsura în care articolele menţionate mai sus se aplică domeniului certificării (inclusiv obiectului certificării); şi

3. o metodă de evaluare a măsurilor de remediere, inclusiv garanţii, elemente de protecţie şi proceduri, pentru asigurarea protecţiei datelor cu caracter personal în contextul prelucrării care urmează să fie atribuite domeniului certificării (inclusiv obiectului certificării), precum şi pentru demonstrarea faptului că cerinţele juridice, astfel cum sunt prevăzute în criterii, sunt respectate; şi

4. documentarea metodelor şi constatărilor.

(2) Organismul de certificare trebuie să se asigure că aceste metode de evaluare sunt standardizate şi aplicabile în mod general. Aceasta înseamnă că se utilizează metode de evaluare similare pentru domenii de certificare (inclusiv obiecte ale certificării) similare. Orice abatere de la această procedură trebuie justificată de organismul de certificare.

(3) În plus faţă de pct. 7.4.2 din ISO/IEC 17065/2012, ar trebui să se permită ca evaluarea să fie efectuată de experţi externi care au fost recunoscuţi de organismul de certificare. De asemenea, organismul de certificare îşi va păstra responsabilitatea pentru luarea deciziilor, chiar şi atunci când foloseşte experţi externi.

(4) În plus faţă de capitolul 7.4.5 din EN-ISO/IEC 17065/2012, trebuie să se impună ca certificarea protecţiei datelor în conformitate cu art. 42 şi 43 din Regulamentul (UE) **2016/679**, care acoperă deja o parte din obiectul certificării, să poată fi inclusă într-o

certificare curentă. Cu toate acestea, nu va fi suficientă înlocuirea completă a evaluărilor (parţiale). Organismul de certificare are obligaţia de a verifica respectarea criteriilor. Recunoaşterea necesită, în orice caz, disponibilitatea unui raport de evaluare complet sau a informaţiilor care să permită o evaluare a activităţii de certificare existente şi a rezultatelor acesteia. O declaraţie de certificare sau atestate de certificare similare nu trebuie considerate suficiente pentru a înlocui un raport.

(5) Certificările existente pot fi luate în considerare în mod special după cum urmează:

1. Certificarea privind protecţia datelor în conformitate cu art. 42 din Regulamentul (UE) **2016/679**, în cazul în care părţi ale obiectului de certificare au fost deja certificate de către un organism de certificare acreditat, poate fi considerată o evaluare parţială.

2. Cu toate acestea, certificările privind protecţia datelor conform art. 42 din Regulamentul (UE) **2016/679** nu sunt acceptabile pentru a înlocui complet evaluările (parţiale). Organismul de certificare continuă să fie obligat să verifice conformitatea actuală cu cerinţele (certificatului depus), cel puţin aleatoriu, şi să evalueze certificările existente. Nu rezultă efecte asupra perioadei de valabilitate a certificării prezentate.

3. Perioada de validitate a certificatelor trebuie documentată şi păstrată disponibilă în conformitate cu capitolul 7.7 din EN-ISO/IEC 17065/2012.

(6) _

În plus faţă de capitolul 7.4.6 din EN-ISO/IEC 17065/2012, trebuie să se impună ca organismul de certificare să stabilească în detaliu, în cadrul mecanismului său de certificare, modul în care, prin datele solicitate la capitolul 7.4.6, clientul (solicitantul certificării) este informat cu privire la neconformităţile din cadrul unui mecanism de certificare. În acest context, trebuie să se definească cel puţin natura şi calendarul acestor date.

În plus faţă de capitolul 7.4.9 din EN-ISO/IEC 17065/2012, trebuie să se impună ca documentaţia să fie pusă integral la dispoziţia ANSPDCP, la cerere.

Documentaţia trebuie să fie complet accesibilă în timpul procedurii de acreditare şi în orice moment, la cererea ANSPDCP.

SECŢIUNEA 5: 7.5. Analiză

În plus faţă de capitolul 7.5 din EN-ISO/IEC 17065/2012, sunt necesare proceduri de acordare, de examinare periodică şi de revocare a certificărilor respective în temeiul art. 43 alin. (2) şi (3).

SECŢIUNEA 6: 7.6. Decizia de certificare

În plus faţă de capitolul 7.6.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să stabilească în detaliu, în cadrul procedurilor sale, modul în care sunt asigurate independenţa şi responsabilitatea cu privire la deciziile de certificare individuale.

În plus faţă de capitolul 7.6.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să precizeze în detaliu criteriile sale, cum sunt asigurate independenţa şi responsabilitatea faţă de deciziile de certificare.

În conformitate cu capitolul 7.8 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să publice o scurtă evaluare publică a rezultatului certificării.

Organismul de certificare informează ANSPDCP cu privire la certificare. Informaţiile scrise trebuie să includă numele clientului, descrierea obiectului certificării şi o scurtă evaluare publică. Această activitate de informare a ANSPDCP se realizează în scop de transparenţă şi nu implică acţiuni din partea ANSPDCP.

În plus faţă de capitolul 7.6.2 din EN-ISO/IEC 17065/2012, decizia privind certificarea trebuie să fie luată de şeful organismului de certificare sau de o persoană calificată desemnată direct de acesta. În acest sens, trebuie să se respecte capitolul 7.6.3 din EN-ISO/IEC 17065/2012. Evaluarea poate fi realizată de experţi, recunoscuţi anterior

de organismul de certificare, aşa cum este descris în plus faţă de capitolul 7.4.2 din EN-ISO/IEC 17065/2012.

În plus faţă de pct. 7.6.6 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să precizeze în criteriile sale modul în care clientul va fi informat despre decizia de a nu acorda certificarea. În plus, trebuie să informeze clientul privind posibilitatea de a cere reconsiderarea deciziei organismului de certificare în cazul menţionat mai sus şi procedura pe care trebuie să o respecte clientul.

SECŢIUNEA 7: 7.7. Documentaţie de certificare

În plus faţă de capitolul 7.7.1 litera (e) din EN-ISO/IEC 17065/2012 şi în conformitate cu art. 42 alin. (7) din Regulamentul (UE) **2016/679**, perioada de validitate a certificatelor emise de organismul de certificare trebuie să nu depăşească trei ani.

În plus faţă de capitolul 7.7.1 litera (e) din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să documenteze perioada de monitorizare în sensul capitolului 7.9 din EN-ISO/IEC 17065/2012.

În plus faţă de capitolul 7.7.1 litera (f) din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să precizeze domeniul certificării în documentaţia certificării (indicând statutul versiunii sau caracteristici similare, dacă este aplicabil).

SECŢIUNEA 8: 7.8. Registrul produselor certificate

(1) În plus faţă de capitolul 7.8 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să menţină informaţiile privind produsele, procesele şi serviciile certificate disponibile pe plan intern şi pentru public. Organismul de certificare va pune la dispoziţia publicului o sinteză a raportului de evaluare. Scopul acestei sinteze este de a contribui la asigurarea transparenţei în ceea ce priveşte elementele certificate şi modul în care au fost evaluate. Aceasta va explica aspecte precum:

a) domeniul certificării şi o descriere pertinentă a obiectului certificării (obiectivul evaluării);

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

c) metodele de evaluare şi testele efectuate, precum şi

d) rezultatul (rezultatele).

(2) În plus, informaţiile trebuie să includă:

1. datele de contact ale solicitantului (persoană juridică sau fizică);

2. un număr de înregistrare;

3. data certificării şi data expirării certificatului;

4. informaţii despre certificarea iniţială sau recertificare;

5. informaţii despre posibilele activităţi de supraveghere pentru a păstra certificarea; precum şi

6. posibila implicare a evaluatorilor externi.

(3) În plus faţă de capitolul 7.8 din EN-ISO/IEC 17065/2012 şi în temeiul art. 43 alin. (5) din Regulamentul (UE) **2016/679**, organismul de certificare informează autorităţile de supraveghere competente cu privire la motivele pentru acordarea sau retragerea certificării solicitate.

SECŢIUNEA 9: 7.9. Supraveghere

În plus faţă de capitolele 7.9.1, 7.9.2 şi 7.9.3 din EN-ISO/IEC 17065/2012 şi în conformitate cu art. 43 alin. (2) lit. (c) din Regulamentul (UE) **2016/679**, organismul de certificare trebuie să impună ca măsurile de monitorizare periodică să fie obligatorii pentru menţinerea certificării.

Supravegherea trebuie efectuată cel puţin o dată pe an. Cu toate acestea, ar trebui să existe o abordare bazată pe riscuri pentru a identifica dacă, în cazuri specifice, activităţile de supraveghere trebuie să se desfăşoare de mai multe ori pe an.

Procedura şi acordul de certificare cu clientul trebuie să fie demonstrate în orice

moment pe parcursul perioadei de valabilitate a acreditării şi la cererea autorităţilor de supraveghere pentru protecţia datelor.

SECŢIUNEA 10: 7.10. Modificări care afectează certificarea

(1) În plus faţă de capitolele 7.10.1 şi 7.10.2 din EN-ISO/IEC 17065/2012, modificările cu impact asupra certificării care trebuie luate în considerare de organismul de certificare includ: modificări ale legislaţiei privind protecţia datelor sau ale stadiului tehnicii, adoptarea de acte delegate ale Comisiei Europene în conformitate cu art. 43 alin. (8) şi (9) din Regulamentul (UE) **2016/679**, documente adoptate ale Comitetului european pentru protecţia datelor şi decizii ale instanţelor judecătoreşti legate de protecţia datelor. Procedurile legate de modificări pot include aspecte precum: perioadele de tranziţie, procesele de aprobare cu ANSPDCP, reevaluarea domeniului certificării (inclusiv obiectul certificării) şi măsuri adecvate de revocare a certificării, în cazul în care operaţiunea de prelucrare certificată nu mai respectă criteriile actualizate.

(2) Pe lângă capitolul 7.10.1 din EN-ISO/IEC 17065/2012, organismul de certificare defineşte în schema sa de certificare:

1. care modificări necesită o notificare şi, dacă este cazul, o ajustare pentru client;

2. care sunt metodele de evaluare de către organismul de certificare într-un astfel de caz; şi

3. ce termene există pentru implementarea măsurilor pentru a menţine certificarea existentă.

(3) Dincolo de acest aspect, organismul de certificare defineşte modul în care se asigură că sunt efectuate audituri comparabile în proceduri de certificare comparabile dacă cerinţele de certificare se modifică.

(4) În plus, organismul de certificare defineşte, de asemenea, ce măsuri şi procese trebuie luate dacă auditul duce la concluzia că certificarea nu poate fi menţinută. Măsurile corespunzătoare şi procesele corespunzătoare sunt puse în aplicare şi menţinute la dispoziţie de către conducerea organismului de certificare.

(5) În plus faţă de capitolul 7.10.2 din EN-ISO/IEC 17065/2012, organismul de certificare va defini în schema sa de certificare în ce cazuri şi în ce fel clientul trebuie să furnizeze organismului de certificare informaţii (în cazul modificărilor iniţiate de client). Acesta este întotdeauna cazul, cel puţin atunci când au apărut modificări în obiectul certificării cu privire la prelucrarea datelor cu caracter personal, modificări în mediul operaţional şi/sau modificări în contextul aplicaţiei sau modificări în alte condiţii-cadru care sunt relevante pentru declaraţia de certificare. Aceasta se aplică în special modificărilor standardelor legale pertinente privind obiectul certificării, precum şi modificărilor tehnologiei de ultimă generaţie care au fost determinate de client. În acest caz, orice măsuri iniţiate prin notificare trebuie definite de organismul de certificare şi de client. De asemenea, organismul de certificare defineşte modul de asigurare a luării unor măsuri comparabile în cazuri comparabile. De asemenea, organismul de certificare are obligaţia să ia în considerare modificările notificate de client pe baza pct. 7.10.2 din EN-ISO/IEC 17065/2012. În plus, măsurile corespunzătoare şi procesele corespunzătoare sunt puse în aplicare şi menţinute la dispoziţie de către conducerea organismului de certificare.

SECŢIUNEA 11: 7.11. Încetarea, reducerea, suspendarea sau retragerea certificării

În plus faţă de capitolul 7.11.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să informeze imediat, în scris, ANSPDCP şi organismul naţional de acreditare (RENAR), după caz, cu privire la măsurile adoptate şi menţinerea, restrângerea, suspendarea certificării în aşteptarea acţiunilor de remediere efectuate de client şi retragerea certificării.

În conformitate cu art. 58 alin. (2) lit. (h) din Regulamentul (UE) **2016/679**, i se impune organismului de certificare să accepte deciziile şi ordinele autorităţii de supraveghere competente de a retrage sau a nu emite certificarea pentru un client (solicitant) în cazul în care cerinţele de certificare nu sunt sau nu mai sunt îndeplinite.

SECŢIUNEA 12: 7.12. Înregistrări

Organismul de certificare trebuie să păstreze toată documentaţia completă, inteligibilă, actualizată şi adecvată pentru a face obiectul unui audit.

Aceasta se aplică atât procedurilor de certificare finalizate fără un rezultat pozitiv, procedurilor de certificare finalizate cu un rezultat pozitiv, cât şi procedurilor de certificare în curs. În procedurile de certificare în curs, criteriile de certificare care sunt îndeplinite şi care nu sunt îndeplinite trebuie să fie evidente.

În plus, organismul de certificare trebuie să păstreze statistici privind procedurile finalizate şi încheiate.

În plus faţă de capitolul 7.12.1 din EN-ISO/IEC 17065/2012, toate înregistrările referitoare la procesul de certificare se păstrează încă trei ani în plus faţă de perioada de validitate a certificării şi după finalizarea acordului de certificare. În cazul disputelor dintre organismul de certificare şi client sau dintre client şi ANSPDCP, această perioadă poate fi prelungită peste perioada de valabilitate a certificării până la încÕeierea acestei proceduri.

