DECIZIA (UE, Euratom) 2015/443 A COMISIEI

din 13 martie 2015

privind securitatea în cadrul Comisiei

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 Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, anexat la tratate, în special articolul 18,

întrucât:

(1) Obiectivul de securitate în cadrul Comisiei constă în a permite Comisiei să își desfășoare activitatea într-un mediu de siguranță și securitate prin stabilirea unei abordări coerente și integrate cu privire la securitatea sa, asigurând niveluri adecvate de protecție a persoanelor, activelor și informațiilor, proporțional cu riscurile identificate, precum și obținerea, în timp util, a unor rezultate eficiente în materie de securitate.

(2) Comisia, la fel ca și alte organisme internaționale, se confruntă cu amenințări și provocări importante în domeniul securității, în special în ceea ce privește terorismul, atacurile cibernetice și spionajul politic și comercial.

(3) Comisia Europeană a lansat, împreună cu guvernele Belgiei, Luxemburgului și Italiei ([1]), instrumente privind aspectele legate de securitate pentru principalele sale locații. Aceste instrumente confirmă faptul că Comisia este responsabilă pentru securitatea sa.

(4) Pentru a asigura securitatea persoanelor, a activelor și a informațiilor, Comisia poate fi nevoită să ia măsuri în domenii protejate prin drepturile fundamentale astfel cum sunt consacrate în Carta drepturilor fundamentale și în Convenția europeană a drepturilor omului și astfel cum sunt recunoscute de Curtea de Justiție a Uniunii Europene.

(5) Prin urmare, orice astfel de măsură ar trebui să fie justificată de importanța interesului pe care este menită să îl protejeze, să fie proporțională și să asigure respectarea deplină a drepturilor fundamentale, în special a dreptului la viață privată și la protecția datelor.

(6) În cadrul unui sistem care sprijină supremația legii și respectarea drepturilor fundamentale, Comisia trebuie să depună eforturi pentru asigurarea unui nivel corespunzător de securitate pentru personalul, activele și informațiile sale, care să îi permită să își desfășoare activitățile, fără limitarea drepturilor fundamentale mai mult decât este strict necesar.

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

(8) Membrii personalului autorizat să ia măsuri de securitate nu ar trebui să fie dezavantajați sub nicio formă ca urmare a desfășurării acțiunilor, cu excepția cazului în care au acționat în afara domeniului de aplicare al mandatului lor sau au încălcat legislația și, prin urmare, în acest sens, prezenta decizie trebuie considerată drept regulament de serviciu în sensul Statutului funcționarilor.

(9) Comisia ar trebui să ia inițiativele corespunzătoare pentru a-și încuraja și consolida propria cultură a securității, prin asigurarea unei implementări mai eficiente a securității, îmbunătățirea guvernanței în materie de siguranță, consolidarea în continuare a rețelelor și a cooperării cu autoritățile relevante la nivel internațional, european și național, și prin îmbunătățirea activităților de monitorizare și control privind punerea în aplicare a măsurilor de securitate.

(10) Înființarea Serviciului European de Acțiune Externă (SEAE), ca organ autonom din punct de vedere funcțional al Uniunii, a avut un impact semnificativ asupra intereselor în materie de securitate ale Comisiei și acest lucru impune, prin urmare, ca SEAE și Comisia să stabilească norme și proceduri de cooperare în ceea ce privește siguranța și securitatea, în special în ceea ce privește îndeplinirea de către Comisie a responsabilităților privind obligația de diligență față de personalul Comisiei din delegațiile Uniunii.

([1]) A se vedea următoarele acorduri: „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité", încheiat la 31 decembrie 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois", încheiat la 20 ianuarie 2007 și „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale", încheiat la 22 iulie 1959.

(11) Politica de securitate a Comisiei ar trebui să fie pusă în aplicare într-un mod care să fie coerent cu alte procese și proceduri interne care pot implica elemente de securitate. Printre acestea se numără, în special, gestionarea continuității activității care are drept scop menținerea funcțiilor critice ale Comisiei în cazul unei întreruperi operaționale, precum și sistemul general de alertă rapidă ARGUS, pentru coordonarea crizelor multisectoriale.

(12) În pofida măsurilor care sunt deja în vigoare la data adoptării prezentei decizii și au fost notificate Autorității Europene pentru Protecția Datelor ([1]), orice măsură adoptată în temeiul prezentei decizii care implică prelucrarea datelor cu caracter personal trebuie să facă obiectul unor norme de punere în aplicare în conformitate cu articolul 21, care stabilește garanții corespunzătoare pentru persoanele vizate.

(13) Prin urmare, este necesar ca Comisia să revizuiască, să actualizeze și să consolideze baza de reglementare existentă privind securitatea din cadrul Comisiei.

(14) Prin urmare, Decizia (94) 2129 a Comisiei ([2]) ar trebui abrogată.

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

DISPOZIȚII GENERALE

Articolul 1

Definiții

În sensul prezentei decizii, se aplică următoarele definiții:

1. „active” înseamnă toate bunurile mobile și imobile și proprietățile deținute de Comisie;

2. „departament al Comisiei” înseamnă fie o direcție generală sau un serviciu al Comisiei, fie un cabinet al unui membru al Comisiei;

3. „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;

4. „control al riscurilor” înseamnă orice măsură de securitate despre care se poate presupune, în mod rezonabil, că va controla în mod efectiv un risc la adresa securității prin prevenire, atenuare, evitare sau transfer;

5. „situație de criză” înseamnă o situație, un eveniment, un incident sau o stare de urgență (sau o succesiune sau o combinație a acestora) care reprezintă o amenințare serioasă sau imediată la adresa securității în cadrul Comisiei, indiferent de originea lor;

6. „date” înseamnă informații într-o formă care permite ca acestea să fie comunicate, înregistrate sau prelucrate;

7. „membrul Comisiei responsabil de securitate” înseamnă un membru al Comisiei în subordinea căruia se află Direcția Generală Resurse Umane și Securitate;

8. „date cu caracter personal” înseamnă datele cu caracter personal astfel cum sunt definite la articolul 2 litera (a) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([3]);

9. „incinte” înseamnă orice bunuri imobile sau bunuri asimilate acestora și aflate în proprietatea Comisiei;

10. „prevenirea riscurilor” înseamnă măsurile de securitate despre care se poate presupune, în mod rezonabil, că vor împiedica, întârzia sau pune capăt unui risc care amenință securitatea.

