ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
email: posta@uoou.cz, www.uoou.cz

Čj. UOOU-04568/20-53

[redacted]
IČO: [redacted]

Praha 24. června 2022

Vyřízení námitek proti kontrolním zjištěním uvedeným v protokolu o kontrole čj. UOOU-04568/20-43 ze dne 13. ledna 2022

Úřad pro ochranu osobních údajů (dále jen „Úřad“) jako kontrolní orgán dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), obdržel dne 31. ledna 2022 od společnosti [redacted], se sídlem [redacted], IČO: [redacted] (dále jen „kontrolovaná“), námitky proti kontrolním zjištěním uvedeným v protokolu o kontrole čj. UOOU-04568/20-43 ze dne 13. ledna 2022 (dále jen „protokol o kontrole“).

V souladu s § 14 odst. 1 kontrolního řádu je příslušný k vyřízení námitek předseda Úřadu.

Podané námitky podle ustanovení § 14 kontrolního řádu vyřizuji takto:

1. **Námitka** směřující proti kontrolnímu zjištění č. 1 protokolu o kontrole, v němž je konstatováno, že zpracování osobních údajů příjemců SMS zprávy rozeslané kontrolovanou osobou v rozsahu telefonního čísla a informace o prokliku na stránku vedoucí k instalaci aplikace eRouška kontrolovaná prováděla bez řádného zákonného titulu, čímž porušila čl. 6 odst. 1 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 (dále jen „nařízení (EU) 2016/679“), **se zamítá.**

   V této souvislosti kontrolovaná osoba sdělila, že konstatované porušení čl. 6 odst. 1 nařízení (EU) 2016/679 je založeno na nesplnění kritéria vhodnosti zvoleného prostředku zpracování ve vztahu k vytyčenému účelu zpracování, avšak k tomuto závěru nelze v protokolu o kontrole nalézt odpovídající skutkové zjištění. Kontrolovaná uvedla, že v průběhu kontroly sdělila, že důvodem předmětného zpracování osobních údajů byla snaha zamezit opakované rozesílce SMS v případě opakované žádosti Ministerstva zdravotnictví České republiky (dále jen „MZČR“) na účastníky, u kterých by to nedávalo smysl. Účelem bylo ušetřit budoucí náklady a také zbytečně neobtěžovat účastníky další rozesílkou, a to ani ty, kteří sice na odkaz vedoucí na stránky www.erouska.cz klikli, ale aplikaci eRouška si nenainstalovali, neboť u těchto subjektů lze předpokládat, že pokud si

aplikaci nestáhli na základě první výzvy, neučiní tak ani napodruhé. Vzhledem k tomu, že podle kontrolované neexistoval prostředek, jak legálně přesně zjistit, kdo si aplikaci již stáhl a kdo ne, považuje kontrolovaná zvolený prostředek zpracování za zcela vhodný, a navíc jediný možný a dostupný k dosažení deklarovaného cíle.

Dále kontrolovaná sdělila, že v průběhu místního šetření dne 5. května 2021 se zavázala, že do 12. května 2021 doloží Úřadu, že před započetím zpracování osobních údajů (souvisejícího s umístěním trackovacího odkazu v SMS vyzývající ke stažení aplikace eRouška) provedla tzv. balanční test, resp. posouzení ve smyslu čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679, zda nad oprávněným zájmem kontrolované na zpracování osobních údajů nemají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů. Tento důkaz kontrolovaná dle svého vyjádření zaslala dne 12. května 2021 neúmyslně na e-mailovou adresu podatelna@uoou.cz a nikoli na adresu posta@uoou.cz, přičemž z e-mailové adresy postmaster@uoou.cz jí bylo doručení potvrzeno. V rámci rozkladového řízení sp. zn. UOOU-00769/21 Úřad podle kontrolované potvrdil, že takové doručení považuje za platné, proto kontrolovaná žádá o zařazení tohoto vyjádření včetně jeho příloh do spisu a o vypořádání se s uvedenými argumenty.

K zaslání vyjádření na elektronickou adresu podatelna@uoou.cz **uvádím**, že tato adresa není a nikdy nebyla oficiální adresou Úřadu určenou pro doručování podání adresovaných Úřadu. V rámci správního řízení vedeného s kontrolovanou pod sp. zn. UOOU-00769/21 byla kontrolovaná o této elektronické adrese jednou (v rámci vyrozumění o pokračování ve správním řízení ze dne 17. března 2021) mylně informována, přičemž podání kontrolované (rozklad) bylo v předmětné e-mailové schránce nalezeno. Vyjádření kontrolované ze dne 12. května 2021 Úřad v e-mailové schránce nenalezl, nicméně kontrolovaná uvedené vyjádření předložila jako součást námitek proti kontrolnímu protokolu, proto se Úřad argumenty obsaženými v tomto podání vypořádává nyní v rámci vyřízení námitek proti protokolu o kontrole.

Kontrolovaná obdržela dne 12. října 2020 (v dopise je uvedeno datum 12. září 2020, podle kontrolované se jedná o chybu v psaní, jelikož e-mail byl odeslán 12. října 2020 v 10:28 hodin) prostřednictvím Asociace provozovatelů mobilních sítí žádost MZČR o rozesílku informačních SMS na všechny zákazníky, která obsahovala výzvu ke stažení aplikace eRouška. Dne 14. října 2020 spustila kontrolovaná rozesílku předmětných SMS, do kterých jako samostatný správce vložila unikátní odkaz obsahující analytický skript, který kontrolované umožnil evidovat informaci o tom, že uživatel příslušného telefonního čísla na zaslaný odkaz klikl a následně byl přesměrován na webové stránky, na kterých bylo možné stáhnout aplikaci eRouška. Kontrolovaná tedy zpracovávala telefonní čísla svých zákazníků (která provozuje, a tedy je již zná) a informaci o prokliku na odkaz, a to (podle jejího vyjádření) na základě čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

Povinností správce před zahájením zpracování údajů na základě čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 je v prvé řadě posoudit, zda má na tomto zpracování oprávněný zájem, zda je toto zpracování z hlediska tohoto oprávněného zájmu nezbytné a zda nad tímto zájmem v tomto konkrétním případě nepřevažují zájmy a práva subjektu údajů (provést tzv. balanční test). Kontrolovaná ve svém vyjádření ze dne 20. ledna 2021 uvedla, že smyslem tohoto zpracování bylo předejít opakování rozesílky SMS (v případě, že by došlo

k opakované žádosti o předmětnou rozesílku ze strany MZČR, což nebylo v době rozesílky vyloučeno) na zákazníky, kteří na odkaz již klikli, a to z důvodu snížení případných budoucích nákladů, a dále z důvodu snahy neobtěžovat opakovaně zákazníky. Kontrolovaná rovněž uvedla, že před započetím předmětného zpracování provedla balanční test, který byl „*založen výhradně na úvaze, že zájem společnosti* [redacted] *na minimalizaci případných dalších nákladů na opakovanou rozesílku informačních SMS pro Ministerstvo zdravotnictví a dále rovněž na snaze neobtěžovat opakovanou rozesílkou uživatele telefonních čísel, pro které by již informace nebyla relevantní, je zcela legitimní, je nezbytný a nelze jej dosáhnout jiným způsobem, nezahrnuje zpracování vysoce citlivých údajů, je realizován v souladu s nařízením (EU) 2016/679 a nemůže subjektu údajů způsobit žádnou újmu, a proto tento zájem společnosti* [redacted] *není nijak v rozporu se zájmem subjektu údajů*“. Stejné důvody a úvahy uvedla kontrolovaná při ústním jednání a místním šetření dne 5. května 2021.

Balanční test kontrolovaná provedla pouze ústně, podle jejího vyjádření nebyl vypracován písemně zejména z důvodu časové tísně. Kontrolovaná v rámci podaných námitek předložila čestné prohlášení ze dne 12. května 2021 o provedení balančního testu (vyjádření, jehož součástí bylo zmíněné čestné prohlášení, kontrolovaná údajně zaslala téhož dne na elektronickou adresu podatelna@uoou.cz), v němž uvedla, že MZČR uvádělo, že „*cílem rozesílky je dosáhnout několika milionů instalací aplikace eRouška, přičemž dosažení tak vysokého čísla úspěšnosti jakékoli kampaně pouze při jedné vlně rozesílky je podle našich zkušeností i objektivního stavu věci zhola nemožné. Protože tedy bylo předpokládáno několik vln rozesílek, bylo třeba třídit ty adresáty, kteří již kliknutím učinili krok k instalaci a adresáty, kteří neudělali žádný krok, protože u těch bylo prakticky jisté, že aplikaci nemají. Z tohoto důvodu se jako vhodný nástroj pro dosažení cíle a eliminace opakované rozesílky na ty, kteří výzvu neignorovali, jevil trackovací link v rámci SMS /…/.*“ Účelem zpracování osobních údajů tedy bylo neobtěžovat adresáty SMS, minimalizovat náklady kontrolované a vyhnout se „*řešení následných dotazů a žádostí na vyřazení z dalších rozesílek od těch adresátů, kteří si skrze odkaz aplikaci instalovali*“, které by zatěžovaly kapacity callcenter a dalších provozů kontrolované. Kontrolovaná v rámci provedeného balančního testu dospěla k závěru, že „*zájmy nebo základní práva a svobody subjektu údajů budou dotčeny v minimálním rozsahu, protože zpracováváno bude pouze telefonní číslo* [redacted] *k dispozici má, protože šlo ve 100 % o účastníky* [redacted] *a dále údaj, zda adresát klikl či neklikl. Link neměl být a nebyl využit pro jiný účel než pro vytřídění těch, kteří klikli, aby mohli být vyřazeni z dalších vln rozesílek, tedy i ve prospěch těchto subjektů.*“

K tomu uvádím, že předložené čestné prohlášení o provedení balančního testu svým obsahem odpovídá vyjádření kontrolované ze dne 20. ledna 2021 i tomu, co kontrolovaná uvedla při ústním jednání a místním šetření dne 10. února 2021 a 5. května 2021 a odpovídá tomu i samotné zpracování osobních údajů (zpracováváno bylo pouze telefonní číslo a údaj o kliknutí na odkaz). Ohledně formy balančního testu je třeba uvést, že nařízení (EU) 2016/679 výslovně nevyžaduje písemnou formu, je však třeba, aby byl správce schopen jeho provedení doložit, tedy nějakým způsobem alespoň zreprodukovat, jak postupoval, co zohlednil a jakými úvahami se řídil. Ve stanovisku WP 29 č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES ze dne 9. dubna 2014 (str. 43) je uvedeno, že „*v rámci osvědčených postupů by provádění tohoto ověření mělo být tam, kde je to vhodné, dostatečně podrobným a transparentním způsobem zdokumentováno tak,*

aby příslušné zúčastněné strany včetně subjektů údajů a orgánů ochrany údajů a v konečném důsledku pak i soudy mohly v případě potřeby zkontrolovat úplnou a správnou aplikaci tohoto ověření“. Z uvedeného vyplývá, že provedení balančního testu nemusí být zdokumentováno vždy, nicméně písemnou formu, či jiný záznam o provedení balančního testu, lze jednoznačně doporučit. V posuzovaném případě je třeba zohlednit také to, že kontrolovaná měla na posouzení předmětného zpracování pouze 2 dny (žádost od MZČR obdržela 12. října 2020 a rozesílku SMS zpráv započala 14. října 2020). Časová tíseň byla podle kontrolované důvodem, proč nevypracovala balanční test písemně.

Neplýtvání finančními zdroji kontrolované (minimalizace nákladů na případnou další rozesílku SMS – kontrolovaná zdarma rozeslala 1 787 616 SMS), neobtěžování zákazníků a nezatěžování kapacity callcenter lze při splnění následujících podmínek považovat za legitimní zájem kontrolované: Z rozsudku Soudního dvora EU ze dne 11. prosince 2019, TK proti Asociația de Proprietari bloc M5A-ScaraA, věc C-708/18, ECLI:EU:C:2019:1064, bod 44 (ve znění opraveném usnesením ze dne 13. února 2020) vyplývá, že oprávněný zájem odůvodňující zpracování osobních údajů musí být vzniklý a trvající k datu zpracování a nesmí mít k tomuto datu hypotetickou povahu. Rovněž podle stanoviska WP 29 č. 6/2014 (str. 24–25) musí oprávněný zájem představovat skutečný a trvající zájem. Z žádosti MZČR o rozesílku předmětných SMS nikterak nevyplývá, že by se žádost měla opakovat. Kontrolovaná tak pouze na základě svých úvah předpokládala několik vln rozesílek, ke kterým však nedošlo. Zájem kontrolované tedy byl pouze hypotetický. K argumentu kontrolované, že o konkrétní podobě textace SMS včetně vložení unikátních analytických skriptů informovala MZČR uvádím, že MZČR dopisem ze dne 22. února 2021 sdělilo, že v případě textace SMS rozeslané kontrolovanou mu nebylo zřejmé finální doplnění textu za lomítkem (info.o2.cz/xy). Z uvedeného vyplývá, že kontrolovaná finální podobu zaslaného linku s MZČR nekonzultovala.

