ROMÂNIA
AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld. Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel. +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

Cerințe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679

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, autoritățile de supraveghere, comitetul și Comisia Europeană încurajează instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă această reglementare, luându-se în considerare necesitățile specifice ale microîntreprinderilor, ale întreprinderilor mici și 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 național de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului, în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea națională de supraveghere.

La nivelul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Carcter Personal a fost elaborat prezentul document care conține ”Cerințe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679”.

La întocmirea documentului conținând cerințele suplimentare au fost luate în considerare o serie de documente, printre care și cerințele EN-ISO/IEC 17065/2012 și Ghidul nr. 1/2018 privind certificarea și identificarea criteriilor de certificare, document adoptat de Comitetul european pentru protecția 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 engleza a standardului european EN-ISO/IEC 17065/2012 care a fost tradus de ASRO (Organismul Național de Standardizare din România), are același statut ca și versiunile oficiale și a fost publicat cu permisiunea CEN (Organizația Comună Europeană de Standardizare).

De asemenea, având în vedere calitatea oficială a Asociației de Acreditare din România – RENAR de organism național de acreditare, în temeiul Regulamentului (CE) nr. 765/2008 și al O.G. nr. 23/2009, acesta a fost consultat cu privire la conținutul documentului intitulat ”Cerințe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679”.

I. CAPITOLUL 3: DEFINIȚII

În contextul prezentului document se aplică termenii și definițiile din îndrumările privind acreditarea (documentul WP 261) și certificarea (”Orientările Comitetului European pentru Protecția Datelor 1/2018”), iar acestea au întâietate față de definițiile oferite de standardul EN-ISO/IEC 17065/2012.

II. CAPITOLUL 4: CERINȚE GENERALE PRIVIND ACREDITAREA

4.1 Aspecte legale și contractuale

4.1.1 Responsabilitate legală

Un organism de certificare trebuie să poată demonstra (în orice moment) către Asociaţiei de Acreditare din România – RENAR că dispune de proceduri actualizate care demonstrează conformitatea cu responsabilitățile juridice stabilite în

condițiile de acreditare, inclusiv cerințele suplimentare referitoare la aplicarea Regulamentului (UE) 2016/679. Trebuie reținut faptul că, întrucât organismul de certificare este el însuși un operator de date/o persoană împuternicită de către un operator, acesta trebuie să poată demonstra existența unor proceduri și măsuri conforme cu Regulamentul (UE) 2016/679 în mod specific pentru controlul și prelucrarea datelor cu caracter personal ale organizației-client ca parte a procesului de certificare.

Autoritatea de supraveghere competentă poate decide să adauge alte cerințe și proceduri pentru a verifica dacă organismele de certificare respectă dispozițiile RGPD înainte de acreditare.

4.1.2 Acord de certificare

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

1. impune solicitantului să respecte întotdeauna atât cerințele de certificare generale în sensul punctului 4.1.2.2 litera (a) din EN-ISO/IEC 17065/2012, cât și criteriile aprobate de autoritatea de supraveghere competentă sau de Comitetul European pentru Protecția Datelor în conformitate cu articolul 43 alineatul (2) litera (b) și articolul 42 alineatul (5) din Regulamentul (UE) 2016/679;

2. impune solicitantului să asigure transparența deplină pentru autoritatea de supraveghere competentă în ceea ce privește procedura de certificare, inclusiv aspectele confidențiale din perspectivă contractuală legate de respectarea protecției datelor în temeiul articolului 42 alineatul (7) și al articolului 58 alineatul (1) litera (c) din Regulamentul (UE) 2016/679;

3. nu reduce responsabilitatea solicitantului în ceea ce privește respectarea Regulamentului (UE) 2016/679 și nu aduc atingere sarcinilor și competențelor autorităților de supraveghere competente în conformitate cu articolul 42 alineatul (5) din Regulamentul (UE) 2016/679;

4. impune solicitantului să furnizeze organismului de certificare toate informațiile și să permită acestuia accesul la activitățile sale de prelucrare necesare pentru desfășurarea procedurii de certificare în temeiul articolului 42 alineatul (6) din Regulamentul (UE) 2016/679;

