ROZHODNUTÍ KOMISE

ze dne 4. května 2010

o bezpečnostním plánu pro provoz Vízového informačního systému

(2010/260/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS) [1], a zejména na článek 32 tohoto nařízení,

vzhledem k těmto důvodům:

(1) Čl. 32 odst. 3 nařízení (ES) č. 767/2008 stanoví, že řídící orgán přijme nezbytná opatření k dosažení cílů v oblasti bezpečnosti stanovených v čl. 32 odst. 2, pokud jde o provoz VIS, včetně přijetí bezpečnostního plánu.

(2) Čl. 26 odst. 4 nařízení (ES) č. 767/2008 stanoví, že v přechodném období, než se řídící orgán ujme svých povinností, je provozním řízením VIS pověřena Komise.

(3) Na zpracovávání osobních údajů Komisí při plnění jejích povinností v oblasti provozního řízení VIS se vztahuje nařízení Evropského parlamentu a Rady (ES) č. 45/2001 [2].

(4) Čl. 26 odst. 7 nařízení (ES) č. 767/2008 stanoví, že v případě, že Komise pověří některý subjekt plněním svých povinností během přechodného období, než se řídící orgán ujme svých povinností, zajistí, aby toto pověření nemělo nepříznivý dopad na žádný účinný kontrolní mechanismus podle práva Unie, ať už se jedná o kontrolu, kterou provádí Soudní dvůr, Účetní dvůr nebo evropský inspektor ochrany údajů.

(5) Jakmile se řídící orgán ujme svých povinností, měl by stanovit vlastní bezpečnostní plán ve vztahu k VIS.

(6) Potřebné bezpečnostní služby vztahující se k síti pro VIS popisuje rozhodnutí Komise 2008/602/ES ze dne 17. června 2008, kterým se pro vývojovou fázi stanoví fyzická architektura a požadavky na vnitrostátní uživatelská rozhraní a komunikační infrastrukturu mezi centrálním VIS a vnitrostátními uživatelskými rozhraními [3].

(7) Článek 27 nařízení (ES) č. 767/2008 stanoví, že hlavní Ústřední VIS, který vykonává technický dohled a správní funkce, se nachází ve Štrasburku (Francie) a záložní Ústřední VIS, který je schopen zajistit všechny funkce hlavního Ústředního VIS v případě poruchy tohoto systému, se nachází v Sankt Johann im Pongau (Rakousko).

(8) Měla by být vymezena úloha bezpečnostních úředníků s cílem zajistit účinnou a okamžitou reakci na bezpečnostní incidenty a jejich hlášení.

(9) Je třeba vypracovat bezpečnostní politiku, která popisuje veškeré technické a organizační podrobnosti v souladu s ustanoveními tohoto rozhodnutí.

(10) Je nutno stanovit opatření s cílem zajistit náležitou úroveň bezpečnosti provozu VIS,

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Toto rozhodnutí upravuje organizaci bezpečnosti a bezpečnostní opatření (bezpečnostní plán) ve smyslu čl. 32 odst. 3 nařízení (ES) č. 767/2008.

KAPITOLA II

ORGANIZACE, POVINNOSTI A ŘEŠENÍ INCIDENTŮ

Článek 2

Úkoly Komise

1. Komise zavede bezpečnostní opatření pro Ústřední VIS a komunikační infrastrukturu a sleduje jejich účinnost, jak je uvedeno v tomto rozhodnutí.

[1] Úř. věst. L 218, 13.8.2008, s. 60.
[2] Úř. věst. L 8, 12.1.2001, s. 1.
[3] Úř. věst. L 194, 23.7.2008, s. 3.

2. Komise určí z řad svých úředníků úředníka pro bezpečnost systému. Úředník pro bezpečnost systému je jmenován generálním ředitelem generálního ředitelství Komise pro spravedlnost, svobodu a bezpečnost. K úkolům úředníka pro bezpečnost systému patří zejména:

a) vypracování, aktualizace a revize bezpečnostní politiky, jak je popsáno v článku 7 tohoto rozhodnutí;

b) sledování účinnosti provádění bezpečnostních postupů Ústředního VIS a komunikační infrastruktury;

c) součinnost při vypracovávání zpráv v souvislosti s bezpečností, jak je stanoveno v čl. 50 odst. 3 a 4 nařízení (ES) č. 767/2008;

d) plnění úkolů v oblasti koordinace a poskytování pomoci při kontrolách a auditech prováděných evropským inspektorem ochrany údajů podle článku 42 nařízení (ES) č. 767/2008;

e) sledování toho, zda jsou toto rozhodnutí a bezpečnostní politika náležitě a plně uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na řízení a provozu VIS;

f) vedení seznamu vnitrostátních jednotných kontaktních míst pro bezpečnost VIS a sdílení tohoto seznamu s místními bezpečnostními úředníky pro Ústřední VIS a komunikační infrastrukturu.

