DECIZII

DECIZIA (UE, Euratom) 2017/46 A COMISIEI

din 10 ianuarie 2017

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,

întrucât:

(1) Sistemele informatice și de comunicații din cadrul Comisiei Europene reprezintă o parte integrantă a funcționării Comisiei, iar incidentele de securitate informatică pot avea un impact grav asupra operațiunilor Comisiei, precum și asupra părților terțe, inclusiv asupra persoanelor fizice, a companiilor și a statelor membre.

(2) Există numeroase amenințări care pot afecta confidențialitatea, integritatea sau disponibilitatea sistemelor informatice și de comunicații ale Comisiei și a informațiilor prelucrate de acestea. Aceste amenințări includ accidente, erori, atacuri deliberate și evenimente naturale și trebuie recunoscute drept riscuri operaționale.

(3) Sistemelor informatice și de comunicații trebuie să li se asigure un nivel de protecție proporțional cu posibilitatea, impactul și natura riscurilor la care acestea sunt expuse.

(4) Securitatea informatică în cadrul Comisiei ar trebui să asigure că sistemele informatice și de comunicații ale Comisiei protejează informațiile pe care le prelucrează și funcționează așa cum este necesar, atunci când este necesar, sub controlul utilizatorilor legitimi.

(5) Politica de securitate informatică a Comisiei ar trebui pusă în aplicare într-un mod consecvent cu politicile privind securitatea la nivelul Comisiei.

(6) Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate deține responsabilitatea generală pentru securitatea în cadrul Comisiei, sub autoritatea și responsabilitatea membrului Comisiei responsabil de securitate.

(7) Abordarea Comisiei ar trebui să țină seama de inițiativele de politică și de legislația UE privind securitatea informațiilor și a rețelelor, de standardele din sector și de bunele practici, pentru a respecta toate actele legislative relevante și a permite interoperabilitatea și compatibilitatea.

(8) Departamentele Comisiei responsabile de sistemele informatice și de comunicații ar trebui să elaboreze și să pună în aplicare măsuri corespunzătoare, iar măsurile de securitate informatică pentru protecția sistemelor informatice și de comunicații ar trebui coordonate în cadrul Comisiei pentru a asigura eficiența și eficacitatea.

(9) Normele și procedurile de acces la informații în contextul securității informatice, inclusiv tratarea incidentelor de securitate informatică, ar trebui să fie proporționale cu amenințarea la adresa Comisiei sau a personalului acesteia și în conformitate cu principiile prevăzute în Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([1]) privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele Uniunii Europene și privind libera circulație a acestor date, precum și să țină seama de principiul secretului profesional, astfel cum se prevede la articolul 339 din TFUE.

([1]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al ConsiliuluI din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

(10) Politicile și normele privind sistemele informatice și de comunicații care prelucrează informații UE clasificate (IUEC), informații sensibile neclasificate și informații neclasificate trebuie să respecte Deciziile (UE, Euratom) 2015/443 ([1]) și (UE, Euratom) 2015/444 ([2]).

(11) Comisia trebuie să revizuiască și să actualizeze dispozițiile privind securitatea sistemelor informatice și de comunicații pe care le utilizează.

(12) Prin urmare, Decizia C(2006)3602 a Comisiei ar trebui abrogată.

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Obiectul și domeniul de aplicare

(1) Prezenta decizie se aplică tuturor sistemelor informatice și de comunicații (SIC) deținute, achiziționate, gestionate sau operate de Comisie sau în numele acesteia și tuturor utilizărilor acestor SIC de către Comisie.

(2) Prezenta decizie stabilește principiile de bază, obiectivele, organizarea și responsabilitățile privind securitatea respectivelor SIC și, în special, pentru departamentele din cadrul Comisiei care dețin, achiziționează, gestionează sau operează SIC și inclusiv SIC puse la dispoziție de un furnizor intern de servicii informatice. Dacă SIC sunt furnizate, deținute, gestionate sau operate de o parte externă pe baza unui acord bilateral sau contract cu Comisia, termenii acordului sau ai contractului respectă prezenta decizie.

(3) Prezenta decizie se aplică tuturor departamentelor Comisiei și agențiilor executive. Dacă alte organisme și instituții utilizează un SIC al Comisiei pe baza unui acord bilateral sau a unui contract cu Comisia, termenii acordului respectă prezenta decizie.

(4) Fără a aduce atingere unor indicații specifice privind un grup specific de personal, prezenta decizie se aplică membrilor Comisiei, personalului Comisiei care face obiectul Statutului funcționarilor Uniunii Europene („Statutul funcționarilor") și Regimului aplicabil celorlalți agenți ai Uniunii Europene ([3]), experților naționali detașați la Comisie (END) ([4]), furnizorilor externi de servicii și personalului acestora, stagiarilor și oricărei persoane fizice cu acces la SIC în sensul prezentei decizii.