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

6. stabilește regulile privind validitatea, reînnoirea și retragerea cerificării în conformitate cu articolul 42 alineatul (7) și articolul 43 alineatul (4) din Regulamentul (UE) 2016/679, inclusiv normele care stabilesc intervalele adecvate pentru reevaluare sau examinare (regularitate) în conformitate cu articolul 42 alineatul (7) din Regulamentul (UE) 2016/679;

7. permite organismului de certificare să publice toate informațiile necesare pentru acordarea sau retragerea certificării în temeiul articolului 42 alineatul (8) și al articolului 43 alineatul (5) din Regulamentul (UE) 2016/679;

8. include norme privind măsurile de precauție necesare pentru investigarea reclamațiilor; conține, de asemenea, declarații explicite privind structura și procedura pentru gestionarea reclamațiilor în conformitate cu articolul 43 alineatul (2) litera (d) din Regulamentul (UE) 2016/679;

9. stabilește consecințele pentru clientul organismului de cerificare în cazul în care acreditarea organismului de certificare a fost suspendată sau retrasă și acest lucru are impact asupra clientului;

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

4.1.3 Utilizarea sigiliilor și mărcilor în domeniul protecției datelor

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

O copie a sigiliului/mărcii/logo-ului va fi furnizată Autorității de supraveghere.

4.2 Managementul imparțialității

Organismul de acreditare (RENAR) asigură că, în plus față de cerința de la punctul 4.2. din EN-ISO/IEC 17065/2012,

1. organismul de certificare respectă cerințele suplimentare ale autorității de supraveghere competente [în temeiul articolului 43 alineatul (1) litera (b) din Regulamentul (UE) 2016/679]

a. în conformitate cu articolul 43 alineatul (2) litera (a) din Regulamentul (UE) 2016/679, oferă dovezi separate ale independenței sale. Aceasta se aplică îndeosebi dovezilor referitoare la finanțarea organismului de certificare în măsura în care aceasta are legătură cu asigurarea imparțialității;

b. sarcinile și obligațiile sale nu conduc la un conflict de interese în temeiul articolului 43 alineatul (2) litera (e) din Regulamentul (UE) 2016/679;

2. organismul de certificare nu are o legătură relevantă cu clientul pe care îl evaluează.

4.3 Răspundere juridică și finanțare

În plus față de cerința de la punctul 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-și acoperi obligațiile în regiunile geografice în care operează.

Organismul de certificare trebuie să-și demonstreze stabilitatea și independența 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 activitățile sale.

4.4 Condiții nediscriminatorii

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

4.5 Confidențialitate

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

4.6 Informații disponibile public

În plus față de cerința de la punctul 4.6 din EN-ISO/IEC 17065/2012, organismul de acreditare solicită organismului de certificare să asigure cel puțin ca:

1. toate versiunile (actuale și anterioare) ale criteriilor aprobate utilizate în sensul articolului 42 alineatul (5) din Regulamentul (UE) 2016/679 să fie publicate și ușor 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 printr-o mod cât mai cuprinzător. Acest lucru este de obicei garantat prin formularul electronic.
2. informațiile privind procedurile de soluționare a reclamațiilor și căile de atac să fie puse la dispoziția publicului în temeiul articolului 43 alineatul (2) litera (d) din Regulamentul (UE) 2016/679. În același timp, această obligație de publicare nu se referă numai la incidente individuale, ci și la structura și procedura de gestionare a reclamațiilor de către organismul de certificare.

III. CAPITOLUL 5: CERINȚE REFERITOARE LA STRUCTURĂ

5.1 Structura organizațională și managementul de cel mai înalt nivel

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

5.2 Mecanismul pentru asigurarea imparțialității

Autoritatea de supraveghere poate formula cerințe suplimentare.

Potrivit cerinței 3.13 din EN-ISO/IEC 17065/2012, imparțialitatea organismului de certificare este dată numai dacă sunt garantate independența și obiectivitatea acestuia.

În plus, la capitolul 5.2 (capitolele 5.1.1 și 5.2) din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să demonstreze autorității de supraveghere competente în domeniul protecției datelor, în cadrul procedurii de acreditare, faptul că mecanismul de asigurare a independenței îndeplinește cerințele art. 43 alineatul (2) literele (a) și (e) din Regulamentul (UE) 2016/679 și că sarcinile și obligațiile sale nu conduc la un conflict de interese. Independența înseamnă că organismul de certificare în cauză poate acționa fără instrucțiuni și presiuni, iar stabilitatea financiară este asigurată.

