DECIZIA (UE, Euratom) 2018/559 A COMISIEI

din 6 aprilie 2018

de stabilire a normelor de punere în aplicare a articolului 6 din Decizia (UE, Euratom) 2017/46 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 249,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice,

având în vedere Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene ([1]), în special articolul 6,

întrucât:

(1) Adoptarea Deciziei (UE, Euratom) 2017/46 a făcut necesară revizuirea, actualizarea și consolidarea de către Comisie a normelor de punere în aplicare legate de Decizia C(2006) 3602 privind securitatea sistemelor informatice și de comunicații utilizate de Comisie, care a fost abrogată.

(2) În deplină conformitate cu regulamentul intern de procedură, membrul Comisiei responsabil cu securitatea a fost mandatat să stabilească norme de punere în aplicare în conformitate cu articolul 13 din Decizia (UE, Euratom) 2017/46 a Comisiei ([2]).

(3) Prin urmare, normele de punere în aplicare prevăzute în Decizia C(2006) 3602 ar trebui abrogate,

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

(1) Obiectul și domeniul de aplicare al prezentei decizii sunt prevăzute la articolul 1 din Decizia (UE, Euratom) 2017/46.

(2) Dispozițiile prezentei decizii se aplică tuturor sistemelor informatice și de comunicații (SIC). Cu toate acestea, responsabilitățile prevăzute în prezenta decizie nu se aplică SIC care prelucrează informații ale UE clasificate. Responsabilitățile relevante pentru aceste sisteme se stabilesc de către proprietarul de sistem și de către Autoritatea de securitate a Comisiei în conformitate cu Decizia (UE, Euratom) 2015/444 a Comisiei ([3]).

(3) Capitolul 2 din prezenta decizie conține o sinteză a aspectelor practice ale organizării și a responsabilităților care au legătură cu securitatea informatică. Capitolul 3 din prezenta decizie conține o prezentare generală a proceselor care au legătură cu articolul 6 din Decizia (UE, Euratom) 2017/46.

Articolul 2

Definiții

Definițiile de la articolul 2 din Decizia (UE, Euratom) 2017/46 se aplică în prezenta decizie. În sensul prezentei decizii, se aplică, de asemenea, următoarele definiții:

1. „autoritatea de aprobare criptografică” (AAC) este o funcție îndeplinită de Autoritatea de securitate a Comisiei care intră sub autoritatea directorului general al Direcției Generale Resurse Umane și Securitate;

([1]) JO L 6, 11.1.2017, p. 40.
([2]) Decizia C(2017) 7428 final a Comisiei din 8 noiembrie 2017 prin care se conferă competența de a adopta norme de punere în aplicare, standarde și orientări privind securitatea sistemelor informatice și de comunicații din Comisia Europeană.
([3]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

2. „conexiune la o rețea externă” înseamnă orice conexiune prin care se efectuează comunicații electronice între rețeaua internă a Comisiei și orice altă rețea, inclusiv rețeaua internet. Această definiție exclude acele rețele ale părților terțe care sunt furnizate, conform contractului, pentru a fi integrate în rețeaua internă a Comisiei;

3. „custodia cheii” înseamnă o procedură de dare în custodia unei părți sau a mai multor părți a unor copii ale cheilor criptografice, asigurând astfel separarea sarcinilor, pentru a permite recuperarea acestora în cazul pierderii copiei operaționale. Cheile pot fi împărțite în două sau mai multe segmente, fiecare dintre acestea fiind dată în custodia altei părți, pentru a se asigura că niciuna dintre părți nu posedă întreaga cheie;

4. „RASCI” este o abreviere care desemnează un sistem de atribuire a responsabilităților pe baza următorilor indicatori de atribuire:

   (a) „responsabil” (R) înseamnă având obligația de a acționa și de a lua decizii în vederea obținerii rezultatelor necesare;

   (b) „răspunzător” (*accountable* – A) înseamnă răspunzător pentru acțiuni, decizii și execuție;

   (c) „sprijină” (S) înseamnă că persoana sau entitatea în cauză are obligația de a colabora la finalizarea unei sarcini cu persoana responsabilă de aceasta;

   (d) „consultat” (C) înseamnă că persoanei sau entității în cauză i se solicită sfatul sau părerea;

   (e) „informat” (I) înseamnă că persoanei sau entității în cauză i se transmit informațiile relevante.

CAPITOLUL 2

ORGANIZARE ȘI RESPONSABILITĂȚI

Articolul 3

Roluri și responsabilități

Rolurile și responsabilitățile care au legătură cu articolele 4-8 din prezenta decizie sunt definite în anexă, în conformitate cu modelul RASCI.

Articolul 4

Aliniere la politica în domeniul securității informațiilor a Comisiei

(1) Direcția Generală Resurse Umane și Securitate examinează politica în domeniul securității informatice a Comisiei și standardele și orientările aferente pentru a se asigura că acestea sunt conforme cu politicile generale în materie de securitate ale Comisiei, în special cu Decizia (UE, Euratom) 2015/443 a Comisiei [1] și cu Decizia (UE, Euratom) 2015/444.

(2) La cererea altor departamente ale Comisiei, Direcția Generală Resurse Umane și Securitate poate examina politicile în domeniul securității informatice sau alte documente având legătură cu securitatea informatică ale acestora pentru a asigura faptul că sunt coerente cu politica în domeniul securității informațiilor a Comisiei. Șeful departamentului Comisiei în cauză se asigură că toate neconcordanțele sunt soluționate.

(3) În cadrul responsabilităților sale legate de securitatea informațiilor, Direcția Generală Resurse Umane și Securitate cooperează cu Direcția Generală Informatică pentru a se asigura că procesele din domeniul securității informatice țin cont pe deplin de clasificarea și principiile de securitate prevăzute în Decizia (UE, Euratom) 2015/443, în special de articolele 3 și 9.

CAPITOLUL 3

PROCESELE DIN DOMENIUL SECURITĂȚII INFORMATICE

Articolul 5

Tehnologii de criptare

(1) Utilizarea tehnologiilor de criptare pentru protecția informațiilor UE clasificate (IUEC) trebuie să respecte Decizia (UE, Euratom) 2015/444.

(2) Deciziile privind utilizarea tehnologiilor de criptare pentru protecția datelor care nu sunt IUEC sunt luate de proprietarul de sistem al fiecărui SIC, ținând cont atât de riscurile pe care încearcă să le atenueze criptarea, cât și de riscurile pe care le introduce aceasta.

(3) Pentru orice utilizare a tehnologiilor de criptare este necesară aprobarea prealabilă a AAC, cu excepția cazurilor în care criptarea este folosită numai pentru a proteja confidențialitatea datelor care nu sunt IUEC transmise în tranzit și utilizează protocoale standard de comunicare în rețea.

[1] Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41).

(4) Cu excepția prevăzută la alineatul (3) din prezentul articol, departamentele Comisiei se asigură că toate copiile de siguranță ale cheilor de decriptare sunt stocate prin procedura custodiei cheii, în vederea recuperării datelor stocate în eventualitatea în care cheia de decriptare nu mai este disponibilă. Recuperarea datelor criptate cu ajutorul copiilor de siguranță ale cheilor de decriptare se efectuează numai dacă aceasta a fost autorizată în conformitate cu standardul definit de către AAC.

(5) Cererile de aprobare a utilizării tehnologiilor de criptare sunt consemnate în scris în mod oficial și includ detalii privind SIC și datele care trebuie protejate, tehnologiile care urmează să fie utilizate și procedurile operaționale de securitate conexe. Aceste solicitări de aprobare trebuie semnate de proprietarul de sistem.

(6) Cererile de aprobare pentru utilizarea tehnologiilor de criptare sunt evaluate de AAC în conformitate cu standardele și cerințele publicate.

Articolul 6

Inspecții de securitate informatică

(1) Direcția Generală Resurse Umane și Securitate efectuează inspecții de securitate informatică pentru a verifica dacă măsurile de securitate informatică sunt conforme cu politicile generale în materie de securitate informatică ale Comisiei și pentru a verifica integritatea acestor măsuri de control.

(2) Direcția Generală Resurse Umane și Securitate poate efectua o inspecție de securitate informatică:

(a) din proprie inițiativă;

(b) la cererea Comitetului director pentru securitatea informațiilor (ISSB);

(c) la cererea unui proprietar de sistem;

(d) în urma producerii unui incident de securitate; sau

(e) în urma identificării unui risc ridicat la adresa unui anumit sistem.

(3) Proprietarii de date pot solicita o inspecție de securitate informatică înainte de a-și stoca informațiile pe un SIC.

(4) Rezultatele unei inspecții trebuie consemnate într-un raport oficial către proprietarul de sistem, transmis și către OLSI, care include constatări și recomandări de îmbunătățire a respectării de către SIC a politicii de securitate informatică. Direcția Generală Resurse Umane și Securitate trebuie să raporteze către ISSB aspectele și recomandările semnificative.

(5) Direcția Generală Resurse Umane și Securitate monitorizează punerea în aplicare a recomandărilor.

(6) Dacă este cazul, inspecțiile de securitate informatică includ inspectarea serviciilor, a spațiilor și a echipamentelor furnizate proprietarului de sistem, atât de către prestatorii de servicii interni, cât și de către cei externi.

Articolul 7

Accesul dinspre rețelele externe

(1) Direcția Generală Resurse Umane și Securitate stabilește norme, sub forma unui standard, privind autorizarea accesului între SIC ale Comisiei și rețelele externe.

(2) Normele trebuie să facă distincție între diferitele tipuri de conexiuni la rețelele externe și să stabilească reguli de securitate adecvate pentru fiecare tip de conexiune, precizând inclusiv dacă pentru conexiunea respectivă este necesară o autorizare prealabilă din partea autorității relevante, astfel cum se prevede la alineatul (4) din prezentul articol.

(3) Dacă este necesar, autorizația se acordă pe baza unui proces oficial de cerere și aprobare. Aprobarea este valabilă pe o durată determinată și trebuie obținută înainte de activarea conexiunii.

(4) Direcția Generală Resurse Umane și Securitate are responsabilitatea generală pentru autorizarea cererilor, dar poate delega responsabilitatea pentru autorizarea anumitor tipuri de conexiuni, la libera sa alegere, în conformitate cu articolul 17 alineatul (3) din Decizia (UE, Euratom) 2015/443 și cu respectarea condițiilor prevăzute la alineatul (8).

(5) Entitatea de autorizare poate impune, ca precondiție pentru aprobare, cerințe suplimentare în materie de securitate, pentru a proteja SIC și rețelele Comisiei de riscurile de acces neautorizat sau de alte încălcări ale securității.

(6) Direcția Generală Informatică este furnizorul standard de servicii de rețea pentru Comisie. Orice alt departament al Comisiei care exploatează o rețea care nu este furnizată de Direcția Generală Informatică trebuie să obțină mai întâi acordul ISSB. Departamentul în cauză al Comisiei prezintă în scris justificarea comercială a cererii și demonstrează că controalele de rețea sunt suficiente pentru a răspunde cerințelor în materie de control al fluxurilor de informații dinspre și înspre instituție.

(7) Proprietarul de sistem al unui SIC stabilește cerințele de securitate pentru accesul la respectivul SIC și asigură aplicarea măsurilor adecvate pentru protejarea securității acestuia, cu sprijinul OLSI.

(8) Măsurile de securitate aplicate pentru conexiunile la rețelele externe se bazează pe principiile necesității de a cunoaște și al privilegiului minim, prin care se asigură că utilizatorii primesc doar informațiile și drepturile de acces de care au nevoie pentru a-și îndeplini sarcinile oficiale în cadrul Comisiei.

(9) Toate conexiunile la rețelele externe sunt filtrate și monitorizate pentru a detecta eventuale încălcări ale securității.

(10) În cazul în care sunt stabilite conexiuni care să permită externalizarea unui SIC, autorizația este condiționată de finalizarea cu succes a procedurii descrise la articolul 8.

Articolul 8

Externalizarea SIC

(1) În sensul prezentei decizii, se consideră că un SIC este externalizat atunci când este furnizat în temeiul unui contract cu un contractant terț, potrivit căruia SIC este amplasat într-un spațiu care nu aparține Comisiei. Sunt incluse în acest concept externalizarea unor SIC individuale sau multiple ori a altor servicii informatice, amplasarea centrelor de date în spații care nu aparțin Comisiei și gestionarea de date ale Comisiei de către servicii externe.

(2) La externalizarea unui SIC trebuie să se țină cont de caracterul sensibil sau clasificat al informațiilor gestionate, după cum urmează:

(a) SIC care gestionează IUEC trebuie să fie acreditate în conformitate cu Decizia (UE, Euratom) 2015/444 și trebuie consultată în prealabil autoritatea de acreditare în materie de securitate a Comisiei. Sistemele care gestionează IUEC nu pot fi externalizate.

(b) Proprietarul de sistem al unui SIC care gestionează informații care nu sunt IUEC instituie măsuri proporționale pentru a răspunde nevoilor în materie de securitate, în conformitate cu obligațiile juridice relevante sau cu caracterul sensibil al informațiilor, ținând cont de riscul prezentat de externalizare. Direcția Generală Resurse Umane și Securitate poate impune cerințe suplimentare.

(c) Proiectele de dezvoltare externalizate trebuie să țină cont de caracterul sensibil al codului elaborat și al datelor de test utilizate în timpul dezvoltării.

(3) În cazul SIC externalizate, pe lângă principiile prevăzute la articolul 3 din Decizia (UE, Euratom) 2017/46, se aplică și următoarele principii:

(a) acordurile de externalizare trebuie să fie concepute de așa natură încât să se evite dependența de anumiți furnizori;

(b) măsurile de securitate aferente externalizării trebuie să reducă la minim posibilitatea ca personalul părții terțe să aibă acces la informațiile Comisiei sau să modifice aceste informații;

(c) membrii personalului părții terțe care au acces la SIC externalizate trebuie să semneze acorduri de confidențialitate;

(d) externalizarea unui SIC trebuie să fie indicată în registrul prin care se ține inventarul SIC.

(4) Cu participarea proprietarilor de date, proprietarul de sistem:

(a) evaluează și consemnează în scris riscurile legate de externalizare;

(b) stabilește cerințele în materie de securitate relevante;

(c) se consultă cu proprietarii tuturor celorlalte sisteme informatice și de comunicații conectate pentru a se asigura că cerințele în materie de securitate ale acestora din urmă au fost incluse;

(d) se asigură că în contractul de externalizare au fost incluse cerințe și drepturi în materie de securitate adecvate;

(e) asigură îndeplinirea tuturor cerințelor prevăzute în procedura detaliată prevăzută la alineatul (8) din prezentul articol.

Aceste acțiuni trebuie să fie finalizate înainte de semnarea unui contract sau a unui alt tip de acord pentru externalizarea unuia sau mai multor SIC.

(5) Proprietarii de sistem gestionează riscurile aferente externalizării pe durata de viață a SIC, astfel încât să fie respectate cerințele de securitate definite.

(6) Proprietarii de sistem se asigură că contractanții terți au obligația să notifice imediat Comisiei toate incidentele informatice care afectează un SIC externalizat al Comisiei.

(7) Proprietarul de sistem este responsabil de asigurarea conformității SIC, a contractului de externalizare și a măsurilor în materie de securitate cu normele Comisiei privind securitatea informațiilor și securitatea informatică.

(8) Direcția Generală Resurse Umane și Securitate trebuie să stabilească un standard detaliat privind responsabilitățile și activitățile prevăzute la alineatele (1)-(7), în conformitate cu articolul 10 de mai jos.

CAPITOLUL 4

DISPOZIȚII DIVERSE ȘI DISPOZIȚII FINALE

Articolul 9

Transparența

Prezenta decizie este adusă la cunoștința personalului Comisiei și a tuturor persoanelor cărora li se aplică și este publicată în *Jurnalul Oficial al Uniunii Europene*.

Articolul 10

Standarde

(1) În cazurile în care acest lucru este necesar, dispozițiile prezentei decizii sunt detaliate suplimentar în standarde și/sau orientări care vor fi adoptate în conformitate cu Decizia (UE, Euratom) 2017/46 și cu Decizia C(2017) 7428. Standardele și orientările în materie de securitate informatică trebuie să prevadă detalii suplimentare referitoare la aceste norme de punere în aplicare și la aplicarea Deciziei (UE, Euratom) 2017/46 în ceea ce privește anumite domenii având legătură cu securitatea, în conformitate cu anexa A la ISO 27001:2013. Aceste standarde și orientări trebuie să fie bazate pe bunele practici din sectorul de profil și să fie alese astfel încât să fie adecvate mediului informatic al Comisiei.

(2) Dacă este necesar, sunt elaborate standarde în conformitate cu anexa A la ISO 27001:2013 în următoarele domenii:

1. organizarea securității informațiilor;
2. securitatea resurselor umane;
3. administrarea activelor;
4. controlul accesului;
5. criptografie;
6. securitatea fizică și a mediului;
7. siguranța în funcționare;
8. securitatea comunicațiilor;
9. achiziționarea, dezvoltarea și întreținerea de sisteme;
10. relațiile cu furnizorii;
11. gestionarea incidentelor de securitate a informațiilor;
12. aspectele legate de securitatea informațiilor ale gestionării continuității activității;
13. conformare.

(3) ISSB aprobă standardele menționate la alineatele (1) și (2) din prezentul articol înainte de adoptare.

(4) Normele de punere în aplicare ale Deciziei C(2006) 3602 care au legătură cu domeniul de aplicare al prezentei decizii se abrogă.

(5) Standardele și orientările adoptate în temeiul Deciziei C(2006) 3602 din 16 august 2006 rămân în vigoare în măsura în care nu intră în conflict cu aceste norme de punere în aplicare, până când vor fi abrogate sau înlocuite de standarde sau norme care urmează să fie adoptate în temeiul articolului 13 din Decizia (UE, Euratom) 2017/46.

Articolul 11

Intrarea în vigoare

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 6 aprilie 2018.

Pentru Comisie,
Pentru Președinte,
Günther OETTINGER
Membru al Comisiei

ANEXĂ

ROLURI ȘI RESPONSABILITĂȚI (RASCI)

În cadrul modelului RASCI, atribuirea de roluri către entități se efectuează cu ajutorul următoarelor abrevieri:

(a) R – Responsabil

(b) A – Răspunzător (*Accountable*)

(c) S – Sprijin

(d) C – Consultare

(e) I – Informare

Rol / Proces	ISSB	HR (DS)	Departamentele Comisiei	Proprietar de sistem	Proprietar de date	OLSI	DIGIT	Contractanți
Alinierea la politica în domeniul securității informațiilor a Comisiei		**R/A**	**S**				**S**	
Tehnologii de criptare		**C**	**A**	**R**	**I**	**C**		
Inspecții de securitate informatică	**I**	**A/R**		**S**	**I**	**I**	**S**	
Accesul dinspre rețelele externe	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externalizarea SIC		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] ISSB este consultat în legătură cu exploatarea rețelelor interne de către orice alt departament al Comisiei decât Direcția Generală Informatică.

[2] Proprietarul de sistem al unui SIC externalizat este responsabil, iar proprietarul de sistem al tuturor celorlalte SIC cu care se interconectează SIC externalizat este consultat.