Článek 3

Místní bezpečnostní úředník pro Ústřední VIS

1. Aniž je dotčen článek 8, Komise určí z řad svých úředníků místního bezpečnostního úředníka pro Ústřední VIS. Je nutno zamezit střetu zájmů mezi funkcí místního bezpečnostního úředníka a jakoukoliv jinou úřední povinností. Místní bezpečnostní úředník pro Ústřední VIS je jmenován generálním ředitelem generálního ředitelství Komise pro spravedlnost, svobodu a bezpečnost.

2. Místní bezpečnostní úředník pro Ústřední VIS zajišťuje, aby v hlavním Ústředním VIS byla prováděna bezpečnostní opatření uvedená v tomto rozhodnutí a byly dodržovány bezpečnostní postupy. Co se týká záložního Ústředního VIS, místní bezpečnostní úředník pro Ústřední VIS zajistí, aby byla prováděna bezpečnostní opatření uvedená v tomto rozhodnutí s výjimkou opatření stanovených v článku 10 a aby byly dodržovány související bezpečnostní postupy.

3. Místní bezpečnostní úředník pro Ústřední VIS může kterýkoliv ze svých úkolů přidělit podřízeným pracovníkům. Je nutno zamezit střetu zájmů mezi povinností plnit tyto úkoly a jakoukoli jinou úřední povinností. Místního bezpečnostního úředníka nebo jeho podřízeného pracovníka ve službě je možno kdykoli zastihnout na jednom kontaktním telefonním čísle a adrese.

4. Místní bezpečnostní úředník pro Ústřední VIS vykonává úkoly vyplývající z bezpečnostních opatření, jež mají být přijata v místech, v nichž se nachází hlavní a záložní Ústřední VIS, a to v mezích uvedených v odstavci 1, včetně zejména:

a) místních operativních bezpečnostních úkolů, včetně kontroly bezpečnostní brány, pravidelného ověřování bezpečnosti, provádění auditů a podávání zpráv;

b) sledování účinnosti plánu zachování provozu a zajištění pořádání pravidelných cvičení;

c) zajišťování důkazů o všech incidentech, jež by mohly mít dopad na bezpečnost Ústředního VIS nebo komunikační infrastruktury, a podávání zpráv úředníkovi pro bezpečnost systému;

d) vyrozumění úředníka pro bezpečnost systému o tom, že je nutno změnit bezpečnostní politiku;

e) sledování toho, zda jsou toto rozhodnutí a bezpečnostní politika uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na řízení a provozu Ústředního VIS;

f) zajištění toho, aby byli pracovníci informováni o svých povinnostech, a sledování uplatňování bezpečnostní politiky;

g) sledování vývoje v oblasti bezpečnosti IT a zajištění pravidelného školení pracovníků v souladu s tímto vývojem;

h) vypracovávání podkladových informací a alternativ pro vytvoření, aktualizaci a přezkum bezpečnostní politiky v souladu s článkem 7.

Článek 4

Místní bezpečnostní úředník pro komunikační infrastrukturu

1. Aniž je dotčen článek 8, Komise určí z řad svých úředníků místního bezpečnostního úředníka pro komunikační infrastrukturu. Je nutno zamezit střetu zájmů mezi funkcí místního bezpečnostního úředníka a jakoukoliv jinou úřední povinností. Místní bezpečnostní úředník pro komunikační infrastrukturu je jmenován generálním ředitelem generálního ředitelství Komise pro spravedlnost, svobodu a bezpečnost.

2. Místní bezpečnostní úředník pro komunikační infrastrukturu sleduje fungování komunikační infrastruktury a zajišťuje, aby byla prováděna bezpečnostní opatření a byly dodržovány bezpečnostní postupy.

