Čj. UOOU-03540/16-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., správní řád, a § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, vydává dne 13. května 2016 v souladu s § 150 odst. 1 správního řádu tento příkaz:

Je prokázáno, že účastník řízení: společnost Perfect Clinic s.r.o., se sídlem nám. Svobody 527, Lyžbice, 739 61 Třinec, IČO: 26865831, v souvislosti se zpracováním osobních údajů při poskytování zdravotních služeb pacientům, jako správce osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb.,

I. tím, že minimálně v období od 10. dubna 2013 do 2. října 2013 a v období od 20. prosince 2013 do 13. května 2015 neměl dispozici nad osobními údaji své pacientky …, nar. …, zpracovanými v souvislosti s poskytováním zdravotních služeb, když tyto v uvedeném období nebyly součástí zdravotnické dokumentace pacientky, tj. že v období od 10. dubna 2013 do 2. října 2013 neměl dispozici nad 5 fotografiemi pořízenými v souvislosti s operačním zákrokem ze dne 10. dubna 2013 ošetřujícím lékařem … prostřednictvím mobilního telefonu, v jehož paměti byly dále dlouhodobě uloženy, a v období od 20. prosince 2013 do 13. května 2015 neměl dispozici nad 1 fotografií pořízenou v souvislosti s operačním zákrokem ze dne 20. prosince 2013,

   porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost správce osobních údajů 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,

II. a dále tím, že v přesně nezjištěné době, nejméně však ke dni 7. října 2015, nezabezpečil dostatečně archiv zdravotnické dokumentace nacházející se v podzemních garážích budovy, tj. osobní údaje včetně informací vypovídajících o zdravotním stavu pacientů účastníka řízení, které jsou citlivými údaji ve smyslu § 4 písm. b) zákona č. 101/2000 Sb., neboť vstup do archivu byl zpřístupněn ze samostatné neuzamčené chodby, dveře do archivu nebyly bezpečnostní, nebyly osazeny bezpečnostním zámkem, v prostoru chodby ani samotného archivu nebyl instalován kamerový systém a dokumenty v archivu nebyly evidovány,

porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost správce osobních údajů 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,

a tím spáchal

v bodě I a II 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 15.000 Kč
(slovy patnáct 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. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je protokol o kontrole čj. UOOU-09427/15 ze dne 25. ledna 2016 pořízený podle zákona č. 101/2000 Sb. a zákona č. 255/2012 Sb., o kontrole (kontrolní řád), inspektorkou Úřadu pro ochranu osobních údajů PaedDr. Janou Rybínovou v rámci kontroly provedené u účastníka řízení ve dnech 19. září 2015 až 4. ledna 2016 a spisový materiál shromážděný v rámci této kontroly.

Z výše uvedeného spisového materiálu vyplývá, že účastník řízení je poskytovatelem zdravotních služeb (oblast plastické a estetické chirurgie), který je podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), povinen vést a uchovávat zdravotnickou dokumentaci. Zdravotnická dokumentace vztahující se k pacientům je účastníkem řízení vedena v listinné i elektronické podobě. V listinné podobě zdravotnické dokumentace jsou vedeny všechny dokumenty, které se týkají konkrétního pacienta. Do elektronické podoby nejsou převáděny všechny listinné dokumenty týkající se zdravotního stavu pacientů, např. chorobopisy, předoperační vyšetření, laboratorní vyšetření apod. Do elektronické zdravotnické dokumentace jsou ukládány všechny fotografie pořízené v rámci dokumentování zdravotnických služeb (např. před a po operaci), a to bezprostředně po pořízení fotodokumentace ošetřujícím lékařem. V souvislosti s provedením zákroku pořizuje ošetřující lékař fotodokumentaci oblasti zákroku, k čemu je používán jeden fotoaparát, který je umístěn na operačním sále, přičemž stopa po snímku není ve fotoaparátu ukládána.

Ze spisového materiálu dále plyne, že pacientka účastníka řízení, …, podstoupila u účastníka řízení celkem 3 operační zákroky, a to dne 10. dubna 2013, dne 20. prosince 2013 a dne 18. prosince 2014. V rámci všech souvisejících poskytovaných zdravotních služeb byla pořizována ošetřujícím lékařem fotodokumentace. V uvedené době, jak vyplývá ze spisového materiálu, neměl účastník řízení přijatu interní směrnici upravující postup při nakládání s obrazovou dokumentací. Tato problematika byla, až do účinnosti interní směrnice „Fotodokumentace klienta“, tj. ke dni 1. září 2014, řešena se zaměstnanci účastníka řízení ústní formou.

Ze spisového materiálu dále vyplývá, že 5 fotografií pacientky … pořídil v souvislosti s operačním zákrokem ze dne 10. dubna 2013 její ošetřující lékař … prostřednictvím mobilního telefonu, v paměti kterého byly následně dlouhodobě uloženy, což vyplývá z e-mailové komunikace mezi pacientkou … a … ze dne 2. a 3. října 2013 a 6. února 2015, získané během kontroly. Uvedené fotografie z operačního zákroku byly přehrány do databáze účastníka řízení nejpozději dne 2. října 2013.

Ze spisového materiálu též plyne, že 1 fotografie vztahující se k poskytnuté zdravotní péči pořízená v souvislosti s operačním zákrokem ze dne 20. prosince 2013 nebyla součástí zdravotnické dokumentace klientky účastníka řízení ještě dne 27. dubna 2015.

Ze spisového materiálu dále též plyne, že archiv zdravotnické dokumentace účastníka řízení se nacházel v podzemních garážích budovy, vstup do archivu byl zpřístupněn ze samostatné neuzamčené chodby, dveře do archivu nebyly bezpečnostní, nebyly osazeny bezpečnostním zámkem, v prostoru chodby ani samotného archivu nebyl instalován kamerový systém a dokumenty uložené v archivu nebyly evidovány.

Podle § 4 písm. a) zákona č. 101/2000 Sb. je osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž subjekt údajů se považuje za určený nebo určitelný, jestliže jde subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Účastník řízení pro účely vedení zdravotnické dokumentace shromažďuje a dále zpracovává mj. osobní údaje v rozsahu nezbytném pro identifikaci pacienta v souladu s § 53 odst. 2 písm. a) zákona č. 372/2011 Sb. Účastník řízení tedy zpracovává informace o pacientech (ale i dalších osobách, např. rodinných příslušnících pacientů), které jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb.

Podle § 4 písm. b) zákona č. 101/2000 Sb. je citlivým údajem mj. osobní údaj vypovídající o zdravotním stavu subjektu údajů. Účastník řízení zpracovává v souladu s § 53 odst. 2 písm. d), e) a g) zákona č. 372/2011 Sb. informace o zdravotním stavu pacienta, o průběhu a výsledku poskytovaných zdravotních služeb a o dalších významných okolnostech souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb, dále údaje zjištěné z rodinné, osobní a pracovní anamnézy pacienta, a je-li to důvodné, též údaje ze sociální anamnézy, jakož i další údaje podle tohoto zákona nebo jiných právních předpisů upravujících zdravotní služby nebo poskytování zdravotní péče. Součástí zdravotnické dokumentace tak může být, a u účastníka řízení také je, i obrazová

dokumentace související s poskytovanou zdravotní péčí. Účastník řízení tedy zpracovává citlivé údaje ve smyslu § 4 písm. b) zákona č. 101/2000 Sb.

Podle § 4 písm. e) zákona č. 101/2000 Sb. se zpracováním osobních údajů rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. Účastník řízení ve zdravotnické dokumentaci shromažďuje, uchovává a používá osobní údaje svých pacientů, a to včetně údajů citlivých, tedy je zpracovává ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. Zdravotnická dokumentace je přitom, jak výše uvedeno, účastníkem řízení vedena v listinné i elektronické podobě.

Podle § 4 písm. j) zákona č. 101/2000 Sb. je správcem osobních údajů každý subjekt, který určuje účel a prostředky zpracování osobních údajů a odpovídá za něj. Účastník řízení je zdravotnickým zařízením a poskytuje zdravotní služby na základě zákona č. 372/2011 Sb.; účel a prostředky zpracování osobních údajů ve zdravotnické dokumentaci má tedy účastník řízení stanoven § 53 odst. 1 uvedeného zákona, dle něhož je zdravotnické zařízení povinno vést a uchovávat zdravotnickou dokumentaci pacienta a nakládat s ní podle tohoto zákona a jiných právních předpisů. Zdravotnická dokumentace je podle § 53 odst. 2 uvedeného zákona souborem informací vztahujících se k pacientovi, o němž je vedena. Účastník řízení je tedy ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. správcem osobních (včetně citlivých) údajů svých pacientů.

Podle § 13 odst. 1 zákona č. 101/2000 Sb. je správce 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 neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. Splnění této povinnosti, tj. povinnosti přijmout dostatečná opatření směřující k tomu, aby osobní údaje nebyly vystaveny riziku jakéhokoli neoprávněného zpracování, předpokládá, že účastník řízení důsledně zváží veškerá rizika, která jsou s jím prováděným zpracováním osobních údajů spojená, a přijme odpovídající opatření k jejich maximálnímu vyloučení.

Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata správního deliktu je formulovaná jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. znamená to, že se správce osobních údajů dopustil také správního deliktu. Odpovědnost za správní delikt je přitom postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 101/2000 Sb. upravuje v § 46 odst. 1 liberační důvod, jehož naplněním se pachatel správního deliktu může odpovědnosti zprostit. K naplnění skutkové podstaty správního deliktu porušením povinnosti podle § 13 odst. 1 zákona č. 101/2000 Sb. přitom postačí pouze vznik stavu, kdy jsou osobní údaje určitým způsobem ohroženy, přestože doposud nedošlo nebo ani nedojde k jejich neoprávněnému zpracování.

Podle § 46 odst. 1 zákona č. 101/2000 Sb. účastník řízení za správní delikt neodpovídá, jestliže prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil. Posuzování naplnění liberačního ustanovení

je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej dle názoru správního orgánu jakkoliv předem zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Správní orgán přitom považuje za nezbytné konstatovat, že v případě § 46 odst. 1 zákona č. 101/2000 Sb. (a ostatně všech liberačních ustanovení) se přenáší důkazní břemeno na účastníka řízení a je to on, kdo musí k prokázání liberace navrhovat důkazy (srov. Mates P. a kolektiv: Základy správního práva trestního, 3. vydání, Praha: C.H. Beck, 2002, str. 12; dále také § 52 správního řádu).

Ve vztahu k výroku I správní orgán na základě shora uvedeného posoudil jednání účastníka řízení, a to že ošetřující lékař pacientky …, …, pořídil mobilním telefonem v souvislosti s operačním zákrokem ze dne 10. dubna 2013 5 fotografií, které nepřehrál neprodleně do databáze účastníka řízení, což učinil až s několikaměsíčním časovým odstupem - nejpozději dne 2. října 2013, a účastník řízení tak neměl v období od 10. dubna 2013 do 2. října 2013 nad pořízenými fotografiemi … dispozici. Takovéto dlouhodobé uložení fotografií v paměti mobilního telefonu ošetřujícího lékaře neposkytuje dostatečnou ochranu těchto snímků a takový způsob uchování součástí zdravotnické dokumentace je nutno považovat za velmi rizikový. Podle dalších zjištění 1 fotografie, pořízená v souvislosti s operačním zákrokem ze dne 20. prosince 2013, navíc nebyla součástí zdravotnické dokumentace ještě dne 27. dubna 2015. Ze strany ošetřujícího lékaře došlo ke zřejmému opomenutí a prodlevě, když tyto fotografie nebyly do zdravotnické dokumentace pacientky … nahrány bezprostředně po jejich pořízení. Správní orgán v této souvislosti dále uvádí, že v době do 1. září 2014 neměl účastník řízení přijatu interní směrnici upravující postup při nakládání s obrazovou dokumentací. Tato problematika byla až do účinnosti interní směrnice „Fotodokumentace klienta“ řešena se zaměstnanci účastníka řízení ústní formou. Jednou z kategorií opatření ve smyslu § 13 odst. 1 zákona č. 101/2000 Sb. jsou přitom vnitřní organizační opatření, tj. závazné interní normy či pokyny stanovící odpovědnost konkrétních osob za bezpečnost zpracování osobních údajů (např. organizační řád, pracovní řád apod.). Z výše uvedeného je zřejmé, že v době pořízení předmětných fotografií ošetřujícím lékařem nebyla účastníkem řízení přijata taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním, resp. citlivým údajům pacientky … zachycených na předmětných fotografiích, případně k jejich změně, zničení, ztrátě, neoprávněnému přenosu či jinému zneužití. Současně účastník řízení neměl přijaty ani dostatečné kontrolní mechanismy, které by zajistily, že takovéto pochybení bude schopen odhalit. Důsledná kontrola, byť i ústní formou nastavených pravidel pro zpracování osobních údajů, je přitom imanentní součástí plnění povinnosti podle § 13 odst. 1 zákona č. 101/2000 Sb.

Na základě výše uvedeného správní orgán dospěl v tomto bodě k závěru, že účastník řízení porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb. Současně účastník řízení ve smyslu § 46 odst. 1 zákona č. 101/2000 Sb. neprokázal, že vynaložil veškeré úsilí, které od něj bylo v dané situaci možné požadovat, aby k porušení povinnosti nedošlo (tj. minimálně neměl přijaty písemné vnitřní předpisy týkající se nakládání s obrazovou fotodokumentací a současně neměl nastaveny kontrolní mechanismy, které by nesprávnému postupu zabránily, či jej odhalily).

Ve vztahu k výroku II správní orgán na základě shora uvedeného posoudil jednání účastníka řízení, a to ponechání zdravotnické dokumentace (tj. též informací

vypovídající o zdravotním stavu pacientů účastníka řízení, které jsou citlivými údaji) v archivu, který se nacházel v podzemních garážích budovy, přičemž vstup do archivu byl zpřístupněn ze samostatné neuzamčené chodby, dveře do archivu nebyly bezpečnostní, nebyly osazeny bezpečnostním zámkem, v prostoru chodby ani samotného archivu nebyl instalován kamerový systém a dokumenty uložené v archivu nebyly evidovány. Takovýto způsob zabezpečení zdravotnické dokumentace je dle názoru správního orgánu zcela nedostatečný, protože není schopen zabránit rizikům neoprávněného přístupu či jinému neoprávněnému zpracování osobních údajů, které jsou ve zdravotnické dokumentaci obsaženy. Účastník řízení tak porušil povinnost stanovenou mu § 13 odst. 1 zákona č. 101/2000 Sb. V návaznosti na tento závěr správní orgán posoudil jednání též z hlediska ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán v této souvislosti uvádí, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.). Účastníkem řízení přijaté technické zabezpečení prostor, kde je umístěn archiv se zdravotnickou dokumentací pacientů, nelze považovat z hlediska zákona č. 101/2000 Sb. za dostatečné. Ochraně osobních údajů v lékařské praxi je třeba věnovat zvláštní pozornost, neboť součástí zdravotnické dokumentace jsou, jak již bylo opakovaně uvedeno, z velké části údaje citlivé, které vyžadují s ohledem na svůj charakter přísnější ochranu. K tomuto typu opatření patří i náležitý stupeň ochrany prostor a objektů, kde jsou osobní údaje uchovávány, před náhodným i úmyslným neoprávněným vstupem (vloupáním) a odcizením dat. Správní orgán má proto za prokázané, že účastník řízení nevynaložil veškeré úsilí, které bylo možné požadovat, a že nepochybně existovaly další možnosti, jak mohl postupovat, aby protiprávnímu následku, tj. ohrožení jím uchovávaných osobních údajů, zabránil; minimálně přijmout další základní technická opatření potřebných k zabezpečení a ochraně uvedených prostor jako např. mříže, či bezpečnostní zámky doplněné poplašnými, protipožárními či kamerovými systémy. Je potřeba zdůraznit, že odpovědnost za porušení tohoto zákona v takovém případě vzniká bez ohledu na následek, tedy zda se s obsahem dokumentů někdo nepovolaný seznámil či nikoli.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutková zjištění za dostatečná a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním vymezeným ve výroku tohoto příkazu povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Podle § 46 odst. 2 zákona č. 101/2000 Sb. při rozhodování o výši pokuty se přihlíží zejména k závažnosti, způsobu, době trvání a následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno.
Při stanovení výše sankce jako k přitěžující okolnosti bylo správním orgánem přihlédnuto zejména k charakteru osobních údajů obsažených ve zdravotnické dokumentaci, tj. informací vypovídajících o zdravotním stavu, které jsou citlivými údaji ve smyslu § 4 písm. b) zákona č. 101/2000 Sb. a požívají vyšší míru právní ochrany. Dále bylo správním orgánem přihlédnuto ke skutečnosti, že s ohledem na množství a charakter ohrožených osobních údajů nacházejících se ve zdravotnické

dokumentaci umístěné v archivu je nesplnění základních technických opatření k jeho zabezpečení hrubým porušením povinnosti zabezpečit osobní údaje. Přitěžující okolností je dále to, že účastník řízení spáchal více správních deliktů.

Po souhrnném zhodnocení výše uvedených okolností případu uložil správní orgán sankci při dolní hranici 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 příkazu.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u oddělení správních činností proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen 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 příkazu do datové schránky.

Praha, 13. května 2016

otisk
úředního
razítka

Vanda Foldová
vedoucí oddělení správních činností