IV. CAPITOLUL 6: CERINȚE REFERITOARE LA RESURSE

6.1 Personalul organismului de certificare

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

1. deține expertiză adecvată și continuă demonstrată (cunoștințe și experiență) în ceea ce privește protecția datelor, în temeiul articolului 43 alineatul (1) din Regulamentul (UE) 2016/679;
2. dispune de independență și expertiză continuă în legătură cu obiectul certificării, în temeiul articolului 43 alineatul (2) litera (a) din Regulamentul (UE) 2016/679, și nu se află în conflict de interese, în temeiul articolului 43 alineatul (2) litera (e) din Regulamentul (UE) 2016/679;
3. se angajează să respecte criteriile menționate la articolul 42 alineatul (5), în temeiul articolului 43 alineatul (2) litera (b) din Regulamentul (UE) 2016/679;
4. dispune de cunoștințe și experiență relevante și adecvate în ceea ce privește aplicarea legislației în materie de protecție a datelor;
5. dispune de cunoștințe și experiență relevante și adecvate în ceea ce privește măsurile tehnice și organizatorice relevante de protecție a datelor.

6. poate demonstra că deține experiență în domeniile menționate în cerințele suplimentare 6.1.1, 6.1.4 și 6.1.5.

În cazul personalului care deține expertiză tehnică:

- trebuie să aibă o calificare într-un domeniu relevant de expertiză tehnică cel puțin la nivelul 6 CEC[1] sau un titlu protejat recunoscut (de exemplu, inginer diplomat) în profesia reglementată relevantă sau deține experiență profesională semnificativă.
- *Personalul responsabil de deciziile de certificare* trebuie să aibă experiență profesională semnificativă în identificarea și punerea în aplicare a măsurilor de protecție a datelor; aceasta poate fi dovedită cu documente referitoare la calificări profesionale adecvate, cursuri, etc., care să ateste calificările sau competețele necesare, în măsura în care sunt relevante.
- *Personalul responsabil de evaluări* trebuie să dețină și să demonstreze cel puțin doi ani de experiență profesională în protecția datelor, precum și cunoștințe tehnice și experiență în ceea ce privește proceduri similare (de exemplu, certificări/audituri); acestea pot fi dovedite cu documente referitoare la calificări profesionale adecvate, cursuri, etc., care să ateste calificările sau competețele necesare, în măsura în care sunt relevante.

Personalul trebuie să demonstreze că își menține cunoștințele specifice domeniului (competențele tehnice și de audit) printr-o dezvoltare profesională continuă.

În cazul personalului care deține expertiză juridică:

- trebuie să aibă studii juridice în cadrul unei universități din UE sau al unei universități recunoscute de stat, pe o perioadă de cel puțin opt semestre, inclusiv diplomă de master (LL.M. - A Master of Laws degree) sau echivalentul acesteia ori experiență profesională semnificativă.
- *Personalul responsabil de deciziile de certificare* trebuie să dețină și să demonstreze o experiență profesională semnificativă în domeniul privind protecția datelor; aceasta poate fi dovedită cu documente referitoare la calificări profesionale adecvate, cursuri, etc., care să ateste calificările sau competețele necesare, în măsura în care sunt relevante.

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

- *Personalul responsabil de evaluări* trebuie să demonstreze cel puțin doi ani de experiență profesională în domeniul privind protecția datelor și cunoștințe și experiență în ceea ce privește procedurile comparabile (de exemplu, certificări/audituri); acestea pot fi dovedite cu documente referitoare la calificări profesionale adecvate, cursuri, etc., care să ateste calificările sau competețele necesare, în măsura în care sunt relevante.

Personalul trebuie să demonstreze că își menține competențele specifice domeniului (competențele tehnice și/sau juridice), precum și de audit printr-o formare profesională continuă.