3. Místní bezpečnostní úředník pro komunikační infrastrukturu může kterýkoliv ze svých úkolů přidělit podřízeným pracovníkům. Je nutno zamezit střetu zájmů mezi povinností plnit tyto úkoly a jakoukoli jinou úřední povinností. Místního bezpečnostního úředníka nebo jeho podřízeného pracovníka ve službě je možno kdykoli zastihnout na jednom kontaktním telefonním čísle a adrese.

4. Místní bezpečnostní úředník pro komunikační infrastrukturu vykonává úkoly vyplývající z bezpečnostních opatření souvisejících s komunikační infrastrukturou, včetně zejména:

a) všech místních operativních bezpečnostních úkolů souvisejících s komunikační infrastrukturou, jako je kontrola bezpečnostní brány, pravidelné ověřování bezpečnosti, provádění auditů, podávání zpráv;

b) sledování účinnosti plánu zachování provozu a zajištění pořádání pravidelných cvičení;

c) zajišťování důkazů o všech incidentech, jež by mohly mít dopad na bezpečnost komunikační infrastruktury nebo Ústředního VIS či na vnitrostátní systémy, a podávání zpráv úředníkovi pro bezpečnost systému;

d) vyrozumění úředníka pro bezpečnost systému o tom, že je nutno změnit bezpečnostní politiku;

e) sledování toho, zda jsou toto rozhodnutí a bezpečnostní politika uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na řízení komunikační infrastruktury;

f) zajištění toho, aby byli pracovníci informováni o svých povinnostech, a sledování uplatňování bezpečnostní politiky;

g) sledování vývoje v oblasti bezpečnosti IT a zajištění pravidelného školení pracovníků v souladu s tímto vývojem;

h) vypracovávání podkladových informací a alternativ pro vytvoření, aktualizaci a přezkum bezpečnostní politiky v souladu s článkem 7.

Článek 5

Bezpečnostní incidenty

1. Každou událost, která má nebo může mít dopad na bezpečnost provozu VIS a může VIS způsobit škodu nebo újmu, je nutno považovat za bezpečnostní incident, zejména v případě, mohlo-li dojít k přístupu k údajům nebo pokud byla či mohla být ohrožena dostupnost, integrita a důvěrnost údajů.

2. Bezpečnostní politika stanoví postupy pro překonání účinků takovéhoto incidentu. Bezpečnostní incidenty jsou řešeny tak, aby byla zajištěna rychlá, účinná a náležitá odezva v souladu s bezpečnostní politikou.

3. Informace o bezpečnostním incidentu, který má nebo může mít dopad na provoz VIS v některém z členských států nebo na dostupnost, integritu a důvěrnost údajů VIS zadaných některým členským státem, jsou poskytnuty dotčenému členskému státu. Bezpečnostní incidenty jsou oznámeny inspektorovi ochrany údajů v Komisi.

Článek 6

Řešení incidentů

1. Všichni zaměstnanci a smluvní dodavatelé podílející se na vývoji, řízení nebo provozu VIS musí zaznamenávat jakékoli zjištěné nebo domnělé bezpečnostní nedostatky v provozu VIS a nahlásit je úředníkovi pro bezpečnost systému nebo místnímu bezpečnostnímu úředníkovi pro Ústřední VIS nebo popřípadě místnímu bezpečnostnímu pracovníkovi pro komunikační infrastrukturu.

2. Je-li zjištěn incident, který má nebo může mít dopad na bezpečnost provozu VIS, informuje místní bezpečnostní úředník pro Ústřední VIS nebo místní bezpečnostní úředník pro komunikační infrastrukturu co nejrychleji úředníka pro bezpečnost systému a popřípadě vnitrostátní jednotné kontaktní místo pro bezpečnost VIS, pokud v dotyčném členském státě takovéto kontaktní místo existuje, a to písemně nebo v případě mimořádně naléhavé situace prostřednictvím jiných komunikačních kanálů. Zpráva obsahuje popis bezpečnostního incidentu, úroveň rizika, možné důsledky a opatření, která byla nebo by měla být přijata k zmírnění rizika.

3. Místní bezpečnostní úředník pro Ústřední VIS nebo popřípadě místní bezpečnostní úředník pro komunikační infrastrukturu neprodleně zajistí veškeré důkazy v souvislosti s bezpečnostním incidentem. Tyto důkazy jsou na žádost poskytnuty úředníkovi pro bezpečnost systému, a to v rozsahu, v jakém platné předpisy o ochraně údajů poskytnutí těchto údajů umožňují.

4. Jsou zavedeny postupy pro poskytování zpětné vazby s cílem zajistit, aby byly předávány informace o výsledcích, jakmile byl incident vyřešen a ukončen.

KAPITOLA III

BEZPEČNOSTNÍ OPATŘENÍ

Článek 7

Bezpečnostní politika

1. Generální ředitel generálního ředitelství pro spravedlnost, svobodu a bezpečnost v souladu s tímto rozhodnutím vypracuje, aktualizuje a pravidelně přezkoumává závaznou bezpečnostní politiku. Bezpečnostní politika stanoví podrobné postupy a opatření na ochranu před ohrožením dostupnosti, integrity a důvěrnosti údajů VIS, včetně plánování mimořádných opatření, s cílem zajistit náležitou úroveň bezpečnosti, jak je stanoveno tímto rozhodnutím. Bezpečnostní politika je v souladu s tímto rozhodnutím.

2. Bezpečnostní politika je založena na posouzení rizik. Opatření popsaná v bezpečnostní politice jsou přiměřená zjištěným rizikům.

3. Je-li to nezbytné v důsledku technologických změn, zjištění nových hrozeb či jakýchkoli jiných okolností, jsou posouzení rizik a bezpečnostní politika aktualizovány. Bezpečnostní politika je každopádně jednou ročně přezkoumávána s cílem zajistit, aby nadále náležitě reagovala na nejnovější posouzení rizik nebo nově zjištěnou technologickou změnu, hrozbu či jinou důležitou okolnost.

4. Bezpečnostní politiku vypracuje úředník pro bezpečnost systému v součinnosti s místním bezpečnostním úředníkem pro VIS a místním bezpečnostním úředníkem pro komunikační infrastrukturu.

Článek 8

Provádění bezpečnostních opatření

1. Provádění úkolů a plnění požadavků stanovených v tomto rozhodnutí a v bezpečnostní politice, včetně úkolu týkajícího se určení místního bezpečnostního úředníka, je možno zajistit smluvně nebo svěřit soukromým či veřejným subjektům.

2. V tomto případě Komise prostřednictvím právně závazné smlouvy zajistí, aby byly v plném rozsahu splněny požadavky stanovené v tomto rozhodnutí a v bezpečnostní politice. V případě svěření nebo smluvního zajištění úkolu týkajícího se určení místního bezpečnostního úředníka Komise prostřednictvím právně závazné smlouvy zajistí, aby byla konzultována ohledně osoby, která má být místním bezpečnostním úředníkem jmenována.

Článek 9

Kontrola přístupu k zařízení

1. K ochraně oblastí, v nichž jsou umístěna zařízení pro zpracování údajů, se využívají bezpečnostní zóny s náležitými překážkami a kontrolami vstupu.

2. V rámci bezpečnostních zón jsou vymezeny bezpečné oblasti za účelem ochrany fyzických součástí (aktiv), včetně technického vybavení, nosičů údajů a ovládacích panelů, plánů a jiných dokumentů týkajících se VIS, jakož i kanceláří a ostatních pracovišť zaměstnanců zajišťujících provoz VIS. Tyto bezpečné oblasti jsou chráněny prostřednictvím odpovídajících kontrol vstupu s cílem zajistit, aby do nich byl povolen přístup pouze oprávněným pracovníkům. Práce v bezpečných oblastech podléhá podrobným bezpečnostním pravidlům stanoveným v bezpečnostní politice.

3. Je naplánována a zajištěna fyzická bezpečnost kanceláří, prostor a zařízení. Přístupové body, například zóny pro zásobování a nakládku a jiná místa, jimiž mohou do prostor vstoupit neoprávněné osoby, jsou kontrolovány, a je-li to možné, jsou odděleny od zařízení pro zpracovávání údajů s cílem zamezit neoprávněnému přístupu.

4. Je navržena a úměrně riziku uplatňována fyzická ochrana bezpečnostních zón před škodami vzniklými v důsledku přírodních nebo člověkem způsobených pohrom.

5. Vybavení je chráněno před fyzickými nebo ekologickými hrozbami a před možností neoprávněného přístupu.

6. Má-li Komise k dispozici takovéto informace, připojí na seznam uvedený v čl. 2 odst. 2) písm. f) jednotné kontaktní místo pro kontrolu provádění ustanovení tohoto článku v prostorách, v nichž se nachází záložní Ústřední VIS.

Článek 10

Kontrola nosičů údajů a aktiv

1. Výměnné nosiče obsahující údaje jsou chráněny před neoprávněným přístupem, zneužitím nebo poškozením a během celé doby používání údajů je zajištěna jejich čitelnost.

2. Nosiče jsou bezpečně odstraněny, jakmile již nejsou zapotřebí, a to v souladu s podrobnými postupy, jež jsou stanoveny v bezpečnostní politice.

3. Prostřednictvím soupisů je zajištěno, aby byly k dispozici informace o místu uložení, platné době uchovávání a oprávněních k přístupu.

4. Jsou určena veškerá důležitá aktiva Ústředního VIS a komunikační infrastruktury, takže je lze chránit v souladu s jejich významem. Je veden aktualizovaný rejstřík příslušného vybavení IT.

5. Je k dispozici aktualizovaná dokumentace Ústředního VIS a komunikační infrastruktury. Tuto dokumentaci je nutno chránit před neoprávněným přístupem.

Článek 11

Kontrola uchovávání

1. Je nutno přijmout vhodná opatření k zajištění náležitého uchovávání informací a zamezení neoprávněnému přístupu k těmto informacím.

2. Veškeré položky vybavení, které obsahují paměťová média, jsou zkontrolovány s cílem zajistit výmaz citlivých údajů či jejich úplné přepsání před jejich odstraněním nebo jsou bezpečně zlikvidovány.

Článek 12

Kontrola hesel

1. Všechna hesla jsou bezpečně uchovávána a je s nimi nakládáno jako s důvěrnými údaji. V případě podezření, že heslo mohlo být vyzrazeno, je nutno heslo neprodleně změnit nebo zablokovat uživatelský účet. Používají se jedinečné a individuální totožnosti uživatelů.

2. Bezpečnostní politika stanoví postupy pro přihlášení a odhlášení s cílem zamezit neoprávněnému přístupu.

Článek 13

Kontrola přístupu

1. Bezpečnostní politika stanoví oficiální postup registrace a zrušení registrace zaměstnanců k udělení a zrušení přístupu k technickému a programovému vybavení VIS v místě Ústředního VIS za účelem provozního řízení. Přidělování a používání odpovídajících přístupových údajů (hesla nebo jiné vhodné prostředky) je kontrolováno prostřednictvím formálního řídícího procesu, který stanoví bezpečnostní politika.

2. Přístup k technickému a programovému vybavení VIS v místě Ústředního VIS

i) je omezen na oprávněné osoby,

ii) je omezen na případy, kdy lze určit legitimní účel v souladu s článkem 42 a čl. 50 odst. 2 nařízení (ES) č. 767/2008,

iii) nepřesáhne dobu a rozsah, které jsou nezbytné pro daný účel přístupu, a

iv) uskutečňuje se pouze v souladu s politikou kontroly přístupu, která je stanovena v bezpečnostní politice.

3. V místě Ústředního VIS se používají pouze ovládací panely a programové vybavení schválené místním bezpečnostním úředníkem pro Ústřední VIS. Je omezeno a kontrolováno používání systémových utilit, které mohou být schopny přepsat nastavení systému a aplikací. Jsou zavedeny postupy pro kontrolu instalace programového vybavení.

Článek 14

Kontrola komunikace

Komunikační infrastruktura je sledována, aby byla u výměn informací zajištěna dostupnost, integrita a důvěrnost údajů. K ochraně údajů předávaných prostřednictvím komunikační infrastruktury se používají kryptografické prostředky.

Článek 15

Kontrola zaznamenávání údajů

Místní bezpečnostní úředník pro Ústřední VIS sleduje účty osob s oprávněným přístupem k programovému vybavení VIS z Ústředního VIS. Je evidováno používání těchto účtů, včetně času a totožnosti uživatelů.

Článek 16

Kontrola přepravy

1. Bezpečnostní politika stanoví vhodná opatření s cílem zamezit neoprávněnému čtení, kopírování, změně nebo výmazu osobních údajů během předávání do a z VIS nebo během přepravy nosičů údajů. Bezpečnostní politika upraví přípustné druhy odesílání nebo přepravy a rovněž odpovědnost v případě přepravy jednotlivých položek a jejich příchod na místo určení. Nosič údajů nesmí obsahovat jiné údaje než údaje, jež mají být zaslány.

