ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-04073/18-5

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 46 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v řízení o přestupku vedeném podle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, a zákona č. 500/2004 Sb., správní řád, rozhodl dne 23. května 2018 takto:

Společnost [redacted], se sídlem [redacted],

I. se uznává vinnou ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijala nebo neprovedla opatření pro zajištění bezpečnosti zpracování osobních údajů, tím, že nezabezpečila osobní údaje nejméně 735 956 zákazníků v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účtu, případně telefon, před neoprávněným přístupem v období minimálně od 31. prosince 2014 do srpna 2017, v důsledku čehož došlo v době od 27. července 2017 do 25. srpna 2017 k jejich zpřístupnění na serveru [redacted],

čímž porušila 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, k jejich změně, zničení, či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů,

II. za což se jí podle § 35 písm. b) zákona č. 250/2016 Sb. a v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. ukládá

pokuta ve výši 1.500.000 Kč
(slovy jeden milion pět set tisíc korun českých)

III. 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 obviněné, konstantní symbol 1148.

Odůvodnění

Správní řízení pro podezření ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů zákazníků, bylo zahájeno oznámením Úřadu pro ochranu osobních údajů (dále jen „Úřad“), které bylo obviněné, společnosti [redacted], doručeno dne 24. dubna 2018. Podkladem pro zahájení řízení byl spisový materiál shromážděný v rámci kontroly provedené u obviněné inspektorem Úřadu MVDr. Františkem Bartošem ve dnech 2. října 2017 až 6. dubna 2018.

Ze spisového materiálu vyplývá, že obviněná v rámci svého podnikání provozuje e-shop a spravuje uživatelské účty svých zákazníků. Úřadu obviněná dne 27. srpna 2017 sdělila, že dne 25. srpna 2017 zaznamenala narušení bezpečnosti při správě osobních údajů. Mělo se jednat o uživatelské účty, které obsahovaly jednoduchá hesla. V systémech obviněné dochází k tzv. „hashování hesel“, kdy jsou hesla uložena v zakódované podobě. Dotčená databáze byla zakódovaná starším, dnes již nepoužívaným způsobem, tzv. [redacted].

Dle sdělení obviněné byly učiněny kroky k minimalizaci následků narušení bezpečnosti. Konkrétně došlo k resetu hesel všech potencionálně ohrožených uživatelských účtů založených před rokem 2015, došlo k písemnému informování dotčených subjektů údajů a také k posílení centra zákaznické péče.

Ze záznamu o bezpečnostní události a výsledcích interního šetření provedeného obviněnou vyplývá, že k bezpečnostní události došlo dne [redacted], kdy neznámá osoba odcizila obviněné databázi záznamů o zákaznících. K nahrání souboru obsahujícího databázi zákazníků obviněné na server [redacted], která obsahovala osobní údaje v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účty a v některých případech také telefonní číslo, došlo dne [redacted] nepřihlášeným uživatelem. Z interní zprávy dále vyplývá, že incident se týkal [redacted] záznamů z roku 2014, z nichž 735 956 obsahovalo unikátní e-mailovou adresu zákazníka.

V rámci provedené kontroly předložila obviněná interní předpisy upravující přijatá technicko-organizační opatření v oblasti ochrany osobních údajů. Z dokumentu označeného jako „[redacted]“ ze dne 1. ledna 2011 vyplývá, že obviněná upravila pravidla pro užívání informačních a komunikačních technologií (dále jen „ICT“) pro soukromé účely v pracovní i mimopracovní době a oprávnění zaměstnanců nakládat s ICT (měnit a zasahovat do konfigurace technických prostředků, užívání flash disků, externích disků, paměťových karet atd.). [redacted]. Dalším předpisem týkajícím se zabezpečení osobních údajů je dokument označený jako „[redacted]“ přijatý dne 1. ledna 2013. Tento předpis upravuje postupy při zjištění bezpečnostního incidentu a jeho řešení, a dále deklaruje, že pro účely detekce události je v systémech spravovaných obviněnou zavedeno automatické hlášení nestandardních stavů. [redacted]

[redacted]

Vnitřní předpis „Směrnice o ochraně osobních údajů zákazníků“ aktualizovaná ke dni 1. dubna 2013 se věnuje zpracování osobních údajů zákazníků, upravuje postavení obviněné jako správce, účel zpracování, povinnosti při zpracování i rozsah zpracovávaných osobních údajů. [redacted] Současně směrnice upravuje minimální standardy ochrany osobních údajů zákazníků, které musí být na pracovišti dodržovány (např. přístup k datům je vyhrazen pouze pověřeným zaměstnancům obviněné, obviněná vede evidenci a dokumentaci všech případů porušení ochrany zpracovávaných dat, obviněná dále zajistí průběžná školení pověřených osob, zajistí rovněž zavedení opaření bránících neoprávněnému nebo nahodilému přístupu k osobním údajům, zajistí odpovídající úroveň šifrování/hashování osobních údajů, zajistí postupy pravidelného testování, posuzování a hodnocení účinnosti přijatých technicko-organizačních opatření, atd.).

Osobním údajem je podle § 4 písm. a) zákona č. 101/2000 Sb. jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze 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. Údaji zpracovávanými obviněnou jsou jméno, příjmení, e-mailová adresa, korespondenční adresa, heslo uživatelského účtu, telefon a informace o uzavřených obchodech. Na základě těchto údajů lze konkrétní fyzickou osobu jednoznačně identifikovat, jedná se tedy o osobní údaje ve smyslu zákona č. 101/2000 Sb.

