DECIZIA COMISIEI

din 4 mai 2010

privind planul de securitate pentru funcționarea Sistemului de informații privind vizele

(2010/260/UE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS) [1], în special articolul 32,

întrucât:

(1) Articolul 32 alineatul (3) din Regulamentul (CE) nr. 767/2008 prevede că autoritatea de administrare ia măsurile necesare în vederea realizării obiectivelor în domeniul securității stabilite la articolul 32 alineatul (2) în ceea ce privește funcționarea VIS, inclusiv adoptarea unui plan de securitate.

(2) Articolul 26 alineatul (4) din Regulamentul (CE) nr. 767/2008 prevede că, în cursul perioadei de tranziție, înainte ca autoritatea de administrare să își preia responsabilitățile, Comisiei îi revine sarcina administrării operative a VIS.

(3) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului [2] se aplică prelucrării datelor cu caracter personal de către Comisie, atunci când aceasta își îndeplinește sarcina administrării operative a VIS.

(4) Articolul 26 alineatul (7) din Regulamentul (CE) nr. 767/2008 prevede că, în cazul în care Comisia își deleagă responsabilitatea în cursul perioadei de tranziție, înainte ca autoritatea de administrare să își preia responsabilitățile, aceasta garantează că delegarea nu aduce atingere vreunui mecanism care permite un control efectiv exercitat, în temeiul legislației Uniunii, de Curtea de Justiție, Curtea de Conturi sau Autoritatea Europeană pentru Protecția Datelor.

(5) Autoritatea de administrare trebuie să-și stabilească propriul plan de securitate în ceea ce privește VIS de îndată ce își preia responsabilitățile.

(6) Decizia 2008/602/CE a Comisei din 17 iunie 2008 de stabilire a arhitecturii fizice și a cerințelor privind interfețele naționale și infrastructura de comunicații dintre Sistemul central de informații privind vizele (VIS) și interfețele naționale pentru etapa de dezvoltare [3] a descris serviciile de securitate necesare aplicabile rețelei pentru VIS.

(7) Articolul 27 din Regulamentul (CE) nr. 767/2008 prevede că VIS central principal, care asigură executarea funcțiilor de supraveghere și gestionare tehnică, este situat la Strasbourg (Franța), iar un VIS central de rezervă, capabil să asigure toate funcționalitățile VIS central principal, în cazul funcționării necorespunzătoare a acestuia, este situat la Sankt Johann im Pongau (Austria).

(8) Ar trebui stabilite rolurile responsabililor cu securitatea pentru a se asigura un răspuns eficient și prompt în cazul incidentelor de securitate și raportarea cu privire la acestea.

(9) Ar trebui definită o politică de securitate, care să descrie toate detaliile tehnice și organizatorice, în conformitate cu dispozițiile prezentei decizii.

(10) Ar trebui definite măsuri pentru a se asigura un nivel adecvat de securitate al funcționării VIS,

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect

Prezenta decizie definește organizarea securității și a măsurilor (planul de securitate) în sensul articolului 32 alineatul (3) din Regulamentul (CE) nr. 767/2008.

CAPITOLUL II

ORGANIZARE, RESPONSABILITĂȚI ȘI GESTIONAREA INCIDENTELOR

Articolul 2

Sarcinile Comisiei

(1) Comisia pune în aplicare măsurile de securitate pentru VIS central și pentru infrastructura de comunicații menționate în prezenta decizie și monitorizează eficacitatea acestor măsuri.

[1] JO L 218, 13.8.2008, p. 60.
[2] JO L 8, 12.1.2001, p. 1.
[3] JO L 194, 23.7.2008, p. 3.

(2) Comisia desemnează dintre funcționarii săi un responsabil cu securitatea sistemului. Responsabilul cu securitatea sistemului este numit de directorul general al Direcției Generale Justiție, Libertate și Securitate din cadrul Comisiei. Sarcinile responsabilului cu securitatea sistemului cuprind, în special:

(a) pregătirea, actualizarea și revizuirea politicii de securitate, astfel cum se prevede la articolul 7 din prezenta decizie;

(b) monitorizarea eficacității punerii în aplicare a procedurilor de securitate pentru VIS central și pentru infrastructura de comunicații;