6.2 Resurse pentru evaluare

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

V. CAPITOLUL 7: CERINȚE REFERITOARE LA PROCES

7.1 Generalități

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

1. organismele de certificare respectă cerințele suplimentare ale autorității de supraveghere competente [în temeiul articolului 43 alineatul (1) litera (b) din Regulamentul (UE) 2016/679] atunci când depun cererea, astfel încât sarcinile și obligațiile să nu conducă la un conflict de interese, în temeiul articolului 43 alineatul (2) litera (b) din Regulamentul (UE) 2016/679;
2. informează autoritățile de supraveghere competente relevante înainte ca un organism de certificare să înceapă să utilizeze un sigiliu european privind protecția datelor într-un stat membru nou.

7.2 Solicitare

În plus față de cerința de la capitolul 7.2 din EN-ISO/IEC 17065/2012, domeniul certificării (inclusiv obiectul certificării/obiectivul evaluării) trebuie să fie

descris în detaliu în cerere. Aceasta include, de asemenea, interfețe și transferuri către alte sisteme și organizații, protocoale și alte elemente de asigurare. De asemenea, cererea trebuie să specifice dacă se recurge la persoane împuternicite de către operatori și, în cazul în care persoanele împuternicite de către operatori au calitatea de solicitant, responsabilitățile și sarcinile acestora trebuie descrise, iar cererea trebuie să conțină contractul (contractele) relevant(e) dintre operatori și persoanele împuternicite de către operatori.

Operatorul și persoana împuternicită de operator au dreptul să solicite certificarea.

7.3 Analiza solicitării

În plus față 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 privește obiectul evaluării. Totodată, evaluarea de la capitolul 7.3 litera (e) privind existența unui nivel suficient de expertiză trebuie să țină seama atât de expertiza tehnică, cât și de cea juridică în domeniul protecției datelor, în măsura adecvată.

În plus față de capitolul 7.3.1 litera (b) din EN-ISO/IEC 17065/2012, acordul de certificare dintre solicitant și organismul de certificare trebuie să prevadă metodele de evaluare planificate, ținând cont de legea privind protecția datelor aplicabilă clientului.

7.4 Evaluare

În plus față de capitolul 7.4 din EN-ISO/IEC 17065/2012, mecanismele de certificare trebuie să descrie metode de evaluare suficiente pentru evaluarea conformității operațiunii (operațiunilor) de prelucrare cu criteriile de certificare, inclusiv, de exemplu, după caz:

1. o metodă de evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu scopul lor și persoanele vizate respective;
2. o metodă de evaluare a acoperirii, alcătuirii și evaluării tuturor riscurilor avute în vedere de către operator și persoana împuternicită de către operator în ceea ce privește consecințele juridice în temeiul articolelor 30, 32, 35 și 36 din

Regulamentul (UE) 2016/679, precum și definiția măsurilor tehnice și organizatorice în temeiul articolelor 24, 25 și 32 din Regulamentul (UE) 2016/679, în măsura în care articolele menționate mai sus se aplică domeniului certificării (inclusiv obiectului certificării); și

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

4. documentarea metodelor și constatărilor.

Organismul de certificare trebuie să se asigure că aceste metode de evaluare sunt standardizate și 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.

În plus față de capitolul 7.4.5 din EN-ISO/IEC 17065/2012, trebuie să se impună ca certificarea protecției datelor în conformitate cu articolele 42 și 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 (parțiale). Organismul de certificare are obligația de a verifica respectarea criteriilor. Recunoașterea necesită, în orice caz, disponibilitatea unui raport de evaluare complet sau a informațiilor care să permită o evaluare a activității de certificare anterioare și a rezultatelor acesteia. O declarație de certificare sau atestate de certificare similare nu trebuie considerate suficiente pentru a înlocui un raport.

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

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

2. Cu toate acestea, certificările privind protecția datelor conform art. 42 din Regulamentul (UE) 2016/679 nu sunt acceptabile pentru a înlocui complet

evaluările (parțiale). Organismul de certificare continuă să fie obligat să verifice conformitatea actuală cu cerințele (certificatului depus), cel puțin aleatoriu, și să evalueze certificările existente. Nu rezultă efecte asupra perioadei de valabilitate a certificării prezentate.

3. Alte certificări, acordate de un organism de certificare acreditat ca atare, pot fi de asemenea considerate un factor de conformitate și pot fi luate în considerare în cadrul certificării. Cu toate acestea, ele nu sunt suficiente pentru a înlocui complet evaluările (parțiale). Totodată, organismul de certificare este obligat să monitorizeze respectarea cerințelor prin verificarea raportului de audit, cel puțin aleatoriu, și să evalueze adecvarea certificărilor existente.

