Čj. 1/04/SŘ-OSR
Výtisk č. 1

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, odbor správního rozhodování, jako příslušný správní orgán podle § 5 odst. 1 zákona č. 71/1967 Sb., o správním řízení (správní řád), § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, rozhodl dne 26. května 2004 takto:

Je prokázáno, že účastník řízení: Univerzita Hradec Králové, se sídlem Víta Nejedlého 573, 500 03 Hradec Králové, IČO: 62690094 při zpracování osobních údajů v souvislosti s provozováním informačního systému Isit Fakultou informatiky a managementu Univerzity Hradec Králové jako správce osobních údajů zpracovávaných prostřednictvím informačního systému Isit, a to identifikačních osobních údajů studentů a dále údajů vypovídajících o průběhu jejich studia, nepřijal nezbytná opatření proti neoprávněnému a nahodilému přístupu k těmto osobním údajům, v důsledku čehož dne 3. února 2003 došlo ke zničení a neoprávněnému přenosu osobních údajů obsažených v tomto informačním systému, který znamenal jejich následné neoprávněné zpracování nezjištěnou osobou, a to zveřejněním části těchto osobních údajů 18 bývalých či současných studentů Fakulty informatiky a managementu Univerzity Hradec Králové na webové stránce umístěné na internetové adrese www.fim-uhk.4t.com;
dále je prokázáno, že účastník řízení uzavřel s Ing. Petrem Markem, místo podnikání Prostějovská 1080, 500 06 Hradec Králové, smlouvy, jejichž předmětem bylo též zpracování osobních údajů zpracovávaných prostřednictvím informačního systému Isit, ve kterých nebylo výslovně uvedeno, v jakém rozsahu a za jakým účelem jsou uzavírány,

čímž porušil povinnost stanovenou v § 13 zákona č. 101/2000 Sb., tedy nepřijal taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů,
a dále porušil povinnost stanovenou v § 6 zákona č. 101/2000 Sb., tedy jím uzavírané smlouvy o zpracování osobních údajů neobsahovaly zákonem stanovené náležitosti,

a tím spáchal správní delikt podle § 46 odst. 1 zákona č. 101/2000 Sb., neboť porušil povinnost stanovenou tímto zákonem při zpracování osobních údajů, za což se účastníku řízení v souladu s § 46 odst. 1 zákona č. 101/2000 Sb. ukládá

pokuta ve výši 20.000 Kč
(slovy dvacet tisíc korun českých)

splatná do 15 dnů ode dne nabytí právní moci tohoto rozhodnutí bezhotovostním převodem na účet vedený u ČNB, č. ú. 3754-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Správní řízení ve věci plnění povinností při zpracování osobních údajů v souvislosti s provozováním informačního systému Isit Fakultou informatiky a managementu Univerzity Hradec Králové (dále jen „Fakulta informatiky a managementu“) bylo zahájeno oznámením Úřadu pro ochranu osobních údajů ze dne 8. ledna 2004, které bylo účastníkovi řízení doručeno dne 12. ledna 2004. Podkladem pro zahájení řízení byl písemný materiál shromážděný v rámci kontroly provedené ve dnech 31. března až 20. června 2003 inspektorem Úřadu pro ochranu osobních údajů Ing. Milošem Šnytrem.

Ze spisového materiálu, obsahujícího zejména písemný materiál získaný inspektorem Úřadu pro ochranu osobních údajů a dále poznatky Policie České republiky, okresního ředitelství Hradec Králové (usnesení o odložení věci ČST: ORHK-644/HK-2003 ze dne 27. února 2004 a souhrn případu), je zřejmé, že dne 3. února 2003 pronikla neznámá osoba do všech hlavních počítačových serverů Univerzity Hradec Králové, a to včetně serveru Isit2, který obsahoval kompletní databázi informačního systému Isit, tedy databázi všech studentů, včetně studentů doktorandů, od roku 1997. Pro přístup k serveru přitom bylo využito uživatelské jméno a heslo Ing. J. S., zaměstnankyně studijního oddělení Fakulty informatiky a managementu.

Následně došlo ke zničení všech dat na serveru Isit2 takovým způsobem, že jejich obnova již nebyla možná (obnova byla proto posléze provedena ze zálohy vytvořené dne 29. ledna 2003), přičemž nebylo možno zjistit, zda došlo pouze ke zničení či též k odcizení všech dat. Na webové stránce umístěné na internetové adrese www.geocities.com/sitcom23/, na kterou byli vybraní zaměstnanci Fakulty informatiky a managementu upozorněni prostřednictvím e-mailové zprávy odeslané z e-mailové adresy petra.poulova@seznam.cz (RNDr. Petra Poulová je proděkankou Fakulty informatiky a managementu, která uvedenou schránku ani nezaložila, ani neužívala), byl posléze zveřejněn odkaz na webovou stránku umístěnou na internetové adrese www.fim-uhk.4t.com, kde byl umístěn seznam 18 bývalých či současných studentů Fakulty informatiky a managementu, kteří k ní mají bližší vztah než obvyklí studenti, obsahující jejich osobní údaje v rozsahu jméno, příjmení, rodné číslo (kde poslední dvě číslice byly u všech osob s výjimkou vedoucího útvaru informačních systémů Fakulty informatiky a managementu nahrazeny písmeny „X“), místo narození, číslo občanského průkazu, adresa bydliště. V průběhu kontrolního šetření, jak je doloženo záznamem z kontrolního šetření ze dne 16. května 2003 a jak vyplývá též z vyjádření Ing. J. S. ze dne 11. dubna 2003 a Ing. P. M. ze dne 1. dubna 2003, bylo zjištěno, že zveřejněné údaje nebyly získány dotazem z informačního systému Isit, ale jednalo se o data z tabulky informačního systému Isit, ve které byly evidovány osobní údaje studentů.

K předmětu řízení se účastník vyjádřil na ústním jednání vedeném dne 20. května 2004 v budově Úřadu pro ochranu osobních údajů v Praze. K otázce zabezpečení informačních systémů se však vyjadřoval již v průběhu kontroly prováděné inspektorem Úřadu pro ochranu osobních údajů.

Z těchto vyjádření vyplývá, že po jmenování Doc. RNDr. Josefa Hynka, MBA, Ph.D. do funkce děkana Fakulty informatiky a managementu, a poté co byl vedením útvaru informačních systémů Fakulty informatiky a managementu pověřen Ing. Karel Šrámek, tj. po měsíci září 2003, došlo k řadě závad a havárií, které se týkaly více serverů Fakulty informatiky a managementu. Dle názoru účastníka řízení byly tyto havárie z části důsledkem neodborných řešení přijatých za předchozího vedení útvaru informačních systémů Fakulty informatiky a managementu a z části byly způsobeny jednáním nezjištěných osob, pravděpodobně, dle vyjádření účastníka řízení, některého ze zaměstnanců tohoto útvaru. Doc. RNDr. Josef Hynek, MBA, Ph.D. na ústním jednání dne 20. května 2004 dále uvedl, že tento závěr byl potvrzen též poznatky Policie České republiky, které zúžily okruh možných pachatelů na tři osoby, které měly vztah k Fakultě informatiky a managementu, a tedy měly příslušné odborné dovednosti, kompetence a znalosti, a dodal, že žádná z těchto osob již v současné době není jejím zaměstnancem.

JUDr. Jaroslav Stach, zmocněný k tomuto jednání účastníkem řízení, dále k předmětu řízení doplnil, že nikdo z osob, jejichž údaje byly zveřejněny na webové stránce umístěné na internetové adrese www.fim-uhk.4t.com, neuplatňuje vůči Univerzitě Hradec Králové žádné nároky v důsledku tohoto zveřejnění.

V souvislosti s výše uvedenými skutečnostmi, tj. zejména s nástupem nových zaměstnanců, byla, dle vyjádření účastníka řízení zachyceného ve vyjádření děkana Fakulty informatiky a managementu Univerzity Hradec Králové k dopisu čj. 81/03/KON ze dne 12. března 2003 a v jeho přílohách, provedena analýza stavu spravované techniky, její funkčnosti a možných rizik z hlediska dalšího provozu a bezpečnosti, jejímž závěrem bylo konstatování potřeby podstatného zvýšení její bezpečnosti. V důsledku toho byl v rámci Univerzity Hradec Králové přijat v průběhu roku 2002 projekt Ochrana dat a řešení bezpečných přístupů v prostředí vysokorychlostních sítí. Současně byly činěny též kroky ke zvýšení objektové bezpečnosti výměnou klíčů v místnosti, ve které jsou umístěny servery Fakulty informatiky a managementu. Dále byly nakoupeny nové servery a došlo též k opravě elektrické a datové sítě. Všemi těmito organizačními opatřeními ve spojení s opatřeními personálními, jež nezbytně probíhala v průběhu delší doby, došlo dle názoru účastníka řízení vyjádřeného na ústním jednání dne 20. května 2004 k vyprovokování pozdějšího pachatele k jeho útoku, s cílem zvrátit celý proces, který měl vést ke změnám ve fungování Fakulty informatiky a managementu.

Ze shromážděných poznatků vyplývá, že dokument, který stanovil základní pravidla bezpečnostní politiky, jak v oblasti projektové, tak provozní, byl vypracován až po předmětném napadení serverů, v průběhu kontroly prováděné inspektorem Úřadu pro ochranu osobních údajů, a pod názvem Provozní řád výpočetní techniky Fakulty informatiky a managementu Univerzity Hradec Králové schválen Akademickým senátem Fakulty informatiky a managementu dne 17. září 2003. V době předmětného napadení informačního systému Fakulty informatiky a managementu

byl již sice v rámci Univerzity Hradec Králové vypracován zmíněný projekt týkající se ochrany dat, ale jeho realizace nebyla dokončena.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení svým jednáním porušil povinnosti stanovené v § 13 zákona č. 101/2000 Sb., a to proto, že jako správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. nepřijal odpovídající pravidla bezpečnostní politiky týkající se informačních systémů, která by zabránila neoprávněnému zpracování předmětných osobních údajů (čímž současně nedodržel bod 7 čl. 2 rektorského výnosu Univerzity Hradec Králové č. 4/01, tj. úkol přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů), a to zejména z toho důvodu, že správně nevyhodnotil rizika, která hrozí osobním údajům zpracovávaným prostřednictvím informačního systému Isit, a jím přijímaná opatření proti neoprávněnému a nahodilému přístupu k osobním údajům nebyla dostatečně razantní a komplexní. Následkem tohoto jednání účastníka řízení došlo ke zničení a neoprávněnému přenosu osobních údajů, který znamenal jejich následné neoprávněné zpracování resp. zveřejnění jejich části nezjištěnou osobou, která měla dle všech dosavadních poznatků v době tohoto neoprávněného zpracování vztah k Fakultě informatiky a managementu.

V průběhu správního řízení bylo též zjištěno, že účastník řízení uzavřel s Ing. Petrem Markem, místo podnikání Prostějovská 1080, 500 06 Hradec Králové, smlouvu o podpoře a rozvoji Isit č. 1/98/FK ze dne 1. dubna 1998 s jejími dodatky ze dne 20. prosince 2002 a 2. ledna 2003, smlouvu o spolupráci ze dne 28. února 2002 a smlouvu o dílo ze dne 20. prosince 2002, na základě kterých docházelo též ke zpracování osobních údajů zpracovávaných prostřednictvím informačního systému Isit.

V důsledku uzavření těchto smluv se tedy Ing. Petr Marek stal zpracovatelem předmětných osobních údajů, neboť tyto smlouvy předpokládají nakládání s databází informačního systému Isit, a je tedy povinností správce zajistit, aby tyto splňovaly též náležitosti § 6 zákona č. 101/2000 Sb. V žádné z výše uvedených smluv však nebylo výslovně uvedeno v jakém rozsahu a za jakým účelem jsou uzavírány, proto má správní orgán za prokázané, že došlo k porušení povinností stanovených správci osobních údajů § 6 zákona č. 101/2000 Sb.

Při stanovení výše sankce považuje správní orgán, mimo výše uvedeného, za nezbytné přihlédnout k rozsahu osobních údajů a zejména k vysokému počtu subjektů údajů (tj. všichni studenti Fakulty informatiky a managementu od roku 1997), jejichž osobní údaje byly v důsledku nedodržení zákonem stanovených opatření proti neoprávněnému nebo nahodilému přístupu účastníkem řízení ohroženy dalším neoprávněným zpracováním. Správní orgán nepovažuje za prokázané a tedy rozhodné, zda je veškerý obsah databáze pachateli útoku k dispozici i v současné době, ale musí zohlednit ohrožení osobních údajů v ní obsažených, včetně neoprávněného zpracování části z nich následným zveřejněním. Nebezpečnost skutku je dána především skutečností, že informační technologie, prostřednictvím kterých byly dotčené osobní údaje zpracovávány, jsou předmětem nejen praktické, ale také metodické a vzdělávací činnosti účastníka řízení, neboť je jeho posláním

naučit své studenty, v rámci práce s informačními technologiemi též pravidla bezpečnosti informačních systémů, které v tomto případě sám nedodržel.

Na druhé straně však správní orgán považuje za významné pro hodnocení jednání účastníka řízení skutečnost, že již před předmětným útokem detekoval z vlastní iniciativy potřebu zvýšení bezpečnosti svého informačního systému a činil kroky k ní vedoucí, které však nebyly, jak bylo prokázáno v tomto řízení, dostatečně účinné. Správní orgán zhodnotil při stanovení výše sankce též skutečnost, že protiprávní jednání nezjištěné osoby, kterým došlo k napadení serverů Fakulty informatiky a managementu, bylo dle zjištění Policie České republiky motivováno nikoli snahou o pouhé zpracování osobních údajů, ale šlo o úmyslné jednání vedené snahou o využití těchto údajů k páchání další trestné činnosti. Uložením sankce při dolní hranici zákonné sazby bylo zohledněno též splnění a doložení splnění nápravných opatření účastníkem řízení ve lhůtě stanovené v kontrolním protokole inspektora Úřadu pro ochranu osobních údajů ze dne 20. června 2003.

S ohledem na výše uvedené, bylo rozhodnuto, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení: V souladu s § 61 odst. 1 zákona č. 71/1967 Sb. lze proti tomuto rozhodnutí do 15 dnů od jeho oznámení podat u odboru správního rozhodování rozklad předsedovi Úřadu pro ochranu osobních údajů.

Praha 26. května 2004

Josef Prokeš
ředitel odboru správního rozhodování