11. „risc la adresa securității” înseamnă combinația dintre nivelul de amenințare, nivelul de vulnerabilitate și impactul posibil al unui eveniment;

12. „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 de comunicații și informații, precum și desfășurarea neobstrucționată a activităților Comisiei;

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Decizia C(94) 2129 a Comisiei din 8 septembrie 1994 privind sarcinile Oficiului de securitate.

([3]) 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).

13. „măsură de securitate" înseamnă orice măsură luată în conformitate cu prezenta decizie în scopul controlării riscurilor la adresa securității;

14. „Statutul funcționarilor" înseamnă Statutul funcționarilor Uniunii Europene, prevăzut de Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([1]) și de actele de modificare a acestuia;

15. „amenințare la adresa securității" înseamnă o împrejurare sau un agent despre care se poate presupune, în mod rezonabil, că va avea efecte negative asupra securității în cazul în care nu se iau măsuri de răspuns și control;

16. „amenințare imediată la adresa securității" înseamnă o amenințare la adresa securității care apare fără vreo avertizare în acest sens sau în contextul unei avertizări cu foarte puțin timp înainte de apariție, și

17. „amenințare majoră la adresa securității" înseamnă o amenințare la adresa securității despre care se poate presupune, în mod rezonabil, că va duce la pierderea de vieți omenești, vătămări sau lezări grave, daune semnificative aduse proprietății, compromiterea unor informații extrem de sensibile, perturbarea sistemelor informatice sau a capacităților operaționale esențiale ale Comisiei;

18. „vulnerabilitate" înseamnă un punct slab de orice natură despre care se poate presupune, în mod rezonabil, că va avea efecte negative asupra securității în cadrul Comisiei în cazul în care este expus uneia sau mai multor amenințări.

Articolul 2

Obiectul

(1) Prezenta decizie stabilește obiectivele, principiile de bază, organizarea și responsabilitățile în materie de securitate în cadrul Comisiei.

(2) Prezenta decizie se aplică tuturor departamentelor Comisiei și în toate incintele acesteia. Personalul Comisiei din delegațiile Uniunii se va supune normelor de securitate pentru Serviciul European de Acțiune Externă ([2]).

(3) În pofida oricăror indicații specifice cu privire la anumite categorii de personal, prezenta decizie se aplică membrilor Comisiei, personalului Comisiei care intră sub incidența Statutului funcționarilor și condițiilor de angajare a altor agenți ai Uniunii Europene, experților naționali detașați (END) pe lângă Comisie, întreprinderilor prestatoare de servicii și angajaților acestora, stagiarilor și oricăror persoane cărora le este permis accesul în clădirile Comisiei sau la alte active ale acesteia ori la informațiile manipulate de Comisie.

(4) Dispozițiile prezentei decizii se aplică fără a aduce atingere Deciziei 2002/47/CE, CECO, Euratom a Comisiei ([3]) și Deciziei 2004/563/CE, Euratom a Comisiei ([4]), deciziilor C(2006) 1623 ([5]) și C(2006) 3602 ([6]) ale Comisiei.

CAPITOLUL 2

PRINCIPII

Articolul 3

Principii de securitate în cadrul Comisiei

(1) Punerea în aplicare a prezentei decizii de către Comisie se desfășoară în conformitate cu tratatele și îndeosebi cu Carta drepturilor fundamentale și Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, cu instrumentele la care se face referire în considerentul 2, cu toate normele de drept intern aplicabile, precum și cu condițiile prevăzute în prezenta decizie. În cazul în care este necesar, se va emite o notificare de securitate în sensul articolului 21 alineatul (2) care să ofere orientări în acest sens.

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

(3) Principiul legalității se referă la necesitatea de a menține strict în cadrul juridic punerea în aplicare a prezentei decizii și de a respecta cerințele legale.

([1]) Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene și a Regimului aplicabil celorlalți agenți ai Comunităților Europene și de instituire de măsuri speciale aplicabile temporar funcționarilor Comisiei (regim aplicabil altor categorii de angajați) (JO L 56, 4.3.1968, p. 1).

([2]) Decizia Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 19 aprilie 2013 privind normele de securitate pentru Serviciul European de Acțiune Externă (2013/C 190/01) (JO C 190, 29.6.2013, p. 1).

([3]) 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) însoțită de anexa referitoare la dispozițiile privind gestionarea documentelor.

([4]) Decizia 2004/563/CE a Comisiei, Euratom din 7 iulie 2004 de modificare a regulamentului său de procedură (JO L 251, 27.7.2004, p. 9) însoțită de anexa referitoare la dispozițiile privind documentele electronice și digitalizate.

([5]) C(2006) 1623 din 21 aprilie 2006 de stabilire a unei politici armonizate în materie de sănătate și securitate la locul de muncă pentru toți membrii personalului Comisiei Europene.

([6]) C(2006) 3602 din 16 august 2006 privind securitatea sistemelor informaționale utilizate de Comisia Europeană.

(4) Toate măsurile de securitate sunt luate într-un climat de deschidere, cu excepția cazului în care se poate presupune, în mod rezonabil, că acest lucru va compromite efectul măsurii în cauză. Destinatarii unei măsuri de securitate sunt informați în prealabil cu privire la motivele și impactul măsurii, cu excepția cazului în care se poate presupune, în mod rezonabil, că efectul măsurii va fi afectat de transmiterea acestor informații. În acest caz, informațiile respective sunt transmise destinatarului măsurii de securitate după încetarea riscului care amenință efectul măsurii de securitate.

