Úřad pro ochranu osobních údajů

k rukám předsedy ÚOOÚ RNDr. Igora Němce

Pplk. Sochora 27

170 00 Praha 7

Zn. KNDČ-3865/11-5/NON

v Praze dne 7.7.2011

Žádost předsedovi ÚOOÚ o prošetření způsobu vyřízení stížnosti dle § 175 odst. 7 správního řádu

Vážený pane předsedo,

dne 7.6.2011jsem obdržel reakci na moji stížnost ze dne 17.5.2011 ve věci Plzeňské karty, kterou jsem reagoval na způsob vyřízení mého podnětu ze dne 6.5.2011, který se týkal tzv. Plzeňské karty.

V reakci je konstatováno, že z podnětu ani jiných zdrojů nevyplývá podezření na žádný konkrétní incident, kdy by došlo k neoprávněnému nebo nahodilému přístupu k osobním údajům. Dle vyjádření ÚOOÚ vyplývá z vyjádření představitele správce (Plzeňské městské dopravní podniky, a.s.), že zabezpečení karty je založeno na kombinaci více prvků, nejen na použité technologii u kartových čipů.

Toto tvrzení, o které ÚOOÚ opírá svoji reakci, nicméně **nebylo žádným způsobem blíže specifikováno**. Není vůbec zřejmé, zda nějaké další prvky zabezpečení vůbec existují, pokud ano, pak o jaké se jedná a zda je poté zabezpečení dostačující. Lze pochybovat o účinnosti kontroly ze strany ÚOOÚ pokud pro rozptýlení podezření postačuje pouhý neurčitý odkaz správce na blíže nespecifikovaná další bezpečnostní opatření.

Posuzovat možné porušení § 13 zákona o ochraně osobních údajů v tomto případě pouze na základě toho, zda došlo nebo nedošlo k neoprávněnému nebo nahodilému přístupu k osobním údajům, **považuji ze strany ÚOOÚ za nešťastné a**

nekonzistentní. Ustanovení § 13 zákona o ochraně osobních údajů jednoznačně říká, že „*správce a zpracovatel jsou povinni **přijmout** taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.*“ **Je tedy irelevantní, jestli k prolomení zabezpečení již došlo nebo nikoli.** Tato skutečnost může pouze dokazovat fakt, že přijatá opatření byla nedostatečná, ale není nezbytným předpokladem toho, aby bylo konstatováno porušení § 13 odst. 1 zákona o ochraně osobních údajů.

Stanovisko ÚOOÚ v této věci považuji za **nekonzistentní** zejména pokud přihlédneme k faktu, že předmětem kontroly ÚOOÚ je zcela běžně například fyzické zabezpečení zdravotní dokumentace v ordinacích nebo systémů bezpečnostních kamer. Nedostatky v tomto zabezpečení byly v minulosti postihovány ze strany ÚOOÚ pro porušení § 13 ZOOÚ, **přestože k žádnému konkrétnímu incidentu, při němž by došlo k úniku osobních údajů, nedošlo**. ÚOOÚ zde uplatňuje dvojí metr na fyzické a softwarové zabezpečení. V případě dat, která jsou zpracovávána softwarově považuji tento postup za **mimořádně nešťastný**, vzhledem k tomu, že o bezpečnostním incidentu v případě úniku digitálních dat se při nesprávném nastavení zabezpečení nemusí nikdo ani dozvědět, případně může jít najednou o tak masivní únik údajů, že případná následná kontrola, konstatování porušení zákona a uložení nápravných opatření jsou vzhledem k následku porušení zákona bezvýznamné (viz například nedávný únik dat desítek milionů klientů společnosti Sony).

Tvrzení, že každé zabezpečení je prolomitelné, je jistě pravdivé, záleží na míře úsilí a na množství času, které je schopen a ochoten případný útočník do tohoto prolomení zabezpečení investovat. Je nutné najít rozumný kompromis mezi nároky na zabezpečení a ochranou osobních údajů. Pokud je zřejmé, že zabezpečení je nedostatečné, což v případě čipu na Plzeňské kartě zřejmé je už vzhledem k typu použitého čipu, k celé řadě případů, kdy k jeho prolomení došlo a ke skutečnosti, že v současné době tento typ čipu již několik let není považován za bezpečný, pak považuji za zcela **nezbytné, aby správce přijal v nejkratší možné době opatření, která povedou k odstranění nebo k významnému snížení bezpečnostního rizika**. Například u pražské karty opencard bylo k výměně čipů (z Mifare Classic na Mifare Desfire) po zjištění nedostatků v zabezpečení, na něž upozornilo naše občanské sdružení, přistoupeno **již v roce 2008**, což mimo jiné dokládá, že požadovat tento postup i po jiném srovnatelném správci není rozhodně nepřiměřený požadavek. **V případě Plzeňské karty se k řešení tohoto problému nepřistoupilo**

již několik let a nic nenasvědčuje tomu, že by se tato situace měla v dohledné době změnit. Problém se naopak prohlubuje zaváděním možnosti využívat telefony s funkcí NFC, které neoprávněný přístup k osobním údajům usnadňují.

Chápu, že kontrola zpracování osobních údajů prostřednictvím multifunkčních čipových karet je personálně i časově náročná. Přesto považuji otázku Plzeňské karty za klíčovou zejména pokud jde o nutnost vyjasnění toho, co lze považovat za porušení povinností zakotvených v čl. 13 odst. 1 ZOOÚ. Pokud ÚOOÚ i v budoucnu u kontrol softwarového zabezpečení sofistikovanějších systémů bude setrvávat na stanovisku, které vedlo k odmítnutí našeho podnětu, tak sám oslabuje svoji pozici při prosazování ochrany osobních údajů a v budoucnu se možná sám odsoudí do role nečinného pozorovatele rozsáhlých úniků osobních údajů, kterých jsme dnes svědky ve světě. Věřím proto, že ještě jednou přehodnotíte stanovisku ÚOOÚ v této věci.

S pozdravem,

RNDr. Ing. Mojmír Janeček