ČESKÁ REPUBLIKA

ROZSUDEK
JMÉNEM REPUBLIKY

Městský soud v Praze rozhodl v senátě složeném z předsedkyně JUDr. Naděždy Řehákové a soudců Mgr. Ing. Silvie Svobodové a JUDr. Ivanky Havlíkové v právní věci

žalobce: **L. B.**
bytem X

zastoupen advokátem Mgr. Michalem Chuchútem, LL. M
sídlem náměstí Junkových 2771/1, 155 00 Praha 5

proti
žalovanému: **Úřad pro ochranu osobních údajů,**
sídlem Pplk. Sochora 27, 170 00 Praha 7

za účasti osoby zúčastněné na řízení:

Česká pošta, s. p.
sídlem Politických vězňů 909/4, 110 00 Praha 1

o žalobě proti rozhodnutí generálního ředitele České pošty, s. p. ze dne 7. 10. 2019, č. j. JID: 838838/2019/ČP,

takto:

I. Rozhodnutí generálního ředitele České pošty, s. p. ze dne 7. 10. 2019, č. j. JID: 838838/2019/ČP, se zrušuje a věc se vrací žalovanému k dalšímu řízení.

II. Žalovaný je povinen zaplatit žalobci náhradu nákladů řízení ve výši 11 228 Kč, a to ve lhůtě 1 měsíce od právní moci rozsudku k rukám právního zástupce žalobce Mgr. Michala Chuchúta, LL. M, advokáta.

III. Osoba zúčastněná na řízení nemá právo na náhradu nákladů řízení.

Odůvodnění:

I. Stručné vymezení věci a dosavadní průběh předchozích řízení

1. Žalobce se žalobou podanou dne 9. 12. 2019 u Městského soudu v Praze (dále jen „městský soud“) domáhal přezkoumání rozhodnutí generálního ředitele České pošty, s. p. (dále též „odvolací orgán“) ze dne 7. 10. 2019, č. j. JID: 838838/2019/ČP (dále jen „napadené rozhodnutí“), kterým bylo zamítnuto odvolání žalobce a potvrzeno rozhodnutí České pošty, s. p. (dále jen „prvostupňový orgán“ nebo „Česká pošta“) ze dne 22. 8. 2019, č. j. JID: 714741/2019/ČP (dále jen „nové prvostupňové rozhodnutí“). Novým prvostupňovým rozhodnutím byla odmítnuta žádost žalobce ze dne 10. 3. 2016 o poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „informační zákon“).

2. Dne 10. 3. 2016 požádal žalobce prvostupňový orgán o poskytnutí výsledku posledního dokončeného bezpečnostního auditu informačního systému datových schránek (dále jen „audit“ nebo „informace“) z titulu žádosti o poskytnutí informace podle informačního zákona. Rozhodnutím prvostupňového orgánu ze dne 24. 3. 2016, č. j. JID: 168839/2016/ČP (dále jen „původní prvostupňové rozhodnutí“) bylo odmítnuto poskytnutí požadovaných informací z důvodu, že tyto informace se vztahují k technickému zabezpečení a bezpečnostním procesům v informačním systému datových schránek (dále jen „ISDS“), jedná se tedy o citlivý dokument, jehož zveřejněním by se státní podnik Česká pošta vystavil riziku zneužití informací v konkurenčním prostředí. Dále prvostupňový orgán uvedl, že by poskytnutí výsledku auditu ohrozilo samotné zabezpečení tohoto systému. Tento dokument proto nelze podle původního prvostupňového rozhodnutí považovat za veřejně dostupný.

3. Proti původnímu prvostupňovému rozhodnutí podal žalobce dne 31. 3. 2016 odvolání (dále jen „původní odvolání“), v němž namítal nedostatek upřesnění konkurenčního a bezpečnostního rizika, pro které mu nebyly požadované informace poskytnuty. Odmítnutí poskytnout informaci z důvodu „zneužití v konkurenčním prostředí“ podle žalobce nemůže obstát, neboť nemůže být důvodem pro odmítnutí žádosti podle informačního zákona. Žádné konkurenční riziko navíc nehrozí, neboť Česká pošta má na poskytování ISDS monopol a není jasné, jak by do něj zveřejnění auditu mohlo zasáhnout. Bezpečnostní riziko zveřejnění auditu pak podle žalobce naznačuje, že audit popisuje kritické chyby v ISDS a pokud tyto chyby skutečně existují, měla by se o nich veřejnost dozvědět co nejdříve, neboť odesílané zprávy jsou vystaveny riziku přečtení či pozměnění, čímž je tedy dán výrazný veřejný zájem na poskytnutí této informace.

4. Na základě původního odvolání bylo dne 15. 4. 2016 vydáno rozhodnutí odvolacího orgánu č. j. JID: 209819/2016/ČP, kterým bylo odvolání zamítnuto a rozhodnutí prvostupňového orgánu potvrzeno (dále jen „původní rozhodnutí o odvolání“), neboť se odvolací orgán ztotožnil se závěry původního prvostupňového rozhodnutí, které považoval za srozumitelné a správné a toto rozhodnutí za vydané v mezích zákona. Odvolací orgán v původním rozhodnutí o odvolání uvedl, že zpráva o provedeném

bezpečnostním auditu ISDS je v případě, kdy je Česká pošta poskytovatelem poštovních služeb ryze komerční povahy, považována za citlivý dokument obsahující významné skutečnosti a informace v něm uvedené jsou podřízeny stupni utajení odpovídajícímu jejich významu. Dle nejlepší praxe a doporučení bezpečnostních norem se informace o způsobu zabezpečení ISDS neposkytují třetím osobám, tzn. nikomu, kdo tyto informace nepotřebuje k výkonu své činnosti nebo role. Poskytnutí těchto informací představuje bezpečnostní riziko pro provoz ISDS, umožňuje výrazné usnadnění případného útoku na informační systém, informace by byly mimo jiné návodem, které nástroje použít, či o které zneužití se pokoušet.

5. Odvolací orgán dále uvedl, že způsob zabezpečení ISDS je duševním vlastnictvím vlastníka a provozovatele ISDS a jejich návrh a nastavení má svoji cenu. Společnosti, které poskytují obdobné systémy, mají zájem o tyto informace k využití v systémech, které konkurují službám, které poskytuje Česká pošta, což není v jejím zájmu. Bezpečnostní audit ISDS a v něm obsažené informace jsou tedy obchodním tajemstvím České pošty stejně, jako by byly obchodním tajemstvím každého jiného podnikatelského subjektu.

6. Odvolací orgán konstatoval, že výsledky auditu potvrzují soulad s požadavky informační bezpečnosti a rizika vyplývající pro uživatele ISDS jsou minimální, přičemž zárukou v tomto ujištění je osvědčení auditora, které odvolací orgán jako přílohu napadeného rozhodnutí žalobci poskytl.

7. Dne 26. 6. 2016 podal žalobce proti původnímu rozhodnutí o odvolání včasnou žalobu k městskému soudu (dále jen „první žaloba“), která byla projednána v řízení sp. zn. 9 A 113/2016. Žalobce v první žalobě namítal nezákonnost původního rozhodnutí o odvolání a jeho nepřezkoumatelnost pro nedostatek důvodů. Konkrétně s odkazem na rozsudek Nejvyššího správního soudu ze dne 27. 3. 2008, č. j. 7 As 24/2007-106, vytýkal nedostatečné posouzení, zda zájem na kontrole veřejné správy v tomto případě převyšuje zájem žalovaného na ochraně informací a dále také absenci posouzení, zda požadované informace skutečně naplňují definici obchodního tajemství obsaženou v § 504 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“). K porovnání zájmů žalobce rozvedl, že na relevantním trhu provozování infrastruktury datových schránek je Česká pošta jediným dodavatelem, který tak má monopolní postavení. Stát platí monopolnímu veřejnému provozovateli dotaci zhruba 10 Kč za každou odeslanou datovou zprávu. Je v zájmu státu, aby veřejnost měla přesvědčivý doklad o zabezpečení státního systému komunikace. Z osvědčení auditora vyplývá, že byly zjištěny blíže neupřesněné „*nedostatky v efektivitě bezpečnostních opatření*“, které byly eliminovány „*na úroveň akceptovatelnou vedením České pošty, s. p.*“. Toto konstatování vyvolává důvodnou obavu z možné nedostatečné úrovně zabezpečení systému datových schránek, a je tak dán veřejný zájem na tom, aby každý uživatel mohl sám posoudit, zda úroveň akceptovatelná vedením České pošty je akceptovatelná i pro jeho písemnosti, které odesílá datovou schránkou. Ke konkrétnímu důvodu odmítnutí informace, jímž je obchodní tajemství, žalobce namítal, že Česká pošta nijak nedoložila, jaké konkrétní části auditu jsou obchodním tajemstvím a to, že skutečnosti v nich obsažené jsou konkurenčně významné, běžně nedostupné a ocenitelné.