(c) contribuția la elaborarea rapoartelor privind securitatea, astfel cum se prevede la articolul 50 alineatele (3) și (4) din Regulamentul (CE) nr. 767/2008;

(d) îndeplinirea sarcinilor de coordonare și asistență în cadrul controalelor și auditurilor efectuate de Autoritatea Europeană pentru Protecția Datelor menționate la articolul 42 din Regulamentul (CE) nr. 767/2008;

(e) monitorizarea aplicării corespunzătoare și integrale a prezentei decizii și a politicii de securitate de către toți contractanții, inclusiv subcontractanții, implicați în orice fel în gestionarea și funcționarea VIS;

(f) stabilirea unei liste de puncte naționale unice de contact pentru securitatea VIS și transmiterea acesteia responsabililor locali pentru securitatea VIS central și a infrastructurii de comunicații.

Articolul 3

Responsabilul local pentru securitatea VIS central

(1) Fără a aduce atingere articolului 8, Comisia desemnează dintre funcționarii săi un responsabil local pentru securitatea VIS central. Se va evita apariția conflictelor de interese între sarcina responsabilului local cu securitatea și orice alte sarcini oficiale. Responsabilul local pentru securitatea VIS central este numit de directorul general al Direcției Generale Justiție, Libertate și Securitate din cadrul Comisiei.

(2) Responsabilul local pentru securitatea VIS central se asigură că măsurile de securitate prevăzute de prezenta decizie sunt puse în aplicare și că procedurile de securitate sunt urmate în VIS central principal. În ceea ce privește VIS central de rezervă, responsabilul local pentru securitatea VIS central se asigură că măsurile de securitate prevăzute de prezenta decizie, cu excepția celor menționate la articolul 10, sunt puse în aplicare și că procedurile de securitate conexe sunt urmate.

(3) Responsabilul local pentru securitatea VIS central poate încredința unui subordonat oricare dintre sarcinile care îi revin. Se va evita apariția conflictelor de interese între misiunea de a executa aceste sarcini și orice alte sarcini oficiale. Un număr de telefon unic și o singură adresă permit contactarea în orice moment a responsabilului local cu securitatea sau a subordonatului său de serviciu.

(4) Responsabilul local pentru securitatea VIS central execută sarcinile decurgând din măsurile de securitate care trebuie luate pe site-ul principal și de rezervă al VIS, în limitele prevăzute la alineatul (1), în special:

(a) sarcini privind securitatea operațională locală, inclusiv auditul sistemului firewall, teste regulate de securitate, audit și raportare;

(b) monitorizarea eficacității planului de continuare a activității și asigurarea efectuării unor exerciții regulate;

(c) culegerea de informații privind orice incident care ar putea avea un impact asupra securității VIS central și a infrastructurii de comunicații și raportarea acestor informații responsabilului cu securitatea sistemului;

(d) informarea responsabilului cu securitatea sistemului în cazul în care politica de securitate trebuie modificată;

(e) monitorizarea aplicării prezentei decizii și a politicii de securitate de către toți contractanții, inclusiv subcontractanți, implicați în orice fel în gestionarea și funcționarea VIS central;

(f) asigurarea faptului că personalul este informat cu privire la obligațiile care îi revin și monitorizarea aplicării politicii de securitate;

(g) monitorizarea evoluțiilor în materie de securitate informatică și asigurarea unei formări corespunzătoare a personalului;

(h) pregătirea informațiilor de bază și a opțiunilor pentru elaborarea, actualizarea și revizuirea politicii de securitate, în conformitate cu articolul 7.

Articolul 4

Responsabilul local pentru securitatea infrastructurii de comunicații

(1) Fără a aduce atingere articolului 8, Comisia desemnează dintre funcționarii săi un responsabil local pentru securitatea infrastructurii de comunicații. Se va evita apariția conflictelor de interese între sarcina responsabilului local cu securitatea și orice alte sarcini oficiale. Responsabilul local pentru securitatea infrastructurii de comunicații este numit de directorul general al Direcției Generale Justiție, Libertate și Securitate din cadrul Comisiei.

(2) Responsabilul local pentru securitatea infrastructurii de comunicații monitorizează funcționarea infrastructurii de comunicații și se asigură că măsurile de securitate sunt puse în aplicare și că procedurile de securitate sunt urmate.

(3) Responsabilul local pentru securitatea infrastructurii de comunicații poate încredința unui subordonat oricare dintre sarcinile care îi revin. Se va evita apariția conflictelor de interese între misiunea de a executa aceste sarcini și orice alte sarcini oficiale. Un număr de telefon unic și o singură adresă permit contactarea în orice moment a responsabilului local cu securitatea sau a subordonatului său de serviciu.

(4) Responsabilul local pentru securitatea infrastructurii de comunicații execută sarcinile decurgând din măsurile de securitate privind infrastructura de comunicații, în special:

(a) toate sarcinile în materie de securitate operațională privind infrastructura de comunicații, inclusiv auditul sistemului firewall, teste regulate de securitate, audit, raportare;

(b) monitorizarea eficacității planului de continuare a activității și asigurarea efectuării unor exerciții regulate;

(c) culegerea de informații privind orice incident care ar putea avea un impact asupra securității infrastructurii de comunicații sau a VIS central sau a sistemelor naționale și raportarea acestor informații responsabilului cu securitatea sistemului;

(d) informarea responsabilului cu securitatea sistemului în cazul în care politica de securitate trebuie modificată;

(e) monitorizarea aplicării prezentei decizii și a politicii de securitate de către orice contractant, inclusiv subcontractanți, implicat în orice fel în gestionarea infrastructurii de comunicații;

(f) asigurarea faptului că personalul este informat cu privire la obligațiile care îi revin și monitorizarea aplicării politicii de securitate;

(g) monitorizarea evoluțiilor în materie de securitate informatică și asigurarea unei formări corespunzătoare a personalului;

(h) pregătirea informațiilor de bază și a opțiunilor pentru elaborarea, actualizarea și revizuirea politicii de securitate, în conformitate cu articolul 7.

Articolul 5

Incidente de securitate

(1) Orice eveniment care are sau ar putea avea un impact asupra securității funcționării VIS și ar putea cauza daune sau pierderi VIS este considerat drept un incident de securitate, în special în situațiile în care s-ar fi putut accesa datele sau în care s-a compromis sau s-ar fi putut compromite disponibilitatea, integritatea și confidențialitatea datelor.

(2) Politica de securitate prevede proceduri de restabilire în urma unui incident. Incidentele de securitate sunt gestionate astfel încât să se asigure un răspuns rapid, eficient și adecvat, în conformitate cu politica de securitate.

(3) Informațiile privind un incident de securitate care are sau ar putea avea un impact asupra funcționării VIS într-un stat membru sau asupra disponibilității, integrității și confidențialității datelor din VIS introduse de un stat membru sunt transmise statului membru respectiv. Incidentele de securitate sunt notificate responsabilului cu protecția datelor din cadrul Comisiei.

Articolul 6

Gestionarea incidentelor

(1) Ansamblul personalului și contractanților implicați în dezvoltarea, gestionarea sau funcționarea VIS trebuie să consemneze orice punct vulnerabil în ceea ce privește securitatea observat sau suspectat în funcționarea VIS și să raporteze acest fapt responsabilului cu securitatea sistemului sau responsabilului local pentru securitatea VIS central sau responsabilului local pentru securitatea infrastructurii de comunicații, după caz.

(2) În cazul detectării unui incident care are sau ar putea avea un impact asupra securității funcționării VIS, responsabilul local pentru securitatea VIS central sau responsabilul local pentru securitatea infrastructurii de comunicații îl informează cât mai curând posibil pe responsabilul cu securitatea sistemului și, după caz, punctul național unic de contact pentru securitatea VIS, dacă în statul membru în cauză există un astfel de punct, în scris sau, în caz de extremă urgență, prin alte canale de comunicare. Raportul cuprinde descrierea incidentului de securitate, nivelul de risc, posibilele consecințe și măsurile care au fost luate sau ar trebui luate pentru reducerea riscului respectiv.

(3) Responsabilul local pentru securitatea VIS central sau responsabilul local pentru securitatea infrastructurii de comunicații, după caz, stochează de îndată într-un loc sigur orice informații privind incidentul de securitate. În măsura în care este posibil în temeiul dispozițiilor aplicabile privind protecția datelor, astfel de informații sunt puse la dispoziția responsabilului cu securitatea sistemului, la cererea acestuia.

