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-04073/18-50

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) zákona č. 500/2004 Sb., správní řád, takto:

I. Rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-41 ze dne 17. června 2022 se **mění** tak, že:

1. z výroku II. rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-41 ze dne 17. června 2022 se vypouští slova: „podle § 35 písm. b) zákona č. 250/2016 Sb. a“,

2. do výroku III. rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-41 ze dne 17. června 2022 se za slova „podle § 95 odst. 1 zákona č. 250/2016 Sb.“ doplňují slova „a vyhlášky 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, ve znění vyhlášky č. 112/2017 Sb.“,

II. ve zbytku se rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-41 ze dne 17. června 2022 potvrzuje a rozklad obviněné, společnosti [redacted] proti rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-41 ze dne 17. června 2022, **se zamítá.**

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 Internet [redacted] (dále jen „obviněná“), byl spisový materiál shromážděný v rámci kontroly provedené u obviněné podle zákona

č. 255/2012 Sb., o kontrole (kontrolní řád), 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 sice bylo prováděno tzv. „hashování hesel" a hesla tedy byla uložena v zakódované podobě. Nicméně dotčená databáze byla zakódovaná starším, dnes již nepoužívaným způsobem, tzv. metodou SHA1 + unikátní solí. V důsledku toho, podle 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 ulozto.cz, 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 jakožto správce 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 www.ulozto.cz. 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 správce a zpracovatele *„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 uznána vinnou ze spáchání přestupku 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 (§ 13)."*) a byla jí uložena pokuta ve výši 1.500.000 Kč.

/5/ Úřad tehdy 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 ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále „směrnice 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 95/46/ES nesmí vést k oslabení ochrany osobních údajů.

/6/ Rozhodnutí čj. UOOU-04073/18-5 ze dne 23. května 2018 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. [redacted], který však obviněná napadla kasační stížností. Té pak Nejvyšší správní soud rozsudkem čj. [redacted] vyhověl a rozsudek Městského soudu v Praze [redacted] i rozhodnutí předsedkyně Úřadu čj. UOOU-04073/18-11 ze dne 21. září 2018 zrušil.

/7/ Svůj rozsudek čj. [redacted] 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, bylo podle Úřadu i Městského soudu v Praze 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 postačuje, 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. postačuje 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. Přestože dikce posledně připomenutého ustanovení 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 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. tudíž, jak uvedl Nejvyšší správní soud, 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) zákona 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.

/10/ Rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04073/18-5 ze dne 23. května 2018 bylo návazně rozhodnutím předsedy Úřadu čj. UOOU-04073/18-25 ze dne 2. prosince 2021 zrušeno a věc vrácena správnímu orgánu prvního stupně k novému projednání.

/11/ Výsledkem nového projednání pak bylo vydání rozhodnutí Úřadu čj. UOOU-04073/18-41 ze dne 17. června 2022 (dále jen „rozhodnutí“). Jím byla obviněná uznána vinnou tím, že v období ode dne 31. prosince 2014 nejméně do dne 27. srpna 2017 jako správce osobních údajů svých zákazníků používala k hashování nejméně 735 956 hesel k zákaznickým účtům nedostatečně odolné hashovací algoritmy, a to algoritmus MD5 a algoritmus SHA-1 s kryptografickou solí, přičemž opatření spočívající v resetování stávajících hesel k zákaznickým účtům hashovaných výše uvedenými hashovacími algoritmy a hashování nově vygenerovaných hesel dostatečně odolným hashovacím algoritmem bcrypt provedla až ke dni 27. srpna 2017, poté, co se dozvěděla, že po úniku databáze jejích zákazníků byla hesla zákazníků hashovaná algoritmy MD5 a SHA-1 s kryptografickou solí v plně čitelné podobě spolu s dalšími kategoriemi osobních údajů jejích zákazníků nejméně v rozsahu jméno, příjmení a e-mailová adresa zveřejněna neznámou osobou na internetových stránkách www.ulozto.cz. Tím obviněná porušila § 13 odst. 1 zákona č. 101/2000 Sb. a spáchala přestupek podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., za což jí byla uložena pokuta ve výši 140.000 Kč.

/12/ Proti rozhodnutí doručenému dne 22.června 2022 se však obviněná ohradila řádným rozkladem podaným dne 7. července 2022, následně doplněným přípisem ze dne 22. července 2022.

II. Obsah rozkladu

/13/ V podaném rozkladu obviněná především napadla samotné vymezení porušení právní povinnosti, co do rozsahu a určení v čase, jelikož byla v této souvislosti ve výroku rozhodnutí užita slova „*nejméně*“, což má rozšiřovat význam a rozsah přestupku. Dále nemělo být prokázáno porušení povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb. Z uvedených důvodů obviněná navrhla napadené rozhodnutí zrušit a řízení zastavit.

/14/ K tomu obviněná konkrétně uvedla, že podle první části výroku rozhodnutí vytýkané porušení právní povinnosti trvalo „*nejméně do dne 27.srpna 2017*“, nicméně v rozporu s tím se v druhé části výroku konstatuje ukončení protiprávního stavu ke dni 27. srpna 2017.

/15/ Ve výroku rozhodnutí se také, jak obviněná připomenula, konstatuje, že vytýkaný přestupek se týká „*nejméně 735 956 hesel k zákaznickým účtům*“, což je více než bylo prokázáno. Počet 735 956 hesel pak koresponduje s počtem hesel, která byla součástí uniklé databáze a nelze ji zaměňovat s „*živou*“ databází užívanou obviněnou. Dále obviněná uvedla, že hesla uživatelů, kteří se ke svému účtu na předmětné nákupní galerii přihlásili v období počínaje listopadem roku 2016, byla převedena na novou účinnější metodu hashování, stejně tak byla touto metodou hashována hesla u nově zřizovaných účtů. V období roku 2017 tedy bylo z uvedených 735 956 hesel zhruba 350 000 hesel hashováno nejnovější technologií. Nadto není možné odvozovat rozsah porušení povinnosti z počtu uživatelských údajů, které se v návaznosti na protiprávní jednání neznámé osoby objevily na stránkách uložto.cz, jelikož se uniklá databáze nacházela ve stavu, do kterého již obviněná nemohla zasáhnout, přičemž k úniku mohlo dojít v době, kdy zabezpečení metodou SHA-1 bylo zcela dostatečné.

/16/ Úřad dále, podle názoru obviněné, neprovedl dokazování dostatečné pro hodnocení zabezpečení předmětného zpracování osobních údajů, jelikož se primárně opíral výhradně o odborný posudek Národního úřadu pro kybernetickou bezpečnost čj. 4177/2022-NÚKIB-E/320 ze dne 11. dubna 2022 a nezkoumal toto zabezpečení komplexně. Namísto toho zjednodušeně dovodil, že pokud obviněná v roce 2013 používala jiný algoritmus než bcrypt a do 31. prosince 2014 na něj nepřešla, dopustila se počínaje 1. lednem 2015 přestupku. Úřad tedy, podle názoru obviněné, nehodnotil integritu a bezpečnost předmětného zpracování jako celek a pominul některé důležité složky jako je např. míra fyzického zabezpečení serverů před neoprávněným přístupem apod. Stejně tak neměl být vzat v úvahu ani běh času, jelikož předmětná část databáze měla být pravděpodobně odcizena před rokem 2014, kdy byla dostatečně zabezpečena a k jejímu prolomení pravděpodobně došlo až v roce 2017.

/17/ Obviněná také shledala některé závěry uvedené v odborném posudku Národního úřadu pro kybernetickou bezpečnost čj. 4177/2022-NÚKIB-E/320 ze dne 11. dubna 2022 jako zjednodušené či teoretické a nereflektující zavedenou praxi. Primárně se jedná o tvrzení, podle něhož měl být bcrypt od roku 2013 průmyslovým standardem používaným mj. i při vývoji e-shopových řešení, jelikož v uvedeném roce se bcrypt teprve začínal prosazovat. Lze sice z ryze technického hlediska souhlasit s názorem vysloveným v uvedeném dokumentu, podle něhož je pro implementaci nového řešení do existujícího systému potřebný čas jednoho roku, ve skutečnosti je ale třeba započítat i další obviněnou připomenuté okolnosti, které lhůtu potřebnou pro implementaci prodlužují. To má v zásadě potvrzovat i dokument Národního bezpečnostního úřadu (dále „NBÚ“) s názvem „*Prohlášení NBÚ k využívání*

hashovacích funkcí" zmiňovaný v bodě 22 odůvodnění rozhodnutí, který stanovuje předmětnou lhůtu v horizontu 3 až 5 let.

/18/ Obviněná, jak má vyplývat z jí poskytnutých podkladů a vyjádření, měla v průběhu času přijímat různá organizační a technická opatření k zabezpečení zpracovávaných osobních údajů. Co se týká hesel, byla zvolena strategie podpory legacy protokolů a postupné změny hesel zákazníky. Zbytek databáze byl převeden na algoritmus bcrypt resetem hesel a zasláním obnovovacích emailů dotčeným zákazníkům jako reaktivní opatření na zjištěný bezpečnostní incident a toto byl jediný realistický způsob přechodu mezi jednotlivými metodami hashování hesel. V této souvislosti obviněná obecně konstatovala, že řádně implementovala nové technologie v okamžiku, kdy se stávaly standardem, tedy přijímala taková opatření a v takové době, kdy to vůči ní bylo možné s ohledem na rozsah, účely a kategorie zpracovávaných osobních údajů spravedlivě požadovat.

/19/ Obviněná také považuje odkaz na dokument *„Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu"* v bodě 23 odůvodnění rozhodnutí za zcela irelevantní.

III. Posouzení odvolacím orgánem

/20/ Odvolací orgán přezkoumal napadené rozhodnutí v celém rozsahu, včetně procesu, který předcházel jeho vydání, a především se zabýval argumentací obviněné.

/21/ Ohledně časového rámce přestupkového jednání obviněné vymezeného ve výroku rozhodnutí, jímž je období ode dne 31. prosince 2014 nejméně do 27. srpna 2017, z čehož lze, podle názoru obviněné, vyvozovat, že porušení relevantní povinnosti mohlo trvat i déle než do dne 27. srpna 2017, což má být v rozporu s další částí téhož výroku, v němž se konstatuje, že protiprávní stav byl ukončen ke dni 27. srpna 2017, jakož i s odůvodněním napadeného rozhodnutí, odvolací orgán na základě jazykového výkladu slov „ode dne 31. prosince 2014 nejméně do 27. srpna 2017" shledal, že posledním dnem trvání protiprávního stavu mohl být právě den 27. srpna 2017. Užití slova „nejméně" při časovém určení přestupku by se proto mohlo jevit nanejvýše jako nadbytečné, nikoli však jako rozporné ve vztahu k další části výroku o vině či k odůvodnění napadeného rozhodnutí. Je totiž zjevné, že výrok rozhodnutí nekonstatuje ukončení protiprávního stavu ke dni 27. srpna 2017, nýbrž pouze provedení opatření směřující k jeho odstranění.

/22/ Ohledně argumentace obviněné týkající se nesprávného vymezení rozsahu přestupkem dotčených osobních údajů založené mimo jiné na tom, že použitím slova „nejméně" před počtem dotčených hesel k zákaznickým účtům čítajícím 735 956 bylo de facto ve výroku rozhodnutí uvedeno „více hesel", než kolik má podle odůvodnění rozhodnutí za prokázané, odvolací orgán konstatuje, že uvedení slova „nejméně" před počtem hesel k zákaznickým účtům, které nebyly v rozhodném období zabezpečeny dostatečně odolným hashovacím algoritmem, neodporuje skutkovým zjištěním uvedeným v odůvodnění napadeného rozhodnutí. Uvedený počet hesel k zákaznickým účtům, které nebyly zabezpečeny dostatečně odolným hashovacím algoritmem v rozhodném období, totiž je třeba chápat jako nejmenší prokázaný počet. Při jeho stanovení pak bylo vycházeno z podkladů předložených obviněnou. Podle jejího „Záznamu o bezpečnostní události a výsledcích šetření" ze dne 8. září 2017 se bezpečnostní incident týkal 766 421 záznamů o zákaznících z roku 2014,

přičemž zhruba 735 956 jich obsahovalo unikátní e-mailovou adresu. Obviněná však rovněž uvedla, že počet hesel k zákaznickým účtům zřízeným před 1. lednem 2015, jež v rámci opatření resetovala a převedla na hashovací algoritmus bcrypt, čítal kolem 1 300 000 těchto hesel, což je uvedeno i v odůvodnění napadeného rozhodnutí. I v těchto souvislostech tak je třeba mít za to, že užití slova „nejméně“ by se mohlo jevit nanejvýš jako nadbytečné, nikoli však jako skutečnost zakládající rozpor výroku o vině ve vztahu k odůvodnění rozhodnutí. Dále je na tomto místě nutno podotknout, že vzhledem k charakteru vytýkaného protiprávního jednání obviněné nelze v popisu skutku z objektivních důvodů zachytit přesný počet hesel zákaznických účtů zabezpečených nedostatečně odolným hashovacím algoritmem (SHA-1 s kryptografickou solí anebo MD5) v průběhu trvání přestupku, neboť tento se v jejím průběhu zřejmě měnil. Ke změně hashovacího algoritmu zabezpečujícího jednotlivá hesla totiž docházelo u zákaznických účtů zřízených před listopadem 2016 nikoli „plošně“, ale na základě (z pohledu obviněné) nahodilé události představované přihlášením jednotlivých zákazníků do jejich zákaznických účtů (vizte níže). Touto skutečností podmíněné případné nedostatky popisu skutku však nemají vliv na podstatu přestupku obviněné – opomenutí povinnosti obviněné poskytnout přiměřenou úroveň ochrany heslům zákaznických účtů. Z dikce výroku pak je nutno vyvozovat, že časové určení přestupku mezi dnem 31. prosince 2014 nejméně ke dni 27. srpna 2017 nelze chápat tak, že oněch nejméně 735 956 hesel bylo nedostatečně hashováno po celou tuto dobu, ale po nějaké údobí v rámci tato vymezeného časového úseku, přičemž obviněná v žádném případě nebyla rozhodnutím sankcionována ani za vadné hashování přesahující počet 735 956 hesel k zákaznickým účtům, ani za vadné hashování po dni 27. srpna 2017.

/23/ Nadto odvolací orgán podotýká, že účelem dostatečně určitého popisu skutku ve výroku rozhodnutí je zejména vyloučení zaměnitelnosti se skutkem jiným. To potvrdil i Nejvyšší správní soud v rozsudku čj. [redacted], který mimo jiné uvedl: *„Aprobovat lze rovněž závěr krajského soudu, dle kterého požadavek na dostatečnou identifikaci postihovaného skutku souvisí především s vyloučením možnosti jeho zaměnitelnosti se skutkem jiným. Z usnesení rozšířeného senátu Nejvyššího správního soudu ze dne 15. 1. 2008, č. j. 2 As 34/2006-73, se podává, že výrok rozhodnutí o jiném správním deliktu musí obsahovat popis skutku uvedením místa, času a způsobu spáchání, popřípadě i uvedením jiných skutečností, jichž je třeba k tomu, aby nemohl být zaměněn s jiným. V rozhodnutí, jímž se trestá za spáchaný správní delikt, je nezbytné postavit najisto, za jaké konkrétní jednání je subjekt postižen. To lze zajistit jen dostatečnou konkretizací údajů, které skutek charakterizují. Taková míra podrobnosti je nezbytná pro celé řízení, a to zejména pro vyloučení překážky litispendence, dvojího postihu pro týž skutek, pro vyloučení překážky věci rozhodnuté, pro určení rozsahu dokazování a pro zajištění řádného práva na obhajobu (obdobně například rozsudek tohoto soudu ze dne 26. 9. 2019, č.j. 2 As 271/2018-44). Měřítkem, jímž na výrok prvoinstančního rozhodnutí nahlížel i krajský soud, je tedy zásadně jeho nezaměnitelnost. Nejde tak o požadavek na jeho vymezení maximálně možným podrobným způsobem* […].“ Časové vymezení přestupku obsažené v rozkladem napadeném rozhodnutí přitom, jak shledal odvolací orgán, požadavky na nezaměnitelnost skutku s jiným skutkem zcela splňuje. Současně nedošlo k ohrožení správné aplikace vyloučení překážky litispendence, dvojího postihu pro týž skutek, pro vyloučení překážky věci rozhodnuté, pro určení rozsahu dokazování a pro zajištění řádného práva na obhajobu.

/24/ Ohledně argumentace vytýkající to, že integrita a bezpečnost systémů nebyla posuzována jako celek, ale bylo přistoupeno k fragmentárnímu hodnocení, a tedy nebyla hodnocena např. míra fyzického zabezpečení serverů před neoprávněným přístupem, míra

zabezpečení síťového provozu, řízení uživatelských práv či dalších složek zabezpečení zpracování osobních údajů jako celku, přičemž byl hodnocen pouze jeden ze sekundárních prvků zabezpečení bez dalších souvislostí a jeho zařazení do celkového systému zabezpečení, je třeba předně uvést, že při hodnocení bezpečnostních opatření obviněné vztahujících se ke zpracování osobních údajů bylo vycházeno z vnitřních předpisů předložených obviněnou. Ty přitom obsahovaly soupis nejen organizačních opatření, ale rovněž i opatření technických (např. čl. 5 Interního předpisu 2013-1-2: Směrnice o ochraně osobních údajů zákazníků společnosti [redacted] či jejích dceřiných společností na území České republiky). Není proto pravdou, že by správní orgán prvního stupně technická opatření vůbec neposuzoval. Bezpečnostní opatření zpracování osobních údajů zákazníků obviněné v rozhodné době tak správní orgán prvního stupně posuzoval komplexně. Pokud pak obviněná namítá, že Úřad veškeré vyšetřovaní směřoval k předmětné části databáze a nezmapoval úroveň zabezpečení systémů obviněné jako celku (zejména v období od 1. ledna 2015 do listopadu 2016 a dále od listopadu 2016 do 27. srpna 2017), je třeba konstatovat, že obviněnou předložené listinné podklady (např. relevantní vnitřní předpisy), jakož i další podklady rozhodnutí poskytující dílčí informace o technických opatřeních přijatých obviněnou (např. Q&A - Vše, co jste chtěli vědět o bezpečnosti na [redacted] Blog [redacted] se vztahují k celému takto vymezenému období.

/25/ Za stěžejní však odvolací orgán pokládá skutečnost, že použití hashovacího algoritmu pro hesla uživatelských účtů představuje sekundární technické opatření. Takto jej ostatně vnímá i sama obviněná, jelikož ve svém vyjádření ze dne 15. ledna 2018 k povaze tohoto technického opatření uvedla: *„V dnešní době je běžné, že se útočníci, jejichž cílem je odcizení databáze, zaměřují primárně na technické mezery v systémech, které však nelze přikládat k tíži správce. Uvedené nedostatky nejsou při vývoji software a jiných aplikací neobvyklé, proto jsou k počítačovým aplikacím jejich tvůrci více či méně pravidelně vydávány různé aktualizace, typicky zaměřené na ‚zalepení' bezpečnostních děr (viz např. široce využívaný operační systém Windows). Právě z toho důvodu je kladen důraz na sekundární typ ochrany, tedy nemožnost data rozšifrovat."* Ze zmíněné „sekundárnosti" tohoto technického opatření pak vyplývá jeho (do jisté míry) svébytná povaha. Zásadně se totiž sekundární typ ochrany uplatní v případě, kdy primární technická (a organizační) opatření selžou a uplatnění této sekundární ochrany tak na účinek primárních opatření nemá přímý vliv. V obecné rovině proto lze shledat, že působení primárních a sekundárních opatření je komplementární. Zákon č. 101/2000 Sb. v § 13 odst. 1, jak již ostatně bylo uvedeno výše, ukládal správci 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, přičemž nestanovil závazné konkrétní způsoby, jak má správce ochranu zpracovávaných osobních údajů zabezpečit. Proto vždy záleží na správci, jaká opatření zvolí, tedy i to, zda bude těžiště jím přijatých organizačních a technických opatření spočívat v oblasti ochrany primární či (s vědomím či předpokladem, že tato opatření primární ochrany možnost úniku osobních údajů nevyloučí) v oblasti ochrany sekundární. Zjištění Úřadu byla vztažena jak k ochraně primární, tak k ochraně sekundární. Pokud jde o úroveň sekundární ochrany, tato je v daném případě významná právě proto, že sama obviněná poukázala na důraz, který na tento typ ochrany kladla v návaznosti na svůj postoj k setrvalém riziku vycházejícímu z „vývojových nedostatků" (každého) softwaru a jejich cíleného využívání různými útočníky; v této souvislosti nelze opominut ani skutečnost, že primární ochrana – v souladu s „předpokladem" obviněné – skutečně úniku dat nezabránila, přičemž skutečnost, že k úniku došlo, nebyla ani detekována. Právě pro tento případ – tedy pro případ úniku (který

nastal) měla být dle rozhodnutí samotné obviněné zabezpečena ochrana osobních údajů použitím hashovacích algoritmů, které měly data učinit pro útočníka nečitelnými a tedy nepoužitelnými. Není proto na překážku, pokud správní orgán prvního stupně obviněné vytýká nedostatečnost použitých hashovacích algoritmů k zabezpečení hesel k zákaznickým účtům.

/26/ Ohledně argumentace obviněné tím, že při posuzování odolnosti hashovacího algoritmu bylo vycházeno pouze z odborného posouzení Národního úřadu pro kybernetickou a informační bezpečnost (dále „NÚKIB“) a správní orgán prvního stupně se nepokusil zajistit jiný názor, důkaz či zjistit skutečný stav na trhu v rozhodném období (2013-2017), odvolací orgán předesílá, že toto odborné vyjádření nebylo pouze obecné, ale týkalo se právě posouzení konkrétních okolností projednávaného případu. V této souvislosti zdůrazňuje, že NÚKIB je podle § 21a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ústřední správní úřad pro oblast kybernetické bezpečnosti a jako takový mimo jiné podle § 22 písm. u) uvedeného zákona provádí analýzu a monitoring kybernetických hrozeb a rizik. NÚKIB je tak kompetentním orgánem pro provedení odborného vyjádření v projednávané věci, přičemž jeho odborné vyjádření obsahuje skutečnosti podstatné pro její posouzení. Správní orgán prvního stupně však při hodnocení skutkového stavu nevycházel pouze z jeho odborného vyjádření. Jmenovitě lze zmínit dokument „*Prohlášení Národního bezpečnostního úřadu k využívání hashovacích funkcí*“ ze dne 1. ledna 2007 a dokument „*Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu*“, zveřejněný Ministerstvem vnitra dne 23. června 2009 (aktualizované znění). Byť je jejich povaha pro obviněnou doporučující, oba tyto podklady shodně poukazují na nedostatečnou bezpečnost hashovacích algoritmů MD5 a SHA-1 v rozhodném období.

/27/ Obviněná také rozporovala závěr odborného vyjádření NÚKIB, že hashovací algoritmus bcrypt se od roku 2013 stal průmyslovým standardem v běžných programovacích jazycích a frameworcích určených mimo jiné pro vytváření internetových nákupních galerií. Přitom však nerozporuje, že z technického hlediska u nových systémů neexistoval důvod pro užití méně odolného hashovacího algoritmu než bcryptu. Má však za to, že užití použití hashovacího algoritmu bcrypt u již existujících systémů nebylo na relevantním trhu průmyslovým standardem a většina subjektů teprve plánovala postupný přechod na novou technologii. Svou argumentaci obviněná zakládá mimo jiné na tezi, že použití konkrétního hashovacího algoritmu se průmyslovým standardem stane v okamžiku, kdy se většina subjektů na relevantním trhu k takovému řešení přikloní a začne jej užívat. Dále obviněná poukázala na tvrzení NÚKIB, podle něhož hashovací algoritmus bcrypt se začal v roce 2013 prosazovat, čímž je, podle názoru obviněné, současně zpochybněno, že by v témže roce mohl být průmyslovým standardem. Dle názoru obviněné tento její závěr dále podporuje i doporučení National Institute of Standards and Technology (dále „NIST“) č. SP800-131A z ledna 2011, které mělo stanovit, že SHA-1 je dostatečným standardem pro užití vládními orgány a úřady do konce roku 2013. Dle obviněné je přitom případná hrozba zneužití údajů, které spravuje správní úřad kteréhokoli státu, mnohonásobně vyšší než hrozba zneužití údajů zákazníků, kterými disponuje „obyčejný“ internetový obchod, přičemž vládní a bezpečnostní instituce a subjekty kritické infrastruktury jsou podle obviněné primárními „early adopters“ nových bezpečnostních řešení a běžná komerční a open source řešení následují až s odstupem.

/28/ Z této argumentace obviněné však není zcela zřejmé, zda se vymezuje proti závěru NÚKIB, že bcrypt považuje v roce 2013 za průmyslový standard, nebo tento závěr rozporuje

„pouze“ ve vztahu k již existujícím systémům. NÚKIB k hashovacímu algoritmu bcrypt uvedl, že byl navržen již v roce 1999 a jedná se o algoritmus přímo navržený pro ukládání otisků hesel. Jeho použití se začalo prosazovat v běžných programovacích jazycích a frameworcích určených mimo jiné pro vytváření internetových nákupních galerií od roku 2013. Doplnil, že např. jazyk PHP algoritmus bcrypt implementoval v roce 2013, Zend Framework, ve své době globálně nejpoužívanější framework pro jazyk PHP, ve výchozím nastavení využívá bcrypt od roku 2012, a Nette Framework určený pro stejný programovací jazyk, ve své době nejpoužívanější v Česku, bcrypt ve výchozím nastavení používá minimálně od roku 2014. Uvedl, že v kontextu České republiky přitom byla problematika nevyhovující odolnosti algoritmu SHA-1 v kombinaci s kryptografickou solí proti útoku hrubou silou řešena na odborných konferencích určených vývojářům e-shopových řešení v roce 2013. Z těchto informací dle NÚKIB plyne, že už od roku 2013 je algoritmus bcrypt považován za průmyslový standard a u nově vznikajících systémů v té době neexistoval technický důvod využít méně odolný algoritmus. Správní orgán prvního stupně se přitom se závěry NÚKIB na základě přesvědčivosti jeho argumentace ztotožnil.

/29/ Tezi obviněné, že použití konkrétního hashovacího algoritmu se průmyslovým standardem stane v okamžiku, kdy se většina subjektů na relevantním trhu k takovému řešení přikloní a začne jej užívat, tedy že teprve od takovéhoto okamžiku je možné, aby dozorový úřad takovouto úroveň zabezpečení od správců požadoval, odvolací orgán pokládá za nesprávnou, či přesněji účelovou. Dovedením této argumentace do jejích důsledků, by totiž bylo možno dospět k závěru, že subjekty na relevantním trhu jsou takto schopné svou nečinností či liknavostí v oblasti zabezpečení „petrifikovat“ stav úrovně zabezpečení osobních údajů bez ohledu na technologický posun v dané oblasti a tedy i bez ohledu na případné zvýšení rizik s tím spojených pro subjekty údajů, a to aniž by dozorový úřad vůči nereflektování zvýšení těchto rizik mohl ve vztahu ke správci osobních údajů uplatnit své pravomoci (nápravné a sankční). Takový závěr by zjevně kolidoval s povinností správce osobních údajů podle § 13 odst. 1 zákona č. 101/2000 Sb. 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, která v sobě implicitně zahrnuje povinnost kontinuálního vyhodnocování rizik zpracování osobních údajů a přijímání adekvátních bezpečnostních opatření. To ostatně potvrzuje i komentářová literatura, která k § 13 odst. 1 zákona č. 101/2000 Sb. uvádí: *„Povinnost podle § 13 odst. 1 OchOsÚ klade na správce a zpracovatele poměrně velké nároky spočívající ve vyhodnocení všech možných rizik, která jsou s jejich činností spojena, a v důsledném přijetí a realizaci opatření, která budou obvykle představovat i nemalé finanční náklady. Současně je nutno jak rizika zpracování, tak i přijatá opatření průběžně přehodnocovat s ohledem na vývoj okolností, rozvoj technologií a efektivitu zvolených řešení. Správce či zpracovatel jsou tedy povinni reagovat i na to, že se v průběhu zpracování osobních údajů objeví nové, dosud neznámé hrozby (typicky při využívání výpočetní techniky a Internetu). S tím souvisí také to, že na základě § 13 odst. 1 OchOsÚ jsou správci a zpracovatelé osobních údajů povinni přijatá bezpečnostní opatření aktualizovat, případně také zavádět nové metody a prostředky, jestliže je to po nich možno rozumně požadovat (tj. půjde v dané oblasti a za daných okolností o opatření považované již za standardní).“*[1]

[1] *Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.*: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, s. 230.

/30/ V této souvislosti lze opakovaně poukázat i na čl. 17 odst. 1 směrnice 95/46/ES. Ten členským státům uložil stanovit, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování, k zajištění přiměřené úrovně bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny, a to s ohledem na stav techniky a na náklady na jejich provedení.

/31/ Z odborného vyjádření NÚKIB přitom zcela jednoznačně plyne, že dostatečně odolné hashovací algoritmy bcrypt (či jeho případný technologický ekvivalent) nejen že v rozhodné době byly k dispozici, ale NÚKIB je dokonce považuje za průmyslový standard v prostředí internetových obchodů (v kontextu České republiky). Odvolací orgán proto vzhledem k rizikům daného zpracování vyplývajícím z předmětu a charakteru činnosti obviněné, povahy dotčených osobních údajů – hesel zákaznických účtů a jejich vysokého množství – považuje používání hashovacího algoritmu bcrypt, resp. jeho technologického ekvivalentu (tedy algoritmu dosahujícího stejné úrovně zabezpečení jako bcrypt) v rozhodné době za technické opatření, které v této dílčí oblasti poskytuje přiměřenou, tedy dostatečné účinnou a současně dostupnou a z hlediska dozorového úřadu (ba i z hlediska samotných zákazníků) „požadovatelnou“ úroveň ochrany dotčených osobních údajů. A naopak za technická opatření poskytující přiměřenou, tedy dostačující, úroveň ochrany dotčených osobních údajů nelze v rozhodné době za uvedených okolností považovat používání hashovacích algoritmů SHA-1 s kryptografickou solí anebo MD5, a to kvůli jejich nedostatečné odolnosti. Byla to ostatně sama obviněná, která si v rámci své strategie ochrany osobních údajů zvolila sekundární technické opatření spočívající v hashování hesel zákaznických účtů a kladla na ni důraz při vědomí možnosti selhání primárních technických opatření.

/32/ Vzhledem k odmítnutí teze obviněné ohledně konstituování průmyslového standardu nelze považovat za relevantní ani navazující tvrzení obviněné, že většina subjektů na relevantním trhu teprve plánovala přechod na novou technologii ve smyslu implementace hashovacího algoritmu bcrypt (či jeho technologického ekvivalentu). Přesto je vhodné pro úplnost alespoň konstatovat, že obviněná ji nezakládá na žádných objektivních skutečnostech a jedná se pouze o její domněnku.

/33/ Argumentace obviněné doporučením NIST vydaným pod č. SP800-131A, podle kterého byl SHA-1 dostatečným standardem pro užití vládními orgány a úřady Spojených států amerických do konce roku 2013, pak nemůže obstát. Je totiž třeba zohlednit, že uvedený dokument NIST představuje doporučení entitám nacházejícím se ve Spojených státech amerických, tedy entitám, na které se zjevně nevztahovala působnost směrnice 95/46/ES ani zákona č. 101/2000 Sb. Ve vztahu k požadavkům kladeným na ochranu osobních údajů směrnicí 95/46/ES tak nemá dostatečnou vypovídací hodnotu. Navazující argumentaci obviněné ohledně mnohonásobně vyšší hrozby zneužití osobních údajů zpracovávaných správním úřadem než těch zpracovávaných internetovým obchodem a názoru o správních úřadech jako o „early adopters“ nových bezpečnostních řešení pak je třeba označit za příliš zjednodušující. Z obsahu námitky není zcela jasné, jaký význam přisuzuje slovu hrozba [např. zda jej používá ve smyslu § 2 písm. e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) nebo ve smyslu rizika podle § 2 písm. h) též vyhlášky]. Zmíněné doporučení NIST pak nereflektuje

parametry konkrétního zpracování osobních údajů, které se mohou mezi jednotlivými správci osobních údajů přináležejícími do veřejného sektoru (např. správní úřady) a i mezi jednotlivými správci osobních údajů přináležejícími do sektoru soukromého podstatně lišit (např. povahou osobních údajů, rozsahem jejich zpracování). Nelze vyloučit, že parametry zpracování osobních údajů u jednotlivých správců osobních údajů z veřejného a soukromého sektoru budou obdobné. Vždy bude záležet na konkrétním nastavení zpracování osobních údajů, když povaha správce bude představovat jeden z důležitých parametrů, nikoli však nutně určující parametr pro „rizikovost" zpracování osobních údajů.

/34/ K tvrzení obviněné, podle kterého je reálná doba potřebná pro implementaci nového hashovacího algoritmu u existujících systémů mnohem delší nežli ze strany NÚKIB uváděný jeden rok, je třeba uvést, že podle § 13 odst. 1 zákona č. 101/2000 Sb. je odpovědností správce osobních údajů (zjednodušeně vyjádřeno), aby přijal technická a organizační opatření potřebná k dosažení adekvátní úrovně zabezpečení osobních údajů v daném čase. V této souvislosti lze opět poukázat na komentářovou literaturu, v níž se k § 13 odst. 1 zákona č. 101/2000 Sb. mimo jiné uvádí: *„Přijatá opatření přitom musí vykazovat náležitou odbornou úroveň odrážející rizika spojená s konkrétními operacemi s osobními údaji a s povahou zpracovávaných údajů. Důležité je také zdůraznit, že jak Směrnice 95/46/ES, tak § 13 OchOsÚ předpokládají, že správci a zpracovatelé osobních údajů budou muset na přijetí vhodných opatření vynaložit jisté náklady. Správce osobních dat tak nemůže argumentovat, že bezpečnostní opatření nepřijal s odkazem na jejich finanční, personální či časovou nákladnost. Je to ostatně správce, kdo o zpracování osobních dat rozhodl (resp. mu bylo uloženo zvláštním zákonem), a proto je povinen nést i související náklady na tato opatření (přiměřené rizikům daného zpracování).“*[2]

/35/ Obviněná jakožto správce osobních údajů svých zákazníků pak byla povinna přizpůsobit své rozhodovací procesy dosažení přiměřené úrovně zabezpečení zpracování osobních údajů svých zákazníků. Přitom v zásadě uznala, že doba jednoho roku jako NÚKIB uvedená doba potřebná pro implementaci hashovacího algoritmu bcrypt u existujících systémů z (pouze) technického hlediska dostatečná je. Pokud by tak obviněná vytvořila podmínky pro včasnou implementaci hashovacího algoritmu bcrypt, byla by tohoto cíle schopna objektivně dosáhnout. Jak vyplývá z výše uvedeného, subjektivní okolnosti spočívající v tom, že při své činnosti měla obviněná jiné priority, k jejichž naplnění alokovala své zdroje, nejsou v posuzovaném případě relevantní. Obviněná navíc tuto svou námitku založila na strohém výčtu tvrzených skutečností ovlivňujících dobu potřebnou pro implementaci hashovacího algoritmu bcrypt, které však nijak nekonkretizovala z hlediska jejich časového určení mimo to, že výsledná implementační doba je mnohem delší než jeden rok. Pokud obviněná na podporu tohoto svého tvrzení poukazuje na „*Prohlášení NBÚ k využívání hashovacích funkcí*“ co do doporučené doby pro přechod na odolnější hashovací algoritmus, pak předně přehlíží, že z uvedeného doporučení NBÚ je třeba dovodit, že po roce 2012 již hashovací algoritmus SHA-1 nebude dostatečně odolný. V této souvislosti pak odvolací orgán připomíná, že obviněná implementovala hashovací algoritmus SHA-1 s kryptografickou solí právě až v roce 2012. To navíc způsobem, jímž nezajistila, že všechna hesla zákaznických účtů budou od okamžiku implementace nového hashovacího algoritmu skutečně prostřednictvím něj zabezpečena, neboť vedle něj „podpůrně“ používala značně zastaralý hashovací algoritmus MD5 (vizte níže). K samotné délce doby uvedené NBÚ pro přechod na nový hashovací

[2] *Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.*: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, s. 230.

algoritmus pak je třeba poznamenat, že ji nelze pouze mechanicky porovnávat s roční dobu uvedenou NÚKIB pro přechod na bcrypt u existujících systémů. Doporučení NBÚ neuvádí důvody, proč jím byla doporučená doba k přechodu na hashovací algoritmus nové generace nastavena na 3 až 5 let počínaje 1. lednem 2007, nelze ji proto bez dalšího zaměňovat či porovnávat s dobou (z technického hlediska) potřebnou na přechod na nový hashovací algoritmus.

/36/ Obviněná dále namítla, že správní orgán prvního stupně nepřihlížel k technickým a organizačním opatřením, které v průběhu času přijímala. Konkrétně přitom uvedla, že v roce 2012 došlo u hesel k zákaznickým účtům k přechodu z hashovacího algoritmu MD5 na hashovací algoritmus SHA-1 s kryptografickou solí. Tuto změnu, podle svého tvrzení, obviněná implementovala pro všechny uživatelské účty s tím, že k faktickému „překlopení" hesla na novou technologii došlo přihlášením konkrétního uživatele do uživatelského účtu, neboť potřebovala znát vlastní uživatelské heslo (v plně čitelné podobě), a nikoli pouze jeho hash (otisk). Tuto metodu „překlopení" hashovacího algoritmu hesla obviněná zvolila proto, že zbylé dvě jí uvedené a v úvahu připadající metody implementace nového hashovacího algoritmu (a) prolomení existujících hashů hrubou silou a následné „zahashování" novým hashovacím algoritmem a (b) resetování hesla u všech uživatelských účtů a zaslání e-mailu s obnovovacím odkazem jejich uživatelům vyloučila. První z důvodu problematičnosti metody spočívající v nutnosti vynaložení značného množství času, výpočetního výkonu a nedostatku záruky nalezení správného hesla (absence odolnosti proti kolizím), druhou z důvodu rizikovosti metody spočívající v nedostatku důvěry uživatelů a možné ignoraci takových sdělení vyplývající z množství phishingových útoků aj.

/37/ Obviněná tím současně zdůvodnila, proč hesla uživatelských účtů uživatelů, kteří se od roku 2012 do svého účtu nepřihlásili, mohla zůstat „zahashovaná" hashovacím algoritmem MD5 až do 27. srpna 2017. Dodala, že po roce 2012 však hashovací algoritmus MD5 pro jeho zastaralost již aktivně nepoužívala, pouze jej podporovala pro případ přihlášení těchto „neaktivních" uživatelů. Obdobným způsobem pak podle obviněné probíhala změna hashovacího algoritmu hesel zákaznických účtů z SHA-1 s kryptografickou solí na bcrypt v listopadu 2016. Dle obviněné tak kterýkoli uživatel, který se přihlásil ke svému účtu či si jej vytvořil od listopadu 2016, měl své heslo hashované hashovacím algoritmem bcrypt. Dříve používané hashovací algoritmy obviněná podporovala z důvodu možného přihlášení „neaktivních" uživatelů. Přitom zdůraznila, že nebylo realistické přecházet mezi hashovacími algoritmy hashování hesel jiným než realizovaným způsobem.

/38/ S tímto názorem o správnosti postupu obviněné při implementaci nového hashovacího algoritmu se však nelze ztotožnit, a to již z toho důvodu, že redukce možných metod změny hashovacího algoritmu hesel k zákaznickým účtům pouze na tři není adekvátní. Obviněná totiž vychází z chybné premisy, že nutnou podmínkou změny hashovacího algoritmu hesla k zákaznickému účtu je její znalost vlastního zákaznického hesla v „nezahashované" podobě. Ve výčtu možných způsobů změny hashovacího algoritmu konkrétních hesel k zákaznickým účtům potom konsekventně zcela pomíjí (ať již účelově či nikoliv) možnost novým hashovacím algoritmem „zahashovat" stávající hash hesla vytvořený hashovacím algoritmem dříve používaným. Prostřednictvím hashovacího algoritmu bcrypt by tedy po jeho implementaci nedošlo k zahashování vlastního hesla k zákaznickému účtu, ale jeho již existujícího hashe vytvořeného předchozím použitím hashovacího algoritmu SHA-1 s kryptografickou solí nebo MD5. Nesporné výhody takového postupu by přitom spočívaly zejména v tom, že by obviněné umožnil poskytovat stejnou úroveň ochrany hesel

k zákaznickým účtům všem jejím zákazníkům bez významného časového rozdílu, a navíc bez nutné součinnosti zákazníků spočívající v přihlášení se k zákaznickému účtu. K tomu odvolací orgán doplňuje, že z obsahu spisového materiálu není patrné, že by obviněná o takovou součinnost zákazníka požádala či jej alespoň o možnosti zvýšení ochrany jeho zákaznického účtu informovala. Uvedená metoda změny hashovacího algoritmu by ani nepřekážela případnému pozdějšímu hashování vlastního hesla (nikoli jeho hashe) v okamžiku, kdy by se zákazník do svého zákaznického účtu přihlásil. Použitím této metody změny hashovacího algoritmu by tak obviněná mimo jiné předešla i tomu, že by ještě v roce 2017 některá z hesel k zákaznickým účtům měla hashována hashovacím algoritmem MD5, který již sama v roce 2012 považovala za zastaralý.

/39/ Obviněná namítla i to, že správní orgán prvního stupně nezohlednil, že část její databáze byla pravděpodobně odcizena před rokem 2014, přičemž v té době bylo zabezpečení hashovacím algoritmem SHA-1 dostatečné i ve světle odborného posouzení NÚKIB. K jejímu prolomení hrubou silou pak, podle jejího názoru, došlo s největší pravděpodobností až v roce 2017, ať již s ohledem na technologický pokrok a nárůst výpočetního výkonu počítačů v tomto období nebo uběhnutím dostatečného množství času potřebného na útok hrubou silou, aby došlo k dešifrování části databáze. Obviněná navíc, podle svého názoru, řádně implementovala nové technologie v okamžiku, kdy se stávaly standardem, a to ve vztahu k celé databázi.

/40/ Odvolací orgán proto v této souvislosti předně poukazuje na skutečnost, že podle skutkových zjištění založených na předchozím vlastním vyjádření obviněné došlo k úniku databáze v roce 2014 (vizte např. dokument „*Záznam o bezpečnostní události a výsledcích šetření*“), protože tato část databáze také obsahovala osobní údaje shromážděné i v uvedeném roce. Pokud tedy obviněná uvádí, že k odcizení předmětné databáze došlo před rokem 2014, jedná se o informaci rozpornou s jejími předchozími vyjádřeními. Lze se však domnívat, že se v tomto případě jedná o chybu v psaní na straně obviněné, neboť na jiných místech rozkladu (případně jeho doplnění) označila jako mezní datum úniku databáze 31. prosinec 2014 (např. bod 4 doplnění rozkladu), což odpovídá zjištěním učiněným jak v rámci provedené kontroly, tak i v následně vedeném správním řízení.

/41/ Realita úniku databáze osobních údajů zákazníků, která obsahovala rovněž hesla k zákaznickým účtům, však nemá vliv na povinnost obviněné zabezpečit zpracování i těch osobních údajů, které byly její součástí. Únik této databáze totiž spočíval v neoprávněném vytvoření její kopie a nedošlo jím tak ke snížení počtu zpracovávaných osobních údajů obviněnou. Obviněná dotčené osobní údaje neztratila ze své dispozice, i nadále je zpracovávala, proto i nadále trvala její povinnost podle § 13 odst. 1 zákona č. 101/2000 Sb. tyto osobní údaje řádně zabezpečit. Skutečnost, že by případná změna hashovacího algoritmu na bcrypt provedená obviněnou po úniku databáze nebyla s to zabránit „odhashování“ hesel k zákaznickým účtům původně hashovaným hashovacími algoritmy SHA-1 s kryptografickou solí anebo MD5 není z hlediska posouzení přestupkové odpovědnosti obviněné relevantní. V posuzovaném případě totiž podstatou přestupkového jednání není skutečnost „odhashování“ dotčených hesel třetí osobou, ale opomenutí obviněné přijmout přiměřené technické opatření k jejich ochraně. Tento názor správního orgánu prvního stupně potvrzuje komentářová literatura, která k § 13 odst. 1 zákona č. 101/2000 Sb. mimo jiné uvádí: „[S] *ohledem na obsah § 13 odst. 1 OchOsÚ, kterým je povinnost přijmout a provést bezpečnostní opatření, dojde k porušení této povinnosti již tím, že vznikne stav, kdy jsou zpracovávané osobní údaje určitým způsobem ohroženy v důsledku*

absence vhodných opatření nebo nedůsledného provedení těchto opatření v praxi. K naplnění příslušné skutkové podstaty správního deliktu tedy postačí vznik určitého rizika, přestože ke ztrátě, zničení či zneužití dat zatím nedošlo anebo dokonce ani nikdy nedojde."[3] Nadto odvolací orgán připomíná, že obviněná používala v rozhodné době nedostatečně odolné hashovací algoritmy SHA-1 s kryptografickou solí a MD5 nejen ve vztahu k heslům zákaznických účtů, které byly součástí odcizené databáze, ale dle jejího vlastního vyjádření dokonce ke 1 300 000 heslům zákaznických účtů.

/42/ S obviněnou sice lze souhlasit v tom, že podle odborného posouzení NÚKIB bylo před rokem 2014 a v jeho průběhu u existujících systémů užívání hashovacího algoritmu SHA-1 dostatečné, neboť podle NÚKIB se bcrypt (či jeho technologický ekvivalent) stal průmyslovým standardem v roce 2013 a doba potřebná na přechod na novější hashovací algoritmus u existujících systémů čítala jeden rok. Obviněná však hashovací algoritmus SHA-1 s kryptografickou solí používala i později, a to dokonce až do dne 27. srpna 2017, ačkoliv k tomu neexistoval rozumný technický důvod (vizte výše). Zároveň obviněná v podaném rozkladu zcela pominula skutečnost, že v roce 2014 stále ještě používala i hashovací algoritmus MD5, který již před rokem 2014 dostatečně odolný nebyl a který sama obviněná již v roce 2012 považovala za zastaralý. Přitom jej však používala rovněž až do dne 27. srpna 2017. Pokud jde o okamžik prolomení uniklé databáze útokem „hrubou silou", který dle obviněné měl s největší pravděpodobností nastat až v roce 2017, je třeba podotknout, že jednak tuto skutečnost nelze mít za prokázanou, a zejména ji pak nutno mít za nepodstatnou z hlediska otázky posuzování odpovědnosti obviněné za vytýkané přestupkové jednání. Jak je zřejmé z napadeného rozhodnutí, přestupkové jednání obviněné spatřuje správní orgán prvního stupně v nedostatečném zabezpečení zpracovávaných hesel k zákaznickým účtům spočívající v používání v rozhodné době nedostatečně odolných hashovacích algoritmů SHA-1 s kryptografickou solí a MD5, přičemž tyto hashovací algoritmy obviněná používala ještě i po prolomení hashů hesel nacházejících se v odcizené databázi osobních údajů. I proto by ani případný časový odstup zhruba tří let od okamžiku úniku databáze do okamžiku prolomení hashování hesel tzv. hrubou silou neměl vliv na závěr o nedostatečné odolnosti hashovacích algoritmů použitých obviněnou.

/43/ Pokud tedy obviněná poukazuje na skutečnost, že řádně implementovala nové technologie v okamžiku, kdy se stávaly standardem, odvolací orgán poznamenává, že toto tvrzení je ohledně hashovacích algoritmů ve zřejmém rozporu s odborným vyjádřením NÚKIB. Doplňuje přitom, že obviněná nijak nekonkretizovala, z jakého důvodu považuje okamžik implementace hashovacího algoritmu SHA-1 a bcrypt za odpovídající okamžiku, v němž se stával standardem. Za spekulativní pak je třeba považovat tvrzení obviněné, že hashovací algoritmy implementovala ve vztahu k celé své databázi, když změna hashovacího algoritmu byla odvislá od skutečnosti přihlášení zákazníků k jejich uživatelskému účtu, o čemž však tito zákazníci ani nebyli informováni.

/44/ Argumentaci obviněné tedy odvolací orgán odmítl. Po celkovém přezkoumání však shledal, že ve výroku II. rozhodnutí je nadbytečně uveden odkaz na ustanovení § 35 písm. b) zákona č. 250/2016 Sb., které stanoví jako druh trestu za spáchání přestupku pokutu, přičemž ve výroku II. rozhodnutí uvedený § 45 odst. 3 zákona č. 101/2000 Sb. konktrétně

[3] *Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.*: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, s. 234.

umožňuje uložení pokuty, a to až do výše 5 000 000 Kč. Dále bylo shledáno, že výrok III. rozhodnutí je vhodné upřesnit odkazem na vyhlášku č. 520/2005 Sb. stanovující paušální částku nákladů řízení. Z těchto důvodů, které však nezpůsobují nezákonnost rozhodnutí, byly pozměněny výroky II. a III. rozhodnutí. Žádná další pochybení v postupu správního orgánu prvního stupně pak nebyla shledána. Z uvedených důvodů proto odvolací orgán rozhodl, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení: Proti tomuto rozhodnutí podle ustanovení § 152 odst. 5 zákona č. 500/2004 Sb., správní řád, nelze podat rozklad.

Praha 2. května 2023

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)