4. Perioada de validitate a certificatelor trebuie documentată și păstrată disponibilă în conformitate cu capitolul 7.7 din EN-ISO/IEC 17065/2012. Perioada de validitate a certificatului se reduce la cea mai scurtă perioadă de valabilitate a certificărilor curente luate în considerare. În cazul unei recertificări a certificatului, perioada de validitate a certificatului este prelungită cu o perioadă egală cu cea a certificatului în cauză. Nu se depășește termenul standard de validitate a unui certificat sau, în cazul altor certificate terțe părți, cea mai scurtă perioadă de validitate (a se vedea mai sus). Dacă nu se efectuează nicio recertificare, cel puțin obiectivul certificat inițial trebuie să fie din nou auditat.

O astfel de conformitate necesită disponibilitatea unei evaluări sau informări complete a certificării, care să permită o evaluare a activității de certificare și a rezultatelor. O declarație de certificare sau atestate de certificare similare nu ar trebui considerate suficiente pentru a înlocui un raport.

Dacă abaterile de la cerințe sau alte nereguli rezultă dintr-un astfel de audit, evaluarea este extinsă în cadrul procedurii de certificare în curs și, dacă este necesar, asupra întregului obiectiv deja certificat.

În plus față 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 neconformitățile din cadrul unui mecanism de certificare. În acest context, trebuie să se definească cel puțin natura și calendarul acestor date.

În plus față de capitolul 7.4.9 din EN-ISO/IEC 17065/2012, trebuie să se impună ca documentația să fie pusă integral la dispoziția autorității de supraveghere din domeniul protecției datelor, la cerere.

Documentația trebuie să fie complet accesibilă în timpul procedurii de acreditare și în orice moment, la cererea autorității de supraveghere pentru protecția datelor.

7.5 Analiză

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

7.6 Decizia de certificare

În plus față 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 independența și responsabilitatea cu privire la deciziile de certificare individuale.

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 autoritatea competentă de supraveghere pentru protecția datelor cu privire la certificare în scris cu cel puțin 30 zile înainte de acordarea certificării. Informațiile scrise trebuie să includă numele clientului, descrierea obiectului certificării și o scurtă evaluare publică.

În plus față de capitolul 7.6.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să precizeze în detaliu criteriile sale, cum este asigurată independența și responsabilitatea față de deciziile de certificare.

În plus față de capitolul 7.6.2 din EN-ISO/IEC 17065/2012, decizia privind certificarea trebuie să fie luată de șeful 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

experți, recunoscuți anterior de organismul de certificare, așa cum este descris în plus față de capitolul 7.4.2 din EN-ISO/IEC 17065/2012.

În plus față de punctul 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 menționat mai sus și procedura pe care trebuie să o respecte clientul.

7.7 Documentație de certificare

În plus față de capitolul 7.7.1 litera (e) din EN-ISO/IEC 17065/2012 și în conformitate cu articolul 42 alineatul (7) din Regulamentul (UE) 2016/679, perioada de validitate a certificatelor emise de organismul de certificare trebuie să nu depășească trei ani.

În plus față 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 standard.

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

7.8 Registrul produselor certificate

În plus față de capitolul 7.8 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să mențină informațiile privind produsele, procesele și serviciile certificate disponibile pe plan intern și pentru public. Organismul de certificare va pune la dispoziția publicului o sinteză a raportului de evaluare. Scopul acestei sinteze este de a contribui la asigurarea transparenței în ceea ce privește elementele certificate și modul în care au fost evaluate. Aceasta va explica aspecte precum:

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

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

(c) metodele de evaluare și testele efectuate, precum și

(d) rezultatul (rezultatele).

În plus, informațiile trebuie să includă:

1. datele de contact ale solicitantului (persoană juridică sau fizică),
2. un număr de înregistrare,
3. data certificării și data expirării certificatului,
4. informații despre certificarea inițială sau recertificare,
5. informații despre posibilele activități de supraveghere pentru a păstra certificarea, precum și
6. posibila implicare a evaluatorilor externi.

În plus față de capitolul 7.8 din EN-ISO/IEC 17065/2012 și în temeiul articolului 43 alineatul (5) din Regulamentul (UE) 2016/679, organismul de certificare informează autoritățile de supraveghere competente cu privire la motivele pentru acordarea sau retragerea certificării solicitate.

7.9 Supraveghere

În plus față de capitolele 7.9.1, 7.9.2 și 7.9.3 din EN-ISO/IEC 17065/2012 și în conformitate cu articolul 43 alineatul (2) litera (c) din Regulamentul (UE) 2016/679, organismul de certificare trebuie să impună ca măsurile de monitorizare periodică să fie obligatorii pentru menținerea certificării.

Supravegherea trebuie efectuată cel puțin odată pe an.

Procedura și acordul de certificare cu clientul trebuie să fie demonstrate în orice moment pe parcursul procedurii de acreditare și la cererea autorităților de supraveghere pentru protecția datelor.

7.10 Modificări care afectează certificarea

În plus față de capitolele 7.10.1 și 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 legislației privind protecția datelor,

adoptarea de acte delegate ale Comisiei Europene în conformitate cu articolul 43 alineatele (8) și (9) din Regulamentul (UE) 2016/679, decizii ale Comitetului European pentru Protecția Datelor și decizii ale instanțelor judecătorești legate de protecția datelor. Procedurile legate de modificări pot include aspecte precum: perioadele de tranziție, procesele de aprobare cu autoritatea de supraveghere competentă, reevaluarea domeniului certificării (inclusiv obiectul certificării) și măsuri adecvate de revocare a certificării, în cazul în care operațiunea de prelucrare certificată nu mai respectă criteriile actualizate.

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

1. care modificări necesită o notificare și, dacă este cazul, o ajustare pentru client,
2. care sunt metodele de evaluare de către organismul de certificare într-un astfel de caz și
3. ce termene există pentru implementarea măsurilor pentru a menține certificarea existentă.

Dincolo de acest aspect, organismul de certificare definește modul în care se asigură că sunt efectuate audituri comparabile în proceduri de certificare comparabile (chiar dacă cerințele de certificare se modifică).

În plus, organismul de certificare definește, de asemenea, ce măsuri și procese trebuie luate dacă auditul duce la concluzia că certificarea nu poate fi menținută. Măsurile corespunzătoare și procesele corespunzătoare sunt puse în aplicare și menținute la dispoziție de către conducerea organismului de certificare.

În plus față de capitolul 7.10.2 din EN-ISO/IEC 17065/2012, organismul de certificare va defini în schema sa de certificare în ce cazuri și în ce fel clientul trebuie să furnizeze organismului de certificare informații (în cazul modificărilor inițiate de client). Acesta este întotdeauna cazul, cel puțin atunci când au apărut modificări în obiectul certificării cu privire la prelucrarea datelor cu caracter personal, modificări în mediul operațional și/sau modificări în contextul aplicației sau modificări în alte condiții-cadru care sunt relevante pentru declarația de certificare. Aceasta se aplică în special modificărilor standardelor legale pertinente privind obiectul certificării, precum și modificărilor tehnologiei de ultimă generație care au fost determinate de client. În acest caz, orice măsuri inițiate prin notificare trebuie

definite de organismul de certificare și de client. De asemenea, organismul de certificare definește modul de asigurare a luării unor măsuri comparabile în cazuri comparabile. În plus, măsurile corespunzătoare și procesele corespunzătoare sunt puse în aplicare și menținute la dispoziție de către conducerea organismului de certificare.

7.11 Încetarea, reducerea, suspendarea sau retragerea certificării

În plus față de capitolul 7.11.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să informeze imediat, în scris, autoritatea de supraveghere competentă și organismul național de acreditare (RENAR), după caz, cu privire la măsurile adoptate și menținerea, restrângerea, suspendarea certificarii în așteptarea acțiunilor de remediere efectuate de client și retragerea certificării.

În conformitate cu articolul 58 alineatul (2) litera (h) din Regulamentul (UE) 2016/679, i se impune organismului de certificare să accepte deciziile și ordinele autorității de supraveghere competente de a retrage sau a nu emite certificarea pentru un client (solicitant) în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite.

În plus, în cazurile în care organismul de certificare determină nerespectarea, acesta trebuie să definească în criteriile sale care sunt măsurile care trebuie luate și care cazuri (de neconformitate) constituie măsuri în primul rând.

7.12 Înregistrări

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

Toate documentațiile organismului de certificare trebuie să fie complete, verificabile, actualizate și auditabile. Aceasta se aplică atât procedurilor de certificare finalizate fără un rezultat pozitiv, cât și procedurilor de certificare în curs. În procedurile de certificare în curs, criteriile de certificare care sunt îndeplinite și care nu sunt îndeplinite trebuie să fie evidente.

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

În plus față 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 față de perioada de validitate a certificării și după finalizarea acordului de certificare. În cazul disputelor dintre organismul de certificare și client sau client și autoritatea de supraveghere competentă, această perioadă poate fi prelungită peste perioada de valabilitate a certificării până la încheierea acestei proceduri.

7.13 Reclamații și căi de atac

În plus față 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 reclamații sau prezenta obiecțiuni;

(b) cine le prelucrează la nivelul organismului de certificare;

(c) ce verificări au loc în acest context; și

(d) posibilitățile de consultare a părților interesate.

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

(a) cum și cui o astfel de confirmare trebuie transmisă;

(b) termenele limită pentru aceasta; și

(c) procesele care urmează să fie inițiate ulterior

În plus față de capitolul 7.13.1 din EN-ISO/IEC 17065/2012, organismul de certificare trebuie să definească modul în care este asigurată separarea între activitățile de certificare și soluționarea a reclamațiilor și căilor de atac.

CAPITOLUL 8: CERINȚELE SISTEMULUI DE MANAGEMENT

O cerință 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 cerințelor din capitolele precedente în sfera de aplicare a mecanismului de certificare de către organismul de certificare acreditat este documentată, evaluată, controlată și monitorizată în mod independent.

Principiul de bază al gestionării este acela de a defini un sistem potrivit căruia obiectivele sale sunt stabilite cu eficacitate și eficiență, în mod specific: punerea în

aplicare a serviciilor de certificare – prin intermediul unor specificații adecvate. Aceasta necesită transparența și posibilitatea verificării punerii în aplicare a cerințelor de acreditare de către organismul de certificare și conformitatea permanentă a acestuia.

În acest scop, sistemul de gestionare trebuie să specifice o metodologie care să îndeplinească și să controleze aceste cerințe, în conformitate cu normele privind protecția datelor și în vederea verificării constante a acestora împreună cu organismul acreditat însuși.

Aceste principii de gestionare și punerea lor documentată în aplicare trebuie să fie transparente și să fie publicate de către organismul de certificare acreditat în baza procedurii de acreditare în temeiul articolului 58 din Regulamentul (UE) 2016/679 și, ulterior, la cererea autorității de supraveghere din domeniul protecției datelor, în orice moment în timpul unei investigații sub forma unor controale privind protecția datelor în temeiul articolului 58 alineatul (1) litera (b) din Regulamentul (UE) 2016/679 sau a unei examinări a certificărilor emise în conformitate cu articolul 42 alineatul (7) din Regulamentul (UE) 2016/679 în temeiul articolului 58 alineatul (1) litera (c) din Regulamentul (UE) 2016/679.

În special, organismul de certificare acreditat trebuie să publice în permanență și în mod continuu certificările efectuate și bazele acestora (sau mecanismele ori schemele de certificare), durata valabilității certificărilor și care sunt cadrele și condițiile aplicabile (considerentul 100 din Regulamentul (UE) 2016/679).

8.1 Opțiuni

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

8.2 Documentația generală a sistemului de management

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

8.3 Controlul documentelor

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

8.4 Controlul înregistrărilor

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

8.5 Analiza efectuată de management

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

8.6 Audituri interne

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

8.7 Acțiuni corective

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

8.8 Acțiuni preventive

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

Avizat:
Alina Săvoiu – Director, Direcția juridică şi comunicare
Georgică Bălăiți – Director, Direcția control
Adina Diaconescu - Director, Direcția plângeri
Luisa Dumitru, Șef serviciu, Serviciu Relații Externe
Participant: Adrian Munteanu, consilier
Întocmit: Simona-Nicoleta ZANFIR, consilier Direcția juridică şi comunicare