K předmětu řízení správní orgán uvádí, že správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Předmětem podnikání obviněné je provozování nákupní galerie, v souvislosti s touto činností také spravuje uživatelské účty svých zákazníků. Je tedy zřejmé, že určila účel i způsob zpracování osobních údajů svých zákazníků a je správcem těchto údajů.

Podle § 4 písm. e) zákona č. 101/2000 Sb. je zpracováním 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. Obviněná osobní údaje svých zákazníků shromažďuje, uchovává, využívá jej za účelem provedení obchodů, provádí tedy jejich zpracování.

Jako na správce osobních údajů se na obviněnou vztahují povinnosti vyplývající ze zákona č. 101/2000 Sb. Jednou z nich je též povinnost stanovená 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, k jejich změně, zničení či

ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Skutková podstata přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. je naplněna již v situaci, kdy zpracovávaným osobním údajům hrozí (v důsledku nepřijetí či neprovedení dostatečných organizačních a technických opatření) riziko nesprávného či neoprávněného zpracování. V případě obviněné je přitom zřejmé, že prokazatelně došlo k odcizení databáze zákazníků, a to již v roce 2014, přičemž tuto událost zjistila až následně poté, co došlo k jejímu zveřejnění.

Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata je formulovaná jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. (neoprávněnému přístupu k osobním údajům apod.), což je v této věci nepochybné, znamená to, že se správce osobních údajů dopustil také přestupku.

Odpovědnost za přestupek právnických osob je přitom postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 250/2016 Sb. upravuje v § 21 odst. 1 liberační důvod, jehož naplněním se pachatel přestupku může odpovědnosti zprostit. Právnická osoba tedy za přestupek neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby přestupku zabránila. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej předem jakkoliv zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Správní orgán přitom považuje za nezbytné konstatovat, že v případě ustanovení § 21 odst. 1 zákona č. 250/2016 Sb. (a ostatně všech liberačních ustanovení) se přenáší důkazní břemeno na obviněnou a je to ona, 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).

Správní orgán tedy na základě shora uvedeného posuzoval jednání obviněné z hlediska ustanovení § 21 odst. 1 zákona č. 250/2016 Sb. a 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.).

Správní orgán po zhodnocení všech výše uvedených skutečností dospěl k závěru, že v případě obviněné § 21 odst. 1 zákona č. 250/2016 Sb. nelze aplikovat. V daném případě je správní orgán názoru, že se ze strany obviněné nejednalo o vynaložení maximálně možného úsilí k ochraně zpracovávaných osobních údajů, neboť jí nastavené mechanismy pro zabezpečení osobních údajů nedokázaly detekovat ani vznik bezpečnostního incidentu, tj. odcizení databáze, a rovněž tak mu nedokázaly zabránit.

Správní orgán tak považuje na základě výše uvedeného za prokázané, že obviněná porušila svým jednáním 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, k jejich změně, zničení, či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tím spáchala přestupek podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb.

Při posouzení možného zániku odpovědnosti ze strany obviněné vycházel správní orgán ze skutečnosti, že nesplnění povinnosti podle § 13 zákona č. 101/2000 Sb., které je vymezeno ve výroku tohoto rozhodnutí, je svou povahou deliktem trvajícím, neboť došlo k vyvolání protiprávního stavu, který byl po daný čas udržován. Doba pro zánik odpovědnosti přitom běží od ukončení protiprávního stavu, neboť tato skutečnost je rozhodná pro spáchání přestupku. K ukončení protiprávního stavu však došlo až resetováním hesel uživatelských účtů, tedy přijetím nových opatření pro zabezpečení osobních údajů zákazníků ze strany obviněné, a to po té, co došlo k zveřejnění zcizené databáze prostřednictvím serveru [redacted]

Podle § 5 zákona č. 250/2016 Sb. je přestupkem společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

Podle § 37 zákona č. 250/2016 Sb. se při určení druhu správního trestu a jeho výměry přihlédne zejména k povaze a závažnosti přestupku, k přitěžujícím a polehčujícím okolnostem a k povaze činnosti obviněného. Při stanovení správního trestu tak správní orgán přihlédl především k povaze a závažnosti přestupku, přičemž má na základě § 38 zákona č. 250/2016 Sb. za to, že závažnost přestupku zvyšuje počet dotčených subjektů údajů, jejichž osobní údaje nebyly řádně zabezpečeny. Závažnost také zvyšuje doba, po kterou protiprávní stav trval, a skutečnost, že součástí databáze byla i uživatelská hesla. Pokud se týká povahy činnosti obviněného, je dle správního orgánu profesionálem v oboru, kde dochází k rozsáhlému zpracování osobních údajů, což míru škodlivosti přestupku zvyšuje. Skutečnost, že po zjištění incidentu, učinila obviněná okamžité kroky k nápravě, hodnotil správní orgán jako polehčující okolnost podle § 39 zákona č. 205/2016 Sb. Přitěžující okolnosti ve smyslu 40 zákona č. 250/2016 Sb. ve věci správní orgán neshledal.

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

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z § 95 odst. 1 zákona č. 250/2016 Sb., který správnímu orgánu ukládá uložit obviněnému, který byl uznán vinným, náklady řízení paušální částkou, 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, podle kterého paušální částka nákladů správního řízení, které účastník vyvolal porušením své právní povinnosti, činí 1.000 Kč.

Poučení: V souladu s § 152 odst. 1 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedkyni 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 23. května 2018

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního