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-04073/18-11

ROZHODNUTÍ

Předsedkyně 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 podle § 10 a § 152 odst. 2 zákona č. 500/2004 Sb., správní řád rozhodla dne 21. září 2018 podle ustanovení § 152 odst. 6 písm. b) zákona č. 500/2004 Sb., správní řád, takto:

Rozklad obviněné, společnosti se sídlem proti rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-5 ze dne 23. května 2018, **se zamítá a napadené rozhodnutí se potvrzuje.**

Odůvodnění

Podkladem k zahájení správního řízení pro podezření ze spáchání přestupku vedeného Úřadem pro ochranu osobních údajů (dále jen „Úřad“) s obviněnou, společností se sídlem (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.

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. „hashování hesel“, kdy jsou hesla uložena v zakódované podobě. Nicméně dotčená databáze byla zakódovaná starším, dnes již nepoužívaným způsobem, tzv. . Dle sdělení obviněné byly učiněny kroky k minimalizaci následků narušení bezpečnosti. Konkrétně došlo k resetu hesel všech potencionálně ohrožených uživatelských účtů založených před rokem , dále byly dotčené subjekty údajů písemně informovány a také bylo posíleno centrum zákaznické péče.

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

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 . 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 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.

Rozhodnutí ovšem obviněná napadla včasným rozkladem. V něm rozhodnutí, s ohledem na údajně téměř absentující odůvodnění, kvalifikovala jako zcela nepřezkoumatelné. Dále, jak se obviněná domnívá, mělo být prokázáno splnění liberačních podmínek podle § 21 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Proto navrhla rozhodnutí zrušit a předmětné řízení zastavit.

V této souvislosti obviněná především polemizovala se závěrem správního orgánu prvního stupně o tom, že dojde-li k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb., znamená to, že se správce osobních údajů dopustil přestupku. Ve skutkové podstatě přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., jak obviněná uvedla, není uvedeno nic o následku a není proto zřejmé, jak správní orgán prvního stupně k tomuto závěru došel. Naopak ze samotné formulace tohoto ustanovení má vyplývat, že povinnost se vztahuje na přijetí patřičných opatření, přičemž pro vznik odpovědnosti není nastalý následek podstatný. Odpovědnost za nepřijetí vhodných opatření vznikne i tehdy, pokud k žádnému následku nedojde a samotný vznik následku nevypovídá nic o tom, zda ze strany správce došlo nebo nedošlo k porušení povinnosti. Následkem je, dle názoru obviněné, v tomto případě přijetí nebo nepřijetí patřičných opatření k ochraně osobních údajů.

Dále obviněná argumentovala tím, že opatření přijatá podle § 13 odst. 1 zákona č. 101/2000 Sb. musí odpovídat povaze a rozsahu zpracování, druhu a množství zpracovávaných údajů a účelu zpracování. Nejedná se tedy o hledisko objektivní, ale posuzuje se pro konkrétní případ. Zkoumání, zda bylo naplněno liberační ustanovení je tak třeba provádět ve vztahu k jednání, které ze strany obviněné předcházelo nepřijetí opatření podle § 13 zákona č. 101/2000 Sb. Liberační důvody, tedy vynaložení maximálního úsilí, by se pak zkoumalo ve vztahu k tomu, jaké jednání obviněná vykonala, aby povinnost splnila. Kvalifikační kritérium pro liberaci se tak má vztahovat pouze na činnosti směřující k tomu,

aby nedošlo k předvídanému následku. Požadovat po obviněné vynaložení maximálního úsilí je dle jejího právního zástupce v rozporu s textem zákona, neboť to nevyplývá ze žádného právního předpisu. V této souvislosti pak obviněná odkázala na komentář k zákonu č. 101/2000 Sb., dle kterého „opatření mají zajistit, s ohledem na stav techniky a náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny."

Následně obviněná popsala všechna jí přijatá opatření organizačního a technického charakteru, která byla implementována a jejich plnění kontrolováno. Jednotlivé technologie zároveň měly být v průběhu času aktualizovány či kompletně měněny s ohledem na technologický pokrok. V této souvislosti obviněná namítla, že se rozhodnutí nevypořádalo s existencí přijatých opatření a nebylo provedeno jejich kritické hodnocení a srovnání. Má tudíž za to, že nebyla prokázána nedostatečnost provedených opatření. Ty považuje za odpovídající účelu, povaze a rozsahu zpracování, druhu a množství zpracovávaných údajů. Zároveň ovšem obviněná nepopírá, že došlo k bezpečnostnímu incidentu, nicméně k němu nedošlo v důsledku porušení povinností obviněnou, ale v důsledku jednání neznámé osoby. Tímto jednáním mohl být neoprávněný vnik do systému zvenčí nebo exces zaměstnance nebo dodavatele systému, což dle názoru právního zástupce nemůže být přičitatelné obviněné.

K charakteru jednání, které bylo správním orgánem prvního stupně kvalifikováno jako trvající delikt, obviněná uvedla, že není jasné, kdy jí provedená opatření měla přestat splňovat kritéria presumována zákonem a kdy tak došlo ke vzniku protiprávního stavu a poté k jeho ukončení. S ohledem na technologický vývoj a implementaci nových technologií dochází průběžně k zesilování úrovně zabezpečení jednotlivých systémů a rovněž tak dochází k úpravě procesů při práci s osobními údaji. Vztáhne-li se trvání protiprávního jednání na část databáze, která byla předmětem incidentu, nemůže jít o trvající delikt, neboť tato databáze není nadále v držení obviněné a k dokonání deliktu došlo okamžikem oddělení. V tomto případě by tak došlo k zániku odpovědnosti za přestupek, která by se vzhledem k době jeho spáchání posuzovala dle předchozí platné úpravy (§ 46 odst. 3 zákona č. 101/2000 Sb.).

Odvolací orgán přezkoumal rozhodnutí v celém rozsahu, včetně procesu, který předcházel jeho vydání a nejprve se zabýval argumentací obviněné.

V této souvislosti ovšem považuje za nezbytné především předeslat, že správce osobních údajů, kterým je, jak již ostatně konstatovalo odůvodnění rozhodnutí, právě obviněná, má podle ustanovení § 13 odst. 1 zákona č. 101/2000 Sb., o jehož aplikaci se v tomto případě jedná, 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. V rámci tohoto pak je také povinen posuzovat určitá rizika a splnit další povinnosti vymezené v § 13 odst. 3 a 4 zákona č. 101/2000 Sb., k nimž kupříkladu náleží i posuzování rizik ve vztahu k zabránění neoprávněným osobám přistupovat k osobním údajům apod. Tudíž pouhým gramatickým výkladem je možno jednoznačně dovodit, že prvotním záměrem uvedeného ustanovení je zakotvit povinnost přijmout určitá opatření. Tato ovšem musí mít kvalitu v té míře, aby bylo zabráněno zneužití osobních údajů, jak je uvedeno v ustanovení § 13 zákona č. 101/2000 Sb. Dojde-li tedy k předmětnému incidentu, je toto nutno a priori chápat jako nesplnění předmětné povinnosti.

S tím koresponduje i vymezení skutkové podstaty přestupku dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. postihujícího správce, který nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů. Na doplnění je možno odkázat i na argumentaci Nejvyššího správního soudu k problematice objektivní odpovědnosti za správní delikt v rozsudku čj. 9 As 36/2007-59 ze dne 24. ledna 2008, byť v jiné oblasti veřejného práva. Z ní ovšem lze obecně vyvodit, že pojem zajistit je nutno interpretovat jako jistou garanci a nikoli pouze jako vytvoření určitých podmínek pro zajištění žádoucího stavu.

Jinými slovy řečeno, správce, jenž nezabránil úniku osobních údajů, zároveň nezajistil bezpečnost zpracování osobních údajů tak, aby byly splněny podmínky stanovené v § 13 zákona č. 101/2000 Sb. a dopustil se tudíž přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. Takto je třeba chápat i obviněným připomínané odkazy na odbornou literaturu. Přijetí argumentace obviněné by pak vedlo k úplnému popření smyslu, resp. formalizaci povinností, které má správce v oblasti zabezpečení ve vztahu k jím zpracovávaným osobním údajům.

