ROZHODNUTÍ KOMISE

ze dne 4. května 2010

o bezpečnostním plánu pro centrální SIS II a komunikační infrastrukturu

(2010/261/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) [1], a zejména na článek 16 tohoto nařízení,

s ohledem na rozhodnutí Rady 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II) [2], a zejména na článek 16 tohoto rozhodnutí,

vzhledem k těmto důvodům:

(1) Článek 16 nařízení (ES) č. 1987/2006 a článek 16 rozhodnutí 2007/533/SVV stanoví, že řídící orgán ve vztahu k centrálnímu SIS II a Komise ve vztahu ke komunikační infrastruktuře přijme nezbytná opatření, včetně bezpečnostního plánu.

(2) Podle čl. 15 odst. 4 nařízení (ES) č. 1987/2006 a čl. 15 odst. 4 rozhodnutí 2007/533/SVV je během přechodného období, než se řídící orgán ujme svých povinností, za provozní řízení centrálního SIS II odpovědná Komise.

(3) Jelikož řídící orgán nebyl dosud zřízen, měl by se bezpečnostní plán, který přijme Komise, během přechodného období vztahovat rovněž na centrální SIS II.

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

(5) V čl. 15 odst. 7 nařízení (ES) č. 1987/2006 a čl. 15 odst. 7 rozhodnutí 2007/533/SVV se stanoví, že v případě, že Komise během přechodného období, než se řídící orgán ujme svých povinností, pověří některý subjekt plněním svých povinností, zajistí, aby toto pověření nepříznivým způsobem neovlivnilo případný účinný kontrolní mechanismus podle práva Evropské unie, ať se jedná o Soudní dvůr, Účetní dvůr nebo evropského inspektora ochrany údajů.

(6) Jakmile se řídící orgán ujme svých povinností, měl by přijmout vlastní bezpečnostní plán pro centrální SIS II. Platnost tohoto bezpečnostního plánu by proto s ohledem na centrální SIS II měla skončit, jakmile se řídící orgán ujme svých povinností.

(7) V čl. 4 odst. 3 nařízení (ES) č. 1987/2006 a čl. 4 odst. 3 rozhodnutí 2007/533/SVV se stanoví, že technická podpůrná funkce (CS-SIS), jež vykonává technický dohled a správu, se nachází ve Štrasburku (Francie) a záložní CS-SIS, jež je schopna zajistit všechny funkce hlavní CS-SIS v případě její poruchy, se nachází v Sankt Johann im Pongau (Rakousko).

(8) Bezpečnostní plán by měl počítat s jedním pracovníkem pro bezpečnost systému, který plní úkoly související s bezpečností ve vztahu k centrálnímu SIS II i komunikační infrastruktuře, a se dvěma místními bezpečnostními pracovníky, kteří plní úkoly související s bezpečností ve vztahu k centrálnímu SIS II a komunikační infrastruktuře. Úloha bezpečnostních úředníků by měla být vymezena s cílem zajistit účinnou a okamžitou reakci na bezpečnostní incidenty a jejich oznamování.

(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 centrálního SIS II a komunikační infrastruktury,

[1] Úř. věst. L 381, 28.12.2006, s. 4.
[2] Úř. věst. L 205, 7.8.2007, s. 63.
[3] Úř. věst. L 8, 12.1.2001, s. 1.

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

1. Toto rozhodnutí stanoví organizaci bezpečnosti a bezpečnostní opatření (bezpečnostní plán) k ochraně centrálního SIS II a údajů zpracovávaných v rámci tohoto systému před ohrožením jejich dostupnosti, neporušenosti a důvěrnosti ve smyslu čl. 16 odst. 1 nařízení (ES) č. 1987/2006 a čl. 16 odst. 1 rozhodnutí 2007/533/SVV o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II) během přechodného období, dokud se řídící orgán neujme svých povinností.

2. Toto rozhodnutí stanoví organizaci bezpečnosti a bezpečnostní opatření (bezpečnostní plán) k ochraně komunikační infrastruktury před ohrožením dostupnosti, neporušenosti a důvěrnosti údajů ve smyslu článku 16 nařízení (ES) č. 1987/2006 a článku 16 rozhodnutí 2007/533/SVV o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II).

KAPITOLA II

ORGANIZACE, POVINNOSTI A ZVLÁDÁNÍ INCIDENTŮ

Článek 2

Úkoly Komise

1. Komise zavede bezpečnostní opatření pro centrální SIS II a sleduje jejich účinnost, jak je uvedeno v tomto rozhodnutí.

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

3. Komise ze svých úředníků určí pracovníka pro bezpečnost systému. Pracovník pro bezpečnost systému je jmenován generálním ředitelem generálního ředitelství Komise pro spravedlnost, svobodu a bezpečnost. K úkolům pracovníka pro bezpečnost systému patří zejména:

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

b) sledování účinnosti provádění bezpečnostních postupů centrálního SIS II;

c) sledování účinnosti provádění bezpečnostních postupů komunikační infrastruktury;

d) přispění k vypracování zpráv o bezpečnosti, jak je stanoveno v článku 50 nařízení (ES) č. 1987/2006 a v článku 66 rozhodnutí 2007/533/SVV;

e) plnění úkolů v oblasti koordinace a poskytování pomoci při kontrolách a auditech prováděných evropským inspektorem ochrany údajů podle článku 45 nařízení (ES) č. 1987/2006 a článku 61 rozhodnutí 2007/533/SVV, jakož i oznamování incidentů ve smyslu čl. 5 odst. 2 inspektorovi ochrany údajů v Komisi;

f) kontrola, zda jsou toto rozhodnutí a bezpečnostní politika náležitě a plně uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na řízení centrálního SIS II;

g) kontrola, zda jsou toto rozhodnutí a bezpečnostní politika náležitě a plně uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na řízení komunikační infrastruktury;

h) vedení seznamu vnitrostátních jednotných kontaktních míst pro bezpečnost SIS II a společné používání tohoto seznamu s místním bezpečnostním pracovníkem pro komunikační infrastrukturu;

i) společné používání seznamu uvedeného v písmenu h) s místním bezpečnostním úředníkem pro centrální SIS II.

Článek 3

Místní bezpečnostní pracovník pro centrální SIS II

1. Aniž je dotčen článek 8, Komise ze svých úředníků určí místního bezpečnostního pracovníka pro centrální SIS II. Je nutno zamezit střetu zájmů mezi funkcí místního bezpečnostního pracovníka a jakoukoliv jinou úřední povinností. Místní bezpečnostní pracovník pro centrální SIS II je jmenován generálním ředitelem generálního ředitelství Komise pro spravedlnost, svobodu a bezpečnost.

2. Místní bezpečnostní pracovník pro centrální SIS II zajistí provádění bezpečnostních opatření uvedených v tomto rozhodnutí a dodržování bezpečnostních postupů v hlavní CS-SIS. Co se týká záložní CS-SIS, místní bezpečnostní pracovník pro centrální SIS II zajistí, aby byla prováděna bezpečnostní opatření uvedená v tomto rozhodnutí s výjimkou opatření stanovených v článku 9 a aby byly dodržovány související bezpečnostní postupy.

3. Místní bezpečnostní pracovník pro centrální SIS II 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 pracovníka nebo jeho podřízeného pracovníka ve službě je možno kdykoli zastihnout na jednom kontaktním telefonním čísle a adrese.

4. Místní bezpečnostní pracovník pro centrální SIS II vykonává úkoly vyplývající z bezpečnostních opatření, jež mají být přijata v místech, v nichž se nachází hlavní CS-SIS a záložní CS-SIS, a to v mezích uvedených v odstavci 1, včetně zejména:

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

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

c) zajištění důkazů o jakémkoli incidentu v centrálním SIS II, který by mohl mít dopad na bezpečnost centrálního SIS II nebo komunikační infrastruktury, a podávání zpráv o těchto incidentech pracovníkovi pro bezpečnost systému;

d) informování pracovníka pro bezpečnost systému, pokud je nutno pozměnit bezpečnostní politiku;

e) kontroly, zda jsou toto rozhodnutí a bezpečnostní politika uplatňovány všemi smluvními dodavateli, včetně subdodavatelů, kteří se jakýmkoli způsobem podílejí na provozním řízení centrálního SIS II;

f) zajištění, 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) vypracování podkladových informací a alternativ pro vytvoření, aktualizaci a přezkum bezpečnostní politiky v souladu s článkem 7.

Článek 4

Místní bezpečnostní pracovník pro komunikační infrastrukturu

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

2. Místní bezpečnostní pracovník pro komunikační infrastrukturu sleduje fungování komunikační infrastruktury a zajišťuje provádění bezpečnostních opatření a dodržování bezpečnostních postupů.

3. Místní bezpečnostní pracovník 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 pracovníka nebo jeho podřízeného pracovníka ve službě je možno kdykoli zastihnout na jednom kontaktním telefonním čísle a adrese.

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

a) místních operativních bezpečnostních úkolů souvisejících s komunikační infrastrukturou, včetně kontroly ochranných prostředků, pravidelného ověřování bezpečnosti, provádění auditů a podávání zpráv;

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

c) zajištění důkazů o jakémkoli incidentu v komunikační infrastruktuře, který by mohl mít dopad na bezpečnost centrálního SIS II nebo komunikační infrastruktury, a podávání zpráv o těchto incidentech pracovníkovi pro bezpečnost systému;

d) informování pracovníka pro bezpečnost systému, pokud je nutno pozměnit bezpečnostní politiku;

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

f) zajištění, 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) vypracování 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 SIS II a může SIS II 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, neporušenost a důvěrnost údajů.

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

3. Informace o bezpečnostním incidentu, který má nebo může mít dopad na provoz SIS II v některém z členských států nebo na dostupnost, neporušenost a důvěrnost údajů vložených či zaslaných některým členským státem, se poskytují dotčenému členskému státu. Bezpečnostní incidenty se oznamují inspektorovi ochrany údajů v Komisi.

Článek 6

Zvládání incidentů

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

2. Je-li zjištěn incident, který má nebo může mít dopad na bezpečnost SIS II, informuje místní bezpečnostní pracovník pro komunikační infrastrukturu co nejrychleji pracovníka pro bezpečnost systému a popřípadě vnitrostátní jednotné kontaktní místo pro bezpečnost SIS II, 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 pracovník pro komunikační infrastrukturu neprodleně zajistí veškeré důkazy v souvislosti s bezpečnostním incidentem. Tyto důkazy jsou v možném rozsahu podle platných předpisů o ochraně údajů na žádost poskytnuty pracovníkovi pro bezpečnost systému.

4. V bezpečnostní politice jsou stanoveny postupy pro poskytování zpětné vazby s cílem zajistit, aby byly úředníkovi pro bezpečnost systému a místnímu bezpečnostnímu pracovníkovi pro komunikační infrastrukturu předávány informace o druhu, řešení a výsledku bezpečnostního incidentu, jakmile byl incident vyřešen a nadále již netrvá.

5. Odstavce 1 až 4 se použijí obdobně na incidenty v centrálním SIS II. Odkazy na místního bezpečnostního pracovníka pro komunikační infrastrukturu v odstavcích 1 až 4 je v tomto případě nutno považovat za odkazy na místního bezpečnostního pracovníka pro centrální SIS II.

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, neporušenosti a důvěrnosti komunikační infrastruktury, 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 pracovník pro bezpečnost systému v koordinaci s místním bezpečnostním pracovníkem pro centrální SIS II a místním bezpečnostním pracovníkem pro komunikační infrastrukturu.

5. Odstavce 1 až 4 se použijí obdobně na bezpečnostní politiku pro centrální SIS II. Odkazy na místního bezpečnostního pracovníka pro komunikační infrastrukturu v odstavcích 1 až 4 je v tomto případě nutno považovat za odkazy na místního bezpečnostního pracovníka pro centrální SIS II.

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 pracovníka, je možno zajistit smluvně nebo svěřit soukromým či veřejným subjektům.

2. V tomto případě Komise prostřednictvím právně závazné smlouvy zajistí, že jsou zcela splněny požadavky stanovené v tomto rozhodnutí a v bezpečnostní politice. V případě delegace úlohy jmenovat místního bezpečnostního pracovníka nebo jejího smluvního zajištění Komise prostřednictvím právně závazné smlouvy zajistí, aby byla konzultována ohledně osoby, která má být jmenována místním bezpečnostním pracovníkem.

Článek 9

Kontrola přístupu k zařízení

1. K ochraně oblastí, které obsahují 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 (majetku), včetně technického vybavení, nosičů údajů a ovládacích panelů, plánů a jiných dokumentů týkajících se SIS II, jakož i kanceláří a ostatních pracovišť zaměstnanců zajišťujících provoz SIS II. 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 zásobovací a nakládací zóny 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 přírodními hrozbami a před možností neoprávněného přístupu.

6. Má-li Komise k dispozici takovéto informace, připojí na seznam uvedený v čl. 2 odst. 3 písm. h) jednotné kontaktní místo pro kontrolu provádění ustanovení tohoto článku v prostorách, v nichž se nachází záložní CS-SIS.

Článek 10

Kontrola nosičů údajů a majetku

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 zneškodněny, jakmile již nejsou zapotřebí, a to v souladu s podrobnými postupy, jež jsou stanoveny v bezpečnostní politice.

3. Prostřednictvím soupisů je zajištěno, že jsou k dispozici informace o místu uložení, příslušné době uchovávání a oprávněních k přístupu.

4. Je vymezen veškerý důležitý majetek komunikační infrastruktury, takže jej lze chránit v souladu s jeho významem. Je veden aktualizovaný rejstřík příslušného vybavení IT.

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

6. Odstavce 1 až 5 se použijí obdobně na centrální SIS II. Odkazy na komunikační infrastrukturu je v tomto případě nutno považovat za odkazy na centrální SIS II.

Článek 11

Kontrola uchovávání

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

2. Veškeré položky vybavení, které obsahují nosiče údajů, 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. V bezpečnostní politice jsou stanoveny postupy pro přihlášení a odhlášení s cílem zamezit neoprávněnému přístupu.

Článek 13

Kontrola přístupu

1. Bezpečnostní politika stanoví oficiální postup pro registraci a zrušení registrace zaměstnanců, který se použije pro udělování a rušení přístupu k technickému a programovému vybavení SIS II pro potřeby provozního řízení. Přidělování a používání odpovídajících údajů zadávaných při přístupu (hesla nebo jiné vhodné prostředky) je kontrolováno prostřednictvím formálního řídícího procesu, jak je stanoveno v bezpečnostní politice.

2. Přístup k technickému a programovému vybavení SIS II v místě CS-SIS:

i) je omezen na oprávněné osoby,

ii) je omezen na případy, kdy lze určit legitimní účel v souladu s článkem 45 nařízení (ES) č. 1987/2006 a článkem 61 rozhodnutí 2007/533/SVV nebo s čl. 50 odst. 2 nařízení (ES) č. 1987/2006 a čl. 66 odst. 2 rozhodnutí 2007/533/SVV,

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 CS-SIS se používají pouze ovládací panely a programové vybavení schválené místním bezpečnostním pracovníkem pro centrální SIS II. Je omezeno a kontrolováno používání systémových nástrojů, které mohou být schopny přepsat systém a kontrolovat aplikace. Jsou zavedeny postupy pro kontrolu instalace programového vybavení.

Článek 14

Kontrola komunikace

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

Článek 15

Kontrola vstupů

Místní bezpečnostní pracovník pro centrální SIS II sleduje účty osob s oprávněným přístupem k programovému vybavení SIS II z CS-SIS. Je evidováno používání těchto účtů, včetně času přístupu a totožnosti uživatelů.

Článek 16

Kontrola přepravy

1. V bezpečnostní politice jsou stanovena vhodná opatření s cílem zamezit neoprávněnému čtení, kopírování, změně nebo výmazu osobních údajů během předávání do a z SIS II nebo během přepravy nosičů údajů. Bezpečnostní politika obsahuje ustanovení o přípustných druzích odesílání nebo přepravy a rovněž o postupech pro stanovení odpovědnosti za přepravu jednotlivých položek a jejich dopravení na místo určení. Nosič údajů nesmí obsahovat jiné údaje než údaje, jež mají být zaslány.

2. Služby poskytované třetími stranami, které zahrnují přístup k údajům, jejich zpracovávání a předávání nebo správu zařízení pro zpracování údajů či přidávání produktů nebo služeb k zařízením pro zpracování údajů, mají odpovídající integrované bezpečnostní kontroly.

Článek 17

Bezpečnost komunikační infrastruktury

1. Komunikační infrastruktura je přiměřeně spravována a kontrolována s cílem chránit ji před hrozbami a zajistit bezpečnost samotné komunikační infrastruktury a centrálního SIS II, včetně údajů, jež jsou jejím prostřednictvím vyměňovány.

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

3. Kromě ochrany přístupových bodů SIS II jsou chráněny rovněž veškeré další služby, které komunikační infrastruktura používá. Vhodná opatření jsou stanovena v bezpečnostní politice.

Článek 18

Monitorování

1. Protokoly zaznamenávající informace uvedené v čl. 18 odst. 1 nařízení (ES) č. 1987/2006 a čl. 18 odst. 1 rozhodnutí 2007/533/SVV týkající se každého přístupu a veškerých výměn osobních údajů v rámci CS-SIS jsou uchovávány bezpečně v prostorách, v nichž se nachází hlavní CS-SIS a záložní CS-SIS, a jsou dostupné z těchto prostor, a to po maximální dobu uvedenou v čl. 18 odst. 3 nařízení (ES) č. 1987/2006 a čl. 18 odst. 3 rozhodnutí 2007/533/SVV.

2. V bezpečnostní politice jsou stanoveny postupy, jak sledovat používání nebo poruchy zařízení pro zpracování informací, a jsou pravidelně přezkoumávány výsledky kontrolních činností. 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

Šifrovací opatření

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

KAPITOLA IV

BEZPEČNOST LIDSKÝCH ZDROJŮ

Článek 20

Profily pracovníků

1. Bezpečnostní politika stanoví funkce a povinnosti osob s oprávněným přístupem k centrálnímu SIS II.

2. Bezpečnostní politika stanoví funkce a povinnosti osob s oprávněným přístupem ke komunikační infrastruktuře.

3. 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.

4. 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 SIS II, 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 smluvní dodavatelé jsou náležitě vyškoleni v oblasti bezpečnosti, právních požadavků, politik a postupů 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 majetku a zrušení přístupových práv.

KAPITOLA V

ZÁVĚREČNÁ USTANOVENÍ

Článek 22

Použitelnost

1. Toto nařízení je použitelné ode dne, který stanoví Rada v souladu s čl. 55 odst. 2 nařízení (ES) č. 1987/2006 a čl. 71 odst. 2 rozhodnutí 2007/533/SVV.

2. Ustanovení čl. 1 odst. 1, čl. 2 odst. 1, čl. 2 odst. 3 písm. b), d), f) a i), článku 3, čl. 6 odst. 5, čl. 7 odst. 5, čl. 9 odst. 6, čl. 10 odst. 6, čl. 13 odst. 2 a 3, článků 15 a 18 a čl. 20 odst. 1 pozbudou platnosti, jakmile se řídící orgán ujme svých povinností.

V Bruselu dne 4. května 2010.

Za Komisi

José Manuel BARROSO

předseda