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-04073/18-25

ROZHODNUTÍ

Předseda Úřadu pro ochranu osobních údajů jako odvolací orgán příslušný podle § 2, § 29 a § 32 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a § 152 odst. 2 zákona č. 500/2004 Sb., správní řád, rozhodl podle ustanovení § 152 odst. 6 písm. a), § 152 odst. 5 a § 90 odst. 1 písm. b) zákona č. 500/2004 Sb., správní řád, takto:

Rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-5 ze dne 23. května 2018 **se zrušuje a věc se vrací správnímu orgánu prvního stupně k novému projednání.**

Odůvodnění

I. Vymezení věci

/1/ Podkladem k zahájení správního řízení pro podezření ze spáchání přestupku vedeného Úřadem pro ochranu osobních údajů (dále jen „Úřad“) s obviněnou, společností XXXXXX, se sídlem XXXXXX (dále jen „obviněná“), byl spisový materiál shromážděný v rámci kontroly provedené u obviněné inspektorem Úřadu MVDr. Františkem Bartošem a ukončené protokolem o kontrole čj. UOOU-08428/17-31 ze dne 21. března 2018.

/2/ Ze spisového materiálu vyplynulo, že obviněná v rámci svého podnikání provozuje e-shop a spravuje uživatelské účty svých zákazníků. V této souvislosti obviněná dne 27. srpna 2017 sdělila Úřadu, 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 totiž bylo prováděno tzv. „XXXXXXX“, kdy jsou hesla uložena v zakódované podobě. Nicméně dotčená databáze byla zakódovaná starším, dnes již nepoužívaným způsobem, tzv. XXXXX. 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, dále byly dotčené subjekty údajů písemně informovány a také bylo posíleno centrum zákaznické péče.

/3/ Ze záznamu o bezpečnostní události a výsledcích interního šetření provedeného obviněnou vyplynulo, že k bezpečnostní události došlo dne 31. prosince 2014, kdy neznámá

osoba odcizila obviněné databázi záznamů o zákaznících. K následnému nahrání souboru obsahujícího databázi zákazníků obviněné na server XXXXX, která obsahovala osobní údaje v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účtu a v některých případech také telefonní číslo, došlo dne 27. července 2017 nepřihlášeným uživatelem. Z interní zprávy dále vyplynulo, že incident se týkal 766 421 záznamů z roku 2014, z nichž 735 956 obsahovalo unikátní e-mailovou adresu zákazníka.

/4/ Na základě takto zjištěného stavu věci měl správní orgán prvního stupně za prokázané, že obviněná nepřijala nebo neprovedla opatření pro zajištění bezpečnosti zpracování předmětných osobních údajů svých zákazníků před neoprávněným přístupem v období minimálně od 31. prosince 2014 do srpna 2017 a v důsledku tohoto v době od 27. července 2017 do 25. srpna 2017 došlo ke zpřístupnění uvedených osobních údajů na serveru XXXXXX. Tím obviněná porušila povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, 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. Z těchto důvodů byla rozhodnutím čj. UOOU-04073/18-5 ze dne 23. května 2018 (dále též jen „rozhodnutí“) uznána vinnou ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. a byla jí uložena pokuta ve výši 1.500.000 Kč.

/5/ Úřad tedy vyvozoval, že prvotním záměrem ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. bylo zakotvit povinnost přijmout určitá opatření. Tato ovšem musí mít kvalitu v té míře, aby bylo zabráněno zneužití osobních údajů, jak se dále uvádí v ustanovení § 13 zákona č. 101/2000 Sb. Dojde-li tedy k předmětnému incidentu, který navíc obviněná v reálném čase ani nezaznamenala, je toto nutno a priori chápat jako nesplnění předmětné povinnosti, a tudíž správce (pro tento případ obviněná), jenž nezabránil úniku osobních údajů, zároveň nezajistil bezpečnost zpracování osobních údajů tak, aby byly splněny podmínky stanovené v § 13 zákona č. 101/2000 Sb., čímž se dopustil přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. postihujícího správce, který nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů. Zároveň ovšem nebylo nijak vyloučeno přiznat liberační důvody dle § 21 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, kdy ovšem bylo na obviněné, aby prokázala veškeré, tedy maximální úsilí, které je možno požadovat. Jedině takovýto výklad, jak se Úřad domníval, by nevedl k popření, resp. formalizaci povinností, které má správce v oblasti zabezpečení ve vztahu k jím zpracovávaným osobním údajům. Tento výklad pak vycházel také z recitálu 46 někdejší směrnice Evropského parlamentu a Rady 95/46/ES, který ve vztahu ke zpracování osobních údajů primárně ukládal, aby byla zajištěna bezpečnost a bylo zabráněno jakémukoli neoprávněnému zpracování, resp. recitálu 10 téhož dokumentu, z něhož se vyvozuje, že právní předpisy o zpracování osobních údajů mají za cíl zajistit dodržování základních práv a svobod, a proto implementace směrnice Evropského parlamentu a Rady 95/46/ES nesmí vést k oslabení ochrany.

/6/ Rozhodnutí obviněná napadla řádným rozkladem, který ovšem předsedkyně Úřadu svým rozhodnutím čj. UOOU-04073/18-11 ze dne 21. září 2018 zamítla. Proti tomuto rozhodnutí předsedkyně Úřadu se obviněná ohradila správní žalobou zamítnutou rozsudkem Městského soudu v Praze čj. 6A 188/2018-57 ze dne 24. června 2021, který však obviněná napadla kasační stížností. Té pak Nejvyšší správní soud rozsudkem čj. 1 As 238/2021 ze dne 11. listopadu 2021 vyhověl a rozsudek Městského soudu v Praze čj. 6A 188/2018-57 ze dne

24. června 2021 i rozhodnutí předsedkyně Úřadu čj. UOOU-04073/18-11 ze dne 21. září 2018 zrušil.

/7/ Svůj rozsudek čj. 1 As 238/2021 ze dne 11. listopadu 2021 pak Nejvyšší správní soud odůvodnil především tím, že v rámci předchozích řízení mělo být považováno za zásadní, zda došlo k ochraně osobních údajů, potažmo zda obviněná zneužití osobních údajů včas odhalila. Vzhledem k tomu, že se tak nestalo, nemělo být zapotřebí zabývat se kvalitou obviněnou přijatých opatření. Jinak řečeno, pokud obviněná osobní údaje neochránila a ani včas nezjistila, že k odcizení došlo, je bez dalšího zjevné, že jí přijatá opatření byla nedostatečná. Na podporu tohoto tvrzení bylo poukázáno i na skutečnost, že přestupek dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. představuje tzv. ohrožovací delikt, pročež postačí, pokud pouze hrozí (v důsledku nedostatečných opatření) neoprávněné nakládání s osobními údaji. Jestliže však k uvedenému negativnímu následku v posuzované věci došlo, nemělo být o naplnění skutkové podstaty přestupku pochyb. S tímto se však Nejvyšší správní soud neztotožnil. Vyjádřil sice souhlas s tím, že pro vznik odpovědnosti za přestupek podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. stačí ohrožení bezpečnosti osobních údajů. Znakem skutkové podstaty dotčeného přestupku tedy není existence následku v podobě neoprávněného nakládání s osobními údaji. To však ještě neznamená, že by existence takového následku vedla bez dalšího k závěru, že správce či zpracovatel osobních údajů si počínal v rozporu s § 13 odst. 1 zákona č. 101/2000 Sb. Posledně citované ustanovení upravuje povinnost „*přijmout taková opatření, aby nemohlo dojít 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*“. Přestože jeho dikce vyznívá poněkud striktně, nelze z ní činit kategorický závěr, že za dostatečná lze považovat pouze taková opatření, která v každém myslitelném případě zabrání zneužití osobních údajů. Nejvyšší správní soud totiž zdůraznil, že nelze vycházet toliko z jazykového výkladu, ale je třeba mít na zřeteli rovněž smysl a účel citovaného ustanovení. V této souvislosti měla posloužit jako výkladové vodítko evropská úprava, v níž nachází citované ustanovení svůj předobraz. Čl. 17 odst. 1 směrnice 95/46/ES pak hovoří o nutnosti přijetí „vhodných opatření“, která mají zajistit „s ohledem na stav techniky a na náklady na jejich provedení přiměřenou úroveň bezpečnosti“. Uvedená úprava tedy nevyznívá ani zdaleka tak přísně jako § 13 odst. 1 zákona č. 101/2000 Sb.

/8/ Odpovědnost za přestupek podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. („*Právnická nebo podnikající fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů…nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů.*“) tak není vázána na vznik poruchového negativního následku spočívajícího v neoprávněném nakládání s osobními údaji, ale na zjištěný deficit v přijetí náležitých opatření za účelem jejich ochrany. Jinak řečeno, pro vznik odpovědnosti za přestupek není rozhodující, zda se osobní údaje v konečném důsledku podaří ochránit či nikoliv. V praxi to pak znamená, že přestupku podle citovaného ustanovení se dopustí osoba, která nepřijme dostatečná opatření za účelem ochrany osobních údajů, a to i v situaci, kdy k neoprávněnému nakládání s těmito údaji nedojde. Častější variantu pak bude představovat situace, kdy k negativnímu následku v podobě neoprávněného nakládání s údaji dojde. V takovém případě se však musí Úřad zabývat tím, jaká opatření dotčený subjekt přijal a dodržoval.

/9/ Nejvyšší správní soud pak považoval za zásadní, že Úřad nezjistil, jakým způsobem k úniku dat došlo. Současně se Úřad měl odmítnout zabývat tím, jaká byla kvalita opatření,

která obviněná přijala a dodržovala v době odcizení dat. Obviněnou tak shledal odpovědnou ze spáchání přestupku podle § 45 odst. 1 písm. h) č. 101/2000 Sb., ačkoliv neznal žádnou ze stran rovnice, z nichž jednu tvoří právě opatření za účelem ochrany osobních údajů, druhou pak způsob odcizení dat ze strany neznámého subjektu. Proto Nejvyšší správní soud shledal kasační stížnost obviněné důvodnou.

II. Posouzení odvolacím orgánem

/10/ Úřad je názorem Nejvyššího správního soudu vyjádřeným v rozsudku čj. 1 As 238/2021 ze dne 11. listopadu 2021 vázán (viz § 78 odst. 5 zákona č. 150/2002 Sb., soudní řád správní).

/11/ Dále je třeba připomenout, že odvolací orgán s ohledem na ustanovení § 152 odst. 6 písm. a) a § 90 odst. 1 písm. c) zákona č. 500/2004 Sb., správní řád, jelikož by obviněné hrozila újma z důvodu ztráty možnosti uplatnit opravný prostředek, není legitimován k tomu, aby ve věci rozhodl tak, že by rozhodnutí správního orgánu prvního stupně čj. UOOU-04073/18-5 ze dne 23. května 2018 bylo změněno v souladu s požadavky uvedenými v rozsudku Nejvyššího správního soudu čj. 1 As 238/2021 ze dne 11. listopadu 2021.

/12/ Z uvedených důvodů proto odvolací orgán rozhodl, jak je uvedeno ve výroku tohoto rozhodnutí. V následujícím řízení by proto správní orgán prvního stupně měl v souladu s požadavky rozsudku Nejvyššího správního soudu čj. 1 As 238/2021 ze dne 11. listopadu 2021 zohlednit všechna obviněnou přijatá opatření a zabývat se tím, jestli byla dostatečná, a to s ohledem na dostupnou úroveň ochrany v rozhodném období, charakter činnosti obviněné a rozsah jí zpracovávaných údajů, přičemž přihlédne ke kritériím vyplývajícím z tzv. evropské úpravy (viz zejména body 36 až 43 odůvodnění rozsudku Nejvyššího správního soudu čj. 1 As 238/2021 ze dne 11. listopadu 2021). V následujícím řízení by proto měly být zejména vyhodnoceny relevantní interní předpisy obviněné (např. uvedené na str. 3, resp. 6 protokolu o kontrole), a to z období předcházejícího úniku osobních údajů. Dále by měla být vzata v úvahu relevantní doporučení, která se věnují bezpečnosti webových služeb a také by mělo být více analyzováno tzv. provádění „XXXXX“ ze strany obviněné, včetně zjištění, zda k němu opravdu docházelo.

Poučení: Proti tomuto rozhodnutí se podle ustanovení § 91 odst. 1 zákona č. 500/2004 Sb., správní řád, nelze odvolat.

Praha 2. prosince 2021

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)