Co se týká konkrétních okolností traktovaného případu, odvolací orgán shledal, že bylo zcela nepochybně prokázáno odcizení části databáze záznamů o zákaznících obviněné. Jak k tomuto došlo, obviněná nezjistila ani v průběhu času, ani na základě jí deklarované aktualizace přijatých opatření. Je tudíž zjevné, že opatření přijatá k zabezpečení zpracovávaných údajů nesplňovala podmínky, které stanoví zákon č. 101/2000 Sb. Navíc vzhledem k těmto okolnostem nelze opatření existující v době incidentu jakkoli spolehlivě hodnotit, a tudíž je již pojmově vyloučeno obviněné přiznat liberační důvody dle § 21 odst. 1 zákona č. 250/2016 Sb., kdy se vyžaduje prokázat veškeré, tedy maximální úsilí, které je možno požadovat.

Nicméně správní orgán prvního stupně správně zhodnotil, a to ve prospěch obviněné, okamžik zjištění úniku dat a přikročení k resetu hesel, jímž byla eliminována zřejmá, ovšem nikoli v uvedených souvislostech naprosto jednoznačně určující bezpečnostní slabina, jako dobu ukončení protiprávního stavu. Teprve tímto dnem počala, v souladu s § 30 písm. b) a § 31 odst. 2 písm. c) zákona č. 250/2016 Sb. a i v souladu s někdejším § 46 odst. 3 zákona č. 101/2000 Sb., běžet tříletá promlčecí lhůta. Pokud by totiž byl kupříkladu přijat výklad obviněné, podle něhož je třeba trvání protiprávního jednání vztáhnout na část databáze, která byla předmětem incidentu, bylo by nutno konstatovat, že skutek nebyl dosud dokonán, jelikož tato databáze není nadále v držení obviněné, a to se všemi důsledky. Z druhé strany ovšem samotný fakt, že se osobní údaje dostaly do držení jiné osoby, nezbavuje obviněnou jejích povinností resp. odpovědnosti ve vztahu k údajům, které jsou předmětem zpracování, které provádí, neboť ona byla jejich správce a měla právě takovémuto jednání resp. stavu předejít. Jako počátek vzniku protiprávního stavu pak bylo, a to opět ve prospěch obviněné, stanoveno samotnou obviněnou vymezené datum odcizení databáze, jelikož tento teoreticky mohl být posunut resp. rozšířen k datu, od kterého fungovala opatření představující relevantní bezpečnostní slabinu.

Pro úplnost možno dodat, že předmětného přestupku by se obviněná, resp. kterýkoli správce či zpracovatel dopustili i za situace naprosté absence předmětných opatření anebo za situace přijetí zjevně nedostatečných opatření, a to aniž by došlo k jakémukoli bezpečnostnímu incidentu, což však není tento případ.

Rozhodnutí pak je, byť v poněkud stručné podobě, řádně odůvodněno a s vývody správního orgánu prvního stupně se odvolací orgán ztotožňuje. To, že s tímto odůvodněním obviněná nesouhlasí, nelze chápat jako jeho absenci, navíc zakládající nepřezkoumatelnost rozhodnutí.

Zároveň byla posouzena i nová právní úprava obsažená v nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), nicméně tato, jak odvolací orgán shledal, nemá na posouzení věci žádný vliv.

Argumentaci obviněné proto odvolací orgán odmítl. Po celkovém přezkoumání pak odvolací orgán konstatuje, že v postupu správního orgánu prvního stupně neshledal žádná pochybení. Na základě všech výše uvedených skutečností proto rozhodl tak, jak je uvedeno ve výroku tohoto rozhodnutí.

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

Praha 21. září 2018

otisk úředního razítka

JUDr. Ivana Janů, v. r.
předsedkyně

Za správnost vyhotovení: