Vyvěšeno dne: 4. 12. 2025
Svěšeno dne: 18. 12. 2025

Alena Filipová

ČESKÁ REPUBLIKA

# ROZSUDEK JMÉNEM REPUBLIKY

Nejvyšší správní soud rozhodl v senátu složeném z předsedy Ondřeje Mrákoty, soudkyně Michaely Bejčkové a soudce Vojtěcha Šimíčka v právní věci žalobkyně: **Allegro Retail a. s.**, U garáží 1611/1, Praha 7, zastoupená advokátem Mgr. Luďkem Šrubařem, U garáží 1611/1, Praha 7, proti žalovanému: **Úřad pro ochranu osobních údajů**, Pplk. Sochora 27, Praha 7, proti rozhodnutí předsedy žalovaného ze dne 2. 5. 2023, čj. UOOU-04073/18-50, v řízení o kasační stížnosti žalobkyně proti rozsudku Městského soudu v Praze ze dne 12. 3. 2025, čj. 5 A 24/2023-82,

**takto:**

**I.** Rozsudek Městského soudu v Praze ze dne 12. 3. 2025, čj. 5 A 24/2023-82, **se ruší**.

**II.** Rozhodnutí předsedy žalovaného ze dne 2. 5. 2023, čj. UOOU-04073/18-50, **se ruší** a věc **se vrací** žalovanému k dalšímu řízení.

**III.** Žalovaný **je povinen** zaplatit žalobkyni na náhradě nákladů řízení částku **29 497 Kč** do 30 dní od právní moci tohoto rozsudku k rukám jejího zástupce, advokáta Mgr. Luďka Šrubaře.

## Odůvodnění:

### 1. Vymezení věci

[1] Žalovaný uznal žalobkyni rozhodnutím ze dne 23. 5. 2018 vinnou ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „ZOOÚ“), kterého se měla dopustit tím, že nepřijala nebo neprovedla dostatečná opatření pro zajištění bezpečnosti zpracování osobních údajů ve smyslu § 13 odst. 1 ZOOÚ. Nezabezpečila tak nejméně od 31. 12. 2014 do srpna 2017 osobní údaje svých zákazníků, čímž došlo k úniku nejméně 766 421 záznamů o jejích zákaznících z roku 2014 (v rozsahu jméno, příjmení, e-mailová adresa, heslo k uživatelskému účtu a některá telefonní čísla), z nichž 735 956 obsahovaly unikátní e-mailovou adresu zákazníka, a jejich zpřístupnění na internetových stránkách ulozto.cz. Tímto jednáním žalobkyně porušila povinnost stanovenou v § 13 odst. 1 ZOOÚ a byla jí uložena pokuta ve výši 1 500 000 Kč.

[2] Žalobkyně podala proti prvostupňovému rozhodnutí rozklad, který předsedkyně žalovaného rozhodnutím ze dne 21. 9. 2018 zamítla. Žalobkyně se dále bránila u městského soudu, jenž její žalobu rozsudkem ze dne 24. 6. 2021 zamítl.

[3] Ke kasační stížnosti žalobkyně zrušil NSS rozsudkem ze dne 11. 11. 2021, čj. 1 As 238/2021-33, napadený rozsudek městského soudu i rozhodnutí předsedkyně žalovaného. Podle NSS považoval městský soud za zásadní, že žalobkyně osobní údaje neochránila a ani včas neodhalila jejich odcizení. Je proto bez potřeby dalšího zkoumání zjevné, že přijatá opatření nebyla dostatečná. NSS se s tímto postojem neztotožnil. Přestupek podle § 45 odst. 1 písm. h) ZOOÚ je tzv. ohrožovací, pro naplnění skutkové podstaty tak není nutná existence následku v podobě neoprávněného nakládání s osobními údaji. To však neznamená, že by existence takového následku vedla bez dalšího k závěru, že si správce či zpracovatel osobních údajů počínal v rozporu s § 13 odst. 1 ZOOÚ. Uvedené ustanovení je podle NSS zapotřebí vykládat souladně s čl. 17 odst. 1 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, který nepředpokládá, že by odpovědnost správců a zpracovatelů osobních údajů byla bezbřehá; klade důraz na to, aby dotčené subjekty vynaložily za účelem ochrany osobních údajů náležité úsilí. Žalovaný a městský soud pochybili tím, že se nezabývali kvalitou přijatých opatření a vycházeli z chybného předpokladu, že k naplnění skutkové podstaty posuzovaného přestupku postačí, došlo-li k neoprávněnému přístupu k osobním údajům a současně žalobkyně tuto skutečnost v rozhodné době neodhalila. Postupovali tak v rozporu se zásadou *nullum crimen sine lege*, podle níž může být přestupkem pouze takové jednání, u něhož tak zákon výslovně stanoví.

[4] Žalovaný opětovně rozhodoval ve věci žalobkyně a rozhodnutím ze dne 17. 6. 2022 shledal žalobkyni vinnou ze spáchání přestupku podle § 45 odst. 1 písm. h) ZOOÚ a uložil jí pokutu ve výši 140 000 Kč. Ve výroku výslovně uvedl, že se žalobkyně dopustila přestupku 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 hashovacími 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*“.

[5] Předseda žalovaného rozhodnutím ze dne 2. 5. 2023 změnil výrok II prvostupňového rozhodnutí tak, že vypustil slova „*podle § 35 písm. b) zákona č. 250/2016 Sb. a*“ a do výroku III doplnil slova „*a 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, ve znění vyhlášky č. 112/2017 Sb.*“. Ve zbytku prvostupňové rozhodnutí potvrdil. Žalobkyně podle názoru žalovaného při volbě prostředků ochrany osobních údajů používala zastaralý a nedostatečně odolný hashovací algoritmus a včas nepřijala dostatečná opatření k zamezení neoprávněného přístupu k heslům zákaznických účtů a jejich zneužití.

[6] Žalobkyně podala i proti druhému rozhodnutí žalovaného žalobu, kterou městský soud opět zamítl.

## 2. Shrnutí argumentů kasační stížnosti a vyjádření žalovaného

[7] **Žalobkyně (stěžovatelka)** podala proti rozsudku městského soudu kasační stížnost. Stěžovatelka trvá na tom, že ve věci nebylo bez důvodných pochybností prokázáno, že naplnila skutkovou podstatu tvrzeného přestupku. Žalovaný se v rozporu s čl. 17 směrnice 95/46/ES

ve svém rozhodnutí věnoval výhradně kritériu stavu techniky. Jeho závěry jsou založeny pouze na závěrech odborného posouzení ze dne 11. 4. 2022 poskytnutého Národním úřadem kybernetické bezpečnosti (NÚKIB), to však zde nelze použít jako důkaz. NÚKIB nevzal v potaz konkrétní skutkové okolnosti věci, posouzení je zkratkovité a jeho závěry nejsou ničím podloženy. Žalovaný i městský soud se těmito námitkami odmítli zabývat. Městský soud dovolil, aby žalovaný zhojil vady správního řízení až během soudního řízení tím, že mu umožnil doplnit napadené rozhodnutí o zhodnocení kritéria nákladnosti.

[8] Stěžovatelka poukázala na to, že k úniku dat došlo před rokem 2014 (zjevně v roce 2012). V tu dobu byla data uživatelů chráněna hashovacím algoritmem SHA-1 s kryptografickou solí. Nejpozději v listopadu 2016 přešly všechny aktivní uživatelské účty na algoritmus bcrypt. V rozhodném období tak bylo starším algoritmem chráněno zhruba 350 000 neaktivních účtů. Městský soud založil závěr, podle něhož stěžovatelka nepřijala v rozhodném období nezbytná opatření, na záznamu o bezpečnostním incidentu. Ten ovšem pouze uvádí, že určité množství uživatelských účtů bylo dotčeno daným incidentem.

[9] Pro posouzení odpovědnosti stěžovatelky je zásadní běh času. Údajné protiprávní jednání bylo ukončeno zavedením algoritmu bcrypt v listopadu 2016. Odpovědnost stěžovatelky proto s ohledem na § 46 odst. 3 ZOOÚ ve znění účinném do 30. 6. 2017 zanikla nejpozději v listopadu 2019. I pokud by stěžovatelka měla být odpovědná též ve vztahu k neaktivní databázi, je třeba přihlédnout k jejímu resetu dne 27. 8. 2017. Městský soud se nezabýval použitelností dřívější právní úpravy a námitku, jíž se stěžovatelka domáhala zohlednění délky správního řízení při stanovení výše trestu, odmítl pro opožděnost.

[10] Stěžovatelka poukázala na chybný výrok o vině. Nejpozději v listopadu 2016 byla většina uživatelských účtů chráněna nejbezpečnější metodou bcrypt. Přesto výrok o vině uvádí, že protiprávní jednání se nejméně do 27. 8. 2017 týkalo nejméně 735 956 účtů. Městský soud si byl této nejasnosti vědom. Namísto nestranného posouzení rozhodnutí žalovaného předložil vlastní úvahy, jak to žalovaný vlastně myslel. Stěžovatelka nesouhlasí s městským soudem, že z odůvodnění rozhodnutí žalovaného je zřejmé, že stěžovatelka byla sankciována za únik dat pouze k 350 000 účtů. Rozhodnutí není v rozsahu uloženého trestu a určení jeho výše přezkoumatelné.

[11] Závěrem stěžovatelka namítla, že jí je v rozporu s rušícím rozsudkem 1 As 238/2021-33 nadále kladen k tíži následek bezpečnostního incidentu.

[12] **Žalovaný** v úvodu vyjádření sdělil, že se ztotožňuje se závěry městského soudu. Stěžovatelka v zásadě jen opakuje shodné argumenty jako v předchozích řízeních. Žalovaný připomněl, že NÚKIB je kompetentním orgánem pro zpracování odborného vyjádření v této věci. To obsahuje posouzení konkrétních okolností případu. NÚKIB v něm uvedl, že již od roku 2013 lze hashovací algoritmus bcrypt považovat za průmyslový standard a u nově vznikajících systémů v té době neexistoval technický důvod využít méně odolný algoritmus. Proto je podle žalovaného v zásadě bezpředmětné, aby byly zevrubněji posuzovány povaha dotčených osobních údajů a nákladnost. Přesto se žalovaný těmito otázkami zabýval.

[13] Opatření k zajištění bezpečnosti osobních údajů přijatá stěžovatelkou byla na takové úrovni, že únik dat v reálném čase nebyl zjištěn a ani nebylo možné spolehlivě zjistit, jak k úniku došlo. Žalovaný vycházel i z dalších dokumentů, byť doporučujícího charakteru, které shodně poukazovaly na nedostatečnou bezpečnost hashovacích algoritmů MD5 a SHA-1 se solí v rozhodném období. Přihlédl též k vnitřním předpisům předloženým stěžovatelkou.

[14] Žalovaný zdůraznil, že stěžovatelka nese za zabezpečení osobních údajů výlučnou odpovědnost, kterou nelze přenášet na subjekty údajů. Stěžovatelka má vést uživatele k tomu, aby nepoužívali triviální hesla. Standardnímu zabezpečení musí podléhat i neaktivní účty. Dostatečně

odolné hashovací algoritmy měly být aplikovány minimálně do konce roku 2014, a to na všechny účty. K potřebné změně hashovacího algoritmu docházelo u zákaznických účtů zřízených před listopadem 2016 nahodile – přihlášením jednotlivých zákazníků do jejich zákaznického účtu. V této souvislosti je irelevantní, kdy došlo k úniku dat. Žalovaný poznamenal, že stěžovatelka ve svém přípise z roku 2018 uvedla, že uniklá data pochází z konce roku 2014. To potvrzují i další listiny ve spise. Není jasné, proč stěžovatelka nyní posouvá únik k roku 2012.

[15] Nelze souhlasit ani s tím, že trestnost skutku zanikla. Žalovaný se o přestupku dozvěděl dne 27. 8. 2017, řízení o přestupku bylo zahájeno oznámením ze dne 19. 4. 2018, doručeným stěžovatelce dne 24. 4. 2018. Žalovaný odkázal na relevantní ustanovení. K další námitce uvedl, že závadové jednání nebylo limitováno listopadem 2016, ale dnem 27. 8. 2017. Z dikce výroku napadeného rozhodnutí je nutné vyvozovat, že časové určení přestupku od 31. 12. 2014 nejméně do 27. 8. 2017 nelze chápat tak, že oněch minimálně 735 956 hesel bylo nedostatečně hashováno po celou tuto dobu, ale po nějaké období v tomto časovém úseku. Sankce byla řádně zdůvodněna a byly zohledněny veškeré relevantní okolnosti. V reakci na rozsudek NSS 1 As 238/2021-33 byla uložená pokuta snížena z částky 1 500 000 Kč na 140 000 Kč.

### 3. Právní hodnocení Nejvyššího správního soudu

[16] Stěžovatelka provozuje internetový obchod pod značkou Mall.cz. V rámci jeho provozu zpracovává osobní údaje svých zákazníků. Dne 25. 8. 2017 zjistila bezpečnostní incident – kybernetický útok, v jehož důsledku unikly údaje z více než 700 000 uživatelských účtů a dne 27. 7. 2017 byly v čitelné formě zveřejněny na webu ulozto.cz. Dne 27. 8. 2017 stěžovatelka oznámila incident žalovanému a provedla opatření k minimalizaci rizik. Žalovaný pojal podezření, zda stěžovatelka neporušila své povinnosti vyplývající z § 13 ZOOÚ, a zahájil u ní kontrolu. Stěžovatelka byla posléze uznána vinnou ze spáchání přestupku podle § 45 odst. 1 písm. h) ZOOÚ (prvním i druhým rozhodnutím žalovaného). Městský soud poté (opakovaně) potvrdil závěr žalovaného, že se stěžovatelka dopustila tohoto přestupku, neboť nepřijala dostatečná opatření k zajištění bezpečnosti zpracovávaných osobních údajů ve smyslu § 13 odst. 1 uvedeného zákona.

[17] Ze spisu dále plyne, že stěžovatelka realizovala zabezpečení osobních údajů zákazníků ve smyslu § 13 odst. 1 ZOOÚ prostřednictvím hashovacích algoritmů. Do roku 2012 využívala hashovací algoritmus MD5, v listopadu 2012 zavedla algoritmus SHA-1 s kryptografickou solí. Od října 2016 pak stěžovatelka přešla na algoritmus bcrypt. Většina hesel k účtům dotčených zákazníků přitom byla hashována algoritmem MD5, ve zbytku pak algoritmem SHA-1 se solí. Stěžovatelka v řízení opakovaně potvrdila, že se uniklá databáze týkala její databáze klientů z roku 2014. Skutečnost, že databáze obsahovala hesla hashovaná algoritmem MD5, a tedy že tento algoritmus byl používán i poté, co od roku 2012 stěžovatelka zavedla algoritmus SHA-1 se solí, potvrdila rovněž sama stěžovatelka. Po zjištění, že odcizená data byla zveřejněna, provedla ve dnech 25. – 27. 8. 2017 reset uživatelských hesel zákazníků registrovaných před 1. 1. 2015 a převedla tato hesla na hashovací metodu bcrypt.

[18] Podle § 13 odst. 1 ZOOÚ *správce a zpracovatel jsou povinni 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. Tato povinnost platí i po ukončení zpracování osobních údajů.*

[19] Podle § 45 odst. 1 písm. h) ZOOÚ *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).*

[20] Podle čl. 17 odst. 1 směrnice 95/46/ES *členské státy stanoví, 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.*
*Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.*

[21] Ke všem citovaným ustanovením je vhodné doplnit, že žádné z nich již neplatí. Právní úprava ochrany osobních údajů byla nahrazena novými právními předpisy (zákon č. 110/2019 Sb., o zpracování osobních údajů, a GDPR[a]), jejichž použití by však nebylo stěžovatelce v této věci ku prospěchu (§ 2 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich[b]).

[22] Jak plyne z textu výše, NSS v této věci již jednou rozhodoval. Rozsudkem ze dne 11. 11. 2021, čj. 1 As 238/2021-33, zrušil první zamítavý rozsudek městského soudu a současně i rozhodnutí předsedkyně žalovaného. Stěžovatelka je přesvědčena, že žalovaný ani městský soud při svém opakovaném rozhodování nedbali názoru Nejvyššího správního soudu vysloveného v tomto rozsudku.

**3.1** *Kritéria pro posouzení naplnění skutkové podstaty přestupku podle § 45 odst. 1 písm. h) ZOOÚ*

[23] NSS v rozsudku 1 As 238/2021-33 potvrdil, že pro vznik odpovědnosti za přestupek podle § 45 odst. 1 písm. h) ZOOÚ postačí ohrožení bezpečnosti osobních údajů, jedná se tedy o tzv. ohrožovací delikt. Není proto rozhodující, zda se osobní údaje v konečném důsledku podaří ochránit, či nikoli. Existence případného následku v podobě neoprávněného nakládání s osobními údaji ještě nutně neznamená, že si správce či zpracovatel osobních údajů počínal v rozporu s § 13 odst. 1 ZOOÚ. Uvedeného přestupku se dopustí osoba, která nepřijme dostatečná opatření za účelem ochrany osobních údajů, a to i v situaci, kdy k neoprávněnému nakládání s údaji nedojde. Nelze přitom vyžadovat, aby přijatá a dodržovaná opatření byla schopna odrazit jakýkoli kybernetický útok. Ustanovení § 13 odst. 1 ZOOÚ je zapotřebí vykládat v souladu s čl. 17 odst. 1 směrnice 95/46/ES, který nepředpokládá, že by odpovědnost správců a zpracovatelů osobních údajů byla bezbřehá.

[24] Žalovaný je tak v každém konkrétním případě povinen zkoumat, zda byla přijatá a dodržovaná opatření dostatečná. Za dostatečná je přitom nutné považovat především taková opatření, která zajišťují *přiměřenou* úroveň ochrany, a to s ohledem na *stav techniky* a *náklady* na jejich provedení. Přiměřenost a vhodnost opatření je pak nezbytné vnímat rovněž jako kategorii, jejíž obsah se bude odvíjet též od *rozsahu* a *obsahu* zpracovávaných údajů.

[25] Byla-li opatření nedostatečná, nastupuje odpovědnost za uvedený přestupek. Jestliže však opatření odpovídají kritériím vyplývajícím z čl. 17 směrnice 95/46/ES, nejsou znaky přestupku podle § 45 odst. 1 písm. h) ZOOÚ naplněny a odpovědnost za přestupek nevzniká, a to i v případě, že k úniku dat došlo (viz zejména body 33 a 37 citovaného rozsudku NSS).

[26] NSS v rozsudku 1 As 238/2021-33 vytkl žalovanému především to, že se v případě stěžovatelky nezabýval kvalitou přijatých a dodržovaných opatření, tedy tím, zda byla opatření dostatečná s ohledem na dostupnou úroveň ochrany v rozhodném období, charakter činnosti stěžovatelky a rozsah zpracovávaných údajů.

[27] Z citovaných ustanovení (zejména z podkladového čl. 17 odst. 1 směrnice 95/46/ES) a závěrů rušícího rozsudku NSS lze vyvodit čtyři základní kritéria, která žalovaný musí

[a] 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), neboli pouze „GDPR".
[b] Podle § 2 odst. 1 zákona č. 250/2016 Sb. *se odpovědnost za přestupek posuzuje podle zákona účinného v době spáchání přestupku; podle pozdějšího zákona se posuzuje jen tehdy, je-li to pro pachatele přestupku příznivější.*

při posuzování, zda subjekt spáchal přestupek podle § 45 odst. 1 písm. h) ZOOÚ, zohlednit. Jsou jimi:

a) stav techniky[c],

b) náklady na provedení opatření,

c) povaha a rozsah zpracovávaných údajů,

d) rizika vyplývající ze zpracování údajů.

[28] NSS považuje za vhodné odkázat též na čl. 32 GDPR, jenž nahradil čl. 17 směrnice 95/46/ES. Podle jeho odstavce 1 platí: *S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku (…)*. Odstavec 2 tohoto článku obsahuje demonstrativní výčet určitých faktorů, které jsou relevantní při posuzování vhodné úrovně zabezpečení s ohledem na rizika dotyčného zpracování. Soudní dvůr Evropské unie (SDEU) v bodě 42 rozsudku ze dne 14. 12. 2023 ve věci C-340/21, *Natsionalna agentsia za prihodite*, vysvětlil, že „*z uvedeného čl. 32 odst. 1 a 2 vyplývá, že vhodnost takových technických a organizačních opatření je třeba posoudit ve dvou fázích. V první fázi je třeba zjistit rizika porušení zabezpečení osobních údajů vyvolaná dotyčným zpracováním a jejich případné důsledky pro práva a svobody fyzických osob. Toto posouzení musí být prováděno konkrétně s přihlédnutím ke stupni pravděpodobnosti zjištěných rizik a stupni jejich závažnosti. V druhé fázi je třeba ověřit, zda opatření zavedená správcem odpovídají těmto rizikům, a to s přihlédnutím ke stavu techniky, nákladům na provedení, jakož i k povaze, rozsahu, kontextu a účelům tohoto zpracování*“ (shodně též rozsudky SDEU ze dne 25. 1. 2024, *MediaMarktSaturn*, C-687/21, body 37 a 38, a ze dne 28. 11. 2024, *Másdi*, C-169/23, bod 71). Z citovaného textu plyne, že při posouzení vhodnosti, resp. dostatečné účinnosti přijatých opatření je vždy nutné s ohledem na konkrétní okolnosti případu, zejména s ohledem na konkrétní rizika a jejich případné důsledky, zvážit veškerá uvedená kritéria (tj. stav techniky, náklady na provedení opatření a dále povahu, rozsah, kontext a účel zpracování osobních údajů). Tyto závěry jsou s ohledem na podobnost právní úpravy a její shodný účel využitelné i v nynější věci (srov. rozsudek NSS ze dne 27. 6. 2019, čj. 4 As 140/2019-27, věta druhá bodu 26).

[29] Stěžovatelka namítla, že žalovaný rezignoval na posouzení uvedených kritérií, resp. věnoval se výhradně kritériu stavu techniky; městský soud poté její námitku nesprávně zamítl. A dále, že žalovaný založil posouzení kritéria stavu techniky pouze na závěrech odborného vyjádření NÚKIB ze dne 11. 4. 2022, které nelze z řady důvodů uvedených v kasační stížnosti použít v její neprospěch.

[30] NSS souhlasí se závěry žalovaného a městského soudu, že z nashromážděných důkazů lze uzavřít, že v rozhodné době (tj. od konce roku 2014 – blíže viz další body rozsudku), stěžovatelka neměla s ohledem na **stav techniky** v dané době a daném odvětví zavedená dostatečná opatření ve smyslu § 13 odst. 1 ZOOÚ. Tento názor NSS (ve shodě s žalovaným a městským soudem) opírá zejména o tato zjištění:

---

[c] V anglickém znění čl. 17 odst. 1 směrnice 95/46/ES je uvedeno: *Having regard to the state of the art…* (v českém znění tohoto článku přeloženo jako: „*S ohledem na stav techniky…*“). „State of the art“ je ustálené spojení, které se doslovně překládá jako „nejmodernější“ typicky ve vztahu k technologickému pokroku. Tudíž při zohlednění tohoto kritéria je nutné posoudit především stav technologického vývoje a jeho dostupnost. K tomu viz též bod 32 stanoviska GA SDEU Giovanniho Pitruzzelly ze dne 27. 4. 2023 k věci C-340/21, *Natsionalna agentsia za prihodite* (více k této věci též bod [28] tohoto rozsudku), podle kterého „*čl. 32 odst. 1* [GDPR] *vyžaduje, aby správce zohlednil ‚stav techniky‘. To znamená omezení technologické úrovně opatření, která mají být provedena, na to, co je v době přijetí opatření rozumně možné: vhodnost opatření k předcházení riziku tedy musí odpovídat řešením, která nabízí současný stav vědy, techniky, technologie a výzkumu* (…)“.

1) Národní bezpečnostní úřad (NBÚ) v prohlášení k využívání hashovacích funkcí zveřejněném na svém webu dne 1. 1. 2007[d] doporučil nadále nepoužívat mj. hashovací funkci MD5 a neprodleně zahájit přípravu k přechodu od hashovací funkce SHA-1 na novou generaci hashovacích funkcí třídy SHA-2 v horizontu 3-5 let;

2) podle článku Ministerstva vnitra „Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu“ zveřejněného dne 17. 10. 2008 a aktualizovaného dne 23. 6. 2009[e] je algoritmus SHA-1 pro elektronické podpisy od 1. 1. 2010 nepoužitelný, a proto je nutné zahájit přechod na bezpečnější algoritmy třídy SHA-2; ministerstvo v článku uvedlo, že se nejedná o nepředvídatelnou změnu, neboť je tato problematika diskutována již několik let a byla publikována řada odborných článků a studií;

3) z článku „Q&A – Vše, co jste chtěli vědět o bezpečnosti na MALL.cz“ zveřejněného dne 27. 8. 2017 na blogu stěžovatelky[f] plyne, že stěžovatelka používala zastaralou hashovací metodu MD5 (u některých účtů) i po zavedení metody SHA-1 se solí v roce 2012 a též i po zavedení algoritmu bcrypt v listopadu 2016;

4) podle článku od experta na IT bezpečnost zveřejněného na webu HN.cz dne 29. 8. 2017[g] nebyla metoda SHA-1 se solí již v roce 2012 bezpečná;

5) ze záznamu o bezpečnostní události a výsledcích šetření ze dne 8. 9. 2017 zpracovaného stěžovatelkou vyplynuly následující informace:

   - k úniku dat došlo pravděpodobně v roce 2014, zveřejněná databáze obsahovala údaje zákazníků z roku 2014,
   - dotčená databáze byla zakódována starším a již nepoužívaným způsobem, který umožnil narušiteli jednodušší hesla rozkódovat: do roku 2012 se jednalo o MD5, od roku 2012 do roku 2016 SHA-1 se solí;

6) interní předpis č. 203-1-2 stěžovatelky „Směrnice o ochraně osobních údajů zákazníků společnosti Internet Mall, a. s., či jejích dceřiných společností na území České republiky“ platný ode dne 1. 4. 2013 obsahoval v bodě 5.7 minimální standardy stanovené pro ochranu osobních údajů zákazníků, mj. povinnost zajistit v daném odvětví odpovídající úroveň šifrování/hashování osobních údajů;

7) během místního šetření stěžovatelka žalovanému potvrdila, že se databáze zveřejněná na portálu Ulož.to shoduje s její vlastní databází zákazníků z roku 2014 (viz úřední záznam o provedení kontrolního úkonu ze dne 26. 10. 2017);

8) v odpovědi žalovanému ze dne 15. 1. 2018 stěžovatelka opět potvrdila, že se bezpečnostní incident uskutečnil v roce 2014;

9) z odpovědi NÚKIB ze dne 11. 4. 2022 na žádost žalovaného vyplynulo:

   - MD5 a SHA-1 (ani v kombinaci se solí) nejsou vhodnými hashovacími algoritmy pro ukládání autentizačních údajů,
   - bcrypt byl navržen přímo pro ukládání otisků hesel již v roce 1999, jeho použití se začalo prosazovat (mj. pro vytváření internetových nákupních galerií) od roku 2013,

[d] Prohlášení NBÚ k využívání hashovacích funkcí ze dne 1. 1. 2007 – založen pod č. l. 76 správního spisu sp. zn. UOOU-04073/18.
[e] Založen pod č. l. 75 správního spisu sp. zn. UOOU-04073/18.
[f] Založen pod č. l. 8 správního spisu sp. zn. UOOU-08428/17.
[g] Bezpečnostní svodka: Únik hesel z Mall.cz není tragédie, firma to zvládla na lepší dvojku | Hospodářské noviny (HN.cz) ze dne 29. 8. 2017 – založen pod č. l. 8 správního spisu sp. zn. UOOU-08428/17.

- v roce 2013 byla v ČR řešena problematika nevyhovující odolnosti algoritmu SHA-1 se solí proti útoku hrubou silou na odborných konferencích určených vývojářům e-shopových řešení, z toho plyne, že bcrypt je už od roku 2013 považován za průmyslový standard – u nově vznikajících systémů v té době neexistoval technický důvod využít méně odolný algoritmus (jako např. SHA-1 + sůl), u existujících systémů NÚKIB považuje jeden rok za dostatečnou dobu přechodu na odolnější algoritmus;

10) stěžovatelka v bodech 10 a 11 podaného rozkladu ze dne 30. 6. 2022 uvedla, že v listopadu 2016 zavedla metodu bcrypt, paralelně s ním byly u existujících účtů podporovány dříve užívané metody MD5 a SHA-1 se solí – hesla uživatelů, kteří se přihlásili ke svému účtu od listopadu 2016, byla současně s přihlášením převedena na bcrypt, stejně tak byla touto metodou hashována hesla u nově zřízených účtů od listopadu 2016 – v období před resetováním hesel databáze dne 27. 8. 2017 tak zůstalo hashováno staršími metodami zhruba 386 000 hesel;

11) v bodě 18 doplnění rozkladu ze dne 22. 7. 2022 stěžovatelka uvedla, že metodu SHA-1 se solí zavedla v roce 2012, přičemž změna byla implementována opět až přihlášením uživatele ke svému účtu; v bodě 24 uvedla, že z čistě technického hlediska lze přisvědčit NÚKIB, že pro implementaci nového řešení do existujících systémů je potřebný čas jednoho roku, reálně je však nutné přihlédnout k řadě dalších okolností (konkrétní prostředí, dostupnost, čas na rozhodnutí apod.) a případná implementace trvá mnohem déle než jeden rok;

12) experti z Google a CWI Amsterdam v článku „Announcing the first SHA1 collision" zveřejněném na blogu Googlu dne 23. 2. 2017[h] oznámili prolomení funkce SHA-1 a zdůraznili nutnost, aby její použití bylo ukončeno; z článku dále plyne, že Google už mnoho let prosazuje vyřazení této metody a v roce 2014 tým Chrome oznámil, že začne SHA-1 postupně opouštět;

13) podle článku zveřejněného na webu idnes.cz dne 24. 2. 2017[i] se již v roce 2005 začaly objevovat útoky cílené na prolomení SHA-1, po zjištěních Googlu a CWI je „*metoda SHA-1 zřejmě – po dlouhé době oprávněných pochybností – konečně zdiskreditována*".[j]

[31] S ohledem na popsaný stav technologického vývoje hashovacích algoritmů NSS ve shodě s žalovaným a městským soudem shledal, že stěžovatelka nejméně od počátku roku 2015 do srpna 2017 nechránila spravované osobní údaje vhodnými opatřeními, jelikož v tomto období používala k hashování nejméně části hesel své zákaznické databáze metody MD5 a SHA-1 s kryptografickou solí, které v tu dobu již nebyly bezpečné a bezrizikové. NSS se ztotožňuje s časovým vymezením protiprávního stavu tak, jak jej určil žalovaný (bod 48 rozhodnutí I. stupně). Z předestřených důkazů plyne, že nejméně v roce 2013 již nebylo možné považovat hashovací algoritmy MD5 a SHA-1 se solí za dostatečně odolné (MD5 ještě mnohem dříve). Jeden rok přitom lze považovat za odpovídající dobu pro přechod na odolnější algoritmus. Po stěžovatelce tak bylo s ohledem na rozsah a povahu zpracovávaných osobních údajů (k těmto kritériím viz níže) možné požadovat, aby hesla uživatelských účtů, která obsahují osobní údaje, byla chráněna hashovacím algoritmem bcrypt, případně jeho ekvivalentem, a to nejpozději od počátku roku 2015. To však stěžovatelka očividně nesplnila. Algoritmus bcrypt zavedla k ochraně hesel spravovaných uživatelských účtů nejdříve v říjnu/listopadu 2016, avšak nikoli vůči všem uživatelským účtům. Kompletní přechod k hashovacímu algoritmu bcrypt měla stěžovatelka realizovat až v průběhu 25. – 27. 8. 2017.

[h] Google Online Security Blog: Announcing the first SHA1 collision ze dne 23. 2. 2017.
[i] „Šifra" SHA-1 překonána: Google dokázal podvrhnout PDF se stejným hashem - iDNES.cz ze dne 24. 2. 2017.
[j] Články uvedené pod body 12 až 13 byly provedeny k důkazu městským soudem na jednání dne 12. 3. 2025 a jsou založeny ve spise městského soudu.

[32] Se stěžovatelkou nelze souhlasit v tom, že protiprávní stav byl ukončen v listopadu 2016, kdy stěžovatelka implementovala algoritmus bcrypt ve vztahu k aktivním uživatelským účtům. Její povinnost vyplývající z § 13 odst. 1 ZOOÚ se nevztahuje pouze k osobním údajům aktivních uživatelských účtů, ale k veškerým osobním údajům, které jako správce osobních údajů spravuje. Ve stejném duchu městský soud v bodě 56 napadeného rozsudku výstižně upozornil, že „*riziko zneužití hesla a e-mailové adresy trvá i v případě, že uživatel svůj účet v e-shopu žalobce nevyužívá, ale používá například stejné heslo k jiným účtům*".

[33] Jak již bylo řečeno, přestupek podle § 45 odst. 1 písm. h) ZOOÚ je tzv. ohrožovacím deliktem. Existence následku pro jeho spáchání není určující. Proto není podstatné, kdy došlo k úniku databáze a jejímu dešifrování. Samotný únik dat není pro posouzení stěžovatelčiny odpovědnosti za dotyčný přestupek relevantní.

[34] Odborné posouzení NÚKIB ze dne 11. 4. 2022 bylo jen jedním z mnoha podkladů, na jejichž základě žalovaný posuzoval dostupný stav techniky v rozhodné době. Není pravda, že bylo podkladem výlučným. Žalovaný v bodech 7 až 24 prvostupňového rozhodnutí vyjmenoval a shrnul dokumenty, z nichž při hodnocení stavu techniky vycházel. Jednalo se mj. o vyjádření stěžovatelky, její vnitřní předpisy (týkající se organizačních i technických opatření) či o odborné články. NSS je částečně shrnuje v bodě [30] výše. Žalovaný ve svých rozhodnutích odkazoval nejčastěji právě na odborné posouzení NÚKIB, což je logické, neboť se jednalo o podklad v posuzované věci nejvíce vypovídající. NÚKIB poskytl své odpovědi k dotazům žalovaného pro potřeby právě tohoto případu. Potvrdil přitom závěr, že v roce 2014 nebyl u existujících systémů z technického hlediska důvod pro užívání méně odolné hashovací metody SHA-1 se solí. Ostatně sama stěžovatelka v bodě 17 doplnění svého rozkladu ze dne 22. 7. 2022 uznala, že nebyl důvod, aby nově vznikající systémy v roce 2013 používaly k zabezpečení hesel k uživatelským účtům jiný algoritmus nežli bcrypt (či jeho ekvivalent). Bylo-li žádoucí a evidentně i technicky možné užít algoritmus bcrypt v nově vznikajících systémech již v roce 2013, nebyl podle NSS důvod, proč tento dostatečně bezpečný algoritmus neimplementovat s ohledem na povinnosti plynoucí z § 13 odst. 1 ZOOÚ také u existujících systémů v téže době. Stěžovatelka takové zdůvodnění ani neposkytuje. Též z článků (č. 12 a 13 v bodě [30] výše), které stěžovatelka předložila v řízení u městského soudu k prokázání, že k materializaci rizik souvisejících s používáním hashovací metody SHA-1 došlo až v roce 2017, vyplývá, že tato metoda nebyla již řadu let bezriziková.

[35] Žalovaný se dále věnoval charakteru činnosti stěžovatelky a **rozsahu zpracovávaných osobních údajů**. V bodech 52-54 prvostupňového rozhodnutí uvedl, že správa osobních údajů zákazníků byla nedílnou součástí podnikatelské činnosti stěžovatelky. To je zjevné již ze skutečnosti, že stěžovatelka se zabývá online prodejem zboží a umožňuje zákazníkům, aby si na jejím webu založili vlastní zákaznický účet. Rozsah zpracovávaných osobních údajů je přitom významný. Tomu odpovídá i počet záznamů, které byly po útoku neznámého pachatele v roce 2014 odcizeny (766 421). Jednalo si přitom o zhruba pětinu tehdejší zákaznické databáze.

[36] **Kritériem nákladů** se žalovaný zabýval především v bodě 53 rozhodnutí I. stupně. Shledal, že v souvislosti s předmětem činnosti stěžovatelky je „*namístě poznamenat, že zavedení hashovacího algoritmu odpovídajícího aktuálním bezpečnostním standardům v daném odvětví v roce 2014 nemohlo z hlediska nákladů ani organizačních opatření s tím spojených představovat tak závažnou překážku*". V poslední větě bodu 52 žalovaný bez dalšího vysvětlení uvedl, že stěžovatelka dosahovala poměrně významného obratu. Žalovaný současně zdůraznil vlastní závazek stěžovatelky v jejích interních předpisech šifrovat/hashovat hesla zákaznických účtů způsobem odpovídajícím standardu v daném odvětví. Z toho lze dovodit, že stěžovatelka neshledávala technicky ani jinak nemožným takováto opatření provést.

[37] Uvedené závěry žalovaného považuje NSS za zkratkovité. Posouzení vhodnosti opatření ve smyslu § 13 odst. 1 ZOOÚ musí být založeno na rovnováze mezi zájmy subjektů údajů, které obecně směřují k vyšší úrovni ochrany, a ekonomickými zájmy a technologickými možnostmi správce osobních údajů. Žalovaný nijak nezkoumal reálné ekonomické postavení stěžovatelky (např. pomocí účetních závěrek), aktuální technickou výbavu stěžovatelky a případnou nákladnost související s přechodem na hashovací algoritmus bcrypt vůči celé zákaznické databázi stěžovatelky v roce 2014 (např. šetřením obdobných subjektů). Fakt, že si stěžovatelka ve vlastních interních předpisech stanovila zajistit odpovídající úroveň ochrany osobních údajů, ještě nic nevypovídá o realizovatelnosti zavedení právě hashovacího algoritmu bcrypt (či obdobného). Osobní údaje zákazníků stěžovatelky byly zahashované a podle názoru stěžovatelky přijatá opatření odpovídala obvyklým bezpečnostním standardům v dané době i daném odvětví (viz záznam o bezpečnostní události a výsledcích šetření ze dne 8. 9. 2017 či oznámení narušení bezpečnosti při správě osobních údajů ze dne 27. 8. 2017).

[38] Posouzení kritéria nákladnosti vhodných opatření nebylo ze strany žalovaného dostatečné. NSS nesouhlasí s názorem městského soudu v bodě 55 napadeného rozsudku, že žalovaný dostál požadavkům rozsudku 1 As 238/2021-33 a posoudil veškerá stanovená kritéria. Je pravda, co naznačuje žalovaný a opakuje městský soud v bodě 57 napadeného rozsudku, že ZOOÚ neumožňuje, aby se správce osobních údajů odvolával při uplatňování prostředků ochrany na svoji finanční situaci či další vnitřní omezení. Je totiž logické, že přijetí opatření bude vyžadovat jisté finanční náklady, a správce se tak nemůže úspěšně bránit tím, že nemůže či nechce náklady na zajištění dostatečných opatření ve smyslu § 13 odst. 1 ZOOÚ vydat. To však neznamená, že lze po správci vyžadovat, aby investoval náklady, které jsou nepřiměřené potřebné úrovni bezpečnosti s přihlédnutím k rizikům v konkrétní věci. V tomto ohledu nebylo ke kritériu nákladů dostatečně přihlédnuto. Žalovaný i městský soud nabídli stěžovatelce „ekonomické" varianty, jimiž mohla dostát své povinnosti zabezpečit hesla uživatelských účtů dostatečně odolným algoritmem (tj. přehashování či včasný reset hesel veškerých uživatelských účtů), ale z žádných podkladů dostupných ve spise jejich ekonomická výhodnost, resp. porovnání jejich finanční náročnosti s jinými variantami, nevyplývá, natož posouzení přiměřené nákladnosti právě ve vztahu ke konkrétním okolnostem stěžovatelky. NSS v této souvislosti odkazuje na závěry SDEU učiněné v bodech 45 a 46 výše citovaného rozsudku ve věci C-340/21: „(…) *vnitrostátní soud se nesmí omezit na zjištění, jakým způsobem měl dotyčný správce v úmyslu splnit povinnosti, které pro něj vyplývají z tohoto článku* [32 GDPR]*, ale musí provést meritorní přezkum těchto opatření s ohledem na všechna kritéria uvedená v tomto článku, jakož i na okolnosti projednávané věci a důkazy, které má v tomto ohledu tento soud k dispozici. Takový přezkum vyžaduje provedení konkrétní analýzy povahy a obsahu opatření zavedených správcem, způsobu, jakým byla tato opatření uplatňována, a jejich praktických účinků na úroveň zabezpečení, kterou byl tento správce povinen zajistit s přihlédnutím k rizikům tohoto zpracování*." Namísto toho městský soud přenáší odpovědnost za posouzení kritéria nákladů na stěžovatelku tím, že jí klade k tíži skutečnost, že netvrdila žádné důvody, proč z hlediska nákladů nemohla zavést opatření dostatečně zabezpečující uživatelská hesla (viz bod 57 napadeného rozsudku).

[39] NSS k námitce stěžovatelky doplňuje, že možnost přehashování uváděl žalovaný již v rozhodnutí o rozkladu (bod 38). Listiny týkající se přehashování, které městský soud provedl k důkazu na jednání dne 12. 3. 2025, sloužily k osvědčení skutkového stavu v době rozhodování žalovaného (§ 75 odst. 1 a § 77 odst. 2 s. ř. s.). Tyto dokumenty se však nijak nevztahovaly přímo k činnosti stěžovatelky, proto ani nebylo možné, aby nahradily posouzení kritéria nákladů, ke kterému byl povinen především žalovaný ve správním řízení.

[40] Výslovně nebyla posouzena **kritéria povahy zpracovávaných údajů** a **rizik vyplývajících ze zpracování údajů**. Okolnosti, a tím i zhodnocení, prvního z uvedených kritérií vyplývají z rozhodnutí žalovaného, jenž opakovaně uvedl, že unikla data v podobě jméno, příjmení, e-mailová adresa, heslo k uživatelskému účtu a některá telefonní čísla. Jednalo se tedy o citlivá data,

jejichž zneužití mohlo mít (a v mnoha případech nejspíš i mělo) velmi neblahé důsledky. Bylo však záhodno, aby toto posouzení učinil výslovně sám žalovaný. Rizika vyplývající ze zpracování údajů plynou z rozhodnutí žalovaného v podstatě jen nepřímo. Je jasné, že správa osobních údajů v takovém rozsahu s sebou ponese řadu rizik. Právní úprava mezi zdroji rizik nerozlišuje, jednat se tak může nejen o lidský faktor, ale též o selhání technických zařízení. Je přitom zřejmé, že pojem bezpečnosti bude mít rozdílný obsah právě v závislosti na rizicích, kterým správce údajů, resp. subjekty údajů, čelí. Rozsáhlé databáze či citlivé údaje budou zpravidla vyžadovat výrazně důkladnější zajištění bezpečnosti dat. NSS opět konstatuje, že bylo žádoucí, aby se žalovaný ve svých rozhodnutích konkrétně vyjádřil k tomu, zda přijatá opatření zajišťovala úroveň bezpečnosti odpovídající stávajícím rizikům právě v případě stěžovatelky. Pro tento účel bylo zapotřebí rizika pojmenovat a vyhodnotit. Bez vytyčení rizik odpovídajících konkrétnímu případu a jejich případných důsledků nelze posoudit vhodnost přijatých opatření (srov. závěry rozsudku SDEU ve věci C-340/21 v bodě [28] výše).

[41] Jelikož žalovaný nedostál své povinnosti a dostatečně neposoudil veškerá kritéria uvedená v bodě [27], zejména pak kritérium nákladů vhodných opatření a v dílčí míře i kritéria povahy zpracovávaných údajů a rizika vyplývající ze zpracování těchto údajů, jak mu ukládal závazný právní názor NSS v rozsudku 1 As 238/2021-33, NSS i v nynějším řízení shledal, že ve věci nebylo zjištěno naplnění skutkové podstaty přestupku podle § 45 odst. 1 písm. h) ZOOÚ. Městský soud nezjistil uvedené pochybení žalovaného, a proto je nutné napadený rozsudek a též rozhodnutí předsedy žalovaného zrušit a věc vrátit žalovanému k dalšímu řízení.

### **3.2** *Zbývající kasační námitky*

[42] I přestože je zřejmé, že stěžovatelka byla s kasační stížností úspěšná, NSS se stručně vyjádří i ke zbývajícím kasačním námitkám. Považuje totiž za žádoucí zamezit dalšímu případnému procesnímu „ping-pongu“.

#### 3.2.1 *Použití § 46 odst. 3 ZOOÚ ve znění účinném do 30. 6. 2017*

[43] Vytýkaný protiprávní stav byl odstraněn nejdříve přijetím dostatečných opatření ve smyslu § 13 odst. 1 ZOOÚ, tedy v případě stěžovatelky převedením celé zákaznické databáze na hashovací metodu bcrypt (viz body [31] a [32] výše). Přechod zákaznických účtů na bcrypt byl podle dosavadních zjištění realizován 25. – 27. 8. 2017. Stěžovatelka se v kasační stížnosti dovolává použití § 46 odst. 3 ZOOÚ ve znění účinném do 30. 6. 2017, podle něhož *odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán*.

[44] Přestupek, který je stěžovatelce kladen za vinu, je přestupkem trvajícím. Podle § 2 odst. 4 písm. c) zákona č. 250/2016 Sb. platí: *jestliže se zákon změní během páchání trvajícího přestupku, použije se zákon účinný v době, kdy došlo k odstranění protiprávního stavu*. V posuzované věci tomu odpovídá den 27. 8. 2017, proto se užije § 46 ZOOÚ ve znění účinném od 1. 7. 2017, který již neobsahoval odkazovaný odstavec 3 týkající se zániku odpovědnosti právnické osoby za přestupek, neboť tuto právní úpravu převzal zákon č. 250/2016 Sb.

[45] Se stěžovatelkou lze souhlasit v tom, že v tomto případě činí promlčecí doba tři roky podle § 30 písm. b) zákona č. 250/2016 Sb., délku této lhůty však dále ovlivňují související ustanovení téhož zákona, zejména § 31 odst. 2 písm. c) upravující počátek běhu promlčecí doby a § 32 upravující stavení a přerušení promlčecí doby, což stěžovatelka opomíjí.

[46] Podle namítaného § 37 písm. i) zákona č. 250/2016 Sb. *se při určení druhu správního trestu a jeho výměry u trvajícího přestupku přihlédne k tomu, zda k části jednání, jímž byl přestupek spáchán, došlo za účinnosti zákona, který za přestupek stanovil správní trest mírnější než zákon, který byl účinný při dokončení tohoto jednání*.

Citované ustanovení se podle své dikce využije při určení druhu a výměry správního trestu, nijak ale neovlivňuje otázku zániku odpovědnosti za přestupek. Současně jak v případě § 45 odst. 3 ZOOÚ účinného do 30. 6. 2017, tak v případě shodného ustanovení účinného od 1. 7. 2017 bylo možné za posuzovaný přestupek podle § 45 odst. 1 písm. h) ZOOÚ uložit pokutu až do výše 5 000 000 Kč.

3.2.2 *Nesprávný výrok v rozhodnutí žalovaného*

[47] Stěžovatelka napadá výrok prvostupňového rozhodnutí žalovaného pro jeho nejednoznačnost a rozpor se zjištěným skutkovým stavem. Konkrétně jí vadí dvakrát použité slovo „nejméně" ve vztahu k určení trvání protiprávního stavu a počtu uniklých osobních údajů (tj. „*nejméně do dne 27. srpna 2017*" a „*nejméně 735 956 hesel*"). NSS se ztotožňuje se stěžovatelkou v tom, že bylo žádoucí, aby byl časový údaj určen konkrétně, jelikož je tento údaj ze spisu znám. Shodný názor zastává NSS i vůči počtu uniklých dat. Z obsahu rozhodnutí správních orgánů však neplyne, že by stěžovatelka byla sankciována za nedostatečné hashování po datu 27. 8. 2017 či za vadné hashování přesahující počet 735 956 hesel (viz bod 22 rozhodnutí o rozkladu).

[48] NSS v této souvislosti odkazuje na již citovaný rozsudek 4 As 140/2019-27, podle kterého je smyslem přesného vymezení skutku ve výroku rozhodnutí, kterým je obviněný uznán vinným ze spáchání přestupku, to, aby jeho jednání nebylo zaměnitelné s jiným jednáním a aby byly řádně vymezeny rozhodné okolnosti z hlediska posouzení překážky litispendence, dodržení zásady *ne bis in idem*, překážky věci rozhodnuté, z hlediska vymezení okruhu dokazování a pro zajištění práva na obhajobu (body 40-42). To výrok prvostupňového rozhodnutí splňuje.

3.2.3 *Posouzení uložené pokuty*

[49] NSS nesdílí stěžovatelčiny výtky ve vztahu k odůvodnění uložené pokuty. Žalovaný pečlivě zvážil veškeré okolnosti věci. Nelze říci ani to, že by odpovědnost stěžovatelky za přestupek byla posuzována s ohledem na následek protiprávního jednání. S ohledem na zrušení napadeného rozsudku i rozhodnutí předsedy žalovaného se NSS k uložené sankci více nevyjadřuje, neboť není zřejmé, zda stěžovatelka bude nakonec shledána vinnou z vytýkaného přestupku. NSS tento závěr nijak nepředjímá.

## 4. Závěr a náklady řízení

[50] NSS s ohledem na shora uvedené důvody zrušil rozsudek městského soudu (§ 110 odst. 1 s. ř. s.). Jelikož v této věci byly důvody k tomu, aby bylo zrušeno rozhodnutí předsedy žalovaného již v řízení před městským soudem, NSS zrušil současně rozhodnutí předsedy žalovaného, kterému věc vrátil k dalšímu řízení [§ 110 odst. 2 písm. a) s. ř. s. ve spojení s § 78 odst. 1 a 4 s. ř. s.]. Žalovaný je vázán právním názorem vysloveným NSS v tomto rozsudku (§ 78 odst. 5 s. ř. s.). NSS nemohl na základě dosavadního stavu řízení učinit jednoznačný závěr, zda byla naplněna skutková podstata přestupku podle § 45 odst. 1 písm. h) ZOOÚ, neboť žalovaný dostatečně neposoudil veškerá kritéria určující naplnění skutkové podstaty uvedeného přestupku. Úkolem žalovaného v dalším řízení bude opětovně posoudit kritéria vyjmenovaná v bodě [27], zejména kritérium nákladů a rizik, a to s ohledem na konkrétní okolnosti této věci, a přezkoumatelně zhodnotit, zda se stěžovatelka dopustila daného přestupku. Žalovaný si za tímto účelem opatří relevantní podklady.

[51] O náhradě nákladů řízení rozhodl NSS v souladu s § 60 odst. 1 ve spojení s § 120 s. ř. s. Žalovaný neměl ve věci úspěch, proto nemá právo na náhradu nákladů řízení. Stěžovatelka měla úspěch, má tedy právo na náhradu nákladů řízení o žalobě i kasační stížnosti. NSS je posledním soudem, který o věci rozhodl, proto musí určit náhradu nákladů celého soudního řízení.

[52] Náklady řízení spočívají v prvé řadě v náhradě za zaplacený soudní poplatek ve výši 4 000 Kč v řízení o žalobě (3 000 Kč podání žaloby, 1 000 Kč návrh na přiznání odkladného účinku) a 5 000 Kč v řízení o kasační stížnosti.

[53] Stěžovatelka byla v řízení o žalobě i o kasační stížnosti zastoupena na základě plné moci advokátem Mgr. Luďkem Šrubařem, který učinil čtyři úkony právní služby. Výše odměny se počítá podle vyhlášky č. 177/1996 Sb. (advokátního tarifu) ve znění účinném v době poskytnutí právních služeb. Zástupce stěžovatelky učinil do 31. 12. 2024 dva úkony právní služby (převzetí a příprava zastoupení, sepsání žaloby), za ty mu náleží odměna ve výši 2 x 3 100 Kč a paušální částka ve výši 2 x 300 Kč [§ 7 bod 5; § 9 odst. 4 písm. d); § 11 odst. 1 písm. a), d) a § 13 odst. 4 advokátního tarifu]. Od 1. 1. 2025 učinil zástupce dva úkony právní služby (účast na jednání a sepsání kasační stížnosti), za ty mu náleží odměna ve výši 2 x 4 620 Kč a paušální částka ve výši 2 x 450 Kč [§ 7 bod 5, § 9 odst. 5; § 11 odst. 1 písm. d), g) a § 13 odst. 4 advokátního tarifu]. NSS nepřiznal odměnu a náhradu hotových výdajů za notifikaci o procesním nástupnictví stěžovatelky a repliku v řízení u městského soudu, neboť tato podání nepovažoval za úkony ve smyslu § 11 advokátního tarifu. Vzhledem k tomu, že advokát je plátcem DPH, zvýšil soud částku odměny o příslušnou daň. Náklady za právní zastoupení proto činí 20 497 Kč.

[54] Žalovaný je povinen uhradit stěžovatelce k rukám jejího zástupce náhradu nákladů soudních řízení ve výši 29 497 Kč, a to ve lhůtě 30 dnů od právní moci tohoto rozsudku.

**P o u č e n í :** Proti tomuto rozsudku **n e j s o u** opravné prostředky přípustné.

V Brně dne 4. prosince 2025

L. S.

Ondřej Mrákota v. r.
předseda senátu