8. Ve vyjádření k první žalobě Česká pošta uvedla, že povinnost podrobovat ISDS auditu vyplývá ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „zákon o systémech VS“). Audit ISDS obsahuje zjištění vztahující se k technickému zabezpečení a bezpečnostním

procesům v ISDS. Jedná se tedy o citlivý dokument, jehož zveřejněním by se Česká pošta vystavila riziku zneužití informací a případnému zneužití informací v konkurenčním prostředí. ISDS patří do systému kritické infrastruktury státu a poskytnutí výsledků auditu bezpečnosti by ohrozilo samotné zabezpečení tohoto systému. Audit bezpečnosti systému ISDS není možné považovat za veřejně dostupný a nelze ho tedy zveřejnit. K informacím o zabezpečení systému ISDS mají přístup jen ty osoby, které je potřebují pro výkon své činnosti. Z bezpečnostních důvodů se informace třetím osobám neposkytují. Pokud by se informace o zabezpečení systému ISDS dostaly do nepovolaných rukou, mohlo by to ohrozit provoz daného systému, výrazně usnadnit případný útok na systém.

9. Česká pošta dále poukázala na to, že bezpečnostní audit ISDS a v něm obsažené informace jsou obchodním tajemstvím, neboť splňují všechny znaky charakterizující obchodní tajemství uvedené v § 504 občanského zákoníku. Požadované informace tedy není možné žalobci poskytnout s odkazem na § 9 odst. 1 informačního zákona.

10. Rozsudkem městského soudu ze dne 29. 4. 2019, č. j. 9 A 113/2016-41, bylo původní rozhodnutí o odvolání zrušeno a věc byla vrácena České poště k dalšímu řízení (dále jen „původní rozsudek“). Městský soud shledal, že odmítnutí informace nevychází z náležitého posouzení a odůvodnění, v jakých údajích a skutečnostech kontrolované činnosti spatřuje prvostupňový orgán naplnění jednotlivých, výše zmíněných znaků obchodního tajemství a jak jsou tyto informace tím, kdo vykonává právo k obchodnímu tajemství za obchodní tajemství označeny. Z původního rozhodnutí o odvolání nebylo zřejmé, zda prvostupňový orgán či někdo jiný již v době před podáním žádosti o informace označil tyto informace za obchodní tajemství a z jakých důvodů považuje Česká pošta provedený bezpečnostní audit za obchodní tajemství jako celek. Jestliže v daném případě o pojmových znacích není v původním rozhodnutí o odvolání pojednáno vůbec, přičemž z definice obchodního tajemství je patrné, že pojmové znaky musejí být naplněny kumulativně, je zřejmé, že se jedná o rozhodnutí nepřezkoumatelné pro nedostatek důvodů.

11. Odvolací orgán povinného subjektu, vázán právním názorem uvedeným v původním rozsudku, vydal dne 29. 7. 2019 rozhodnutí č. j. JID:646152/2019/ČP, o zrušení původního prvostupňového rozhodnutí a vrácení věci prvostupňovému orgánu k dalšímu řízení v prvním stupni (dále jen „nové rozhodnutí o odvolání“). V dalším řízení měl prvostupňový orgán odstranit vytýkané vady - nedostatek odůvodnění rozhodnutí, v intencích závazného názoru městského soudu a ustálené judikatury správních soudů v původním rozsudku uvedené.

12. Prvostupňový orgán vydal dne 22. 8. 2019 nové prvostupňové rozhodnutí, jímž žádost žalobce opětovně odmítl. K odmítnutí postupem podle § 15 odst. 2 informačního zákona ve spojení s § 9 odst. 1 byl doplněn další důvod odmítnutí podle § 11 odst. 1 písm. d) informačního zákona a § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“). V novém prvostupňovém rozhodnutí prvostupňový orgán nejprve vymezil postavení povinného subjektu, Ministerstva vnitra a Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Dále se zabýval důvodem pro poskytnutí informací, které žalobce uvedl v předchozích podáních, přičemž zohlednil i účel žádosti o poskytnutí informací. V této části došel k závěru, že veřejný zájem na poskytnutí informací (informovanost uživatelů) nepřevažuje veřejný zájem na ochranu informací (z důvodu bezpečnosti systému kritické informační infrastruktury).

13. Hlavní důvod pro neposkytnutí informací povinný subjekt shledal v ustanovení § 10a ZKB. Uvedl, že ustanovení § 10a ZKB je ve vztahu speciality k informačnímu zákonu. Zabýval se otázkou, zda jsou požadované informace toho charakteru, že by jejich zpřístupnění mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle ZKB. Prvostupňový orgán zároveň konzultoval možnost poskytnutí informací též s dozorovým orgánem, jímž je v oblasti kybernetické bezpečnosti NÚKIB. Podle vyjádření NÚKIB by poskytnutí informací znamenalo porušení ZKB. Z hlediska důvěrnosti jsou informace – aktiva, dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „VKB“) označena stupněm „vysoká“. Bezpečnostní audit ISDS (tj. zpráva jako celek) je označena jako „citlivé - interní“. Rovněž provedl test oddělitelnosti, kdy dospěl k závěru, že žádnou část výsledku bezpečnostního auditu ISDS nemůže poskytnout.

14. Prvostupňový orgán se dále v poslední části odůvodnění nového prvostupňového rozhodnutí zabýval neposkytnutím informací podle § 9 odst. 1 informačního zákona a jednotlivými definičními znaky obchodního tajemství se závěrem, že popis technické specifikace ISDS představuje obchodní tajemství povinného subjektu.

II. Napadené rozhodnutí

15. Žalobce podal dne 6. 9. 2019 proti novému prvostupňovému rozhodnutí odvolání, v němž uvedl, že nové prvostupňové rozhodnutí o odmítnutí žádosti o informace trpí vadou nepřezkoumatelnosti stejně jako původní prvostupňové rozhodnutí. *První odvolací námitkou* napadl, že požadovaný audit je označen pouze jako interní, tudíž jeho neposkytnutí neodpovídá ani doporučení NÚKIB dle §10a ZKB. Ve *druhé odvolací námitce* se zabýval testem proporcionality, kdy dle jeho názoru prvostupňový orgán žádným způsobem nevysvětlil, jak by mohlo poskytnutí jednotlivých informací obsažených v auditu ohrozit zajišťování kybernetické bezpečnosti. V části vztahující se k veřejnému zájmu se prvostupňový orgán nijak nevypořádal s informací, že bezpečnostní audit zjistil nedostatky. K obchodnímu tajemství v poslední, *třetí odvolací námitce* uvedl, že odůvodnění nového prvostupňového rozhodnutí neobsahuje vyhodnocení všech definičních znaků obchodního tajemství. Zároveň uvedl, že prvostupňový orgán zcela pominul to, že audit zjistil bezpečnostní nedostatky, ačkoliv tato informace je součástí správního spisu.

16. V napadeném rozhodnutí se odvolací orgán zcela ztotožnil se závěry uvedenými v novém prvostupňovém rozhodnutí, zejména se závěry, které vedly povinný subjekt k odmítnutí žádosti z důvodu uvedeného v § 10a ZKB. Napadeným rozhodnutím shledal, že prvostupňový orgán postupoval při vydání nového prvostupňového rozhodnutí v souladu s právními předpisy. Nové prvostupňové rozhodnutí obsahuje, dle jeho mínění, podrobné zdůvodnění neposkytnutí informací, včetně uvedení testu proporcionality. Odvolací orgán neshledal v novém prvostupňovém rozhodnutí žádné vady, které by vedly k jeho nepřezkoumatelnosti pro nedostatek důvodů.

17. Odvolací orgán uvedl, že ISDS jako systém kritické infrastruktury státu je zvlášť chráněn v oblasti kybernetické bezpečnosti. Tato ochrana spočívá nejen v technickém zabezpečení systému, ale rovněž v ochraně informací, které by mohly ohrozit bezpečnost systému. Pouhá možnost ohrožení bezpečnosti je v tomto případě dostatečná pro zajištění utajení informací podle § 10a ZKB. Každá jedna informace představuje riziko kompromitace ISDS, proto je celá zpráva vnímána z pohledu bezpečnosti, jako významný zdroj citlivých

informací. Po jednotlivých kapitolách obsahuje zpráva vždy úplnou informaci o tom, jak lze konkrétní oblast kompromitovat, resp. jaké zabezpečení je použito k tomu, aby k narušení bezpečnosti nedošlo.

18. K *první odvolací námitce* odvolací orgán uvedl, že již v novém prvostupňovém rozhodnutí bylo zcela bez pochyb uvedeno, že se podle vyhlášky o kybernetické bezpečnosti označuje požadovaná informace stupněm „vysoká“. Klasifikace dokumentu jako „interní“ je jiné povahy a znamená, že dokument jako takový není určen pro osoby mimo povinný subjekt.

19. Ohledně *druhé odvolací námitky* vztahující se k testu proporcionality odvolací orgán uvedl, že test proporcionality je proveden v odstavcích (18) až (21), přičemž závěr je uveden v odstavci (20) nového prvostupňového rozhodnutí. Podrobný popis bezpečnostního rizika se promítá téměř v celém odůvodnění [např. odstavce (15), (16) či (24) nového prvostupňového rozhodnutí]. K námitce, že část věnovaná veřejnému zájmu zcela pomíjí to, že audit zjistil bezpečnostní nedostatky, odvolací orgán uvádí, že taková informace součástí správního spisu není. Naopak, součástí správního spisu je osvědčení auditora, které bylo zasláno již v rámci prvního rozhodnutí o odvolání a které zcela jasně uvádí, že výsledky auditu potvrzují soulad ISDS s požadavky informační bezpečnosti. Tato skutečnost je rovněž v novém prvostupňovém rozhodnutí uvedena.

20. K nedostatečnému vymezení obchodního tajemství, namítaného *třetí odvolací námitkou* odvolací orgán uvedl, že popis naplnění jednotlivých znaků obchodního tajemství dle části V. nového prvostupňového rozhodnutí pokládá za vyčerpávající.

21. Napadeným rozhodnutím proto odvolací orgán dospěl k závěru, že odvolání je nedůvodné a nové prvostupňové rozhodnutí potvrdil.

III. Žaloba

22. Žalobou podanou u městského soudu žalobce navrhoval zrušení napadeného rozhodnutí, jakož i nového prvostupňového rozhodnutí.

23. *První žalobní námitkou,* ve vztahu k označení technické specifikace datových schránek za obchodní tajemství, žalobce namítal, že takový závěr nelze bez dalšího zdůvodnění konstatovat. Technická specifikace byla z větší části Českou poštou zveřejněna způsobem umožňujícím dálkový přístup, ať už přímo (např. pro vývojáře externích aplikací, kteří používají rozhraní datových schránek), v provozním řádu datových schránek (v technických přílohách 1 - 7) nebo v rozsahu nutném pro zadávání veřejných zakázek. Žalobce ale ani poskytnutí technické specifikace datových schránek nepožadoval. Požadoval pouze poskytnutí auditu datových schránek, který je fakticky tabulkou, do které se doplňují informace o splnění jednotlivých zákonných náležitostí. Samotný audit obsahuje kapitoly definující cíle, předmět a kritéria auditu, v kapitole zjištění pak uvádí například to, zda jsou pravidelně prováděny audity nebo zda jsou zaměstnanci školeni, tedy informace o tom, zda byl audit proveden dle vyhlášky a zda jsou splněny zákonné náležitosti. Žádná z těchto informací nemůže být, dle názoru žalobce, obchodním tajemstvím, neboť vůbec není obchodního charakteru. Stejně tak nemohou být obchodním tajemstvím cíle auditu, předmět auditu a jeho kritéria, neboť by měly přesně odpovídat požadavkům vyhlášky, která je veřejně dostupná.

24. Městský soud v původním rozsudku v této věci analogicky odkázal na rozsudek Nejvyššího správního soudu (dále také jen „NSS“) ze dne 17. 12. 2014, č. j. 9 As 180/2014-

37, dle kterého obchodním tajemstvím není forenzní audit ve svém celku. Žalovaný tento rozsudek nereflektoval a opět bez dalšího uvedl, že „*obchodní tajemství tvoří převážnou část požadovaných informací*“, aniž by tento závěr blíže odůvodnil.

25. *Druhá žalobní námitka* se vztahovala k důvodu odmítnutí poskytnutí informace z důvodu ohrožení účinnosti bezpečnostního opatření, kdy Česká pošta uvedla, že audit obsahuje například výsledky z provedení penetračního testování. Žalobce se domníval, že tato informace je nepravdivá, neboť v takovém případě by audit nebyl proveden dle vyhlášky. Uvedl, že nepožadoval ani poskytnutí penetračního testu (pokus o průnik do systému s popisem konkrétních zranitelností), stejně tak nežádal například o poskytnutí code review (analýza kvality zdrojového kódu s popisem konkrétních zranitelností).

26. Obsahem *třetí žalobní námitky* je tvrzení, že Česká pošta neprovedla vážení zájmu na ochranu informací a veřejného zájmu, když k tomuto pouze konstatovala, že běžný uživatel není schopen tyto technické aspekty zabezpečení posoudit.

27. *Čtvrtou žalobní námitkou* žalobce konstatoval, že i pokud by některé požadované informace mohly ohrozit účinnost bezpečnostního opatření a tento zájem by převážil nad veřejným zájmem na straně žalobce, měla Česká pošta postupovat analogicky dle původního rozsudku v této věci a poskytnout alespoň část auditu v anonymizované verzi.

IV. Vyjádření České pošty

28. Česká pošta ve vyjádření k žalobě po rekapitulaci předchozích řízení vymezila, že bezpečnostní audit ISDS obsahuje popis technické specifikace ISDS, která je unikátním zákaznickým řešením. Zveřejněna byla dle žalobce pouze malá část tohoto popisu. Vymezení definičních znaků obchodního tajemství bylo podrobně rozebráno ve vztahu k této části auditu a výsledkem bylo, že popis technické specifikace ISDS je obchodním tajemstvím. Česká pošta rovněž nesouhlasila s přirovnáním k forenznímu auditu. K tomuto dále uvedla, že zbytek auditu neposkytla, neboť poskytnutí informace jako celku bylo odmítnuto z jiného důvodu.

29. K druhé žalobní námitce Česká pošta uvedla, že není zřejmé, kterou vyhlášku žalobce myslí, neboť VKB nebyla v době auditu platná a v platnosti byla dnes již neúčinná vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „SVKB“). Soulad auditu s blíže nespecifikovanou vyhláškou navíc není dle České pošty předmětem tohoto řízení.

30. V reakci na třetí žalobní námitku uvedla, že test proporcionality byl proveden řádně správním orgánem prvního i druhého stupně. K poslední, čtvrté žalobní námitce lze z vyjádření seznat, že dle mínění České pošty byly naplněny důvody pro neposkytnutí informace v celém rozsahu, právě z důvodu § 10a ZKB.

31. Z uvedených důvodů Česká pošta navrhla, aby soud podanou žalobu jako nedůvodnou zamítl.

V. Změna v osobě žalovaného a jeho vyjádření

32. Městský soud konstatuje, že na základě článku XV bodu 17 zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů (dále jen „zákon č. 111/2019 Sb.“), byl novelizován § 20 odst. 5 informačního

zákona. Dle § 20 odst. 5 informačního zákona, ve znění předcházejícím této novele, nebylo-li podle dřívější úpravy možné určit nadřízený orgán dle § 178 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“), rozhodoval v odvolacím řízení a řízení o stížnosti ten, kdo stál v čele povinného subjektu (tedy v nyní posuzované věci generální ředitel České pošty). Dle novelizovaného znění § 20 odst. 5 informačního zákona v takových případech rozhoduje v odvolacím řízení a v řízení o stížnosti Úřad pro ochranu osobních údajů (dále též „Úřad“ nebo „žalovaný“). Dřívější úpravu § 20 odst. 5 informačního zákona bylo možno použít jen do 1. 1. 2020 (čl. XVI zákona č. 111/2019 Sb.), počínaje následujícím dnem se proto použije úprava nová, a to i na probíhající řízení. U povinné osoby (České pošty) není možné určit podle § 178 správního řádu, kdo je jejím nadřízeným správním orgánem. V projednávané věci tedy s účinností od 2. 1. 2020 přešla ze zákona působnost k rozhodování o odvolání proti rozhodnutí o odmítnutí poskytnutí informace z osoby stojící v čele povinného subjektu, u nějž nelze nadřízený orgán určit dle § 178 správního řádu, na Úřad.

33. Dle § 69 zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů (dále jen „s. ř. s.“) je v řízení o žalobě proti rozhodnutí správního orgánu žalovaným správní orgán, který rozhodl v posledním stupni, nebo správní orgán, na který jeho působnost přešla. Ustanovení § 69 s. ř. s. tak upravuje specifický případ procesního nástupnictví, odlišný od úpravy obsažené v § 107 a § 107a zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů (dále jen „o. s. ř.“). Při přechodu působnosti v důsledku změny zákona proto musí soud jednat s orgánem, na který přešla působnost. Neučiní-li tak, zatíží řízení vadou, která má za následek nezákonnost rozhodnutí o věci samé (obdobně rozsudek Nejvyššího správního soudu ze dne 30. 10. 2020, č. j. 4 As 155/2020-42). Žaloba byla podána ke zdejšímu soudu dne 9. 12. 2019, působnost rozhodovat o odvolání žalobce však přešla dne 2. 1. 2020 na Úřad. Městský soud tedy nadále jednal s Úřadem jako žalovaným a vyzval jej k vyjádření k žalobě.

34. Úřad ve vyjádření k žalobě ze dne 15. 8. 2022 odkázal na argumentaci České pošty, která se ke všem žalobním bodům ve svém podání vyjádřila. Z důvodu procesní opatrnosti poté navrhl, aby soud žalobu jako nedůvodnou zamítl.

35. Úřad se dále vyjádřil k možné náhradě nákladů řízení pro případ úspěchu žalobce ve věci. K tomu poukázal na specifické okolnosti přechodu působnosti strany žalované na Úřad, které s ohledem na judikaturu správních soudů při rozhodování o nákladech řízení považoval za důvody zvláštního zřetele hodné, pro které by žalovanému neměla být povinnost nahradit náklady uložena.

36. Česká pošta podáním ze dne 19. 9. 2022 uplatnila práva osoby zúčastněné na řízení s tím, že setrvala na svém vyjádření k žalobě, které soudu zaslala jako původní strana žalovaná.

VI. Posouzení věci Městským soudem v Praze

37. Městský soud v Praze nejprve ověřil, že žaloba byla podána včas. Podle § 72 odst. 1 s. ř. s. „*žalobu lze podat do dvou měsíců poté, kdy rozhodnutí bylo žalobci oznámeno doručením písemného vyhotovení nebo jiným zákonem stanoveným způsobem, nestanoví-li zvláštní zákon lhůtu jinou.*“ Podle § 40 odst. 3 s. ř. s. „*připadne-li poslední den lhůty na sobotu, neděli nebo svátek, je posledním dnem lhůty nejblíže následující pracovní den*“. V daném případě bylo napadené rozhodnutí žalobci doručeno dne 8. 10. 2019, posledním dnem lhůty pro podání žaloby tak bylo v souladu s § 72 odst. 1 s. ř. s. ve spojení s § 40 odst. 3 s. ř. s. pondělí 9. 12.

2019, kdy byla také žaloba doručena soudu. Dále soud ověřil, že žaloba byla podána osobou k tomu oprávněnou (§ 65 odst. 1 s. ř. s.) a že se jedná o žalobu přípustnou, splňující všechny formální náležitosti na ni kladené (§ 65, § 68 a § 70 s. ř. s.).

38. Soud přezkoumal žalobou napadené rozhodnutí i řízení, které mu předcházelo, podle skutkového a právního stavu ke dni rozhodování žalovaného (§ 75 odst. 1 s. ř. s.), a to v mezích uplatněných žalobních bodů (§ 75 odst. 2 s. ř. s.), jakož i z pohledu vad, k nimž je povinen přihlížet z úřední povinnosti a dospěl k závěru, že žaloba je důvodná.

39. O podané žalobě rozhodl soud v souladu s § 51 odst. 1 s. ř. s. bez nařízení jednání, když souhlas účastníků byl v souladu s § 51 odst. 1 věty druhé s. ř. s. presumován; nadto soud shledal důvody pro zrušení napadeného rozhodnutí bez nařízení jednání podle § 76 odst. 1 písm. a) s. ř. s.

40. Soud předesílá, že z hlediska soudního přezkumu představují rozhodnutí správních orgánů obou stupňů jeden celek (srov. usnesení rozšířeného senátu Nejvyššího správního soudu ze dne 12. 10. 2004, č. j. 5 Afs 16/2003-56).

41. V souzené věci je mezi účastníky řízení spor o poskytnutí informace na základě informačního zákona, kterou je výsledek bezpečnostního auditu ISDS vyhotovený dle zákona o systémech VS.

42. Právo na informace je garantováno každému na základě čl. 17 odst. 4 Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdější předpisů (dále jen „LZPS“). Provádění tohoto základního práva zabezpečuje informační zákon, jenž je vystavěn na principu obecné povinnosti poskytovat veškeré informace týkající se působnosti povinných subjektů s taxativně vymezenými výlukami z této povinnosti.

43. Dle Nejvyššího správního soudu „*je smyslem práva na informace kontrola činnosti veřejné správy, mj. též kontrola vynakládání veřejných prostředků a hospodaření s veřejným majetkem*“ (NSS 1 As 17/2008-67, Sb. NSS č. 1627/2008) a „*poskytování informací o činnosti orgánů veřejné moci je v našem civilizačním prostoru obecným standardem demokratických právních států, který logicky vyžaduje jisté finanční zatížení orgánů veřejné správy*“ (NSS 6 As 79/2006-58, Sb. NSS č. 1342/2007), jakož i to, že „*povinný subjekt není oprávněn jakkoli zkoumat a zabývat se otázkou účelnosti a důvodnosti žadatelovy žádosti či jeho motivy*“ (NSS 6 As 79/2006-58, Sb. NSS č. 1342/2007).

44. Při posouzení věci vycházel soud z následující právní úpravy.

45. Dle čl. 17 odst. 4 LZPS lze „*svobodu projevu a právo vyhledávat a šířit informace omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti*“.

46. Dle § 9 odst. 1 informačního zákona „*povinný subjekt informaci neposkytne, pokud je požadovaná informace obchodním tajemstvím*“.

47. Dle § 9 odst. 2 informačního zákona se „*při poskytování informace, která se týká používání veřejných prostředků, nepovažuje poskytnutí informace o rozsahu a příjemci těchto prostředků za porušení obchodního tajemství*“.

48. Dle § 11 odst. 1 písm. d) informačního zákona (vložen do § 11 novelou účinnou od 23. 4. 2019) může „*povinný subjekt omezit poskytnutí informace, pokud: její poskytnutí významně*

nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku".

49. Dle § 12 informačního zákona „*všechna omezení práva na informace provede povinný subjekt tak, že poskytne požadované informace včetně doprovodných informací po vyloučení těch informací, u nichž to stanoví zákon. Právo odepřít informaci trvá pouze po dobu, po kterou trvá důvod odepření. V odůvodněných případech povinný subjekt ověří, zda důvod odepření trvá*".

50. Dle § 15 odst. 1 informačního zákona „*pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, popřípadě o odmítnutí části žádosti, s výjimkou případů, kdy se žádost odloží*".

51. Dle § 15 odst. 2 informačního zákona „*nebylo-li žádosti vyhověno z důvodů ochrany obchodního tajemství podle § 9 nebo ochrany práv třetích osob k předmětu práva autorského podle § 11 odst. 2 písm. c), musí být v odůvodnění rozhodnutí uvedeno, kdo vykonává právo k tomuto obchodnímu tajemství nebo kdo vykonává majetková práva k tomuto předmětu ochrany práva autorského, je-li tato osoba povinnému subjektu známa*".

52. Dle § 10a ZKB (vložen do ZKB novelou účinnou od 1. 8. 2017) se „*informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, podle předpisů upravujících svobodný přístup k informacím neposkytují*".