(4) Se pun în aplicare mecanisme de informare astfel încât, după soluționarea și finalizarea unui incident, să se asigure comunicarea informațiilor cu privire la rezultate.

CAPITOLUL III

MĂSURI DE SECURITATE

Articolul 7

Politica de securitate

(1) Directorul general al Direcției Generale Justiție, Libertate și Securitate elaborează, actualizează și revizuiește în mod regulat o politică de securitate obligatorie, în conformitate cu prezenta decizie. Politica de securitate prevede proceduri și măsuri detaliate de protecție împotriva amenințărilor la adresa disponibilității, integrității și confidențialității VIS, inclusiv planuri de urgență, pentru a se asigura un nivel corespunzător de securitate, astfel cum prevede prezenta decizie. Politica de securitate se conformează prezentei decizii.

(2) Politica de securitate se bazează pe o evaluare a riscului. Măsurile descrise de politica de securitate sunt proporționale cu riscurile identificate.

(3) Evaluarea riscului și politica de securitate sunt actualizate în cazul în care modificări tehnologice, identificarea unor noi amenințări sau orice alte circumstanțe o impun. În orice caz, politica de securitate este revizuită anual, pentru a se asigura că această răspunde în continuare celei mai recente evaluări a riscului sau oricărei modificări tehnologice, amenințări sau oricărei alte circumstanțe relevante nou-identificate.

(4) Politica de securitate este elaborată de responsabilul cu securitatea sistemului, în coordonare cu responsabilul local pentru securitatea VIS și responsabilul local pentru securitatea infrastructurii de comunicații.

Articolul 8

Punerea în aplicare a măsurilor de securitate

(1) Punerea în aplicare a sarcinilor și cerințelor prevăzute de prezenta decizie și de politica de securitate, inclusiv a sarcinii de a desemna un responsabil local cu securitatea, poate fi subcontractată sau încredințată unor organisme private sau publice.

(2) În acest caz, Comisia se asigură, prin intermediul unui acord cu forță juridică obligatorie, că cerințele prevăzute de prezenta decizie și de politica de securitate sunt pe deplin respectate. În cazul delegării sau subcontractării sarcinii de a desemna un responsabil local cu securitatea, Comisia se asigură, prin intermediul unui acord cu forță juridică obligatorie, că va fi consultată în legătură cu persoana care urmează a fi desemnată ca responsabil local cu securitatea.

Articolul 9

Controlul accesului la instalații

(1) Se utilizează perimetre de securitate delimitate corespunzător și se efectuează controale de acces pentru a proteja zonele în care se află instalațiile de prelucrare a datelor.

(2) În interiorul perimetrelor de securitate sunt create zone securizate pentru protejarea componentelor fizice (active), inclusiv hardware, suporturi de date și console, planuri și alte documente privind VIS, precum și birouri și alte spații de lucru ale personalului implicat în funcționarea VIS. Zonele securizate sunt protejate printr-un control corespunzător la intrare, astfel încât numai personalul autorizat să poată avea acces la acestea. În zonele securizate, activitățile fac obiectul unor norme de securitate detaliate, stabilite în cadrul politicii de securitate.

(3) Se prevăd și se aplică măsuri de securitate fizică pentru birouri, săli și instalații. Punctele de acces, cum ar fi zonele de livrare sau de încărcare, și alte puncte prin care persoane neautorizate pot intra în localuri sunt controlate și, dacă este posibil, izolate de instalațiile de prelucrare a datelor, pentru a împiedica accesul neautorizat.

(4) În mod proporțional cu riscurile, se elaborează și se aplică măsuri de protecție fizică a perimetrelor de securitate, împotriva deteriorării cauzate de catastrofe naturale sau provocate de om.

(5) Echipamentul este protejat împotriva amenințărilor fizice și de mediu, precum și împotriva accesului neautorizat.

(6) În cazul în care dispune de informații în acest sens, Comisia adaugă la lista prevăzută la articolul 2 alineatul (2) litera (f) un punct de contact unic pentru monitorizarea punerii în aplicare a dispozițiilor prezentului articol în sediile VIS central de rezervă.

Articolul 10

Controlul suporturilor de date și al activelor

(1) Suporturile amovibile care conțin date sunt protejate împotriva accesului neautorizat, a utilizării frauduloase sau a deteriorării și se asigură lizibilitatea datelor pe întreaga durată de viață a acestora.