(5) Prezenta decizie se aplică Oficiului European de Luptă Antifraudă (OLAF) în măsura în care aceasta este compatibilă cu legislația Uniunii și cu Decizia 1999/352/CE, CECO, Euratom a Comisiei ([5]). În special, este posibil ca măsurile prevăzute în prezenta decizie, inclusiv instrucțiuni, inspecții, solicitări și măsuri echivalente, să nu se aplice SIC din cadrul Oficiului în caz de incompatibilitate cu independența funcției de investigare a acestuia și/sau cu confidențialitatea informațiilor obținute de Oficiu în exercitarea acestei funcții.

Articolul 2

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

1. „răspunzător" înseamnă persoana care răspunde pentru acțiuni, decizii și execuție

([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).
([2]) 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).
([3]) Prevăzut în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene, precum și a Regimului aplicabil celorlalți agenți ai acestor comunități și de instituire a unor măsuri speciale tranzitorii aplicabile funcționarilor Comisiei (JO L 56, 4.3.1968, p. 1).
([4]) Decizia Comisiei din 12 noiembrie 2008 de stabilire a normelor privind experții naționali detașați și experții naționali în formare profesională pe lângă serviciile Comisiei [C(2008) 6866 final].
([5]) Decizia 1999/352/CE, CECO, Euratom a Comisiei din 28 aprilie 1999 de instituire a Oficiului European de Lupta Antifraudă (OLAF) (JO L 136, 31.5.1999, p. 20).

2. „CERT-UE” înseamnă Centru de răspuns la incidente de securitate cibernetică pentru instituțiile și agențiile UE. Misiunea acestuia este aceea de a sprijini instituțiile europene în ceea ce privește protecția acestora împotriva atacurilor intenționate și răuvoitoare care ar afecta integritatea activelor lor informatice și interesele UE. Domeniul de aplicare al activităților CERT-UE acoperă prevenirea, detectarea, răspunsul și redresarea.

3. „departament al Comisiei” înseamnă orice direcție generală ori serviciu al Comisiei sau orice cabinet al unui membru al Comisiei.

4. „Autoritatea de securitate a Comisiei” se referă la rolul prevăzut în Decizia (UE, Euratom) 2015/444.

5. „sistem informatic și de comunicații” sau „SIC” înseamnă orice sistem care permite manipularea informațiilor în format electronic, inclusiv toate activele necesare funcționării sale, precum și infrastructura, organizarea, personalul și resursele informaționale. Această definiție include aplicațiile de afaceri, serviciile informatice partajate, sistemele externalizate și dispozitivele utilizatorilor finali.

6. „Consiliul pentru gestiunea corporativă” (CGC) asigură cel mai înalt nivel de monitorizare a gestiunii corporative pentru aspecte operaționale și administrative la nivelul Comisiei.

7. „proprietarul datelor” înseamnă persoana fizică responsabilă de asigurarea protecției și utilizării unui set de date specific manipulat de un SIC.

8. „set de date” înseamnă un set de informații care servește unui proces de activitate specific sau unei activități specifice a Comisiei.

9. „procedură de urgență” înseamnă un set prestabilit de metode și responsabilități utilizate pentru a răspunde la situațiile de urgență în scopul prevenirii unui impact major asupra Comisiei.

10. „politica de securitate a informațiilor” înseamnă un set de obiective de securitate a informațiilor care sunt sau trebuie să fie stabilite, puse în aplicare și verificate. Acesta conține Deciziile (UE, Euratom) 2015/444 și (UE, Euratom) 2015/443, fără a se limita la acestea.

11. „Comitetul director pentru securitatea informațiilor” (CDSI) înseamnă organismul de guvernanță care sprijină Consiliul pentru gestiunea corporativă în sarcinile sale legate de securitatea informatică.

12. „furnizor intern de servicii informatice” înseamnă un departament al Comisiei care furnizează servicii informatice partajate.

13. „securitate informatică” sau „securitatea SIC” înseamnă păstrarea confidențialității, integrității și disponibilității SIC și a seturilor de date pe care acestea le prelucrează.

14. „orientări privind securitatea informatică” constă în măsuri recomandate, dar cu caracter voluntar, care contribuie la sprijinirea standardelor de securitate informatică sau servesc drept referință atunci când nu există un standard aplicabil.

15. „incident de securitate informatică” înseamnă un eveniment care ar putea afecta negativ confidențialitatea, integritatea sau disponibilitatea unui SIC.

16. „măsură de securitate informatică” înseamnă o măsură tehnică sau organizatorică destinată atenuării riscurilor la adresa securității informatice.

17. „nevoie de securitate informatică” înseamnă o definire precisă și clară a nivelurilor de confidențialitate, integritate și disponibilitate asociate cu o informație sau un sistem informatic în vederea determinării nivelului de protecție necesar.

18. „obiectiv de securitate informatică” înseamnă o declarație de intenție pentru a contracara amenințările specificate și/sau a răspunde cerințelor sau ipotezelor specifice privind securitatea organizatorică.

