Zn. SPR-6781/09-74

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., 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 10. února 2010 takto:

Je prokázáno, že účastník řízení: Česká republika – Státní ústav pro kontrolu léčiv, se sídlem Šrobárova 48, 100 41 Praha 10, IČ: 00023817, v souvislosti se zpracováním osobních údajů v centrálním úložišti elektronických receptů (dále jen „centrální úložiště“) v době od ledna 2009 do září 2009 tím,
že stanovil účel tohoto zpracování jako shromáždění relevantních dat o humánních léčivých přípravcích v celém distribučním řetězci, a to v souvislosti s působností Státního ústavu pro kontrolu léčiv, dále jako plnění úkolů a působnosti Státního ústavu pro kontrolu léčiv na úseku dohledu nad jakostí léčivých přípravků a bezpečnosti při jejich používání a na úseku zajištění a provozování systému farmakovigilance, dále jako splnění požadavku sledovatelnosti a dohledatelnosti cesty každého léčivého přípravku v celém řetězci od výroby až po spotřebitele, dále jako splnění povinnosti Státního ústavu pro kontrolu léčiv zajistit předání informací shromážděných v rámci systému farmakovigilance ostatním členským státům v Evropské lékové agentuře, dále pro zvolení správného řešení každého konkrétního případu a pro zvolení nejvhodnější formy stahování léčivého přípravku z oběhu, či jiných obdobných opatření, dále pro splnění požadavku operativně, účinně a adekvátně v národním prostředí reagovat na opatření přijatá Evropskou komisí, Evropskou lékovou agenturou, dalšími orgány Evropské unie a WHO, a dále pro pomoc při plnění úkolů v oblasti cenové a úhradové agendy léčivých přípravků,
dále tím, že zpracovával bez souhlasu osobní údaje osob, kterým byl vydán léčivý přípravek na základě listinného receptu v lékárně připojené k centrálnímu úložišti, a osob, kterým byl vydán léčivý přípravek bez lékařského předpisu s omezením, v obou případech v rozsahu identifikační údaje pacienta (číslo pojištěnce nebo jméno, příjmení, datum narození a adresa), kód zdravotní pojišťovny, identifikace lékárny a údaje o vydaném léčivém přípravku,
a dále tím, že vůči centrálnímu úložišti byla při přenosu osobních údajů mezi lékárnou a centrálním úložištěm autentizována celá lékárna a ne jednotlivé fyzické osoby (lékárníci),

spáchal správní delikt podle § 45 odst. 1 písm. a) zákona č. 101/2000 Sb., neboť nestanovil účel, prostředky nebo způsob zpracování, nebo stanoveným účelem zpracování porušil povinnost nebo překročil oprávnění vyplývající ze zvláštního

zákona, správní delikt podle § 45 odst. 1 písm. e) zákona č. 101/2000 Sb., neboť zpracovával osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně, a správní delikt podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijal nebo neprovedl opatření pro zajištění bezpečnosti zpracování osobních údajů, za což se mu v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. ukládá

pokuta ve výši 2.300.000 Kč
(slovy dva miliony tři sta tisíc korun českých)

a dále podle § 79 odst. 5 správního řádu povinnost nahradit **náklady řízení ve výši 1.000 Kč,**

obojí splatné do 30 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 pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. a), e) a h) zákona č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů v centrálním úložišti bylo zahájeno oznámením Úřadu pro ochranu osobních údajů, které bylo účastníku řízení, České republice – Státnímu ústavu pro kontrolu léčiv, doručeno dne 9. prosince 2009. Podkladem pro zahájení řízení byl písemný materiál shromážděný v rámci kontroly provedené inspektorem Úřadu pro ochranu osobních údajů Ing. Bc. Milošem Dokoupilem ve dnech 20. ledna 2009 až 15. července 2009.

Ze spisového materiálu vyplývá, že účastník řízení v souladu s § 13 odst. 3 písm. n) a § 113 odst. 13 zákona č. 387/2007 Sb., o léčivech a o změně a doplnění některých souvisejících zákonů, zřídil centrální úložiště, přičemž v době od ledna 2009 přinejmenším do září 2009 v něm shromažďoval a zpracovával osobní údaje. Ze spisového materiálu, konkrétně z pokynu účastníka řízení LEK-13 vyplývá, že účastník řízení stanovil jako účel zpracování osobních údajů shromáždění relevantních dat o humánních léčivých přípravcích v celém distribučním řetězci, a to v souvislosti s působností Státního ústavu pro kontrolu léčiv; z dokumentu „Účel a rozsah zpracování dat získaných z hlášení lékáren a odůvodnění nezbytnosti rozsahu poskytovaných dat, jak byly stanoveny pokynem Ústavu“ poté vyplývá, že účastník řízení stanovil jako další účely zpracování osobních údajů plnění úkolů a působnosti Státního ústavu pro kontrolu léčiv na úseku dohledu nad jakostí léčivých přípravků a bezpečnosti při jejich používání a na úseku zajištění a provozování systému farmakovigilance, dále splnění požadavku sledovatelnosti a dohledatelnosti cesty každého léčivého přípravku v celém řetězci od výroby až po spotřebitele, dále splnění povinnosti Státního ústavu pro kontrolu léčiv zajistit předání informací shromážděných v rámci systému farmakovigilance ostatním členským státům v Evropské lékové agentuře, dále zvolení správného řešení každého konkrétního případu a pro zvolení nejvhodnější formy stahování léčivého přípravku z oběhu, či jiných obdobných opatření, dále splnění požadavku operativně, účinně a adekvátně v národním prostředí reagovat na opatření přijatá Evropskou komisí, Evropskou

lékovou agenturou, dalšími orgány Evropské unie a WHO, a dále pomoc při plnění úkolů v oblasti cenové a úhradové agendy léčivých přípravků.

Ze spisového materiálu dále vyplývá, že účastník řízení shromažďoval v centrálním úložišti osobní údaje osob, kterým byl vydán léčivý přípravek na základě listinného receptu v lékárně připojené k centrálnímu úložišti, a osob, kterým byl vydán léčivý přípravek bez lékařského předpisu s omezením, v obou případech v rozsahu číslo pojištěnce (tj. rodné číslo), kód zdravotní pojišťovny, a pokud pacient neměl přidělené číslo pojištěnce pak jméno, příjmení, datum narození a adresa, identifikace lékárny a lékárníka, údaje o vydaném léčivém přípravku [pořadové číslo položky, datum výdeje, množství, návod k použití, cena celkem, úhrada zdravotní pojišťovny, poplatek, zdravotní stav, diagnóza, započitatelný doplatek na celé množství, symbol, zda přípravek hradí pacient a dále pokud byl léčivý přípravek registrovaný, tak jednoznačný identifikační kód léčivého přípravku registrovaného účastníkem řízení, kód anatomicko-terapeuticko-chemické klasifikace léčiv (dále jen „kód ATC“), číslo šarže léčivého přípravku a čárový kód, pokud léčivý přípravek registrován nebyl tak kód, který přidělila VZP, ATC skupina, do které je léčivý přípravek zařazen, obchodní název léčivého přípravku, kód lékové formy, síla, kód balení a šarže léčivého přípravku, a čárový kód, a v případě individuálně připravovaného léčivého přípravku kód přidělený od VZP, postup přípravy léčivého přípravku, lékopisný název a množství suroviny]. Ze spisového materiálu dále vyplývá, že do centrálního úložiště bylo jenom za měsíc září odesláno přibližně 2 800 000 hlášení o vydaných léčivých přípravcích, z čehož lze důvodně usuzovat, že v centrálním úložišti byly uloženy osobní údaje osob přinejmenším v řádu statisíců.

Ze spisového materiálu konečně vyplývá, že komunikace a zasílání dat do centrálního úložiště probíhala prostřednictvím VPN (Virtual Private Network) v rámci sítě internet, kdy jednotlivé lékárny jsou vybaveny routery, které zajišťují šifrovaný přenos dat, a identifikují (autentizují) lékárnu vůči centrálnímu úložišti na základě přístupových kódů a k nim příslušných hesel. Ze spisového materiálu dále vyplývá, že účastník řízení přiděluje jednu sadu přístupových kódů a hesel pro jednu lékárnu bez ohledu na počet zde pracujících lékárníků, kteří mají mít přístup k centrálnímu úložišti.

Informace shromažďované v centrálním úložišti účastníkem řízení jsou nepochybně osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se týkají identifikovaných fyzických osob (číslo pojištěnce je současně rodným číslem a tedy jednoznačným a individuálním identifikátorem každé fyzické osoby, které bylo přiděleno). Informace o vydaných léčivých přípravcích, resp. o diagnóze, k jejíž léčbě mají sloužit, jsou informacemi, vypovídajícími o zdravotním stavu subjektu údajů, a tedy citlivými osobními údaji ve smyslu § 4 písm. b) zákona č. 101/2000 Sb. Operace prováděné s osobními údaji v centrálním úložišti jsou nepochybně operacemi, které definují zpracování osobních údajů dle § 4 písm. e) zákona č. 101/2000 Sb.

Účastník řízení stanovil účel zpracování osobních údajů v centrálním úložišti, stanovil také prostředky tohoto zpracování a zpracování sám prováděl, a je tedy správcem předmětných osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb.

Podle § 5 odst. 1 písm. a) zákona č. 101/2000 Sb. je každý správce povinen stanovit účel zpracování osobních údajů. Jak je zřejmé z výše uvedeného, účastník řízení tak učinil, přičemž stanovil řadu jednotlivých účelů zpracování. V daném případě je ovšem třeba zdůraznit, že účel zpracování nemůže být stanoven naprosto libovolně; podle čl. 6 odst. 1 písm. b) směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, mohou být osobní údaje shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní. V zákoně č. 101/2000 Sb. je toto pravidlo vyjádřeno v § 5 odst. 1 písm. a) ve spojení s § 45 odst. 1 písm. a), který upravuje skutkovou podstatu správního deliktu pro případy, kdy stanovený účel bude v rozporu s povinností vyplývající ze zvláštního zákona, nebo překročí oprávnění vyplývající ze zvláštního zákona. Účastník řízení byl nepochybně při stanovení účelu zpracování limitován tím, že je orgánem veřejné moci (správním úřadem), na který se vztahuje ústavní princip vyjádřený v čl. 2 odst. 3 Ústavy České republiky, resp. v čl. 2 odst. 2 Listiny základních práv a svobod, dle kterého lze státní moc uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví. Sběr osobních údajů o občanech státem (resp. jeho orgánem) bez jejich souhlasu je nepochybně v dané souvislosti výkonem a uplatněním státní moci vůči těmto občanům.

Ve smyslu shora uvedeného je tedy zřejmé, že účastník řízení byl oprávněn stanovit účel zpracování osobních údajů v centrálním úložišti jenom v tom rozsahu, který mu vyplýval z výslovného zákonného zmocnění. V daném případě z § 13 odst. 3 písm. n) zákona č. 378/2007 Sb. jednoznačně vyplývá oprávnění účastníka řízení v oblasti humánních léčiv zřídit a provozovat centrální úložiště. Současně ovšem uvedené ustanovení jednoznačně vymezuje účel tohoto centrálního úložiště, a tedy i účel zpracování osobních údajů, a to jako sběr a zpracování elektronicky předepisovaných léčivých přípravků. Ještě podrobněji jsou poté jednotlivé povinnosti účastníka řízení v souvislosti s centrálním úložištěm vyjádřeny v § 81 zákona č. 378/2007 Sb., přičemž všechny zde uvedené úkoly opět souvisejí jenom a pouze s elektronickými recepty.

Pokud tedy účastník řízení vymezil účely zpracování osobních údajů tak, jak je shora uvedeno, správní orgán konstatuje, že pro tento postup neměl žádnou oporu v zákoně, neboť stanovené účely nijak nesouvisely se sběrem a zpracováním elektronicky předepisovaných léčivých prostředků, a nelze je proto podřadit pod ustanovení § 81 zákona č. 378/2007 Sb. Správní orgán proto dospěl k závěru, že účastník řízení těmito stanovenými účely překročil oprávnění vyplývající ze zákona, konkrétně ze zákona č. 378/2007 Sb., a naplnil tak skutkovou podstatu správního deliktu dle § 45 odst. 1 písm. a) zákona č. 101/2000 Sb.

