ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

Čj. UOOU-06436/13-3.

MĚSTSKÝ SOUD V PRAZE
pracoviště Hybernská 18, Praha 1
osobně: 011 obálka:
Došlo dne: 28 -08- 2013 (3)
1 krát přílohy
kolky podpis

Městský soud v Praze
pracoviště Hybernská
Hybernská 18
111 21 PRAHA 1

Praha 26. srpna 2013

Vyjádření žalovaného k obsahu žaloby a předložení úplného spisového materiálu
ke sp. zn. 10 A 154/2013

Žalobce: Česká republika – Vězeňská služba České republiky
se sídlem Soudní 1672/1a, 140 67 Praha 4
IČ: 00212423

Žalovaný: Úřad pro ochranu osobních údajů
se sídlem Pplk. Sochora 27, 170 00 Praha 7

DVOJMO

K výzvě Vašeho soudu podává Úřad pro ochranu osobních údajů (dále jen „Úřad" nebo „žalovaný") ve stanovené lhůtě jednoho měsíce (výzva s žalobou byla Úřadu doručena dne 30. července 2013) následující vyjádření žalovaného k obsahu žaloby, resp. k jejím podstatným bodům.

Současně žalovaný soudu předkládá úplný spisový materiál ve věci, tj. správní spis sp. zn. UOOU-00182/13.

Žalovaný neuplatňuje námitku podjatosti a souhlasí s projednáním věci bez jednání.

I.

Žalobou napadené rozhodnutí předsedy Úřadu ze dne 20. května 2013 čj. UOOU-00182/13-27 bylo vydáno v rámci správního řízení vedeného Úřadem s žalobcem ve věci zabezpečení vězeňského informačního systému.

V průběhu správního řízení bylo prokázáno, že žalobce měl nastavená přístupová práva v tomto informačním systému takovým způsobem, že všichni zaměstnanci oprávnění v něm pracovat měli přístup ke všem údajům vedeným v tomto systému bez rozdílu.

Úřad proto rozhodnutím čj. UOOU-00182/13-21 ze dne 25. března 2013 rozhodl o tom, že se žalobce shora uvedeným jednáním dopustil správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., a uložil mu pokutu ve výši 50.000 Kč a povinnost uhradit náklady řízení ve výši 1.000 Kč. Rozklad proti tomuto rozhodnutí byl zamítnut rozhodnutím předsedy Úřadu čj. UOOU-00182/13-27 ze dne 20. května 2013, které nabylo právní moci dne 22. května 2013.

II.

Žalobce uvádí, že skutek, tak jak je vymezen v napadených rozhodnutích, je vnitřně rozporný. Není možné, aby osoba oprávněná k přístupu a vkládání údajů v informačním systému z něj získala údaje neoprávněně. Tato skutečnost dle žalobce svědčí o tom, že nedošlo k porušení § 13 odst. 1 zákona č. 101/2000 Sb.

K tomuto žalovaný uvádí, že uvedený výrok není vnitřně rozporný a tvrzení žalobce vyplývá spíše z jeho nepochopení principů zabezpečení osobních údajů a systematiky zákona č. 101/2000 Sb. Pro přehlednost žalovaný uvádí následující příklad: zaměstnanec orgánu veřejné moci má přístup do evidence obyvatel, tj. k údajům o všech občanech České republiky; přesto tento zaměstnanec může oprávněně přistupovat k osobním údajům pouze tehdy, pokud je to nutné při výkonu jeho konkrétní pracovní činnosti; tzn. že pokud si takový zaměstnanec bude v lepším případě náhodně „brouzdat" v evidenci obyvatel a vyhledávat známé, přátele apod., a v horším případě bude vyhledávat osobní údaje na zakázku a za úplatu, jedná se v obou případech o neoprávněný přístup ke konkrétním osobním údajům, ačkoliv je daný zaměstnanec osobou oprávněnou k přístupu a vkládání osobních údajů do informačního systému. Žalovaný tedy uvádí, že se v žádném případě nemůže jednat o dvě vzájemně rozporné skutečnosti. Proto také žalovaný považuje tvrzení žalobce o tom, že jeho zaměstnanci získali fotografie řádně a oprávněně, a nezákonnost spočívala až v jejich dalším nakládání, za dosti alarmující a závažné. Znamená to, že jednotliví zaměstnanci žalobce si zřejmě mohou bez relevantního důvodu spočívajícího v předmětu jejich práce prohlížet veškeré záznamy ve vězeňském informačním systému.

Žalovaný k otázce zabezpečení osobních údajů dále uvádí, že § 13 zákona č. 101/2000 Sb. zahrnuje celý komplex činností a opatření, které je každý správce povinen učinit. Z ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. vyplývá cíl a smysl těchto opatření, tedy zabránit tomu, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, přičemž k tomuto v daném případě nepochybně došlo. Zákon č. 101/2000 Sb. poté v § 13 odst. 3 stanovuje, jakým způsobem správce posuzuje některá rizika, přičemž přijatá opatření by měla zajistit, aby zaměstnanci plnili pokyny pro zpracování osobních údajů, aby opatření zabránila neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje. V případě automatizovaného zpracování, kterým nepochybně vězeňský informační systém je, je poté dle odst. 4 uvedeného ustanovení povinností správce zajistit, aby systém používaly pouze oprávněné osoby a aby tyto osoby měly přístup pouze k údajům odpovídajícím oprávnění těchto osob.

Žalovaný je toho přesvědčení, že informační systém obsahující osobní údaje vězňů nemůže být nastaven tak, aby mělo cca 5.000 osob (tj. 1/2 všech zaměstnanců žalobce) přístup ke všem osobním údajům vězňů, které jsou v něm evidovány. Takto široce nastavená přístupová práva sama o sobě vytvářejí riziko zneužití osobních údajů ze strany zaměstnanců a správci (žalobci) neumožňují efektivní kontrolu toho, zda zaměstnanci svá přístupová práva nezneužívají a nevynášejí osobní údaje. Žalovaný tedy konstatuje, že žalobce nedostatečně vyhodnotil rizika zpracování osobních údajů, neboť přijatá opatření neumožňují zajistit, aby zaměstnanci plnili pokyny pro zpracování osobních údajů, a aby přijatá opatření (nastavení přístupu) bránilo neoprávněnému čtení, vytváření, kopírování atd. osobních údajů.

Žalovaný poté uvádí, že porušení povinnosti dle § 13 zákona č. 101/2000 Sb. nezávisí na konkrétním počtu osob s přístupem, jak naznačuje žalobce, ale na jejich pracovním zařazení a úkolech ve spojení s nastaveným oprávněním přístupu. Žalovaný tedy uvádí, že není nejmenší důvod pro to, aby např. vychovatelé, psychologové a zvláštní pedagogové měli přístup k osobním údajům vězňů mimo věznici, kde jsou zaměstnáni. Je poté nepochybně možné systém nastavit tak, aby v případě přesunu vězně získali přístup k údajům tohoto konkrétního vězně (a to např. na základě systémového nastavení, tj. vložení pokynu k přesunu do systému, které by automaticky zpřístupnilo údaje oprávněným osobám v cílové věznici, nebo na základě dodatečného schválení nadřízeným). Proto ani důvody uváděné žalobcem neshledává žalovaný relevantními pro nastavení informačního systému zjištěným způsobem.

Žalovaný tedy výše uvedené shrnuje tak, že dle jeho názoru z ustanovení § 13 zákona č. 101/2000 Sb. vyplývá povinnost každého správce nastavit přístupová práva k osobním údajům takovým způsobem, aby byl schopen relevantně vysvětlit důvodnost a nezbytnost přístupu konkrétního zaměstnance, přičemž toto nastavení musí z důvodu zajištění ochrany osobních údajů vycházet z minimálního rozsahu přístupových práv (s případnými výjimkami stanovovanými a případně i schvalovanými individuálně) a nikoliv z maximálního možného nastavení jako v případě žalobce. V opačném případě ztrácejí bezpečnostní opatření a nastavení přístupových práv svůj hlavní smysl, a to omezit počet osob s přístupem k osobním údajům a předejít tak jejich neoprávněnému zneužití. Teprve na tato opatření navazují další, jako je např. logování přístupu, která ovšem sama o sobě zneužití osobních údajů nezabrání a působí až následně při vyšetřování.

K otázce liberace dle § 46 odst. 1 zákona č. 101/2000 Sb. žalovaný odkazuje na napadená rozhodnutí, přičemž se nejednalo o rozkladovou námitku žalobce (a ani tuto námitku neuplatnil v prvostupňovém řízení) a v tomto smyslu je tedy jako žalobní námitka pro žalovaného nesrozumitelná.

K chybné aplikaci § 45 odst. 1 zákona č. 101/2000 Sb. žalovaný uvádí, že argumentace žalobce by možná platila ve chvíli, kdy by toto ustanovení znělo „Právnická nebo fyzická osoba podnikající...". Za platného znění je zřejmé, že uvedené ustanovení rozlišuje dvě skupiny subjektů správního deliktu, na straně jedné právnickou osobou, a na straně druhé fyzickou osobou podnikající podle zvláštních předpisů, přičemž spojka „nebo" bez čárky zde vyjadřuje slučovací význam ve smyslu volby alternativy (viz např. prirucka.ujc.cas.cz).

K odpovědnosti státu za správní delikt žalovaný uvádí, že stát je i v oblasti veřejného práva nepochybně právnickou osobou (veřejnoprávní korporací). Stát má tedy správněděliktní odpovědnost za svoje jednání. Žalovaný v podrobnostech odkazuje na rozsudek Nejvyššího správního soudu čj. 2 As 36/2004-46 ze dne 11. listopadu 2004 (č. 475/2005 Sb. NSS), který tento závěr potvrzuje. Dále lze *a contrario* odkázat na § 6 odst. 1 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, a důvodovou zprávu k tomuto zákonu.

Závěrem žalovaný uvádí, že nijak nezpochybňuje, že ke zveřejnění osobních údajů v kauze MUDr. Davida Ratha došlo osobním pochybením konkrétních zaměstnanců, toto pochybení však bylo ovšem umožněno pochybením na straně žalobce při nastavení přístupových práv. Ačkoliv lze souhlasit s žalobcem, že žádné nastavení oprávnění v informačním systému neumí zabránit individuálnímu selhání lidského faktoru, je povinností každého správce v souladu s § 13 zákona č. 101/2000 Sb. těmto rizikům na straně lidského faktoru předcházet a minimalizovat je; toto žalobce neučinil.

III.

S ohledem na uvedené se žalovaný domnívá, že žaloba je nedůvodná a založená na nesprávném právním názoru žalobce, a proto navrhuje, aby byla zamítnuta jako nedůvodná (§ 78 odst. 7 s.ř.s.).

Úřad pro ochranu osobních údajů
RNDr. Igor Němec, předseda Úřadu