

ROZHODNUTIE KOMISIE

zo 4. mája 2010

o bezpečnostnom pláne na prevádzku vízového informačného systému

(2010/260/EÚ)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 767/2008 z 9. júla 2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (nariadenie o VIS) ⁽¹⁾, a najmä na jeho článok 32,

keďže:

(1) V článku 32 ods. 3 nariadenia (ES) č. 767/2008 sa ustanovuje, že riadiaci orgán prijme potrebné opatrenia na dosiahnutie cieľov v oblasti bezpečnosti stanovených v článku 32 ods. 2 v súvislosti s prevádzkou VIS vrátane prijatia bezpečnostného plánu.

(2) V článku 26 ods. 4 nariadenia (ES) č. 767/2008 sa ustanovuje, že počas prechodného obdobia, predtým ako riadiaci orgán prevezme svoje povinnosti, zodpovedá za prevádzkové riadenie VIS Komisia.

(3) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 ⁽²⁾ sa vzťahuje na spracovanie osobných údajov Komisiou pri plnení jej úloh v rámci prevádzkového riadenia VIS.

(4) V článku 26 ods. 7 nariadenia (ES) č. 767/2008 sa ustanovuje, že ak Komisia počas prechodného obdobia poverí plnením svojich úloh iný orgán, predtým ako riadiaci orgán prevezme svoje povinnosti, zabezpečí, aby takéto poverenie nepriaznivo neovplyvnilo platný kontrolný mechanizmus podľa právnych predpisov Únie, či už prostredníctvom Súdneho dvora, Dvora audítorov, alebo európskeho dozorného úradníka pre ochranu údajov.

(5) Po tom, ako riadiaci orgán prevezme svoje povinnosti, mal by si určiť vlastný bezpečnostný plán v súvislosti s VIS.

(6) V rozhodnutí Komisie 2008/602/ES zo 17. júna 2008, ktorým sa určuje fyzická architektúra a požiadavky

národných rozhraní a komunikačnej infraštruktúry medzi centrálnym VIS a národnými rozhraniami v etape vývoja systému ⁽³⁾, sa uvádzajú požadované bezpečnostné služby platné pre siete pre VIS.

(7) V článku 27 nariadenia (ES) č. 767/2008 sa ustanovuje, že hlavný centrálny VIS, ktorý vykonáva technický dohľad a správu, sa nachádza v Štrasburgu (Francúzsko) a záložný centrálny VIS, ktorý je schopný zabezpečiť všetky funkcie hlavného centrálného VIS v prípade zlyhania systému, sa nachádza v Sankt Johann im Pongau (Rakúsko).

(8) Na zabezpečenie účinnej a pohotovej reakcie na bezpečnostné incidenty a ich vykazovania by sa mali určiť úlohy bezpečnostných pracovníkov.

(9) Mala by sa vypracovať bezpečnostná politika opisujúca všetky technické a organizačné podrobnosti v súlade s ustanoveniami tohto rozhodnutia.

(10) Na zaručenie primeranej úrovne bezpečnosti prevádzky VIS by sa mali stanoviť opatrenia,

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet

Týmto rozhodnutím sa zriaďuje bezpečnostná organizácia a opatrenia (bezpečnostný plán) v zmysle článku 32 ods. 3 nariadenia (ES) č. 767/2008.

KAPITOLA II

ORGANIZÁCIA, POVINNOSTI A RIADENIE INCIDENTOV

Článok 2

Úlohy Komisie

1. Komisia zavedie bezpečnostné opatrenia pre centrálny VIS a komunikačnú infraštruktúru uvedenú v tomto rozhodnutí a monitoruje ich účinnosť.

⁽¹⁾ Ú. v. EÚ L 218, 13.8.2008, s. 60.

⁽²⁾ Ú. v. ES L 8, 12.1.2001, s. 1.

⁽³⁾ Ú. v. EÚ L 194, 23.7.2008, s. 3.