19. „plan de securitate informatică” înseamnă documentarea măsurilor de securitate informatică necesare pentru a răspunde nevoilor de securitate informatică ale unui SIC.

20. „politica de securitate informatică” înseamnă un set de obiective de securitate informatică care sunt sau trebuie să fie stabilite, puse în aplicare și verificate. Acesta cuprinde prezenta decizie și normele sale de aplicare.

21. „cerință de securitate informatică” înseamnă o nevoie de securitate informatică formalizată printr-un proces prestabilit.

22. „risc la adresa securității informatice” înseamnă un efect pe care o amenințare la adresa securității informatice l-ar putea avea asupra unui SIC prin exploatarea unei vulnerabilități. Astfel, un risc la adresa securității informatice se caracterizează prin doi factori: 1. incertitudinea, adică posibilitatea ca o amenințare la adresa securității informatice să cauzeze un eveniment nedorit; și 2. impactul, adică consecințele pe care un astfel de eveniment nedorit le-ar putea avea asupra unui SIC.

23. „standarde de securitate informatică” înseamnă măsuri de securitate informatică obligatorii și specifice, care contribuie la aplicarea și sprijinirea politicii de securitate informatică.

24. „strategie de securitate informatică” înseamnă un set de proiecte și activități concepute pentru a atinge obiectivele Comisiei și care trebuie stabilite, puse în aplicare și verificate.

25. „amenințare la adresa securității informatice” înseamnă un factor care poate conduce la un eveniment nedorit care poate avea un efect nefavorabil asupra unui SIC. Aceste amenințări pot fi accidentale sau deliberate și se caracterizează prin elemente amenințătoare, ținte potențiale și metode de atac.

26. „ofițerul local de securitate informatică” sau „OLSI” înseamnă ofițerul responsabil de legătura cu un departament al Comisiei în ceea ce privește securitatea informatică.

27. termenii „date cu caracter personal”, „prelucrarea datelor cu caracter personal”, „operator” și „sistem de evidență a datelor cu caracter personal” au același sens ca în Regulamentul (CE) nr. 45/2001 și, în special, la articolul 2.

28. „prelucrarea informațiilor” înseamnă toate funcțiile unui SIC cu privire la seturile de date, inclusiv crearea, modificarea, afișarea, stocarea, transmiterea, ștergerea și arhivarea informațiilor. Prelucrarea informațiilor poate fi realizată de un SIC ca set de funcționalități pentru utilizatori și ca servicii informatice pentru alte SIC.

29. „secretul profesional” înseamnă protecția informațiilor referitoare la datele de afaceri de genul celor acoperite de obligația păstrării secretului profesional, în special informațiile referitoare la întreprinderi și la relațiile lor comerciale sau la elementele de preț de cost, astfel cum se prevede la articolul 339 din TFUE.

30. „responsabil” înseamnă o persoană care are obligația de a acționa și de a lua decizii în vederea obținerii rezultatelor necesare.

31. „securitate în cadrul Comisiei” înseamnă securitatea persoanelor, a activelor și a informațiilor în cadrul Comisiei și, în special, integritatea fizică a persoanelor și a activelor, integritatea, confidențialitatea și disponibilitatea informațiilor și a sistemelor informatice și de comunicații, precum și desfășurarea neobstrucționată a activităților Comisiei.

32. „serviciu informatic partajat” înseamnă serviciul pe care un SIC îl prestează pentru alte SIC în cadrul prelucrării informațiilor.

33. „proprietar de sistem” este persoana responsabilă de achiziționarea, dezvoltarea, integrarea, modificarea, operarea, întreținerea și retragerea în ansamblu a unui SIC.

34. „utilizator” înseamnă orice persoană care utilizează funcționalitatea furnizată de un SIC, fie în cadrul, fie în afara Comisiei.

Articolul 3

Principiile securității informatice în cadrul Comisiei

(1) Securitatea informatică în cadrul Comisiei se bazează pe principiile legalității, transparenței, proporționalității și responsabilității.

(2) Problemele de securitate informatică sunt luate în considerare de la începutul elaborării și punerii în aplicare a SIC ale Comisiei. În acest sens, Direcția Generală Informatică și Direcția Generală Resurse Umane și Securitate sunt implicate pentru domeniile proprii de responsabilitate.

(3) Securitatea informatică efectivă asigură niveluri adecvate de:

(a) autenticitate: garanția faptului că informațiile sunt originale și provin de la surse de bună credință;

(b) disponibilitate: proprietatea informațiilor de a putea fi accesate și utilizate la cerere de către o entitate autorizată;

(c) confidențialitate: proprietatea informațiilor de a nu fi divulgate persoanelor, entităților sau proceselor neautorizate;

(d) integritate: proprietate care constă în garantarea acurateței și a exhaustivității activelor și a informațiilor;

(e) nerepudiere: capacitatea de a dovedi că o acțiune sau un eveniment a avut loc, astfel încât acțiunea sau evenimentul în cauză să nu poată fi negate ulterior;

(f) protecția datelor cu caracter personal: asigurarea protecției adecvate în ceea ce privește datele cu caracter personal, în deplină conformitate cu Regulamentul (CE) nr. 45/2001;

(g) secretul profesional: protecția informațiilor de genul celor care fac obiectul obligației de păstrare a secretului profesional, în special a informațiilor referitoare la întreprinderi și la relațiile lor comerciale sau la elementele de preț de cost, astfel cum se prevede la articolul 339 din TFUE.

(4) Securitatea informatică se bazează pe un proces de management al riscului. Acest proces vizează stabilirea nivelurilor de riscuri la adresa securității informatice și definirea măsurilor de securitate pentru a reduce aceste riscuri la un nivel adecvat și cu un cost proporțional.

(5) Toate SIC sunt identificate, alocate unui proprietar de sistem și înregistrate într-un inventar.

(6) Cerințele de securitate aferente tuturor SIC se stabilesc pe baza nevoilor de securitate ale acestora și a nevoilor de securitate a informațiilor pe care acestea le prelucrează. SIC care furnizează servicii altor SIC pot fi concepute pentru a sprijini niveluri specificate ale nevoilor de securitate.

(7) Planurile de securitate informatică și măsurile de securitate informatică sunt proporționale cu nevoile de securitate ale SIC.

Procesele legate de aceste principii și activități sunt detaliate în continuare în normele de aplicare.

CAPITOLUL 2

ORGANIZARE ȘI RESPONSABILITĂȚI

Articolul 4

Consiliul pentru gestiunea corporativă

Consiliul pentru gestiunea corporativă își asumă responsabilitatea integrală pentru guvernanța securității informatice în ansamblu în cadrul Comisiei.

Articolul 5

Comitetul director pentru securitatea informațiilor (CDSI)

(1) CDSI este prezidat de Secretarul General adjunct responsabil de guvernanța securității informatice în cadrul Comisiei. Membrii acestuia reprezintă interesele comerciale, tehnologice și de securitate din cadrul departamentelor Comisiei și includ reprezentanți ai Direcției Generale Informatică, ai Direcției Generale Resurse Umane și Securitate, ai Direcției Generale Buget și, o dată la doi ani, prin rotație, reprezentanți ai altor patru departamente ale Comisiei implicate în cazul în care securitatea informatică constituie o preocupare majoră pentru operațiunile lor. Participarea în calitate de membri se realizează la nivel de management superior.

(2) CDSI susține Consiliul pentru gestiunea corporativă în ceea ce privește atribuțiile legate de securitatea informatică ale acestuia. CDSI își asumă responsabilitatea operațională pentru guvernanța securității informatice în ansamblu în cadrul Comisiei.

(3) CDSI recomandă Comisiei, spre adoptare, politica de securitate informatică a acesteia.

(4) CDSI revizuiește aspecte ale guvernanței, precum și aspecte legate de securitatea informatică, inclusiv incidente grave de securitate informatică, și raportează de două ori pe an Consiliului pentru gestiunea corporativă cu privire la acestea.

(5) CDSI monitorizează și revizuiește punerea în aplicare generală a prezentei decizii și raportează cu privire la aceasta Consiliului pentru gestiunea corporativă.

(6) La propunerea Direcției Generale Informatică, CDSI revizuiește, aprobă și monitorizează punerea în aplicare a strategiei de securitate informatică în curs. CDSI raportează cu privire la aceasta Consiliului pentru gestiunea corporativă.

(7) CDSI monitorizează, evaluează și controlează situația tratării riscurilor la adresa informațiilor corporative și are competența de a emite cerințe oficiale de îmbunătățire, ori de câte ori este necesar.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 6

Direcția Generală Resurse Umane și Securitate

În ceea ce privește securitatea informatică, Direcția Generală Resurse Umane și Securitate are următoarele responsabilități. Aceasta:

1. asigură alinierea între politica de securitate informatică și politica de securitate a informațiilor din cadrul Comisiei;

2. stabilește un cadru de autorizare a utilizării tehnologiilor de criptare pentru stocarea și comunicarea informațiilor de către SIC;

3. informează Direcția Generală Informatică cu privire la amenințările specifice care ar putea avea un impact semnificativ asupra securității SIC și a seturilor de date pe care acestea le prelucrează;

4. efectuează inspecții din punctul de vedere al securității informatice pentru a evalua modul în care SIC ale Comisiei respectă politica de securitate și raportează rezultatele către CDSI;

5. stabilește un cadru pentru autorizarea accesului și normele de securitate adecvate asociate pentru SIC ale Comisiei din rețele externe și elaborează standarde și orientări de securitate informatică conexe în strânsă cooperare cu Direcția Generală Informatică;

6. propune principii și norme pentru externalizarea SIC în vederea menținerii unui control adecvat asupra securității informațiilor;

7. elaborează standardele și orientările de securitate informatică conexe în legătură cu articolul 6, în strânsă cooperare cu Direcția Generală Informatică.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 7

Direcția Generală Informatică

În ceea ce privește securitatea informatică în general a Comisiei, Direcția Generală Informatică are responsabilitățile următoare. Aceasta:

1. elaborează standarde și orientări de securitate informatică, mai puțin în cazurile prevăzute la articolul 6, în strânsă cooperare cu Direcția Generală Resurse Umane și Securitate, pentru a asigura consecvența între politica de securitate informatică și politica de securitate a informațiilor din cadrul Comisiei, și le propune CDSI;

2. evaluează metodele de gestionare a riscurilor la adresa securității informatice, procesele și rezultatele aferente acestora în cadrul tuturor departamentelor Comisiei și raportează periodic CDSI cu privire la acestea;

3. propune o strategie graduală de securitate informatică care să fie revizuită și aprobată de CDSI și adoptată, ulterior, de Consiliul pentru gestiunea corporativă, și propune un program, inclusiv planificarea de proiecte și activități de punere în aplicare a strategiei de securitate informatică;

4. monitorizează execuția strategiei de securitate informatică a Comisiei și raportează periodic CDSI cu privire la aceasta;

5. monitorizează riscurile la adresa securității informatice și măsurile de securitate informatică puse în aplicare în cadrul SIC și raportează periodic CDSI cu privire la aceasta;

6. raportează periodic CDSI cu privire la aplicarea la nivel global a deciziei și la conformitatea cu aceasta;

7. după consultarea Direcției Generale Resurse Umane și Securitate, solicită proprietarilor de sistem să ia măsuri specifice de securitate informatică pentru a atenua riscurile la adresa securității informatice în cadrul SIC ale Comisiei;

8. asigură existența unui catalog adecvat al Direcției Generale Informatică cu serviciile de securitate informatică disponibile pentru ca proprietarii de sistem și proprietarii de date să își îndeplinească responsabilitățile cu privire la securitatea informatică și să respecte standardele și politica de securitate informatică;

9. oferă documentație adecvată proprietarilor de sistem și proprietarilor de date și îi consultă, după caz, cu privire la măsurile de securitate informatică puse în aplicare pentru serviciile lor informatice în vederea facilitării respectării politicii de securitate informatică și a sprijinirii proprietarilor de sistem în ceea ce privește gestionarea riscurilor informatice;

10. organizează reuniuni periodice ale rețelei OLSI și sprijină OLSI în îndeplinirea atribuțiilor lor;

11. definește nevoile de formare și coordonează programe de formare în materie de securitate informatică în cooperare cu departamentele Comisiei și elaborează, pune în aplicare și coordonează campanii de sensibilizare referitoare la securitatea informatică în strânsă cooperare cu Direcția Generală Resurse Umane;

12. asigură informarea proprietarilor de sistem, a proprietarilor de date și a altor părți cu responsabilități în materie de securitate informatică din departamentele Comisiei, cu privire la politica de securitate informatică;

13. informează Direcția Generală Resurse Umane și Securitate cu privire la amenințările specifice la adresa securității informatice, la incidente și la excepții de la politica de securitate informatică a Comisiei, notificate de proprietarii de sistem, care ar putea avea un impact semnificativ asupra securității în cadrul Comisiei;

14. în ceea ce privește rolul său de furnizor intern de servicii informatice, oferă Comisiei un catalog al serviciilor informatice partajate care asigură nivelurile de securitate stabilite. Aceasta se va realiza prin evaluarea, gestionarea și monitorizarea sistematică a riscurilor la adresa securității informatice, pentru a pune în aplicare măsurile de securitate în vederea atingerii nivelului de securitate stabilit.

Procesele conexe și responsabilitățile mai detaliate sunt stabilite în continuare în normele de aplicare.

Articolul 8

Departamentele Comisiei

În ceea ce privește securitatea informatică din propriul departament, fiecare șef de departament din cadrul Comisiei:

1. numește în mod oficial un proprietar de sistem, care este un agent oficial sau temporar, pentru fiecare SIC, care va fi responsabil de securitatea informatică a SIC respectiv și numește în mod oficial un proprietar de date pentru fiecare set de date prelucrat într-un SIC, care ar trebui să aparțină de aceeași entitate administrativă, care este operatorul de date pentru seturile de date vizate de Regulamentul (CE) nr. 45/2001;

2. desemnează în mod oficial un ofițer local de securitate informatică (OLSI), care poate îndeplini responsabilitățile independent de proprietarii de sistem și proprietarii de date. Un OLSI poate fi desemnat pentru unul sau mai multe departamente ale Comisiei;

3. asigură efectuarea și punerea în aplicare a evaluărilor adecvate ale riscurilor la adresa securității informatice și a planurilor de securitate informatică;

4. asigură că, periodic, un rezumat al riscurilor la adresa securității informatice și al măsurilor este raportat Direcției Generale Informatică;

5. asigură, cu sprijinul Direcției Generale Informatică, instituirea proceselor, procedurilor și soluțiilor adecvate pentru a asigura detectarea, raportarea și soluționarea eficientă a incidentelor de securitate informatică legate de SIC ale acestora;

6. lansează o procedură de urgență în caz de urgențe în materie de securitate informatică;

7. deține răspunderea în ultimă instanță pentru securitatea informatică, inclusiv responsabilități în calitate de proprietar de sistem și proprietar de date;

8. își asumă riscurile legate de SIC și de seturile de date;

9. soluționează dezacordurile dintre proprietarii de date și proprietarii de sistem și, în cazul unui dezacord prelungit, prezintă chestiunea în fața CDSI pentru soluționare;

10. asigură punerea în aplicare a planurilor de securitate informatică și a măsurilor de securitate informatică și acoperirea adecvată a riscurilor;

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 9

Proprietarii de sistem

(1) Proprietarul de sistem este responsabil de securitatea informatică a SIC și raportează șefului departamentului Comisiei.

(2) În ceea ce privește securitatea informatică, proprietarul de sistem:

(a) asigură conformitatea SIC cu politica de securitate informatică;

(b) asigură înregistrarea corectă a SIC în inventarul relevant;

(c) evaluează riscurile la adresa securității informatice și determină nevoile de securitate informatică pentru fiecare SIC, în colaborare cu proprietarii de date și în consultare cu Direcția Generală Informatică;

(d) elaborează un plan de securitate, incluzând, după caz, detalii ale riscurilor evaluate și orice măsuri de securitate suplimentare necesare;

(e) pune în aplicare măsurile de securitate informatică adecvate, proporționale cu riscurile la adresa securității informatice identificate și urmează recomandările susținute de CDSI;

(f) identifică orice dependențe de alte SIC sau servicii informatice partajate și pune în aplicare măsuri de securitate, după caz, bazate pe nivelurile de securitate propuse de către SIC sau serviciile informatice partajate respective;

(g) gestionează și monitorizează riscurile la adresa securității informatice;

(h) raportează cu regularitate șefului departamentului Comisiei cu privire la profilul riscurilor la adresa securității informatice a SIC și raportează Direcției Generale Informatică cu privire la riscurile conexe, activitățile de management al riscurilor și măsurile de securitate adoptate;

(i) consultă OLSI din cadrul departamentului (departamentelor) relevant(e) al(e) Comisiei cu privire la aspecte ale securității informatice;

(j) emite instrucțiuni pentru utilizatori privind utilizarea SIC și a datelor asociate, precum și responsabilitățile utilizatorilor în ceea ce privește SIC;

(k) solicită autorizarea din partea Direcției Generale Resurse Umane și Securitate, în calitate de autoritate în materie criptografică, pentru orice SIC care utilizează tehnologie de criptare;

(l) consultă în prealabil Autoritatea de securitate a Comisiei cu privire la orice sistem care prelucrează informații UE clasificate;

(m) asigură stocarea copiilor de rezervă ale cheilor de decriptare într-un cont de garanție. Recuperarea datelor criptate se efectuează numai atunci când este autorizată, conform cadrului stabilit de Direcția Generală Resurse Umane și Securitate;

(n) respectă orice instrucțiuni de la operatorii de date relevanți referitoare la protejarea datelor cu caracter personal și la aplicarea normelor de protecție a datelor în legătură cu securitatea prelucrării;

(o) notifică Direcției Generale Informatică orice excepții de la politica de securitate informatică a Comisiei, inclusiv justificările relevante;

(p) raportează șefului departamentului din cadrul Comisiei orice dezacorduri care nu pot fi soluționate între proprietarul de date și proprietarul de sistem, comunică incidentele de securitate informatică părților interesate relevante în timp util, în funcție de gravitatea acestora, astfel cum se prevede la articolul 15;

(q) pentru sistemele externalizate, asigură includerea dispozițiilor adecvate privind securitatea informatică în contractele de externalizare, precum și raportarea incidentelor de securitate informatică care au loc în SIC externalizate, în conformitate cu articolul 15;

(r) pentru SIC care oferă servicii informatice partajate, asigură garantarea unui nivel de securitate stabilit, punerea în aplicare de măsuri de securitate clar documentate pentru SIC respectiv, în vederea atingerii nivelului de securitate stabilit.

(3) Proprietarii de sistem își pot delega în mod oficial o parte sau toate sarcinile în materie de securitate informatică, însă rămân responsabili de securitatea informatică a propriului SIC.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 10

Proprietarii de date

(1) Proprietarul de date este responsabil de securitatea informatică a unui set de date specific în fața șefului departamentului Comisiei și este răspunzător pentru confidențialitatea, integritatea și disponibilitatea setului de date.

(2) În legătură cu acest set de date, proprietarul de date:

(a) asigură clasificarea adecvată a tuturor seturilor de date aflate în responsabilitatea sa, în conformitate cu deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444;

(b) definește nevoile de securitate a informațiilor și informează proprietarii de sistem relevanți cu privire la aceste nevoi;

(c) participă la evaluarea riscurilor la adresa SIC;

(d) raportează șefului departamentului Comisiei orice dezacorduri care nu pot fi soluționate între proprietarul de date și proprietarul de sistem;

(e) comunică incidentele de securitate informatică, astfel cum se prevede la articolul 15;

(3) proprietarii de date își pot delega în mod oficial o parte sau toate sarcinile în materie de securitate informatică, însă rămân responsabili astfel cum se prevede la prezentul articol.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 11

Ofițerii locali de securitate informatică (OLSI)

În ceea ce privește securitatea informatică, ofițerul local de securitate informatică (OLSI):

(a) identifică și informează în mod proactiv proprietarii de sistem, proprietarii de date și alte părți cu responsabilități în materie de securitate informatică din cadrul departamentului (departamentelor) Comisiei cu privire la politica de securitate informatică;

(b) asigură legătura cu Direcția Generală Informatică cu privire la aspectele referitoare la securitatea informatică din cadrul departamentului (departamentelor) Comisiei, ca parte a rețelei OLSI;

(c) participă la ședințele OLSI periodice;

(d) păstrează o imagine de ansamblu asupra proceselor de management al riscurilor la adresa securității informațiilor și asupra elaborării și aplicării planurilor de securitate a sistemelor de informații;

(e) oferă consiliere proprietarilor de date, proprietarilor de sistem și șefilor departamentelor Comisiei cu privire la aspecte legate de securitatea informatică;

(f) cooperează cu Direcția Generală Informatică în ceea ce privește diseminarea bunelor practici în materie de securitate informatică și propune programe specifice de sensibilizare și de formare;

(g) raportează șefului departamentului (departamentelor) Comisiei cu privire la securitatea informatică și identifică deficiențele și posibilitățile de îmbunătățire, pe care le transmite acestuia.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 12

Utilizatorii

(1) În ceea ce privește securitatea informatică, utilizatorii îndeplinesc următoarele:

(a) respectă politica de securitate informatică și instrucțiunile emise de proprietarul de sistem cu privire la utilizarea fiecărui SIC;

(b) comunică incidentele de securitate informatică, astfel cum se prevede la articolul 15.

(2) Utilizarea SIC ale Comisiei cu încălcarea politicii de securitate informatică și a instrucțiunilor emise de proprietarul de sistem poate duce la proceduri disciplinare.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

CAPITOLUL 3

CERINȚE ȘI OBLIGAȚII PRIVIND SECURITATEA

Articolul 13

Punerea în aplicare a deciziei

(1) Adoptarea normelor de aplicare referitoare la articolul 6 și a standardelor și orientărilor conexe face obiectul unei decizii a Comisiei prin care este abilitat membrul Comisiei responsabil în materie de securitate.

(2) Adoptarea tuturor celorlalte norme de aplicare în legătură cu prezenta decizie și a standardelor și orientărilor conexe în materie de securitate informatică face obiectul unei decizii a Comisiei prin care este abilitat membrul Comisiei responsabil în materie de informatică.

(3) CDSI aprobă normele de aplicare, standardele și orientările menționate la alineatele (1) și (2) de mai sus înainte de adoptarea lor.

Articolul 14

Obligația de conformitate

(1) Respectarea dispozițiilor prevăzute în politica și standardele de securitate informatică este obligatorie.

(2) Nerespectarea politicii și a standardelor de securitate informatică poate atrage răspunderea disciplinară, în conformitate cu tratatele, Statutul funcționarilor și Regimul aplicabil celorlalți agenți ai Uniunii Europene, sancțiunile contractuale și/sau acțiunile în justiție prevăzute de actele cu putere de lege și dispozițiile administrative naționale.

(3) Direcția Generală Informatică este notificată cu privire la excepțiile de la politica de securitate informatică.

(4) În eventualitatea în care CDSI decide că există un risc persistent inacceptabil la adresa unui SIC al Comisiei, Direcția Generală Informatică, în cooperare cu proprietarul de sisteme, propune CDSI spre aprobare măsuri de atenuare. Aceste măsuri pot include, printre altele, monitorizare și raportare consolidate, limitări ale serviciului și deconectarea.

(5) CDSI impune aplicarea măsurilor de atenuare aprobate ori de câte ori este necesar. De asemenea, CDSI poate recomanda directorului general al Direcției General Resurse Umane și Securitate să lanseze o anchetă administrativă. Direcția Generală Informatică raportează CDSI cu privire la fiecare situație în care sunt impuse măsuri de atenuare.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

Articolul 15

Tratarea incidentelor de securitate informatică

(1) Direcția Generală Informatică este responsabilă de asigurarea capacității operaționale principale de răspuns la un incident de securitate informatică în cadrul Comisiei Europene.

(2) Direcția Generală Resurse Umane și Securitate, ca parte interesată care contribuie la răspunsul la incidentele de securitate informatică:

(a) are dreptul de a accesa informații sumare cu privire la toate registrele de incidente și la registrele complete, la cerere;

(b) participă la grupurile de gestionare a crizelor cauzate de incidentele de securitate informatică și la procedurile de urgență în domeniul securității informatice;

(c) este responsabilă de relațiile cu serviciile de aplicare a legii și de informații;

(d) efectuează analize criminalistice în materie de securitate cibernetică în conformitate cu articolul 11 din Decizia (UE, Euratom) 2015/443;

(e) decide cu privire la nevoia de a lansa o anchetă oficială;

(f) informează Direcția Generală Informatică cu privire la orice incidente de securitate informatică care pot prezenta riscuri pentru alte SIC.

(3) Între Direcția Generală Informatică și Direcția Generală Resurse Umane și Securitate au loc comunicări periodice în vederea schimbului de informații și a coordonării tratării incidentelor de securitate, în special a oricărui incident de securitate informatică care poate necesita o anchetă oficială.

(4) Serviciile de coordonare în materie de incidente ale Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile și agențiile UE (CERT-UE) pot fi utilizate pentru a sprijini procesul de gestionare a incidentelor, după caz, și pentru partajarea de cunoștințe cu alte instituții și agenții ale UE care pot fi afectate.

(5) Proprietarii de sistem implicați într-un incident de securitate informatică:

(a) notifică imediat șefii departamentelor Comisiei, Direcția Generală Informatică, Direcția Generală Resurse Umane, OLSI și, după caz, proprietarul de date cu privire la incidentele de securitate informatică majore, în special la cele care implică încălcarea confidențialității datelor;

(b) cooperează cu autoritățile relevante din cadrul Comisiei și respectă instrucțiunile acestora cu privire la comunicare, răspuns și remediere în caz de incidente.

(6) Utilizatorii raportează în timp util serviciului de asistență informatică cu privire la toate incidentele de securitate informatică reale sau suspectate.

(7) Proprietarii de date raportează în timp util echipei relevante de răspuns la incidentele de securitate informatică cu privire la toate incidentele de securitate informatică reale sau suspectate.

(8) Direcția Generală Informatică, cu sprijinul celorlalte părți interesate care au o contribuție, este responsabilă de tratarea incidentelor de securitate informatică detectate în legătură cu SIC ale Comisiei care nu sunt sisteme externalizate.

(9) Direcția Generală Informatică informează departamentele afectate ale Comisiei cu privire la incidentele de securitate informatică, OLSI relevanți și, după caz, CERT-UE, pe baza principiului necesității de a cunoaște.

(10) Direcția Generală Informatică raportează periodic CDSI cu privire la incidentele de securitate informatică majore care afectează SIC ale Comisiei.

(11) La cerere, OLSI relevanți au acces la registrele de incidente de securitate informatică privind SIC din cadrul departamentului Comisiei.

(12) În cazul unui incident de securitate informatică major, Direcția Generală Informatică reprezintă punctul de contact pentru gestionarea situațiilor de criză prin coordonarea grupurilor de gestionare a crizelor cauzate de incidentele de securitate informatică.

(13) În cazul unei urgențe, directorul general al Direcției Generale Informatică poate decide să lanseze o procedură de urgență în materie de securitate informatică. Direcția Generală Informatică elaborează proceduri de urgență care trebuie aprobate de CDSI.

(14) Direcția Generală Informatică raportează CDSI și șefilor departamentelor afectate din cadrul Comisiei cu privire la execuția procedurilor de urgență.

Procesele legate de aceste responsabilități și activități sunt detaliate în continuare în normele de aplicare.

CAPITOLUL 4

DISPOZIȚII FINALE

Articolul 16

Transparență

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 17

Legătura cu alte acte

Dispozițiile din prezenta decizie nu aduc atingere Deciziei (UE, Euratom) 2015/443, Deciziei (UE, Euratom) 2015/444, Regulamentului (CE) nr. 45/2001, Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([1]), Deciziei 2002/47/CE, CECO, Euratom a Comisiei ([2]), Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului ([3]), Deciziei 1999/352/EC, CECO, Euratom.

Articolul 18

Abrogare și măsuri tranzitorii

Decizia C(2006) 3602 din 16 august 2006 se abrogă.

Normele de punere în aplicare și standardele de securitate informatică adoptate în temeiul articolului 10 din Decizia C(2006) 3602 rămân în vigoare în măsura în care acestea nu contravin prezentei decizii, până când sunt înlocuite de normele de aplicare și standardele care urmează să fie adoptate în conformitate cu articolul 13 din prezenta decizie. Orice referință la articolul 10 din Decizia C(2006)3602 se înțelege ca referință la articolul 13 din prezenta decizie.

Articolul 19

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, 10 ianuarie 2017.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

([1]) Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

([2]) Decizia 2002/47/CE, CECO, Euratom a Comisiei din 23 ianuarie 2002 de modificare a regulamentului de procedură (JO L 21, 24.1.2002, p. 23).

([3]) Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1).