(2) Atunci când nu mai sunt necesare, suporturile sunt îndepărtate în mod securizat, în conformitate cu procedurile detaliate stabilite în cadrul politicii de securitate.

(3) Inventarele asigură că informațiile privind locul de stocare, durata de păstrare aplicabilă și autorizațiile de acces sunt disponibile.

(4) Toate activele importante ale VIS central și ale infrastructurii de comunicații sunt inventariate, astfel încât să poată fi protejate în funcție de importanța lor. Se păstrează un registru actualizat al echipamentului informatic relevant.

(5) Se furnizează o documentație actualizată privind VIS central și infrastructura de comunicații. O astfel de documentație trebuie protejată împotriva accesului neautorizat.

Articolul 11

Controlul stocării

(1) Se iau măsuri corespunzătoare pentru a se asigura stocarea adecvată a informațiilor și a se preveni accesul neautorizat la acestea.

(2) Toate echipamentele care conțin suporturi de stocare sunt verificate pentru a asigura că datele sensibile au fost șterse sau modificate integral înainte de îndepărtarea echipamentelor sau sunt distruse în mod securizat.

Articolul 12

Controlul parolelor

(1) Toate parolele sunt păstrate în siguranță și tratate în regim confidențial. În cazul în care există suspiciunea că o parolă a fost dezvăluită, aceasta trebuie schimbată imediat, sau contul utilizatorului trebuie dezactivat. Se folosesc nume de utilizator individuale și unice.

(2) În cadrul politicii de securitate se definesc procedurile de conectare și deconectare, pentru a preveni orice acces neautorizat.

Articolul 13

Controlul accesului

(1) Politica de securitate prevede o procedură oficială prin care personalul se poate înregistra și poate anula această înregistrare, pentru acordarea sau retragerea accesului la hardware-ul și software-ul VIS la VIS central, în scopul gestionării operaționale. Atribuirea și utilizarea unor identificatori de acces adecvați (parole sau alte mijloace corespunzătoare) sunt controlate printr-o procedură de gestionare formală definită în cadrul politicii de securitate.

(2) În ceea ce privește VIS central, accesul la hardware-ul și software-ul VIS:

(i) este limitat la persoanele autorizate;

(ii) este limitat la cazurile în care se poate determina un motiv legitim de acces la sistem, în conformitate cu articolul 42 și articolul 50 alineatul (2) din Regulamentul (CE) nr. 767/2008;

(iii) nu depășește durata și amploarea necesare motivului de acces la sistem; precum și

(iv) se efectuează numai în conformitate cu o politică de control al accesului definită în cadrul politicii de securitate.

(3) VIS central utilizează numai consolele și software-ul autorizate de responsabilul local pentru securitatea VIS central. Folosirea utilitarelor de sistem care s-ar putea sustrage controalelor sistemului și aplicațiilor este restricționată și controlată. Sunt prevăzute proceduri pentru a controla instalarea de software.

Articolul 14

Controlul comunicațiilor

Infrastructura de comunicații este monitorizată în vederea asigurării disponibilității, integrității și confidențialității schimburilor de informații. Sunt utilizate procedee criptografice pentru a proteja datele transmise prin infrastructura de comunicații.

Articolul 15

Controlul înregistrării datelor

Conturile persoanelor autorizate să aibă acces la software-ul VIS din VIS central sunt monitorizate de responsabilul local pentru securitatea VIS central. Utilizarea acestor conturi, inclusiv data, ora și identitatea utilizatorului, se înregistrează.

Articolul 16

Controlul transportului

(1) Politica de securitate definește măsuri corespunzătoare pentru a preveni citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transmiterii către sau dinspre VIS sau pe parcursul transportului suporturilor de date. Politica de securitate prevede dispoziții privind tipurile admisibile de expediție sau de transport, precum și în ceea ce privește procedurile de stabilire a responsabilității pentru transportul elementelor și sosirea acestora la locul de destinație. Suporturile de date nu conțin decât datele care trebuie trimise.

(2) Serviciile furnizate de părți terțe care implică accesarea, prelucrarea, comunicarea sau gestionarea instalațiilor de prelucrare a datelor sau adăugarea unor produse și servicii la instalațiile de prelucrare a datelor fac obiectul unor controale de securitate integrate corespunzătoare.