2. Komisia určí spomedzi svojich zamestnancov pracovníka zodpovedného za bezpečnosť systému. Pracovníka zodpovedného za bezpečnosť systému vymenúva generálny riaditeľ Generálneho riaditeľstva pre spravodlivosť, slobodu a bezpečnosť Európskej komisie. Medzi úlohy pracovníka zodpovedného za bezpečnosť systému patrí najmä:

- a) príprava, aktualizácia a revízia bezpečnostnej politiky, ako sú opísané v článku 7 tohto rozhodnutia;
- b) monitorovanie účinnosti realizácie bezpečnostných postupov centrálneho VIS a komunikačnej infraštruktúry;
- c) prispievanie k príprave správ v súvislosti s bezpečnosťou v zmysle článku 50 ods. 3 a článku 50 ods. 4 nariadenia (ES) č. 767/2008;
- d) koordinácia a podpora pri kontrole a auditoch vykonávaných európskym dozorným úradníkom pre ochranu údajov, uvedených v článku 42 nariadenia (ES) č. 767/2008;
- e) monitorovanie riadneho a úplného uplatňovania tohto rozhodnutia a bezpečnostnej politiky každým dodávateľom vrátane subdodávateľov, ktorí sa akýmkoľvek spôsobom zúčastňujú na riadení a prevádzkovaní VIS;
- f) vedenie zoznamu jednotlivých národných kontaktných miest pre bezpečnosť VIS a jeho spoločné používanie s miestnymi bezpečnostnými pracovníkmi pre centrálny VIS a komunikačnú infraštruktúru.

Článok 3

Miestny bezpečnostný pracovník pre centrálny VIS

1. Komisia určí miestneho bezpečnostného pracovníka pre centrálny VIS spomedzi úradníkov Komisie bez toho, aby bol dotknutý článok 8. Treba zabrániť konfliktom záujmov medzi povinnosťami miestneho bezpečnostného pracovníka a inými úradnými povinnosťami. Miestneho bezpečnostného pracovníka pre centrálny VIS vymenúva generálny riaditeľ Generálneho riaditeľstva pre spravodlivosť, slobodu a bezpečnosť Európskej komisie.

2. Miestny bezpečnostný pracovník pre centrálny VIS zaručí, že v hlavnom centrálnom VIS sa vykonávajú bezpečnostné opatrenia uvedené v tomto rozhodnutí a že sa dodržiavajú bezpečnostné postupy. Miestny bezpečnostný pracovník pre centrálny VIS zaručí, že v súvislosti so záložným centrálnym VIS sa vykonávajú bezpečnostné opatrenia uvedené v tomto rozhodnutí okrem tých opatrení, ktoré sú uvedené v článku 10, a že sa dodržiavajú súvisiace bezpečnostné postupy.

3. Miestny bezpečnostný pracovník pre centrálny VIS môže poveriť plnením svojich úloh niektorého zo svojich podriadených pracovníkov. Treba zabrániť konfliktom záujmov medzi povinnosťou plniť tieto úlohy a inými úradnými povinnosťami. Jedno kontaktné telefónne číslo a adresa umožnia kedykoľvek spojenie s miestnym bezpečnostným pracovníkom alebo s jeho či jej podriadeným.

4. Miestny bezpečnostný pracovník pre centrálny VIS plní úlohy vyplývajúce z bezpečnostných opatrení, ktoré sa majú prijať na hlavnej a záložnej lokalite centrálneho VIS v rámci vymedzení uvedených v odseku 1, a to najmä:

- a) miestne prevádzkové bezpečnostné úlohy vrátane firewall auditu, pravidelného bezpečnostného testovania, auditu a podávania správ;
- b) monitorovanie účinnosti plánu na zabezpečenie kontinuity činnosti a zabezpečenie vykonávania pravidelných cvičení;
- c) zabezpečenie dôkazov o akomkoľvek incidente, ktorý môže mať dosah na bezpečnosť centrálneho VIS alebo komunikačnej infraštruktúry, a podanie správ o incidente pracovníkovi zodpovednému za bezpečnosť systému;
- d) informovanie pracovníka zodpovedného za bezpečnosť systému, ak je potrebné zmeniť a doplniť bezpečnostnú politiku;
- e) monitorovanie uplatňovania tohto rozhodnutia a bezpečnostnej politiky každým dodávateľom vrátane subdodávateľov, ktorí sa akýmkoľvek spôsobom zúčastňujú na riadení a prevádzkovaní centrálneho VIS;
- f) zabezpečenie, že pracovníci poznajú svoje povinnosti, a monitorovanie uplatňovania bezpečnostnej politiky;
- g) monitorovanie vývoja bezpečnosti IT a zabezpečenie primeranej odbornej prípravy pracovníkov;
- h) príprava podkladových informácií a možností na vytvorenie, aktualizáciu a revíziu bezpečnostnej politiky v súlade s článkom 7.

Článok 4

Miestny bezpečnostný pracovník pre komunikačnú infraštruktúru

1. Komisia určí miestneho bezpečnostného pracovníka pre komunikačnú infraštruktúru spomedzi úradníkov Komisie bez toho, aby bol dotknutý článok 8. Treba zabrániť konfliktom záujmov medzi povinnosťami miestneho bezpečnostného pracovníka a inými úradnými povinnosťami. Miestneho bezpečnostného pracovníka pre komunikačnú infraštruktúru vymenúva generálny riaditeľ Generálneho riaditeľstva pre spravodlivosť, slobodu a bezpečnosť Komisie.

2. Miestny bezpečnostný pracovník pre komunikačnú infraštruktúru monitoruje fungovanie komunikačnej infraštruktúry a zabezpečuje vykonávanie bezpečnostných opatrení a dodržiavanie bezpečnostných postupov.

3. Miestny bezpečnostný pracovník pre komunikačnú infraštruktúru môže poveriť plnením akýchkoľvek svojich úloh niektorého zo svojich podriadených pracovníkov. Treba zabrániť konfliktom záujmov medzi povinnosťou vykonávať tieto úlohy a inými úradnými povinnosťami. Jedno kontaktné telefónne číslo a adresa umožnia kedykoľvek spojenie s miestnym bezpečnostným pracovníkom alebo s jeho či jej podriadeným.

4. Miestny bezpečnostný pracovník pre komunikačnú infraštruktúru plní úlohy vyplývajúce z bezpečnostných opatrení súvisiacich s komunikačnou infraštruktúrou, a to najmä:

- a) všetky prevádzkové bezpečnostné úlohy súvisiace s komunikačnou infraštruktúrou ako firewall audit, pravidelné bezpečnostné testovanie, audit a podávanie správ;
- b) monitorovanie účinnosti plánu na zabezpečenie kontinuity činnosti a zabezpečenie vykonávania pravidelných cvičení;
- c) zabezpečenie dôkazov o akomkoľvek incidente, ktorý môže mať dosah na bezpečnosť komunikačnej infraštruktúry alebo centrálnemu VIS, alebo národných systémov, a podávanie správ o incidente pracovníkovi zodpovednému za bezpečnosť systému;
- d) informovanie pracovníka zodpovedného za bezpečnosť systému, ak je potrebné zmeniť a doplniť bezpečnostnú politiku;
- e) monitorovanie uplatňovania tohto rozhodnutia a bezpečnostnej politiky každým dodávateľom vrátane subdodávateľov, ktorí sa akýmkoľvek spôsobom zúčastňujú na riadení komunikačnej infraštruktúry;
- f) zabezpečenie, že pracovníci poznajú svoje povinnosti, a monitorovanie uplatňovania bezpečnostnej politiky;
- g) monitorovanie vývoja bezpečnosti IT a zabezpečenie primeranej odbornej prípravy pracovníkov;
- h) príprava podkladových informácií a možností na vytvorenie, aktualizáciu a revíziu bezpečnostnej politiky v súlade s článkom 7.

Článok 5

Bezpečnostné incidenty

1. Akákoľvek udalosť, ktorá má alebo môže mať vplyv na bezpečnosť prevádzky VIS a môže spôsobiť poškodenie alebo stratu VIS, sa považuje za bezpečnostný incident, a to najmä v prípade, ak mohlo dôjsť k prístupu k údajom, alebo v prípade, ak došlo alebo by mohlo dôjsť k ohrozeniu dostupnosti, integrity a dôvernosti údajov.

2. V bezpečnostnej politike sa stanovujú postupy na obnovu po incidente. Riadenie bezpečnostných incidentov má zabezpečiť rýchlu, účinnú a správnu reakciu v súlade s bezpečnostnou politikou.

3. Informácie týkajúce sa bezpečnostného incidentu, ktorý má alebo môže mať vplyv na prevádzku VIS v členskom štáte alebo na dostupnosť, integritu a dôvernosť údajov VIS vložených členským štátom, sa poskytujú príslušným členským štátom. Bezpečnostné incidenty sa oznamujú úradníkom pre ochranu údajov Komisie.

Článok 6

Riadenie incidentov

1. Všetci zamestnanci a dodávatelia, ktorí sa podieľajú na vývoji, riadení alebo prevádzkovaní VIS, sú povinní zaznamenať a ohlásiť akékoľvek zistené alebo predpokladané bezpečnostné nedostatky v prevádzke systému VIS pracovníkovi zodpovednému za bezpečnosť systému alebo miestnemu bezpečnostnému pracovníkovi pre centrálny VIS alebo miestnemu bezpečnostnému pracovníkovi pre komunikačnú infraštruktúru.

2. V prípade zistenia akéhokoľvek incidentu, ktorý má alebo môže mať vplyv na bezpečnosť prevádzky VIS, miestny bezpečnostný pracovník pre centrálny VIS alebo miestny bezpečnostný pracovník pre komunikačnú infraštruktúru bezodkladne informuje pracovníka zodpovedného za bezpečnosť systému a v prípade, ak je to primerané, príslušné národné kontaktné miesto pre bezpečnosť VIS, ak takéto kontaktné miesto existuje v členskom štáte, a to písomne alebo v prípade mimoriadnej naliehavosti prostredníctvom iných komunikačných kanálov. Správa obsahuje opis bezpečnostného incidentu, úroveň rizika, možné dôsledky a opatrenia, ktoré sa prijali alebo by sa mali prijať na zmiernenie rizika.

3. Miestny bezpečnostný pracovník pre centrálny VIS alebo miestny bezpečnostný pracovník pre komunikačnú infraštruktúru (podľa vhodnosti) okamžite zaistí všetky dôkazy v súvislosti s bezpečnostným incidentom. Takéto dôkazy sa pracovníkovi zodpovednému za bezpečnosť systému sprístupnia na jeho požiadanie v rozsahu, aký umožňujú platné predpisy o ochrane údajov.

4. Uplatňujú sa postupy spätnej väzby, ktoré zaručujú oznámenie informácií o výsledkoch po vyriešení a ukončení incidentu.

KAPITOLA III

BEZPEČNOSTNÉ OPATRENIA

Článok 7

Bezpečnostná politika

1. Generálny riaditeľ Generálneho riaditeľstva pre spravodlivosť, slobodu a bezpečnosť vytvára, aktualizuje a pravidelne prehodnocuje záväznú bezpečnostnú politiku v súlade s týmto rozhodnutím. V bezpečnostnej politike sa ustanovujú podrobné postupy a opatrenia na ochranu pred ohrozeniami dostupnosti, integrity a dôvernosti VIS vrátane núdzového plánovania s cieľom zabezpečiť primeranú úroveň bezpečnosti v zmysle tohto rozhodnutia. Je potrebné zabezpečiť súlad bezpečnostnej politiky s týmto rozhodnutím.

2. Bezpečnostná politika vychádza z posúdenia rizík. Opatrenia opísané v bezpečnostnej politike zodpovedajú identifikovaným rizikám.

3. Posúdenie rizík a bezpečnostná politika sa aktualizujú, ak si to vyžadujú technologické zmeny, identifikácia nových hrozieb alebo akékoľvek iné okolnosti. Bezpečnostná politika sa v každom prípade prehodnocuje každoročne s cieľom zaručiť, že naďalej predstavuje primeranú reakciu na posledné posúdenie rizík alebo akúkoľvek novoidentifikovanú technologickú zmenu, hrozbu alebo iné relevantné okolnosti.

4. Pracovník zodpovedný za bezpečnosť systému v súčinnosti s miestnym bezpečnostným pracovníkom pre VIS a miestnym bezpečnostným pracovníkom pre komunikačnú infraštruktúru vypracuje bezpečnostnú politiku.

Článok 8

Vykonávanie bezpečnostných opatrení

1. Plnenie úloh a požiadaviek ustanovených v tomto rozhodnutí a v bezpečnostnej politike vrátane úlohy vymenovať miestneho bezpečnostného pracovníka sa môže zabezpečiť externe alebo sa môžu poveriť súkromné či verejné orgány.

2. V takom prípade Komisia zabezpečí prostredníctvom právne záväznej dohody, že požiadavky ustanovené v tomto rozhodnutí a v bezpečnostnej politike sa v plnej miere dodržiavajú. V prípade delegovania úlohy vymenovať miestneho bezpečnostného pracovníka alebo jej externého zabezpečenia Komisia zaručí prostredníctvom právne záväznej dohody, že o výbere osoby, ktorá sa stane miestnym bezpečnostným pracovníkom, sa s ňou bude konzultovať.

Článok 9

Kontrola prístupu k zariadeniam

1. Na ochranu priestorov, kde sa nachádzajú zariadenia na spracovanie údajov, sa použije zabezpečenie obvodu primeranými prekážkami a vstupné kontroly.

2. V rámci bezpečnostného obvodu sa vymedzia bezpečné zóny na ochranu fyzických prvkov (majetku) vrátane hardvéru, nosičov údajov a konzol, plánov a ostatných dokumentov o VIS, ako aj kancelárií a ďalších pracovísk pracovníkov zapojených do prevádzky VIS. Tieto bezpečné zóny sú chránené primeranými vstupnými kontrolami, aby sa zaručilo, že prístup majú povolený len oprávnení pracovníci. Na prácu v bezpečných zónach sa vzťahujú podrobné bezpečnostné pravidlá uvedené v bezpečnostnej politike.

3. Fyzické zabezpečenie kancelárií, miestností a zariadení sa naplánuje a nainštaluje vopred. Prístupové body, ako sú zásobovacie a nakladacie zóny a ďalšie miesta, kde môžu do priestorov vstupovať neoprávnené osoby, sa kontrolujú a podľa možnosti sú izolované od zariadení na spracovanie údajov, aby sa zabránilo neoprávnenému prístupu.

4. Fyzická ochrana bezpečnostného obvodu proti škodám spôsobeným prírodnou katastrofou alebo katastrofou spôsobenou človekom je navrhnutá a použitá primerane k riziku.

5. Zariadenia musia byť chránené pred fyzickými a environmentálnymi hrozbami a možnosťami neoprávneného prístupu.

6. Komisia doplní do zoznamu uvedeného v článku 2 ods. 2 písm. f) jednotlivé kontaktné miesta na monitorovanie vykonávania ustanovení tohto článku v priestoroch, kde sa nachádza záložný centrálny VIS, ak má tieto informácie k dispozícii.

Článok 10

Kontrola nosičov údajov a majetku

1. Odstrániteľné nosiče s údajmi sú chránené pred neoprávneným prístupom, zneužitím alebo poškodením a ich čitateľnosť je zaručená počas celého obdobia životnosti údajov.

2. Nepotrebné nosiče sa zneškodňujú bezpečným a neohrozujúcim spôsobom v súlade s podrobnými postupmi, ktoré sa stanovujú v bezpečnostnej politike.

3. Súpis zabezpečujú, že informácie o miestach uloženia, príslušných lehotách uchovávaní a povoleniach na prístup sú k dispozícii.

4. Všetok dôležitý majetok centrálnej VIS a komunikačná infraštruktúra sú označené tak, aby mohli byť chránené podľa svojho významu. Vedie sa aktuálny register relevantnej informačnej techniky.

5. K dispozícii je aktuálna dokumentácia centrálnej VIS a komunikačnej infraštruktúry. Táto dokumentácia musí byť chránená pred neoprávneným prístupom.

Článok 11**Kontrola uloženia**

1. Prijmú sa vhodné opatrenia zamerané na zabezpečenie riadneho uloženia informácií a zabránenie neoprávnenému prístupu.

2. Všetky časti zariadenia s pamäťovými nosičmi sa kontrolujú, aby sa zabezpečilo, že citlivé údaje sa pred likvidáciou odstránia alebo úplne prepíšu, alebo sa bezpečne zničia.

Článok 12**Kontrola hesiel**

1. Všetky heslá sa uchovávajú bezpečným spôsobom a považujú sa za dôverné. V prípade podozrenia zo zverejnenia hesla je potrebné heslo okamžite zmeniť alebo používateľský účet treba zablokovať. Používajú sa jedinečné a individuálne používateľské identity.

2. Bezpečnostná politika definuje postupy na prihlásenie a odhlásenie, aby sa zabránilo neoprávnenému prístupu.

Článok 13**Kontrola prístupu**

1. V rámci bezpečnostnej politiky sa vytvorí formálny postup registrovania a zrušenia registrovania zamestnancov na účely povolenia a zrušenia prístupu k hardvéru a softvéru VIS v centrálnom VIS na účely prevádzkového riadenia. Pridelenie a použitie primeraných prístupových poverení (heslá alebo iné vhodné prostriedky) sa kontroluje pomocou formálneho riadiaceho procesu uvedeného v bezpečnostnej politike.

2. Prístup k hardvéru a softvéru VIS v centrálnom VIS:

- i) sa obmedzuje na oprávnené osoby;
 - ii) sa obmedzuje na prípady, keď možno určiť legitímny účel v súlade s článkom 42 a článkom 50 ods. 2 nariadenia (ES) č. 767/2008;
 - iii) neprekročí obdobie trvania a rozsah, ktoré sú potrebné na účel prístupu, a
 - iv) prebieha len v súlade s politikou riadenia prístupu, ktorá sa ustanoví v bezpečnostnej politike.
3. V centrálnom VIS sa používajú len konzoly a softvér povolený miestnym bezpečnostným pracovníkom pre centrálny

VIS. Používanie systémových nástrojov, prostredníctvom ktorých by bolo možné obísť systém a aplikačné kontroly, je obmedzené a kontrolované. Je potrebné zaviesť postupy na kontrolu inštalácie softvéru.

Článok 14**Kontrola prenosu údajov**

Komunikačná infraštruktúra sa monitoruje, aby sa zabezpečila dostupnosť, integrita a dôverynosť výmeny informácií. Na ochranu prenášaných údajov v komunikačnej infraštruktúre sa používajú šifrovacie prostriedky.

Článok 15**Kontrola zaznamenávania údajov**

Účty osôb s oprávneným prístupom k softvéru VIS z centrálnom VIS monitoruje miestny bezpečnostný pracovník pre centrálny VIS. Použitie týchto účtov vrátane času a identity používateľov sa zaznamenáva.

Článok 16**Kontrola prepravy**

1. V rámci bezpečnostnej politiky sa ustanovia primerané opatrenia na zabránenie neoprávneného čítania, kopírovania, upravovania alebo vymazania osobných údajov počas prenosu do VIS alebo z neho alebo počas prepravy údajových nosičov. Bezpečnostná politika uvádza ustanovenia týkajúce sa prípustných spôsobov odoslania alebo prepravy, ako aj postupov týkajúcich sa zodpovednosti pri preprave položiek a ich doručenia na miesto určenia. Nosiče s údajmi neobsahujú žiadne iné údaje ako tie, ktoré sa majú odoslať.

2. Služby poskytované tretími osobami, zahŕňajúce prístup, spracovanie, prenos alebo spravovanie zariadení na spracovanie údajov alebo pridávanie produktov či služieb k zariadeniam na spracovanie údajov, podliehajú zodpovedajúcim integrovaným bezpečnostným kontrolám.

Článok 17**Bezpečnosť komunikačnej infraštruktúry**

1. Komunikačná infraštruktúra sa primerane spravuje a kontroluje, aby sa ochránila pred hrozbami a aby sa zaručila bezpečnosť samotnej komunikačnej infraštruktúry a centrálnom VIS vrátane údajov, ktorých výmenu sprostredkúva.