2. Služby poskytované třetími osobami, jejichž součástí je přístup k údajům, jejich zpracovávání a předávání nebo správa zařízení pro zpracování údajů či přidávání produktů nebo služeb k zařízením pro zpracování údajů, musí obsahovat odpovídající integrované bezpečnostní kontroly.

Článek 17

Bezpečnost komunikační infrastruktury

1. Komunikační infrastruktura je náležitě spravována a kontrolována s cílem chránit ji před hrozbami a zajistit bezpečnost samotné komunikační infrastruktury a Ústředního VIS, včetně údajů, jež jsou jejím prostřednictvím vyměňovány.

2. Bezpečnostní prvky, úrovně služeb a požadavky na řízení veškerých síťových služeb jsou stanoveny ve smlouvě o síťových službách uzavřené s poskytovatelem služeb.

3. Kromě přístupových bodů VIS jsou chráněny rovněž veškeré další služby, které komunikační infrastruktura používá. Bezpečnostní politika stanoví vhodná opatření.

Článek 18

Sledování

1. Protokoly zaznamenávající informace uvedené v čl. 34 odst. 1 nařízení (ES) č. 767/2008 týkající se každého přístupu a veškerých operací zpracování údajů v Ústředním VIS jsou uchovávány bezpečně v prostorách, v nichž se nachází hlavní a záložní Ústřední VIS, a jsou dostupné z těchto prostor, a to po dobu uvedenou v čl. 34 odst. 2 nařízení (ES) č. 767/2008.

2. Bezpečnostní politika stanoví postupy ke sledování používání nebo poruch zařízení pro zpracování informací a výsledky tohoto sledování jsou pravidelně přezkoumávány. V případě potřeby jsou přijata vhodná opatření.

3. Zařízení pro protokolování a protokoly jsou chráněny před nedovolenou manipulací a neoprávněným přístupem za účelem splnění požadavků na shromažďování a uchovávání důkazů po stanovenou dobu.

Článek 19

Kryptografická opatření

K ochraně informací se případně používají kryptografická opatření. Jejich používání spolu s jejich účelem a podmínkami musí předem schválit úředník pro bezpečnost systému.

KAPITOLA IV

BEZPEČNOST LIDSKÝCH ZDROJŮ

Článek 20

Profily pracovníků

1. Bezpečnostní politika stanoví funkce a povinnosti osob s oprávněným přístupem k VIS, včetně komunikační infrastruktury.

2. Jsou stanoveny a zdokumentovány úlohy a povinnosti zaměstnanců Komise, smluvních dodavatelů a pracovníků podílejících se na provozním řízení v oblasti bezpečnosti a sděleny dotčeným osobám. Tyto úlohy a povinnosti jsou v případě zaměstnanců Komise stanoveny v popisu pracovní náplně a cílů; u smluvních dodavatelů jsou stanoveny ve smlouvách nebo dohodách o úrovni služeb.

3. S osobami, na něž se nevztahují pravidla Evropské unie nebo členských států týkající se veřejné služby, jsou uzavřeny smlouvy o zachování důvěrnosti údajů a mlčenlivosti. Zaměstnanci, kteří pracují s údaji VIS, mají potřebnou bezpečnostní prověrku nebo osvědčení v souladu s podrobnými postupy, jež budou stanoveny v bezpečnostní politice.

Článek 21

Informování pracovníků

1. Všichni zaměstnanci a v případě potřeby smluvní dodavatelé jsou náležitě vyškoleni s ohledem na informovanost o bezpečnosti, právní požadavky, politiky a postupy v rozsahu, v jakém to vyžadují jejich povinnosti.

2. Pro případ ukončení pracovního poměru nebo smlouvy jsou v bezpečnostní politice stanoveny povinnosti pracovníků a smluvních dodavatelů související se změnou pracovního místa nebo ukončením pracovního poměru a bezpečnostní politika stanoví rovněž postupy, jimiž se řídí vrácení aktiv a zrušení přístupových práv.

KAPITOLA V

ZÁVĚREČNÁ USTANOVENÍ

Článek 22

Použitelnost

1. Toto rozhodnutí se použije ode dne, který stanoví Komise v souladu s čl. 48 odst. 1 nařízení (ES) č. 767/2008.

2. Použitelnost tohoto rozhodnutí končí, jakmile se řídící orgán ujme svých povinností.

V Bruselu dne 4. května 2010.

Za Komisi

José Manuel BARROSO

předseda