V této souvislosti správní orgán konstatuje, že s odkazem na čl. 10 odst. 3 Listiny základních práv a svobod a na povinnosti stanovené zákonem č. 101/2000 Sb. je zcela nepřípustné, aby jakýkoli státní orgán svévolně rozšiřoval své kompetence vymezené právními předpisy, a bez řádné opory v zákoně zřídil a provozoval informační systém sdružující rozsáhlé množství osobních a dokonce i citlivých údajů.

Podle § 5 odst. 2 zákona č. 101/2000 Sb. je správce osobních údajů povinen zpracovávat osobní údaje pouze se souhlasem subjektu údajů nebo v případech

uvedených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Podle § 9 zákona č. 101/2000 Sb. je poté správce povinen zpracovávat osobní údaje pouze s výslovným souhlasem subjektu údajů [§ 9 písm. a) zákona č. 101/2000 Sb.], nebo bez tohoto souhlasu v případech uvedených v § 9 písm. b) až i) zákona č. 101/2000 Sb.

Ze spisového materiálu je zřejmé, že souhlasem subjektů údajů účastník řízení nedisponoval. Účastník řízení proto mohl shromažďovat a dále zpracovávat osobní a citlivé údaje osob, kterým byl vydán léčivý přípravek na listinný recept v lékárně připojené k centrálnímu úložišti, a osobám, kterým byl vydán léčivý přípravek bez lékařského předpisu s omezením, pouze za naplnění některé z výjimek ze souhlasu. Správní orgán přitom neshledal, že by byla naplněna některá z možných výjimek, zejména dle § 5 odst. 2 písm. a), resp. § 9 písm. c) zákona č. 101/2000 Sb. Dle správního orgánu nevyplývá právní povinnost účastníkovi řízení zpracovávat osobní údaje ve shora uvedeném rozsahu a uvedeným způsobem ani z § 13 odst. 3, § 82 odst. 3 písm. d) zákona č. 378/2007 Sb., ani ze směrnice Evropského parlamentu a Rady ze dne 6. listopadu 2001 č. 2001/83/ES, o kodexu Společenství týkajícím se humánních léčivých přípravků, ani z § 67b odst. 10 písm. b) zákona č. 20/1966 Sb., o péči o zdraví lidu. Správní orgán se tedy ztotožnil ve vztahu k možným právním titulům pro zpracování osobních údajů s argumenty uvedenými v rozhodnutí předsedy Úřadu pro ochranu osobních údajů zn. INSP2-0277/09-62, resp. INSP2-0277/09-63, na které, s ohledem na to, že účastník řízení ve správním řízení žádné návrhy a námitky (ve smyslu § 68 odst. 3 správního řádu) neuplatnil, v plném rozsahu odkazuje.

Jak již bylo shora uvedeno, účastník řízení je správcem osobních údajů v centrálním úložišti. Správní orgán na základě vyhodnocení spisového materiálu dospěl k závěru, že jednotlivé lékárny, které byly připojeny k centrálnímu úložišti a které do něj předávaly osobní údaje dle pokynu účastníka řízení, byly v pozici zpracovatelů osobních údajů dle § 4 písm. k) zákona č. 101/2000 Sb. V daném případě je nepochybné, že účel a prostředky zpracování stanovil účastník řízení a pověřil jeho částí (shromažďování a předávání osobních údajů do centrálního úložiště) jednotlivé lékárny. Z uvedeného vyplývá, že jsou na straně lékáren naplněny všechny definiční znaky zpracovatele osobních údajů.

Podle § 13 odst. 1 zákona č. 101/2000 Sb. je účastník řízení jako správce osobních údajů povinen 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. Pro případy automatizovaných zpracování, kterým nepochybně zpracování osobních údajů v centrálním úložišti je, jsou bezpečnostní opatření stanovena podrobněji v § 13 odst. 4 písm. a) až d) zákona č. 101/2000 Sb. Ze spisového materiálu přitom vyplývá, že při předávání dat z lékárny do centrálního úložiště se vůči centrálnímu úložišti (tedy vůči systému pro automatizované zpracování osobních údajů) autentizuje lékárna jako celek, a nikoliv jednotlivá fyzická osoba (lékárník). Z uvedeného tedy dle správního orgánu vyplývá, že účastník řízení nesplnil povinnost dle § 13 odst. 4 písm. a) zákona č. 101/2000 Sb., tedy nezajistil, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby; v daném případě může zaslat

osobní údaje každý zaměstnanec lékárny, který zná přístupové jméno a heslo této lékárny. Účastník řízení dále nesplnil povinnost dle § 13 odst. 4 písm. b) zákona č. 101/2000 Sb., tj. aby každá fyzická osoba oprávněná k používání systému pro automatizované zpracování měla přístup k osobním údajům na základě zvláštních uživatelských oprávnění zřízených výlučně pro ni, neboť přístupové údaje a heslo jsou společné pro celou lékárnu.

Jak je shora uvedeno, jednotlivé lékárny jsou ve vztahu k údajům předávaným do centrálního úložiště v pozici zpracovatele osobních údajů; povinnosti dle § 13 zákona č. 101/2000 Sb. musí plnit jak správce osobních údajů, tak i zpracovatel. V daném případě ovšem účastník řízení jako správce nastavil sám automatizovaný systém zpracování a vydal lékárnám takové pokyny, které neumožnily, aby lékárny samy mohly splnit povinnosti dle § 13 odst. 4 zákona č. 101/2000 Sb. Z uvedeného vyplývá, že za nesplnění těchto povinností je plně odpovědný pouze účastník řízení jako správce osobních údajů.

Správní orgán je toho názoru, že důsledné posouzení všech relevantních rizik a přijetí tomu odpovídajících opatření, minimálně v míře dodržení všech povinností uvedených v § 13 zákona č. 101/2000 Sb., musí být jednou z priorit správce osobních údajů, zejména pokud dochází ke zpracování osobních a citlivých údajů v uvedeném rozsahu. Zjištěný způsob nastavení bezpečnostních opatření, resp. jejich absence, vede k závěru, že účastník řízení rizika realizovaného zpracování zásadně podcenil. Skutečnost, že v daném případě nebylo zjištěno žádné navazující zneužití osobních či citlivých údajů je tedy ryze náhodnou okolností, kterou v žádném případě nelze hodnotit ve prospěch účastníka řízení.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení svým jednáním při stanovení účelu zpracování překročil oprávnění vyplývající ze zvláštního zákona, porušil povinnost dle § 5 odst. 2, § 9 a § 13 odst. 1, 4 písm. a) a b) zákona č. 101/2000 Sb.

Při stanovení výše sankce bylo přihlédnuto zejména ke skutečnosti, že účastník řízení nebyl ze zákona vůbec oprávněn zpracovávat stanoveným způsobem osobní údaje, resp. stanovit jím vymezené účely zpracování, čímž jako orgán veřejné moci jednal v rozporu s ústavními principy, kterými je vázán a zásadním způsobem tak zasáhl do práva na ochranu soukromí a ochranu před neoprávněným shromažďováním osobních údajů. Správní orgán dále zohlednil, že neoprávněné zpracování se týkalo jak „běžných“ osobních údajů včetně rodného čísla, tak především citlivých údajů, které s ohledem na svoji povahu požívají zvýšené právní ochrany a jejich neoprávněné zpracování znamená významnější zásah do soukromí subjektů údajů. Správní orgán také přihlédl k množství neoprávněné zpracovávaných osobních údajů, které se pohybovalo v řádech statisíců dotčených subjektů osobních údajů. Po posouzení všech shora uvedených skutečností rozhodl správní orgán o uložení sankce v polovině zákonné sazby.

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z ustanovení § 79 odst. 5 správního řádu, který správnímu orgánu ukládá povinnost uložit paušální částkou náhradu nákladů řízení účastníkovi, který řízení vyvolal porušením své právní povinnosti, a z § 6 odst. 1 vyhlášky č. 520/2005 Sb., o rozsahu

hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, kterou se stanoví paušální částka nákladů správního řízení ve výši 1.000 Kč.

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

Poučení: V souladu s § 152 odst. 1 správního řádu lze u odboru správních činností proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedovi Úřadu pro ochranu osobních údajů.

Rozhodnutí je doručeno dnem převzetí stejnopisu, nejpozději ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání rozhodnutí do datové schránky.

Praha, 10. února 2010

otisk
úředního
razítka

Daniel Pospíšil
ředitel odboru správních činností