2. Bezpečnostné charakteristiky, úrovne služieb a požiadavky na riadenie všetkých sieťových služieb sa určia v dohode o sieťových službách s poskytovateľom služieb.

3. Okrem ochrany prístupových bodov VIS sa tiež chráni akákoľvek ďalšia služba využívaná komunikačnou infraštruktúrou. V bezpečnostnej politike sa stanovujú primerané opatrenia.

Článok 18**Monitorovanie**

1. Zápisy, na ktorých sú zaznamenané informácie uvedené v článku 34 ods. 1 nariadenia (ES) č. 767/2008 o každom prístupe a všetkých operáciách spracovania údajov v centrálnom VIS, sú bezpečne uložené v priestoroch, kde sa nachádza hlavná a záložná centrálna lokalita VIS, a sú z nich prístupné počas obdobia uvedeného v článku 34 ods. 2 nariadenia (ES) č. 767/2008.

2. Postupy monitorovania použitia alebo porúch zariadení na spracovanie informácií sú uvedené v bezpečnostnej politike a výsledky monitorovacích činností sa pravidelne prehodnocujú. Ak je to potrebné, prijímajú sa primerané opatrenia.

3. Zariadenia na zaznamenávanie a zápisy sú chránené pred manipuláciou a neoprávneným prístupom, aby sa dodržali požiadavky na zhromažďovanie a uchovávanie dôkazov počas obdobia ich uchovávania.

Článok 19**Šifrovacie opatrenia**

Na ochranu informácií sa primerane uplatňujú šifrovacie opatrenia. Ich použitie spolu s účelom a podmienkami musí vopred schváliť pracovník zodpovedný za bezpečnosť systému.

KAPITOLA IV**BEZPEČNOSŤ ĽUDSKÝCH ZDROJOV****Článok 20****Profily zamestnancov**

1. V rámci bezpečnostnej politiky sa ustanovia funkcie a povinnosti osôb, ktoré majú oprávnenie na prístup do VIS vrátane komunikačnej infraštruktúry.

2. Bezpečnostné úlohy a povinnosti zamestnancov Komisie, dodávateľov a pracovníkov zapojených do prevádzkového riadenia sa stanovujú, zdokumentujú a oznámia osobám, ktorých sa týkajú. Tieto úlohy a povinnosti zamestnancov Komisie sa uvádzajú v pracovnej náplni a cieľoch, pre dodávateľov sa uvádzajú v zmluvách alebo v dohodách o úrovni služieb.

3. Dohody o mlčanlivosti a utajení sa uzatvoria so všetkými osobami, na ktoré sa nevzťahujú pravidlá pre zamestnancov vo verejnej správe Európskej únie alebo členského štátu. Zamestnanci, ktorí musia pracovať s údajmi VIS, majú potrebné previerky alebo certifikáciu v súlade s podrobnými postupmi, ktoré sa ustanovia v rámci bezpečnostnej politiky.

Článok 21**Informácie o zamestnancoch**

1. Všetci pracovníci a prípadne aj dodávatelia absolvujú primeranú odbornú prípravu v oblasti bezpečnosti, právnych požiadaviek, politík a postupov v potrebnom rozsahu, aký si vyžadujú ich povinnosti.

2. Pri ukončení zamestnania alebo zmluvy sa vymedzia povinnosti súvisiace so zmenou zamestnania alebo s ukončením pracovného pomeru zamestnancov a dodávateľov v bezpečnostnej politike a v bezpečnostnej politike sa stanovujú postupy s cieľom zabezpečiť vrátenie majetku a zrušiť prístupové práva.

KAPITOLA V**ZÁVEREČNÉ USTANOVENIA****Článok 22****Uplatniteľnosť**

1. Toto rozhodnutie sa uplatňuje od dátumu stanoveného Komisiou v súlade s článkom 48 ods. 1 nariadenia (ES) č. 767/2008.

2. Účinnosť tohto rozhodnutia sa končí, keď riadiaci orgán prevezme svoje povinnosti.

V Bruseli 4. mája 2010

*Za Komisiu
predseda*

José Manuel BARROSO