53. Dle přílohy č. 4 SVKB obsahuje „*Zpráva z auditu kybernetické bezpečnosti: a) Cíle auditu kybernetické bezpečnosti, b) Předmět auditu kybernetické bezpečnosti, c) Kritéria auditu kybernetické bezpečnosti, d) Identifikování týmu auditorů a osob, které se auditu kybernetické bezpečnosti zúčastnily, e) Datum a místo, kde byly prováděny činnosti při auditu kybernetické bezpečnosti, f) Zjištění z auditu kybernetické bezpečnosti, g) Závěry auditu kybernetické bezpečnosti*".

54. Dle § 16 VKB „*Povinná osoba v rámci auditu kybernetické bezpečnosti (a) provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a (b) posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu*".

55. Dle § 504 občanského zákoníku „*obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení*".

56. Soud o věci uvážil následovně.

57. Podle obsahu správního spisu bylo v původním prvostupňovém rozhodnutí odmítnutí poskytnutí informace jako celku odůvodněno ochranou obchodního tajemství podle § 9 odst. 1 informačního zákona. V novém prvostupňovém a následně v napadeném rozhodnutí žalovaný setrval u zdůvodnění odepření poskytnutí informace ochranou obchodního tajemství podle § 9 odst. 1 informačního zákona pouze ve vztahu k části informace (technická specifikace). Nově pak žalovaný zdůvodnil odepření poskytnutí informace jako celku ochranou kybernetické bezpečnosti podle § 10a ZKB a ohrožením

bezpečnostního opatření podle zvláštního předpisu na základě § 11 odst. 1 písm. d) informačního zákona.

58. Jelikož v části nyní projednávané věci (odmítnutí poskytnutí informace z důvodu ochrany obchodního tajemství) již bylo správním soudem dříve rozhodnuto a původní prvostupňové rozhodnutí bylo následně novým rozhodnutím o odvolání zrušeno, zabýval se městský soud nejprve naplněním § 78 odst. 5 s. ř. s., tedy otázkou vázanosti správního orgánu zrušujícím rozhodnutím soudu. V původním rozsudku zdejšího soudu lze vymezit dva zásadní okruhy pochybení správního orgánu, a to neuvedení, v čem žalovaný spatřuje naplnění jednotlivých znaků obchodního tajemství dle obchodního zákoníku, a absenci poskytnutí anonymizované části informace.

59. Naplnění definice obchodního tajemství bylo v původním prvostupňovém rozhodnutí pouze obecně vymezeno výčtem jednotlivých pojmových znaků a konstatováním, že došlo k jejich naplnění. Jak je přiléhavě uvedeno v rozsudku NSS ze dne 22. 3. 2016, č. j. 9 As 155/2015 - 195, *„aplikace ochrany obchodního tajemství vůči konkrétním informacím vyžaduje, aby povinný subjekt v rozhodnutí o (částečném) odmítnutí žádosti - má-li rozhodnutí dostát požadavkům kladeným správním řádem (jeho § 68 odst. 3) na přezkoumatelnost rozhodnutí - náležitě a vyčerpávajícím způsobem odůvodnil, jaké informace obsažené v požadovaném (a plně nebo částečně odepřeném) dokumentu považuje za obchodní tajemství a uplatňuje u nich ochranu dle § 9 odst. 1 informačního zákona. To především znamená, že povinný subjekt musí v odůvodnění svého rozhodnutí ve vztahu ke každé odepřené informaci objasnit, v čem spatřuje naplnění všech znaků legální definice obchodního tajemství*“.

60. Prvostupňový orgán v novém prvostupňovém rozhodnutí uvádí, že obchodním tajemstvím je popis technické specifikace ISDS, jenž je unikátním zákaznickým řešením. S vymezením jednotlivých definičních znaků ve vztahu k části auditu – k technické specifikaci ISDS se prvostupňový orgán dostatečně vypořádal v odstavcích (30) až (37) prvostupňového rozhodnutí, kdy ke každému z pojmových znaků konkrétně uvedl, jak jej technická specifikace naplňuje.

61. K tomuto soud uzavírá, že se ztotožňuje s tvrzením žalovaného, že v novém prvostupňovém rozhodnutí již došlo k dostatečnému vymezení části auditu jako obchodního tajemství v intencích původního rozsudku městského soudu a ve smyslu shora citované judikatury správních soudů.. V tomto rozsahu proto považuje městský soud odmítnutí poskytnutí informace za souladné s právními předpisy. Nedostatečné zdůvodnění označení technické specifikace jako obchodního tajemství bylo namítáno žalobcem v první žalobní námitce, kterou soud tímto považuje za vypořádanou a nedůvodnou, neboť již bylo náležitě a vyčerpávajícím způsobem odůvodněno, jaké informace obsažené v požadovaném dokumentu považuje povinný subjekt za obchodní tajemství a uplatňuje u nich ochranu dle § 9 odst. 1 informačního zákona a rovněž náležitě objasněno, v čem je spatřováno naplnění všech znaků legální definice obchodního tajemství ve vztahu ke konkrétní části požadované informace.

62. Technická specifikace však tvoří pouze část požadovaného auditu, proto bylo nezbytné, aby povinný subjekt aplikoval další ze závazných názorů vyslovených městským soudem v původním rozsudku, a to povinnost zveřejnit tu část auditu, ke které se uplatněná výjimka nevztahuje, byť v podobě výrazně anonymizované. Jak vymezil městský soud v původním rozsudku: *„je-li v dokumentu obchodní tajemství (nebo alespoň zčásti) obsaženo, je z praxe zřejmé, že obchodní tajemství tvoří ve většině případů jen část určitého dokumentu.*

Povinný subjekt tedy v souladu s § 12 informačního zákona může poskytnout žadateli ty části dokumentů, z nichž eliminuje (většinou anonymizací) ty části či pasáže, které mají povahu obchodního tajemství. Takto povinný subjekt postupuje i v případě, kdy poskytnutý text bude anonymizován tak výrazně, že se jeho poskytnutá část může jevit jako nesrozumitelná".

63. Obchodním tajemstvím mohou být pouze „skutečnosti," tj. ve smyslu informačního zákona „informace" (§ 3 odst. 3), vykazující pojmové znaky obchodního tajemství. To především znamená, že předmětem ochrany obchodního tajemství ve smyslu komentovaného ustanovení zásadně není určitý dokument (např. smlouva) jako celek, nýbrž toliko skutečnosti (informace) ve smlouvě uvedené, které splňují pojmové definiční znaky stanovené zákonem (srov. např. rozsudek KS v Hradci Králové č. j. 31 Ca 189/2000-27, 857/2001 SJS, rozsudek NSS č. j. 2 As 27/2007-87, rozsudek NSS č. j. A 2/2003-73, 1469/2008 Sb. NSS, rozsudek MS v Praze sp. zn. 7 Ca 30/2003-39, rozsudek KS v Praze sp. zn. 44 Ca 82/2005 aj.).

64. V projednávané věci prvostupňový orgán zbývající část požadovaného auditu nezveřejnil, a to s odkazem na existenci nových důvodů pro odmítnutí poskytnutí informace podle § 10a ZKB a podle § 11 odst. 1 písm. d) informačního zákona, kdy byly dle prvostupňového orgánu naplněny důvody pro odmítnutí poskytnutí informace jako celku, což žalobce rozporuje druhou žalobní námitkou.

65. Ve vztahu k poskytnutí zbývající části požadované informace je nutné posoudit, zda jde o informace spadající pod dikci § 10a ZKB. Předmětné ustanovení bylo do ZKB vloženo novelou účinnou od 1. 8. 2017. Dle důvodové zprávy k novelizačnímu zákonu „*stávající úprava* (pozn. soudu: tedy před 1. 8. 2017) *obsažená v § 11 odst. 4 zmiňovaného zákona však cílí pouze na úzký okruh informací, konkrétně na informace z evidence incidentů vedené podle § 9 zákona o kybernetické bezpečnosti.* [...]*Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. Z tohoto důvodu se předkladatel rozhodl [...] pro doplnění výjimky z povinnosti poskytovat informace na základě zákona o svobodném přístupu k informacím o údaje, které se týkají zajišťování kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti*".

66. Důvodová zpráva dále uvádí, že jde o „*informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle tohoto zákona. Těmito opatřeními jsou varování, reaktivní opatření a ochranná opatření. Jedná se o instituty, jejichž zveřejnění ne vždy může ohrozit jejich účinnost, případně mít dopad na zajišťování kybernetické bezpečnosti, z tohoto důvodu jsou v návrhu ustanovení § 10a uvedeny zvlášť. Předkladatel návrhu zákona se domnívá, že toto omezení práva na informace je plně v souladu s čl. 17 odst. 4 LZPS, když dospěl k názoru, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převážil požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti, přičemž považuje za nutné konstatovat, že povinný subjekt bude vždy při rozhodování o žádosti o poskytnutí informací povinen posoudit, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a pečlivě v daném případě zvažovat potřebu omezení práva na informace*".

67. Dle doporučení NÚKIB k ustanovení § 10a ZKB ze dne 29. 1. 2019 (dostupné na internetových
stránkách NÚKIB zde: https://www.nukib.cz/download/publikace/podpurne_materialy/

Doporuceni-NUKIB_ustanoveni-10a_v1.2.pdf, a v rozšířené a aktualizované verzi ze dne 24. 8. 2020 zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Doporuceni_Poskytovani-informaci_v2.0.pdf) se *„při posuzování, zda informace poskytnout či nikoliv, je nezbytné zvážit, které informace jsou z hlediska zachování kybernetické bezpečnosti natolik důvěrné, že by jejich vyzrazením mohlo dojít k jejímu narušení. Taková informace by také měla z pohledu důvěrnosti odpovídat úrovni „Vysoká" nebo „Kritická" podle přílohy č. 1 vyhlášky o kybernetické bezpečnosti. Pokud by zpřístupněním takové informace mohlo dojít k narušení kybernetické bezpečnosti, je podle názoru NÚKIB vhodné uvažovat o použití § 10a zákona kybernetické bezpečnosti a takovou informaci neposkytnout. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci"* (pozn. zvýraznění doplněno soudem).

68. NÚKIB se ve shora uvedené publikaci vyjadřuje i k soudnímu přezkumu, kdy upozorňuje, že *„při případném soudním řízení o oprávněnosti neposkytnutí informace podle § 10a zákona o kybernetické bezpečnosti jsou předmětem soudního přezkumu zejména důvody neposkytnutí informací, tedy také to, zda informace naplní definici tohoto ustanovení zákona. Argumentace prostřednictvím klasifikace informací při hodnocení aktiv se tak prima vista jeví jako nezbytná"*.

69. Omezení práva na informace uvedené v § 10a ZKB se vztahuje na tři druhy informací: *(1)* informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti; *(2)* jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle zákona o kybernetické bezpečnosti, *(3)* které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila.

70. V aktuálně posuzované věci jde dle obsahu napadeného rozhodnutí o neposkytnutí informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti a o neposkytnutí informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle ZKB. Opatřeními jsou podle § 11 odst. 2 písm. a) až c) ZKB: varování; reaktivní opatření; ochranné opatření. K těmto důvodům pro odmítnutí poskytnutí informace povinný subjekt uvádí, dle jakých kritérií se posuzuje hodnota aktiv, tedy informací. Blíže ale posouzení jednotlivých aspektů aktiv úrovně vysoké nebo kritické nespecifikuje, pouze odkazuje na přílohu č. 1 k ZKB a na metodiku NÚKIB. Podle obsahu správního spisu je jediným zdrojem o klasifikaci aktiva z hlediska důvěrnosti interní e-mailová zpráva pracovníka České pošty ze dne 16. 8. 2019, ve kterém je klasifikace aktiva z hlediska důvěrnosti pouze konstatována, bez uvedení zdroje informace nebo jakéhokoliv zdůvodnění.

71. Povinný subjekt se v bodu 23 nového prvostupňového rozhodnutí mýlí, pokud uvádí, že *„povinný subjekt nemá možnost uvážení, zda v daném případě poskytne či neposkytne požadované informace"*. Tento závěr nelze s ohledem na ústavně konformní výklad právních předpisů potvrdit. V demokratickém právním státě založeném na úctě k základním právům a svobodám člověka a občana nelze ústavně zaručené právo odejmout bez jakékoliv úvahy a pečlivého posouzení všech okolností každého individuálního případu. Shodně je § 10a ZKB vyložen i NÚKIB ve shora uvedeném doporučení, kde je konstatováno, že *„ustanovení ZKB o neposkytnutí informace však neplatí neomezeně, neposkytnutí informací musí být řádně a prokazatelně odůvodněno a vycházet ze zákonných důvodů"*. Pokud je dle Ústavního soudu *„k dispozici více výkladů veřejnoprávní normy, je třeba volit ten, který vůbec, resp. co nejméně zasahuje do toho kterého základního práva či*

svobody. Tento princip in dubio pro libertate plyne přímo z ústavního pořádku (čl. 1 odst. 1 a čl. 2 odst. 4 Ústavy České republiky nebo čl. 2 odst. 3 a čl. 4 Listiny základních práv a svobod; viz i stanovisko menšiny pléna Nejvyššího správního soudu v usnesení ze dne 29. 4. 2004 sp. zn. Sst 2/2003, in 215/2004 Sb. NSS)" (srov. nález Ústavního soudu ze dne 29. 11. 2007, sp. zn. III. ÚS 783/06).

72. Městský soud nezpochybňuje význam role kybernetické bezpečnosti v současné technologické společnosti. Žalovaný i prvostupňový orgán však zdůvodňují neposkytnutí informace podle § 10a zákona o kybernetické bezpečnosti pouhým výčtem znaků, podle nichž se posuzuje hodnota aktiv (informací), aniž by je však na informace obsažené ve výsledku auditu aplikovali a konkrétně vymezili, v čem jejich naplnění shledali. K tomuto NÚKIB ve shora uvedených metodických materiálech upozorňuje, že „*při případném soudním řízení o oprávněnosti neposkytnutí informace podle § 10a ZKB jsou předmětem soudního přezkumu zejména důvody neposkytnutí informací, tedy také to, zda informace naplní definici tohoto ustanovení zákona. Argumentace prostřednictvím klasifikace informací při hodnocení aktiv se tak prima vista jeví jako nezbytná*".

73. Pomůckou k tomuto určení mohou být přílohy VKB a metodický materiál: „Vodítka pro hodnocení dopadů" (dostupné zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf), jejichž účelem je poskytnutí vodítek pro hodnocení důležitosti informačních a komunikačních systémů, hodnocení důležitost aktiv a s tím související řízení rizik, odvození požadavků na bezpečnost zpracovávaných informací a informačních systémů, a dále na internetových stránkách NÚKIB zpřístupněný podpůrný materiál: „Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti" (dostupné zde: https://www.nukib.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf).

74. Argumentaci žalovaného opřenou o § 11 odst. 1 písm. d) informačního zákona považuje soud rovněž za neúplnou. Dle důvodové zprávy a doporučení NÚKIB ve vztahu k citovanému ustanovení „*další konkretizací navržené výjimky jsou parametry významného nebo přímého účinku posuzované informace. Významné ohrožení účinnosti by mělo být takové, které by samo o sobě vedlo k nemožnosti zajistit chráněný účel. Například při ostraze budov by znamenalo úplnou nejistotu o tom, zda se do budovy dostane či dostala neoprávněná osoba, tedy například výpadek části senzorů, monitoringu apod., způsobený tím, že by se útočník dozvěděl údaje, které to umožní. Přímé ohrožení účinnosti by mělo být takové, které k ohrožení účinnosti bezpečnostního opatření vede přímo, tzn., nevyžaduje řady dalších informací a zjištění, náročné analýzy, filtrace a separace údajů apod. Ochranu by měly získat jen ty informace, u kterých lze prokázat kombinaci uvedených rysů – poskytnutí by významně a přímo ohrozilo účinnost bezpečnostního opatření, například v případě kybernetické bezpečnosti kybernetickou bezpečnost a bezpečnost sítí a informačních systémů. Dalším vymezujícím parametrem je nezbytnost opatření. Nebylo by totiž přiměřené, pokud by se umožnilo rozsáhlé a neobvyklé utajování informací jen proto, že si některý povinný subjekt vytvořil natolik mimořádné, komplikované či sofistikované bezpečnostní opatření, které již není nezbytné, ale jehož funkce je na mimořádném rozsahu utajování závislá. Vždy totiž existuje určitá úměrnost mezi účinností bezpečnostního opatření a tím, do jaké míry jsou o něm dostupné informace – čím méně dostupných informací, tím vyšší účinnost. Tak lze teoreticky eskalovat potřebu utajování do nekonečna. Takové opatření nemůže požívat ústavní ochranu a nemůže být oprávněným*

důvodem pro rozsáhlé utajování a omezení přístupu k informacím. Chránit lze toliko nezbytná opatření, což mj. plyne z ústavní kautely v čl. 17 odst. 4 Listiny, kde se přístup k informacím umožňuje omezit jen potud, pokud „jde o opatření v demokratické společnosti nezbytná“.

75. K omezení poskytnutí informace podle § 11 odst. 1 písm. d) informačního zákona povinný subjekt nejprve citoval zákonnou právní úpravu a poté odkázal na posouzení a zdůvodnění uvedené v předchozích bodech prvostupňového rozhodnutí (ve vztahu k odmítnutí podle § 10a ZKB). Následně konstatoval, že *„významné i přímé ohrožení účinnosti bezpečnostních opatření lze s ohledem na povahu požadovaných informací dovodit“* a dále, že *„riziko ohrožení účinnosti bezpečnostních opatření je opravdu významné a přímé“*. Žádné konkrétní argumenty, z nichž by bylo možno dovodit významné i přímé ohrožení účinnosti bezpečnostních opatření, však správní orgán v prvostupňovém ani v napadeném rozhodnutí nepředložil. Pouhé vymezení odkazem na nedostatečné zdůvodnění odmítnutí poskytnutí informace podle jiných ustanovení (§ 10a ZKB) nelze považovat za dostačující.

76. Přestože v případě §10a ZKB a § 11 odst. 1 písm. d) informačního zákona jde o ustanovení zavedená do právního řádu s účinností v roce 2017 a 2019, neexistuje k jejich výkladu doposud relevantní judikatura vysokých soudů. Rozhodně ale nelze na odůvodnění neposkytnutí informací z důvodu ochrany kybernetické bezpečnosti nebo z důvodu ohrožení účinnosti bezpečnostního opatření klást bezdůvodně nižší nároky než na odůvodnění odmítnutí poskytnutí informace ochranou obchodního tajemství. Z tohoto důvodu je nezbytné v rozhodnutí o odmítnutí informace vymezit a náležitě zdůvodnit, v čem jsou spatřovány jednotlivé aspekty odůvodňující neposkytnutí informace podle §10a ZKB a podle § 11 odst. 1 písm. d) informačního zákona.

77. K otázce proporcionality namítané ve třetí žalobní námitce bylo povinným subjektem v novém prvostupňovém rozhodnutí uvedeno, že veřejný zájem na informování uživatelů o zabezpečení datových schránek – tedy zachování ústavně zaručeného práva na informace není vyšší než ochrana informací chráněných dle ZKB (zde analogicky veřejného statku – zájmu na ochraně kybernetické bezpečnosti datových schránek). Konkrétní poměření jednotlivých aspektů veřejného zájmu a ochrany informací ale ani nové prvostupňové, ani napadené rozhodnutí neobsahuje. Jak uvádí Ústavní soud v nálezu sp. zn. Pl. ÚS 4/94 *„v případě kolize je nutné stanovit podmínky, za splnění kterých má prioritu jedno základní právo či svoboda, a za splnění kterých jiné, resp. určitý veřejný statek. Základní je v této souvislosti maxima, podle které základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody nebo veřejného statku.“* V tomtéž nálezu vymezil ÚS i určitý algoritmus vzájemného „vážení“ v kolizi stojících základních práv a svobod, když určil několik základních kritérií tohoto postupu, jimiž jsou: 1. *Vhodnost* (v tom smyslu, zdali institut, omezující určité základní právo, umožňuje dosáhnout sledovaný cíl, tj. ochranu jiného základního práva nebo veřejného statku), 2. *potřebnost* (která se posoudí porovnáváním legislativního prostředku, omezujícího základní právo, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod, resp. dotýkajícími se jich v menší intenzitě), 3. *porovnání závažnosti* obou v kolizi stojících základních práv (jež spočívá ve „zvažování empirických, systémových, kontextových i hodnotových argumentů“ – blíže viz níže citovaná judikatura k § 1). Řešení dané otázky jde tedy ruku v ruce s principem proporcionality, neboť závěr o upřednostnění jednoho práva před druhým musí být spojen s minimalizací zásahu do jiného – konkurujícího – práva tak, aby byla mezi dotčenými právy (jež jsou obecně, jak bylo výše uvedeno,

rovnocenná) zachována proporcionalita (*Zákon o svobodném přístupu k informacím: Komentář, 1. vydání, 2016, s. 1 - 21: L. Rothanzl).*

78. Žalovaný se ale zabýval proporcionalitou pouze jednostranně, když k veřejnému zájmu na poskytnutí informace pouze vymezil dva možné následky zveřejnění, a to situaci, kdy běžný uživatel nebude výsledky auditu schopen posoudit, proto nemá dle jeho mínění poskytnutí těchto informací význam. Druhá, dle názoru žalovaného kritičtější situace nastane, pokud by uživatel byl schopen výsledky posoudit, neboť poté by mohlo dojít k narušení bezpečnosti ISDS.

79. Aby žalovaný mohl odmítnout poskytnutí informací obsažených ve výsledku auditu, musel by vymezit ke každé jednotlivé části, kapitole, nebo dle kontextu i k odstavci, proč existuje pro odmítnutí poskytnutí informace silnější zájem než pro zachování ústavně zaručeného práva na informace.

80. Nad rámec výše uvedeného soud poznamenává, že opakované odmítnutí poskytnutí informací jako celku, může pramenit z nepochopení tohoto institutu povinným subjektem. Z interní e-mailové komunikace povinného subjektu a komunikace povinného subjektu s Ministerstvem vnitra (dále jen „MV"), jež je obsahem správního spisu, je totiž zjevné, že správní orgán při vyřizování žádosti o poskytnutí informace zvolil přístup, kdy se snažil nalézt důvody, jak vyhovění žádosti o poskytnutí informace zabránit. Postup souladný se smyslem a účelem právní úpravy vztahující se k právu na informace podle LZPS a podle informačního zákona je však zcela odlišný. Je třeba připomenout, že povinný subjekt měl naopak hledat způsoby, které by umožnily žádosti o informace v co možná největším rozsahu vyhovět. Tento názor vyslovil též Ústavní soud, když zdůraznil, že *„povinný subjekt má hledat způsoby maximálního vyhovění podané žádosti a nikoliv důvody, jak jejímu vyhovění zabránit"* (srov. nález ÚS z 29. 6. 2021, sp. zn. III. ÚS 3339/20).

81. Podle obsahu správního spisu povinný subjekt v e-mailové zprávě ze dne 30. 7. 2019 uvedl: *„předpokládáme, že odmítnutím vydání auditu získáme pouze čas. Vlastníkem auditu je MVČR, pokud se tedy rozhodne předmětnou auditní zprávu vydat, pak se musíme dohodnout, zda bude zpráva předána v plném rozsahu nebo jen její část"*. V e-mailové zprávě ze dne 9. 8. 2019 povinný subjekt konstatoval: *„aktuálně je stanovisko ČP auditní zprávu nevydat a najít pro to opodstatnění dle výše uvedených znaků"*. Následně je v e-mailové zprávě ze dne 18. 8. 2019 uvedeno: *„Městský soud v předmětném rozsudku zdůvodnil, proč nemůže přisvědčit tomu, že auditní závěr by byl obchodním tajemstvím podle § 504 obč. zák. – tady je polemika s jeho názorem asi zbytečná, audit DS není předmětem obchodní činnosti pošty"*. Dále jsou v citované e-mailové zprávě vymezeny *„další možnosti nevydání podle informačního zákona"* s následným výčtem v úvahu připadajících důvodů pro odmítnutí žádosti. Takový postup a projednávání záležitosti, při které má být zasaženo do ústavně zaručeného práva je zcela nepřijatelným projevem despektu k základním hodnotám, na kterých stojí právní řád České republiky.

82. *„Limit pro omezení základních práv a svobod stanovený v čl. 4 odst. 4 se s ohledem na výše uvedené uplatní nejen v rámci tvorby práva, ale také jeho aplikace ze strany soudů a dalších orgánů veřejné moci, a to v případech vzájemné kolize základních práv a svobod nebo jejich kolize s veřejným statkem. Řešení těchto vzájemných střetů s sebou vždy nutně nese riziko i nepřiměřeného omezení jednoho z nich v důsledku nadměrné preference druhého. Právě v souvislosti s kolizí základních práv a svobod ÚS dovodil z čl. 4 odst. 4 požadavek minimalizace zásahu do základního práva a svobody, resp. princip zachování maxima z obsahu*

vzájemně kolidujících základních práv“ (srov. Komentář: Listina základních práv a svobod. 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021, marg. č. 26–27.) Princip minimalizace zásahu a maximalizace zachování obou ústavně zaručených práv (analogicky v nyní posuzovaném případě ústavně zaručeného práva na informace a veřejného statku – zájmu na ochraně kybernetické bezpečnosti) není přístupem povinného subjektu dodržen. Pokud žalovaný dospěje v novém rozhodnutí o žádosti žalobce ke stejným závěrům, je nezbytné, aby důsledně konkretizoval, proč nelze poskytnout každou jednu část auditu nebo jeho anonymizovanou verzi.

83. Důvodem nepřezkoumatelnosti rozhodnutí je tedy v kontextu čtvrté žalobní námitky absence zdůvodnění, proč nedošlo k poskytnutí anonymizované verze auditu, když dle judikatury citované městským soudem v původním rozsudku je na místě i poskytnutí výrazně anonymizované informace. V situaci, kdy žalobce explicitně vyjmenovává některé z částí auditu, jejichž poskytnutí požaduje, je potom nezbytné vzít každou jednu požadovanou informaci (například informaci, zda je audit prováděn pravidelně, zda existují metodiky pro identifikaci a hodnocení aktiv, zda jsou zaměstnanci školeni, atd.) a náležitě zdůvodnit, dle výše uvedeného, proč ji žalovaný odmítá poskytnout.

84. Po důkladném právním posouzení všech aspektů projednávané věci nezbývá než konstatovat, že ani v nyní napadeném rozhodnutí se žalovanému nepodařilo předložit dostatek přezkoumatelných důvodů, které by odůvodňovaly odmítnutí žalobcem požadovaných informací v plném rozsahu.

VII. Závěr a náklady řízení

85. S ohledem na shora uvedené soud napadené rozhodnutí pro nepřezkoumatelnost podle § 78 odst. 1 a 4 s. ř. s. zrušil a vrátil žalovanému k dalšímu řízení. Právním názorem, který vyslovil soud ve zrušujícím rozsudku, je v dalším řízení správní orgán vázán (§ 78 odst. 5 s. ř. s.).

86. O náhradě nákladů řízení rozhodl soud dle § 60 odst. 1 s. ř. s. Soud se zabýval návrhem žalovaného na nepřiznání náhrady nákladů řízení žalobci podle § 70 odst. 6 s. ř. s., tj. z důvodů zvláštního zřetele hodných, neshledal jej však opodstatněným. Lze souhlasit s tím, že situace, kdy standardní. Rozhodování o nákladech řízení se nicméně primárně řídí zásadou úspěchu ve věci. Dle náhledu soudu není na místě upustit od přiznání náhrady nákladů řízení procesně úspěšnému žalobci toliko z toho důvodu, že v důsledku novelizace informačního zákona provedené zákonem č. 111/2019 Sb., nelze náklady, které žalobce v souvislosti se soudním řízením důvodně vynaložil, přičítat zaviněnému jednání (nového) žalovaného. Soud posuzoval, zda procesní nástupnictví zakládá důvody zvláštního zřetele hodné pro nepřiznání nákladů řízení, a dospěl k závěru, že tomu tak není. Komentářová literatura k tomu uvádí, že „*(j)udikatura správních soudů se doposud systematicky nezabývala výkladem pojmu ‚důvod hodný zvláštního zřetele‘. Lze proto vyjít z judikatury ÚS a navazující civilistické judikatury vztahující se k obsahově obdobnému § 150 o. s. ř.*“ (KÜHN, Zdeněk. Soudní řád správní: komentář. Praha: Wolters Kluwer, 2019). Podle usnesení Nejvyššího soudu ze dne 29. 9. 2014 sp. zn. 21 Cdo 379/2014 „*(z)a výjimečný důvod hodný zvláštního zřetele ve smyslu § 150 o. s. ř. nelze považovat procesní nástupnictví, neboť - jak správně poukazuje dovolatelka – procesní nástupce podle § 107 odst. 4 o. s. ř. vstupuje do práv a povinností svého předchůdce (dosavadního účastníka řízení) a přijímá stav řízení, jaký tu je v době jeho nástupu do řízení.*“ Citovaný závěr civilistické judikatury je plně aplikovatelný i na nyní projednávanou věc. Soud k tomu dodává, že aplikace ustanovení § 60 odst. 7 s. ř. s.

je možná jen ve *výjimečných* případech. Bude se zpravidla jednat o takové případy, kdy procesně úspěšný žalobce sám zavinil vznik nákladů řízení. Lze uzavřít, že žalobci při rozhodování o nákladech řízení nelze klást k tíži změnu právní úpravy, kterou nemohl ovlivnit a která měla za následek přechod působnosti správních orgánů vystupujících v řízení před soudem na straně žalovaného.

87. V řízení měl plný úspěch žalobce, a proto soud rozhodl, že žalovaný je povinen zaplatit žalobci do rukou jeho zástupce na nákladech řízení částku 11 228 Kč do 1 měsíce od právní moci tohoto rozsudku. Výše nákladů řízení o žalobě sestává ze zaplaceného soudního poplatku ve výši 3 000 Kč [položka 18 bod 2 písm. a) sazebníku poplatků k zákonu č. 549/1991 Sb., o soudních poplatcích] a z odměny za zastoupení advokátem v rozsahu dvou úkonů právní služby (převzetí a příprava zastoupení, podání žaloby) po 3 100 Kč za úkon dle § 11 odst. 1 písm. a), d) na základě § 9 odst. 4 písm. d) ve spojení s § 7 bod 5 vyhlášky Ministerstva spravedlnosti č. 177/1996 Sb., advokátní tarif, včetně dvou režijních paušálů po 300 Kč (§ 13 odst. 3 advokátního tarifu). Jelikož zástupce žalobce doložil, že je plátcem DPH, zvyšují se náklady řízení v rozsahu odměny za právní zastoupení ve smyslu § 57 odst. 2 s. ř. s. o částku 1 428 Kč odpovídající této dani.

88. Výrok o náhradě nákladů řízení osobě zúčastněné na řízení je odůvodněn § 60 odst. 5 s. ř. s. a contrario, neboť soud této osobě žádnou povinnost v řízení neuložil.

Poučení:

Proti tomuto rozhodnutí lze podat kasační stížnost ve lhůtě dvou týdnů ode dne jeho doručení. Kasační stížnost se podává ve dvou (více) vyhotoveních u Nejvyššího správního soudu, se sídlem Moravské náměstí 6, Brno. O kasační stížnosti rozhoduje Nejvyšší správní soud.

Lhůta pro podání kasační stížnosti končí uplynutím dne, který se svým označením shoduje se dnem, který určil počátek lhůty (den doručení rozhodnutí). Připadne-li poslední den lhůty na sobotu, neděli nebo svátek, je posledním dnem lhůty nejblíže následující pracovní den. Zmeškání lhůty k podání kasační stížnosti nelze prominout.

Kasační stížnost lze podat pouze z důvodů uvedených v § 103 odst. 1 s. ř. s. a kromě obecných náležitostí podání musí obsahovat označení rozhodnutí, proti němuž směřuje, v jakém rozsahu a z jakých důvodů jej stěžovatel napadá, a údaj o tom, kdy mu bylo rozhodnutí doručeno.

V řízení o kasační stížnosti musí být stěžovatel zastoupen advokátem; to neplatí, má-li stěžovatel, jeho zaměstnanec nebo člen, který za něj jedná nebo jej zastupuje, vysokoškolské právnické vzdělání, které je podle zvláštních zákonů vyžadováno pro výkon advokacie.

Soudní poplatek za kasační stížnost vybírá Nejvyšší správní soud. Variabilní symbol pro zaplacení soudního poplatku na účet Nejvyššího správního soudu lze získat na jeho internetových stránkách: www.nssoud.cz.

Praha 31. října 2022

JUDr. Naděžda Řeháková v. r.
předsedkyně senátu