Articolul 17

Securitatea infrastructurii de comunicare

(1) Infrastructura de comunicații este gestionată și controlată în mod adecvat, pentru a fi protejată de amenințări și pentru a se asigura securitatea infrastructurii de comunicații în sine sau a VIS central, inclusiv a datelor schimbate prin intermediul său.

(2) În acordul privind serviciile de rețea cu furnizorul de servicii sunt definite elementele de securizare, nivelul de servicii și cerințele de gestionare a tuturor serviciilor de rețea.

(3) În afară de protejarea punctelor de acces la VIS, sunt protejate toate serviciile suplimentare utilizate de infrastructura de comunicații. Politica de securitate prevede măsuri adecvate în acest sens.

Articolul 18

Monitorizare

(1) Fișierele jurnal care înregistrează informațiile prevăzute la articolul 34 alineatul (1) din Regulamentul (CE) nr. 767/2008 privind orice acces la VIS central și toate operațiunile de prelucrare a datelor în VIS central sunt păstrate într-un loc sigur și sunt accesibile în sediile site-ului principal și de rezervă al VIS, pe perioada menționată la articolul 34 alineatul (2) din Regulamentul (CE) nr. 767/2008.

(2) Politica de securitate prevede proceduri pentru monitorizarea utilizării instalațiilor de prelucrare a informațiilor sau monitorizarea disfuncționalităților acestor instalații, iar rezultatele activității de monitorizare sunt analizate în mod regulat. Dacă este necesar, se iau măsuri corespunzătoare.

(3) Facilitățile de înregistrare și fișierele jurnal sunt protejate împotriva falsificării și accesului neautorizat pentru a îndeplini cerințele în ceea ce privește culegerea și păstrarea în timpul perioadei de păstrare a datelor.

Articolul 19

Procedee criptografice

Atunci când este necesar, se utilizează procedee criptografice pentru protejarea informațiilor. Utilizarea acestora, precum și scopul și condițiile în care sunt folosite, trebuie aprobate în prealabil de responsabilul cu securitatea sistemului.

CAPITOLUL IV

SECURITATEA RESURSELOR UMANE

Articolul 20

Profilurile membrilor personalului

(1) Politica de securitate definește funcțiile și responsabilitățile persoanelor autorizate să aibă acces la VIS, în special la infrastructura de comunicații.

(2) Rolurile și responsabilitățile în materie de securitate ale personalului Comisiei, ale contractanților și ale personalului implicat în gestionarea operațională sunt definite, descrise și comunicate persoanelor în cauză. Descrierea postului și a obiectivelor precizează aceste roluri și responsabilități pentru personalul Comisiei; contractele sau acordurile privind nivelul serviciilor precizează aceste aspecte pentru contractanți.

(3) Se încheie acorduri de confidențialitate cu toate persoanele cărora nu li se aplică normele funcției publice ale Uniunii Europene sau ale unui stat membru. Personalul care lucrează cu date VIS trebuie să aibă autorizația sau certificarea de securitate necesară, în conformitate cu procedurile detaliate stabilite în cadrul politicii de securitate.

Articolul 21

Informarea personalului

(1) Toți membrii personalului și, dacă este cazul, toți contractanții beneficiază de o formare corespunzătoare în domeniul conștientizării în materie de securitate, al dispozițiilor legale, politicilor și procedurilor, în măsura necesară pentru exercitarea sarcinilor care le revin.

(2) În cazul în care activitatea s-a încheiat sau contractul a luat sfârșit, politica de securitate definește responsabilitățile legate de schimbarea locului de muncă sau încetarea contractului pentru membrii personalului și pentru contractanți; politica de securitate prevede proceduri pentru restituirea activelor și retragerea drepturilor de acces.

CAPITOLUL V

DISPOZIȚIE FINALĂ

Articolul 22

Aplicabilitate

(1) Prezenta decizie se aplică de la data stabilită de Comisie în conformitate cu articolul 48 alineatul (1) din Regulamentul (CE) nr. 767/2008.

(2) Prezenta decizie expiră în momentul în care autoritatea de administrare își preia responsabilitățile.

Adoptată la Bruxelles, 4 mai 2010.

Pentru Comisie

Președintele

José Manuel BARROSO