SECŢIUNEA 13: 7.13. Reclamaţii şi căi de atac

(1) În plus faţă de capitolul 7.13.1 din EN-ISO/IEC 17065/2012, trebuie să i se impună organismului de certificare să definească:

a) cine poate depune reclamaţii sau prezenta obiecţiuni;

b) cine le prelucrează la nivelul organismului de certificare;

c) ce verificări au loc în acest context; şi

d) posibilităţile de consultare a părţilor interesate.

(2) În plus faţă de capitolul 7.13.2 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să definească:

a) cum şi cui o astfel de confirmare trebuie transmisă;

b) termenele-limită pentru aceasta; şi

c) procesele care urmează să fie iniţiate ulterior.

(3) În plus faţă de capitolul 7.13.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să definească modul în care este asigurată separarea între activităţile de certificare şi soluţionare a reclamaţiilor şi căilor de atac.

CAPITOLUL VIII: Cerinţele sistemului de management

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

Principiul de bază al gestionării este acela de a defini un sistem potrivit căruia obiectivele sale sunt stabilite cu eficacitate şi eficienţă, în mod specific: punerea în aplicare a serviciilor de certificare - prin intermediul unor specificaţii adecvate. Aceasta necesită transparenţa şi posibilitatea verificării punerii în aplicare a cerinţelor de acreditare de către organismul de certificare şi conformitatea permanentă a acestuia.

În acest scop, sistemul de gestionare trebuie să specifice o metodologie care să îndeplinească şi să controleze aceste cerinţe, în conformitate cu normele privind protecţia datelor şi în vederea verificării constante a acestora împreună cu organismul acreditat însuşi.

Aceste principii de gestionare şi punerea lor documentată în aplicare trebuie să fie

transparente şi să fie publicate de către organismul de certificare acreditat în baza procedurii de acreditare în temeiul art. 58 din Regulamentul (UE) **2016/679** şi, ulterior, la cererea ANSPDCP, în orice moment în timpul unei investigaţii sub forma unor controale privind protecţia datelor în temeiul art. 58 alin. (1) lit. (b) din Regulamentul (UE) **2016/679**, sau a unei examinări a certificărilor emise în conformitate cu art. 42 alin. (7) din Regulamentul (UE) **2016/679**, în temeiul art. 58 alin. (1) lit. (c) din Regulamentul (UE) **2016/679**.

În special, organismul de certificare acreditat trebuie să publice în permanenţă şi în mod continuu certificările efectuate şi bazele acestora (sau mecanismele ori schemele de certificare), durata valabilităţii certificărilor şi care sunt cadrele şi condiţiile aplicabile [considerentul 100 din Regulamentul (UE) **2016/679**].

8.1. Opţiuni

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.2. Documentaţia generală a sistemului de management

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.3. Controlul documentelor

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.4. Controlul înregistrărilor

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.5. Analiza efectuată de management

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.6. Audituri interne

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.7. Acţiuni corective

Se aplică cerinţele EN-ISO/IEC 17065/2012.

8.8. Acţiuni preventive

Se aplică cerinţele EN-ISO/IEC 17065/2012.

CAPITOLUL IX: Alte cerinţe suplimentare

SECŢIUNEA 1: 9.1. Actualizarea metodelor de evaluare

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

SECŢIUNEA 2: 9.2. Menţinerea expertizei

Organismele de certificare stabilesc proceduri pentru a asigura formarea angajaţilor lor în vederea actualizării competenţelor acestora, ţinând seama de evoluţiile enumerate la pct. 9.1.

SECŢIUNEA 3: 9.3. Responsabilităţi şi competenţe

(1) 9.3.1. Comunicarea între organismele de certificare şi clienţii lor

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

1. păstrarea documentaţiei referitoare la sarcini şi responsabilităţi de către organismul de certificare acreditat, în scopul:

a) cererilor de informaţii sau

b) pentru a permite contactul în eventualitatea unei plângeri legate de o certificare;

2. menţinerea unui proces de solicitare în scopul:

a) informării cu privire la statutul solicitării;

b) evaluării efectuate de ANSPDCP cu privire la:

(i)feedback;

(ii)deciziile ANSPDCP.

(2) 9.3.2. Documentarea activităţilor de evaluare

Nu sunt stabilite cerinţe suplimentare.

(3) 9.3.3. Gestionarea soluţionării plângerilor

Se instituie o procedură de soluţionare a plângerilor ca parte integrantă a sistemului de gestionare, care pune în aplicare, în mod special, cerinţele de la pct. 4.1.2.2 lit. (c), pct. 4.1.2.2 lit. (j), pct. 4.6 lit. (d) şi pct. 7.13 din ISO/IEC 17065/2012.

Plângerile şi obiecţiunile relevante ar trebui împărtăşite cu ANSPDCP.

(4) 9.3.4. Gestionarea retragerilor

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

Publicat în Monitorul Oficial cu numărul 689 din data de 12 iulie 2021