(5) Departamentele Comisiei se asigură că aspectele de securitate sunt luate în considerare de la începutul elaborării și punerii în aplicare a politicilor, deciziilor, programelor, proiectelor și activităților Comisiei pentru care acestea sunt responsabile. Pentru a proceda astfel, vor fi implicați, încă din primele stadii ale preparativelor, Direcția Generală Resurse Umane și Securitate, în ceea ce privește aspectele generale, și responsabilul principal cu securitatea informațiilor Comisiei, în ceea ce privește sistemele IT.

(6) Comisia urmărește, după caz, să coopereze cu autoritățile competente ale statului-gazdă, ale altor state membre și ale altor instituții, agenții sau organe ale UE, în cazul în care acest lucru este fezabil, ținând seama de măsurile luate sau planificate de autoritățile respective pentru a aborda riscurile de securitate în cauză.

Articolul 4

Obligația de conformitate

(1) Conformitatea cu dispozițiile prezentei decizii și normele sale de punere în aplicare, precum și cu măsurile și instrucțiunile de securitate furnizate de personalul autorizat este obligatorie.

(2) Nerespectarea normelor de securitate poate atrage răspunderea disciplinară, în conformitate cu tratatele, Statutul funcționarilor, sancțiunile contractuale și/sau acțiunile în justiție prevăzute de actele cu putere de lege și dispozițiile administrative naționale.

CAPITOLUL 3

ASIGURAREA SECURITĂȚII

Articolul 5

Personalul autorizat

(1) Numai personalului autorizat pe baza unui mandat nominativ, conferit de către directorul general al DG Resurse Umane și Securitate, având în vedere sarcinile care le revin, i se poate acorda competența de a adopta una sau mai multe dintre următoarele măsuri:

1. portul armelor de mână;

2. desfășurarea unor anchete de securitate, astfel cum se menționează la articolul 13;

3. adoptarea unor măsuri de securitate, astfel cum se menționează la articolul 12, conform mandatului.

(2) Mandatele menționate la alineatul (1) se conferă pe o durată care nu depășește perioada în care persoana în cauză deține postul sau funcția pentru care i s-a acordat mandatul respectiv. Acestea se acordă în conformitate cu dispozițiile aplicabile prevăzute la articolul 3 alineatul (1).

(3) În ceea ce privește personalul autorizat, prezenta decizie constituie un regulament de serviciu în sensul articolului 21 din Statutul funcționarilor.

Articolul 6

Dispoziții generale privind măsurile de securitate

(1) Atunci când ia măsuri de securitate, Comisia se asigură, în special, în măsura în care acest lucru este posibil în mod rezonabil, că:

(a) solicită sprijin sau asistență numai din partea statului implicat, cu condiția ca acesta să fie un stat membru al Uniunii Europene sau, în caz contrar, să fie parte la Convenția europeană a drepturilor omului sau să garanteze drepturi care să fie cel puțin echivalente cu drepturile garantate prin această convenție;

(b) transferă informații cu privire la o persoană numai către acei destinatari, alții decât instituțiile și organele comunitare, care nu se supun legislației naționale adoptate în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului ([1]), în conformitate cu articolul 9 din Regulamentul (CE) nr. 45/2001;

([1]) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

(c) în cazul în care o persoană reprezintă o amenințare la adresa securității, orice măsură de securitate trebuie să fie îndreptată împotriva persoanei respective, căreia i se poate impune obligația de a suporta costurile aferente. Aceste măsuri de securitate pot fi îndreptate împotriva altor persoane numai în cazul în care este necesar să se țină sub control o amenințare imediată sau importantă la adresa securității și dacă sunt îndeplinite următoarele condiții:

(a) nu este posibil să se ia măsurile preconizate împotriva persoanei care reprezintă o amenințare la adresa securității sau aceste măsuri riscă să nu fie eficace;

(b) Comisia nu poate controla amenințarea la adresa securității prin propriile sale acțiuni sau nu pot face acest lucru în timp util;

(c) măsura nu constituie un pericol disproporționat pentru alte persoane și drepturile lor.

(2) Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate elaborează o prezentare generală a măsurilor de securitate care pot presupune emiterea unui ordin judecătoresc, în conformitate cu actele cu putere de lege și normele administrative ale statelor membre în care se află incinte ale Comisiei.

(3) Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate poate recurge la un contractant care să efectueze, sub conducerea și supravegherea Direcției de Securitate, sarcini legate de asigurarea securității.

Articolul 7

Măsuri de securitate cu privire la persoane

(1) Se asigură un nivel adecvat de protecție a persoanelor aflate în incintele Comisiei, ținându-se seama de cerințele de securitate și siguranță.

(2) În cazul existenței unor riscuri majore de securitate, Direcția Generală Resurse Umane și Securitate oferă protecție personală membrilor Comisiei sau altor agenți în situația în care o evaluare a riscului a evidențiat că o astfel de protecție este necesară pentru a asigura siguranța și securitatea acestora.

(3) În cazul unor riscuri majore de securitate, Comisia poate dispune evacuarea incintelor sale.

(4) Victimele accidentelor sau atacurilor care au avut loc în incintele Comisiei beneficiază de asistență.

(5) Pentru a preveni și a controla riscurile la adresa securității, membrii personalului autorizat pot efectua verificări ale antecedentelor persoanelor cărora li se aplică prezenta decizie, pentru a stabili dacă faptul că acestor persoane li se permite accesul în incintele sau la informațiile Comisiei prezintă o amenințare la adresa securității. În acest scop și în conformitate cu Regulamentul (CE) nr. 45/2001 și dispozițiile la care se face referire în articolul 3 alineatul (1), membrii personalului autorizat pot:

(a) utiliza orice sursă de informare de care dispune Comisia, ținând seama de fiabilitatea sursei de informare;

(b) avea acces la dosarul de personal sau la datele personale de care dispune Comisia cu privire la persoanele pe care le-a angajat sau pe care intenționează să le angajeze sau referitoare la membrii personalului contractanților, atunci când acest lucru se justifică în mod corespunzător.

Articolul 8

Măsuri de securitate cu privire la securitatea fizică și activele fixe

(1) Securitatea activelor trebuie să fie asigurată prin aplicarea unor măsuri adecvate de protecție fizică și tehnică și a procedurilor corespunzătoare, denumite în continuare „securitate fizică”, creându-se un sistem organizat pe mai multe niveluri.

(2) În temeiul prezentului articol se pot adopta măsuri în vederea protejării persoanelor sau a informațiilor la nivelul Comisiei, precum și pentru protejarea activelor.

(3) Obiectivele securității fizice sunt următoarele:

— prevenirea actelor de violență îndreptate împotriva membrilor Comisiei sau a persoanelor care intră sub incidența prezentei decizii;

— prevenirea spionajului și a interceptării informațiilor sensibile sau clasificate;

— prevenirea furturilor, a actelor de vandalism, sabotaj și a altor acțiuni violente care vizează vătămarea sau distrugerea clădirilor și activelor Comisiei;

— să permită efectuarea unor investigații și anchete cu privire la incidentele de securitate, inclusiv prin controale vizând fișierele de control al intrărilor și ieșirilor, monitorizarea prin intermediul televiziunii cu circuit închis (CCTV), înregistrările convorbirilor telefonice și ale unor date similare, astfel cum se menționează la articolul 22 alineatul (2) de mai jos și alte surse de informații.

(4) Securitatea fizică trebuie să includă:

— o politică de acces care se aplică tuturor persoanelor sau vehiculelor care solicită accesul la incintele Comisiei, inclusiv la locurile de parcare;

— un sistem de control al accesului care să cuprindă agenți de securitate, echipament și măsuri tehnice, sisteme de informații sau o combinație a tuturor acestor elemente.

(5) Pentru a asigura securitatea fizică, pot fi întreprinse următoarele acțiuni:

— înregistrarea persoanelor, a vehiculelor, a bunurilor și a echipamentelor care intră sau ies din incintele Comisiei;

— efectuarea de controale de identitate în incintele Comisiei;

— efectuarea de controale ale vehiculelor, bunurilor și echipamentelor cu ajutorul unor mijloace vizuale sau tehnice;

— împiedicarea accesului persoanelor, vehiculelor și bunurilor neautorizate în incintele Comisiei.

Articolul 9

Măsuri de securitate cu privire la informații

(1) Securitatea informațiilor se referă la toate informațiile gestionate de Comisie.

(2) Securitatea informațiilor, indiferent de forma acestora, trebuie să se caracterizeze printr-un echilibru între transparență, proporționalitate, responsabilitate și eficiență, pe de o parte, și necesitatea de a proteja informațiile împotriva accesului, a utilizării, a divulgării, a modificării sau a distrugerii neautorizate, pe de altă parte.

(3) Securitatea informațiilor are ca scop protejarea confidențialității, a integrității și a disponibilității acestora.

(4) Prin urmare, trebuie să se utilizeze proceduri de management al riscurilor pentru a clasifica activele informaționale și a se elabora măsuri, proceduri și standarde de securitate proporționale,, inclusiv măsuri de atenuare.

(5) Aceste principii generale care stau la baza securității informațiilor se aplică în special în ceea ce privește:

(a) „informațiile clasificate ale Uniunii Europene" (denumite în continuare IUEC), și anume orice informații sau materiale desemnate ca atare printr-o clasificare în materie de securitate a UE a căror divulgare neautorizată ar putea cauza prejudicii de diferite grade intereselor Uniunii Europene sau ale unora sau mai multor state membre;

(b) „informațiile sensibile neclasificate", și anume informațiile sau materialele pe care Comisia trebuie să le protejeze ca urmare a obligațiilor legale stabilite prin tratate sau prin actele adoptate pentru punerea în aplicare a acestora și/sau din cauza caracterului lor sensibil. Informațiile sensibile neclasificate includ, fără a se limita la acestea, informații sau materiale care fac obiectul obligației de păstrare a secretului profesional, astfel cum se menționează la articolul 339 din TFUE, informații care fac obiectul intereselor protejate, în conformitate cu articolul 4 din Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului [1], coroborat cu jurisprudența relevantă a Curții de Justiție a Uniunii Europene, sau date cu caracter personal care intră sub incidența Regulamentului (CE) nr. 45/2001.

(6) Informațiile sensibile neclasificate fac obiectul normelor privind operațiunile de manipulare și păstrare a acestora. Aceste informații pot fi transmise numai acelor persoane cărora li se aplică principiul „necesității de a cunoaște". Atunci când se consideră că acest lucru este necesar pentru protecția efectivă a caracterului lor confidențial, aceste informații trebuie să fie identificate printr-un marcaj de securitate și prin instrucțiuni de manipulare corespunzătoare, aprobate de directorul general al DG Resurse Umane și Securitate. Atunci când sunt gestionate sau păstrate în sisteme informatice și de comunicații, aceste informații trebuie să fie protejate, de asemenea, în conformitate cu Decizia (2006) 3602 a Comisiei, cu normele de aplicare a acesteia și cu standardele corespunzătoare.

(7) Orice persoană responsabilă de compromiterea sau pierderea IUEC sau a unor informații sensibile neclasificate, care sunt identificate ca atare în normele privind manipularea și păstrarea acestora, este pasibilă de măsuri disciplinare, în conformitate cu Statutul funcționarilor. Aceste măsuri disciplinare nu aduc atingere niciunei alte proceduri contencioase sau penale puse în aplicare de către autoritățile naționale competente ale statelor membre în conformitate cu actele cu putere de lege și normele lor administrative și nici căilor de atac contractuale.

[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).

Articolul 10

Măsuri de securitate cu privire la sistemele informatice și de comunicații

(1) Toate sistemele informatice și de comunicații („SIC") utilizate de Comisie sunt conforme cu politica de securitate privind sistemele de informații ale Comisiei, prevăzută în Decizia C (2006) 3602 a Comisiei, în normele de aplicare a acesteia și în standardele de securitate corespunzătoare.

(2) Serviciile Comisiei care dețin, gestionează sau utilizează SIC permit accesul instituțiilor, al agențiilor, al organelor Uniunii sau al altor organizații la aceste sisteme, numai cu condiția ca aceste instituții, agenții, organe ale Uniunii sau alte organizații să fie în măsură să ofere o asigurare rezonabilă că sistemele lor informatice sunt protejate la un nivel echivalent cu cel al politicii Comisiei privind securitatea sistemelor informatice, prevăzută în Decizia C (2006) 3602 a Comisiei, în normele de aplicare a acesteia și în standardele de securitate corespunzătoare. Comisia monitorizează respectarea acestor cerințe, și, în caz de neconformitate gravă sau neconformare persistentă, are dreptul să interzică accesul.

Articolul 11

Analiza criminalistică în materie de securitate cibernetică

Direcției Generale Resurse Umane și Securitate îi revine în special responsabilitatea efectuării de analize criminalistice tehnice în cooperare cu departamentele competente ale Comisiei, în sprijinul anchetelor de securitate prevăzute la articolul 13, referitoare la contrainformații, scurgerea de date, atacuri cibernetice și securitatea sistemelor informatice.

Articolul 12

Măsuri de securitate cu privire la persoane și obiecte

(1) Pentru a asigura securitatea în cadrul Comisiei și pentru a preveni și a controla riscurile, membrii personalului autorizat în temeiul articolului 5 pot lua, în conformitate cu principiile prevăzute la articolul 3, printre altele, una sau mai multe dintre următoarele măsuri de securitate:

(a) securizarea spațiilor și a probelor, inclusiv prin intermediul fișierelor-jurnal de control al accesului și ieșirilor și al imaginilor CCTV în cazul unor incidente sau comportamente care pot duce la proceduri administrative, disciplinare, civile sau penale;

(b) un număr limitat de măsuri vizând persoanele care prezintă o amenințare la adresa securității, inclusiv să ordone persoanelor să părăsească incintele Comisiei, să însoțească persoanele atunci când părăsesc incintele Comisiei, să interzică persoanelor accesul în incintele Comisiei pe o perioadă de timp stabilită în conformitate cu criteriile care urmează a fi definite în normele de punere în aplicare;

(c) un număr limitat de măsuri referitoare la obiecte care prezintă o amenințare la adresa securității, inclusiv eliminarea, confiscarea și distrugerea obiectelor;

(d) efectuarea de percheziții în incintele Comisiei, inclusiv în birourile situate în aceste incinte;

(e) efectuarea de controale având ca obiect sistemele informatice și de comunicare și echipamentele, datele privind traficul telefonic și de telecomunicații, fișierele-jurnal, conturile de utilizator etc.;

(f) alte măsuri de securitate specifice cu efect similar, în scopul de a preveni sau de a controla riscurile la adresa securității, în special în contextul drepturilor de care beneficiază Comisia în calitate de proprietar sau angajator, în conformitate cu legile naționale aplicabile.

(2) În situații excepționale, membrii personalului din Direcția Securitate din cadrul Direcției Generale Resurse Umane și Securitate, autorizați în conformitate cu articolul 5, pot lua orice măsuri urgente necesare, în strictă conformitate cu principiile stabilite la articolul 3. Cât mai curând posibil după luarea măsurilor respective, aceștia îl informează în acest sens pe directorul Direcției Securitate, care va solicita un mandat corespunzător din partea directorului general al Direcției Generale Resurse Umane și Securitate, confirmând măsurile adoptate și autorizând luarea oricăror altor acțiuni necesare, și cooperează, după caz, cu autoritățile naționale competente.

(3) Măsurile de securitate adoptate în temeiul prezentului articol trebuie consemnate în momentul adoptării sau, în cazul unui risc imediat sau al unei situații de criză, într-un termen rezonabil după adoptarea lor. În acest din urmă caz, documentația trebuie să includă, de asemenea, elementele care au stat la baza evaluării referitoare la existența unui risc imediat sau a unei situații de criză. Documentația poate fi concisă, dar ar trebui să fie întocmită într-un mod care să îi permită persoanei care face obiectul măsurii să își exercite dreptul la apărare și la protecția datelor cu caracter personal, în conformitate cu Regulamentul (CE) nr. 45/2001, și care să permită efectuarea unui control cu privire la legalitatea măsurii. Nicio informație cu privire la măsurile de securitate specifice vizând un membru al personalului nu figurează în dosarul personal al persoanei în cauză.

(4) Atunci când ia măsuri de securitate în temeiul literei (b), Comisia se asigură, de asemenea, că persoana în cauză are posibilitatea de a contacta un avocat sau o persoană de încredere și că i se aduce la cunoștință faptul că are dreptul să se adreseze Autorității Europene pentru Protecția Datelor.

Articolul 13

Anchetele

(1) Fără a aduce atingere articolului 86 și anexei IX din Statutul funcționarilor sau oricăror acorduri speciale încheiate între Comisie și SEAE, precum acordul special privind obligația de diligență față de personalul Comisiei care își desfășoară activitatea în delegațiile Uniunii, încheiat la 28 mai 2014 între Direcția Generală Resurse Umane și Securitate a Comisiei Europene și Serviciul European de Acțiune Externă, pot fi efectuate anchete privind securitatea:

(a) în cazul unor incidente care afectează securitatea la nivelul Comisiei, inclusiv în cazul unor presupuse infracțiuni;

(b) în cazul unor eventuale scurgeri de informații, al utilizării necorespunzătoare sau al compromiterii informațiilor sensibile neclasificate, a informațiilor UE clasificate (IUEC) sau a datelor clasificate ale Euratom;

(c) în contextul activităților de contrainformații și de contracarare a terorismului;

(d) în cazul unor incidente cibernetice grave.

(2) Decizia de a desfășura o anchetă privind securitatea este luată de către directorul general al DG Resurse Umane și Securitate care este, de asemenea, destinatarul raportului de anchetă.

(3) Anchetele privind securitatea sunt efectuate numai de către membrii specializați ai personalului din cadrul Direcției Generale Resurse Umane și Securitate, autorizați în mod corespunzător în conformitate cu articolul 5.

(4) Personalul autorizat își exercită în mod independent atribuțiile cu privire la anchetele privind securitatea, astfel cum se specifică în mandat, și deține competențele enumerate la articolul 12.

(5) Membrii personalului autorizat care au competența de a desfășura anchete privind securitatea pot colecta informații din toate sursele disponibile referitoare la orice contravenții sau infracțiuni comise în incintele Comisiei sau în care sunt implicate persoanele menționate la articolul 2 alineatul (3), fie în calitate de victimă, fie ca autori ai unor astfel de infracțiuni.

(6) Direcția Generală Resurse Umane și Securitate informează autoritățile competente din statul membru gazdă sau din oricare alt stat membru în cauză, dacă este cazul și, în special, dacă anchetele au oferit indicii cu privire la faptul că s-ar fi comis o infracțiune. În acest context, Direcția Generală Resurse Umane și Securitate poate, în cazul în care este oportun sau necesar, să ofere sprijin autorităților din statul membru gazdă sau din oricare alt stat membru implicat.

(7) În cazul incidentelor cibernetice grave, Direcția Generală Informatică colaborează îndeaproape cu Direcția Generală Resurse Umane și Securitate pentru acordarea de sprijin privind toate aspectele tehnice. Direcția Generală Resurse Umane și Securitate decide, după consultarea Direcției Generale Informatică, să informeze, atunci când este oportun, autoritățile competente din țara gazdă sau din oricare alt stat membru implicat. Serviciile de coordonare a incidentelor din cadrul Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile europene („CERT-UE") sunt utilizate pentru acordarea de sprijin altor instituții și agenții ale UE care pot fi afectate.

(8) Anchetele privind securitatea sunt documentate.

Articolul 14

Delimitarea competențelor în ceea ce privește anchetele privind securitatea și alte tipuri de investigații

(1) În cazul în care Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate efectuează anchete privind securitatea, astfel cum se prevede la articolul 13, și dacă aceste anchete intră în sfera de competență a Oficiului European de Luptă Antifraudă (OLAF) sau a Oficiului de investigație și de disciplină al Comisiei (IDOC), aceasta ia imediat legătura cu organismele respective, cu scopul, în special, de a nu compromite acțiunile ulterioare ale OLAF sau ale IDOC. După caz, Direcția de Securitate din cadrul Direcției Generale Resurse Umane și Securitate invită OLAF sau IDOC să participe la anchetă.

(2) Efectuarea anchetelor privind securitatea menționate la articolul 13 nu aduce atingere competențelor OLAF și IDOC, astfel cum sunt prevăzute în normele care reglementează aceste organisme. Direcției de Securitate din cadrul Direcției Generale Resurse Umane și Securitate i se poate solicita acordarea de asistență tehnică în cadrul anchetelor inițiate de OLAF sau de IDOC.

(3) Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate i se poate solicita acordarea de asistență agenților OLAF atunci când intră în incintele Comisiei, în conformitate cu articolul 3 alineatul (5) și cu articolul 4 alineatul (4) din Regulamentul 883/2013 al Parlamentului European și al Consiliului ([1]), pentru a le facilita

([1]) 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).

sarcinile. Direcția Securitate aduce aceste cereri de asistență la cunoștința Secretarului General și a directorului general al Direcției Generale Resurse Umane și Securitate sau, în cazul în care aceste anchete se desfășoară în spațiile Comisiei ocupate de membrii săi sau de către Secretarul General, a președintelui Comisiei Europene și a comisarului responsabil pentru resurse umane.

(4) Fără a aduce atingere articolului 22 litera (a) din Statutul funcționarilor, dacă un caz este susceptibil de a intra atât în competența Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, cât și în competența IDOC, în momentul în care aduce acest lucru la cunoștința directorului general al DG Resurse Umane, în conformitate cu articolul 13, Direcția Securitate examinează, în stadiul cel mai timpuriu posibil, dacă există motive care justifică sesizarea IDOC cu privire la această problemă. Se consideră că acest stadiu a fost atins atunci când o amenințare imediată la adresa securității a luat sfârșit. Directorul general al DG Resurse Umane și Securitate ia o decizie cu privire la această chestiune.

(5) În situația în care un caz un caz este susceptibil de a intra atât în competența Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, cât și în competența OLAF, Direcția Securitate aduce imediat acest lucru la cunoștința directorului general al DG Resurse Umane și Securitate și îl informează, în acest sens, în stadiul cel mai timpuriu posibil, pe directorul general al OLAF. Se consideră că acest stadiu a fost atins atunci când o amenințare imediată la adresa securității a luat sfârșit.

Articolul 15

Inspecții de securitate

(1) Direcția Generală Resurse Umane și Securitate efectuează inspecții de securitate pentru a verifica respectarea de către serviciile Comisiei și de către cetățeni a prezentei decizii și a normelor de aplicare a acesteia și pentru a formula recomandări atunci când consideră că acest lucru este necesar.

(2) Atunci când este cazul, Direcția Generală Resurse Umane și Securitate efectuează inspecții de securitate și vizite de monitorizare sau de evaluare a securității, pentru a verifica dacă securitatea personalului Comisiei, a bunurilor și a informațiilor care intră în sfera de responsabilitate a instituțiilor, a agențiilor sau a altor organisme ale Uniunii, a statelor membre, a țărilor terțe sau a organizațiilor internaționale sunt protejate în mod corespunzător, în conformitate cu norme, reglementări și standarde de securitate care sunt cel puțin echivalente cu cele ale Comisiei. Atunci când este oportun și în spiritul bunei cooperări între administrații, aceste inspecții de securitate includ, de asemenea, inspecțiile efectuate în contextul schimbului de informații clasificate cu alte instituții, organe și agenții ale Uniunii, cu statele membre, cu state terțe sau cu organizații internaționale.

(3) Prezentul articol se aplică, *mutatis mutandis*, personalului Comisiei din delegațiile Uniunii, fără a aduce atingere acordurilor speciale încheiate între Comisie și SEAE, precum acordul special privind obligația de diligență față de personalul Comisiei care își desfășoară activitatea în delegațiile Uniunii, încheiat la 28 mai 2014 între Direcția Generală Resurse Umane și Securitate a Comisiei Europene și Serviciul European de Acțiune Externă.

Articolul 16

Niveluri de alertă și gestionarea situațiilor de criză

(1) Direcția Generală Resurse Umane și Securitate este responsabilă atât pentru punerea în aplicare a unor măsuri adecvate pentru nivelurile de alertă, pentru a anticipa sau a răspunde amenințărilor și incidentelor care afectează securitatea în spațiile Comisiei, cât și pentru măsurile necesare pentru gestionarea situațiilor de criză.

(2) Măsurile corespunzătoare nivelurilor de alertă menționate la alineatul (1) sunt proporționale cu nivelul de amenințare la adresa securității. Nivelurile de alertă trebuie să fie definite în strânsă colaborare cu serviciile competente ale celorlalte instituții, agenții și organe ale Uniunii și ale statului membru sau statelor membre în care sunt situate sediile Comisiei.

(3) Direcția Generală Resurse Umane și Securitate este punctul de contact pentru nivelurile de alertă și gestionarea situațiilor de criză.

CAPITOLUL 4

ORGANIZARE

Articolul 17

Responsabilitățile generale ale serviciilor Comisiei

(1) Responsabilitățile Comisiei menționate în prezenta decizie sunt exercitate de Direcția Generală Resurse Umane și Securitate, sub autoritatea și responsabilitatea membrului Comisiei responsabil de securitate.

(2) Acordurile specifice în ceea ce privește securitatea cibernetică sunt definite în Decizia (2006) 3602.

(3) Responsabilitățile privind punerea în aplicare a prezentei decizii și normele de punere în aplicare a acesteia, precum și asigurarea respectării zilnice a acestora pot fi delegate altor departamente ale Comisiei, ori de câte ori asigurarea descentralizată a serviciilor de securitate oferă câștiguri importante în materie de eficiență, resurse sau timp, de exemplu datorită localizării geografice a serviciilor în cauză.

(4) În cazul în care se aplică alineatul (3), Direcția Generală Resurse Umane și Securitate și, după caz, directorul general al DG Informatică încheie acorduri cu anumite departamente din cadrul Comisiei, care stabilesc roluri și responsabilități clare privind punerea în aplicare și monitorizarea politicilor de securitate.

Articolul 18

Direcția Generală Resurse Umane și Securitate

(1) Direcției Generale Resurse Umane și Securitate îi revin, în special, următoarele responsabilități:

1. elaborarea politicii de securitate a Comisiei, a normelor de punere în aplicare și a notificărilor de securitate;
2. colectarea de informații în vederea evaluării amenințărilor și a riscurilor la adresa securității și cu privire la toate problemele care pot afecta securitatea în spațiile Comisiei;
3. furnizarea de supraveghere electronică și protecție în toate spațiile de lucru ale Comisiei, ținând seama în mod corespunzător de evaluările amenințărilor și dovezile privind desfășurarea unor activități neautorizate care deservesc interesele Comisiei;
4. punerea la dispoziția serviciilor și a personalului Comisiei a unui serviciu de urgență permanent (24 de ore/7 zile) pentru toate aspectele legate de siguranță și securitate;
5. punerea în aplicare a măsurilor de securitate menite să reducă riscurile la adresa securității și dezvoltarea și menținerea unui sistem informatic și de comunicații adecvat pentru a acoperi necesitățile operaționale ale acesteia, în special în domeniile controlului accesului fizic, al administrării autorizațiilor de securitate și al manipulării informațiilor sensibile și clasificate ale UE;
6. acțiuni de conștientizare, organizarea de exerciții și antrenamente și oferirea de cursuri de pregătire și de servicii de consiliere cu privire la toate aspectele legate de securitate în spațiile Comisiei, în vederea promovării unei culturi a securității și a creării unei echipe de membri ai personalului pregătiți în mod corespunzător în materie de securitate.

(2) Direcția Generală Resurse Umane și Securitate asigură, fără a aduce atingere competențelor și responsabilităților altor servicii ale Comisiei, legătura cu următoarele servicii externe:

1. serviciile de securitate ale celorlalte instituții, agenții și organe ale Uniunii, cu privire la chestiuni legate de securitatea persoanelor, a bunurilor și a informațiilor în spațiile Comisiei;
2. serviciile de securitate, de informații și de evaluare a amenințărilor, inclusiv cu autoritățile naționale de securitate, din state membre, țări terțe și din cadrul unor organizații sau instituții internaționale, cu privire la chestiuni care afectează securitatea persoanelor, a activelor și a informațiilor în spațiile Comisiei;
3. poliția și alte servicii de urgență, cu privire la toate chestiunile obișnuite și urgente care afectează securitatea Comisiei;
4. autoritățile responsabile cu securitatea din cadrul altor instituții, agenții și organe ale Uniunii, din state membre și țări terțe, în domeniul combaterii atacurilor cibernetice cu un impact potențial asupra securității Comisiei;
5. în ceea ce privește primirea, evaluarea și difuzarea de informații referitoare la amenințările reprezentate de terorism și de activitățile de spionaj care afectează securitatea Comisiei;
6. în ceea ce privește aspectele referitoare la informații clasificate, astfel cum se specifică în continuare în Decizia (UE, Euratom) 2015/444 a Comisiei ([1]).

(3) Direcția Generală Resurse Umane și Securitate este responsabilă pentru securitatea transmiterii informațiilor efectuate în temeiul prezentului articol, inclusiv pentru transmiterea de date cu caracter personal.

Articolul 19

Grupul de experți pe probleme de securitate din cadrul Comisiei (ComSEG)

Se înființează Grupul de experți pe probleme de securitate din cadrul Comisiei, având drept mandat consilierea Comisiei, după caz, cu privire la chestiuni legate de politica de securitate internă și, în special, cu privire la protejarea informațiilor clasificate ale UE.

([1]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (a se vedea pagina 53 din prezentul Jurnal Oficial)

Articolul 20

Ofițeri locali de securitate (LSO)

(1) Fiecare departament sau cabinet al Comisiei numește un ofițer local de securitate (LSO), care acționează ca principal punct de contact între serviciul său și Direcția Generală Resurse Umane și Securitate cu privire la toate aspectele legate de securitate în spațiile Comisiei. Dacă este necesar, pot fi numiți unul sau mai mulți adjuncți ai LSO. Funcția de LSO est îndeplinită de un funcționar sau un agent temporar.

(2) În calitate de principal punct de contact privind securitatea în departamentul sau cabinetul Comisiei pe care îl reprezintă, LSO raportează periodic Direcției Generale Resurse Umane și Securitate și superiorilor săi ierarhici cu privire la problemele de securitate cu care se confruntă departamentul Comisiei din care face parte și aduce imediat la cunoștința acestora orice incidente legate de securitate, inclusiv pe cele care ar putea compromite informațiile IUEC sau informațiile sensibile neclasificate.

(3) În ceea ce privește aspectele legate de securitatea sistemelor informatice și de comunicații, LSO ține legătura cu ofițerii locali de securitate informatică (LISO) din cadrul departamentului Comisiei pe care îl reprezintă, ale cărui rol și responsabilități sunt prevăzute în Decizia C (2006) 3602 a Comisiei.

(4) Acesta contribuie la activitățile de formare și conștientizare în domeniul securității care răspund nevoilor specifice ale personalului, ale contractanților și ale altor persoane care acționează sub autoritatea departamentului Comisiei din care acesta face parte.

(5) La cererea Direcției Generale Resurse Umane și Securitate, în cazul apariției unor riscuri majore care amenință securitatea sau în situații de urgență, ofițerului local de securitate LSO i se pot atribui sarcini specifice. Directorul general sau directorul de resurse umane din cadrul Direcției Generale din care face parte LSO este informat cu privire la aceste sarcini specifice de către Direcția Generală Resurse Umane și Securitate.

(6) Responsabilitățile LSO nu aduc atingere rolului și responsabilităților atribuite ofițerilor locali de securitate informatică (LISO), responsabililor cu sănătatea și securitatea, ofițerilor de control ai registraturii (RCO) sau oricărei alte funcții care implică responsabilități în materie de securitate sau siguranță. LSO ține legătura cu persoanele menționate pentru a asigura o abordare coerentă și consecventă a politicii de securitate și un flux eficient de informații cu privire la aspectele legate de securitate în spațiile Comisiei.

(7) Atunci când LSO transmite informații superiorilor săi imediați, acesta are acces direct la directorul său general sau la șeful său de serviciu. LSO deține un certificat de securitate care să îi permite accesul la informațiile UE clasificate, cel puțin până la nivelul SECRET UE/EU SECRET.

(8) În vederea promovării schimbului de informații și a celor mai bune practici, Direcția Generală Resurse Umane și Securitate organizează, cel puțin de două ori pe an, o conferință a LSO. Participarea LSO la aceste conferințe este obligatorie.

CAPITOLUL 5

PUNEREA ÎN APLICARE

Articolul 21

Norme de punere în aplicare și notificări în materie de securitate

(1) Dacă este necesar, adoptarea normelor de punere în aplicare a prezentei decizii face obiectul unei decizii separate a Comisiei prin care este abilitat, în deplină conformitate cu regulamentul intern de procedură, membrul Comisiei însărcinat cu probleme de securitate.

(2) După abilitarea sa, în urma deciziei susmenționate a Comisiei, membrul Comisiei însărcinat cu probleme de securitate poate elabora notificări în materie de securitate care să stabilească orientări în materie de securitate și cele mai bune practici din domeniul de aplicare al prezentei decizii și al normelor de punere în aplicare a acesteia.

(3) Comisia poate delega directorului general al Direcției Generale Resurse Umane și Securitate, pe baza unei decizii de delegare separate, în deplină conformitate cu regulamentul intern de procedură, sarcinile menționate la primul și al doilea alineat din prezentul articol.

CAPITOLUL 6

DISPOZIȚII DIVERSE ȘI DISPOZIȚII FINALE

Articolul 22

Prelucrarea datelor cu caracter personal

(1) Comisia prelucrează datele cu caracter personal necesare pentru punerea în aplicare a prezentei decizii în conformitate cu Regulamentul (CE) nr. 45/2001.

(2) În pofida măsurilor deja în vigoare la data adoptării prezentei decizii, notificate Autorității Europene pentru Protecția Datelor ([1]), orice măsură adoptată în temeiul prezentei decizii care implică prelucrarea de date cu caracter personal, de exemplu date referitoare la fișierele privind intrările și ieșirile, înregistrări TVCI, înregistrări ale unor convorbiri telefonice cu serviciile de permanență sau centrele de expediere și date similare, care sunt necesare din motive de securitate sau pentru a interveni în situații de criză, trebuie să facă obiectul unor norme de punere în aplicare în conformitate cu articolul 21, care să stabilească garanții corespunzătoare pentru persoanele vizate.

(3) Directorul general al Direcției Generale Resurse Umane și Securitate este responsabil pentru securitatea oricărei operațiuni de prelucrare a datelor cu caracter personal efectuate în cadrul prezentei decizii.

(4) Normele și procedurile de punere în aplicare menționate se adoptă după consultarea responsabilului cu protecția datelor și a Autorității Europene pentru Protecția Datelor, în conformitate cu Regulamentul (CE) nr. 45/2001.

Articolul 23

Transparență

Prezenta decizie și normele de punere în aplicare a acesteia sunt aduse la cunoștința personalului Comisiei și a tuturor persoanelor cărora li se aplică aceste dispoziții.

Articolul 24

Abrogarea deciziilor anterioare

Decizia (94) 2129 se abrogă.

Articolul 25

Intrarea în vigoare

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 13 martie 2015.

Pentru Comisie

Președintele

Jean-Claude JUNCKER

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.