V případě zpracování osobních údajů podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 je třeba vzít v úvahu také to, zda subjekt údajů takové zpracování může důvodně očekávat (viz recitál č. 47 nařízení (EU) 2016/679). Vzhledem ke konstrukci odkazu (URL adresy) [redacted] v SMS, kde v části za lomítkem je série deseti alfanumerických znaků, bylo možné předpokládat, že k nějakému zpracování údajů bude docházet, o čemž svědčí i stížnost (čj. UOOU-04568/20-1 ze dne 15. října 2020) doručená Úřadu i článek [redacted] v [redacted] ze dne [redacted]. Zároveň bylo možné předpokládat, že kontrolovaná nebo MZČR bude mít zájem na sledování úspěšnosti rozesílky SMS, jak ostatně vyplývá i ze zmíněného článku v [redacted], v němž je uvedeno, že „*sledování úspěšnosti odkazů je běžná marketingová technika*“. Důležité je však posoudit, zda zpracování osobních údajů mohl očekávat průměrný uživatel. Mám za to, a to i vzhledem k nedostatečnému informování subjektů údajů (viz vyřízení námitky č. 2), že průměrný uživatel (adresát předmětné SMS) zpracování svých osobních údajů prostřednictvím kliknutí na odkaz neočekával. Kontrolovaná tedy zpracovávala osobní údaje příjemců SMS obsahující odkaz na stažení aplikace eRouška, kteří na odkaz klikli, bez právního titulu podle čl. 6 odst. 1 písm. f) nařízení (EU)2016/679.

Nad rámec výše uvedeného uvádím, že kontrolovaná za jí stanoveným účelem zpracovávala telefonní čísla svých zákazníků a údaj o tom, že uživatel daného telefonního čísla klikl na odkaz v zaslané SMS (nikoli údaj o tom, že si uživatel aplikaci eRouška nainstaloval). Lze

souhlasit s kontrolovanou, že pokud uživatel klikl na odkaz vedoucí na webové stránky, kde bylo možné stáhnout aplikaci eRouška, buď si aplikaci instaloval, nebo se rozhodl, že aplikaci nechce, proto by nebylo potřeba těmto uživatelům zprávu vyzývající k instalaci aplikace eRouška znovu posílat. Tím, že kontrolovaná zpracovávala pouze údaje o kliknutí na odkaz, a nikoli informaci o stažení aplikace, minimalizovala zásah do soukromí uživatelů, jelikož tato informace nevypovídá o tom, zda uživatel telefonního čísla aplikaci eRouška využíval. To však nemění nic na tom, že kontrolovaná v posuzovaném případě zpracovávala osobní údaje bez právního titulu.

2. **Námitka** směřující proti kontrolnímu zjištění č. 2 protokolu o kontrole, v němž je konstatováno, že kontrolovaná osoba porušila ustanovení čl. 13 nařízení (EU) 2016/679, neboť řádně neinformovala příjemce SMS zprávy rozeslané kontrolovanou osobou o zpracování osobních údajů v rozsahu telefonního čísla a informace vedoucí k instalaci aplikace eRouška, **se zamítá.**

K tomu kontrolovaná osoba uvedla, že závěr kontrolujících, že v dokumentu Zásady zpracování osobních údajů sice jsou obsaženy informace požadované čl. 13 odst. 1 a 2 nařízení (EU) 2016/679, avšak tyto informace měl mít subjekt údajů dostupné v okamžiku, kdy se rozhoduje, jestli klikne na odkaz [redacted] v příchozí SMS, nemá žádnou oporu v právních předpisech, výkladových stanoviscích ani v rozhodovací praxi. Takový požadavek by byl podle kontrolované splnitelný pouze tak, že by před započetím zpracování na základě oprávněného zájmu musel subjekt údajů dostat SMS informující o tom, jak se dá zpracování zamezit, takže by v konečném důsledku vedl k enormnímu zatížení sítí elektronických komunikací a též k nadměrnému obtěžování zákazníků. Kontrolovaná dále uvedla, že způsob, jakým účastníky o předmětném zpracování informovala v dokumentu Zásady zpracování osobních údajů, na které je účastník služeb elektronických komunikací odkazován ve smlouvě na počátku smluvního vztahu a v souvislosti s každou jeho změnou, je zcela vyhovující a v souladu s právními předpisy. Kontrolovaná je přesvědčena o tom, že všichni její účastníci jsou na základě informací z uvedeného dokumentu schopni dovodit, že v případě, že nechtějí, aby se kontrolovaná dozvěděla, že na zaslaný odkaz klikli, nemají na něho klikat.

K tomu uvádím, že kontrolovaná ve svém vyjádření ze dne 20. ledna 2021 uvedla, že informace o předmětném zpracování jsou obsaženy v dokumentu Zásady zpracování osobních údajů, který je dostupný na jejích internetových stránkách (dále jen „Zásady“). Kontrolovaná zaslala předmětné SMS pouze svým zákazníkům, přičemž tito jsou na Zásady odkazováni na počátku smluvního vztahu a v souvislosti s každou jeho změnou. Zákazníci kontrolované jsou tedy informováni o existenci těchto Zásad a je na rozhodnutí každého zákazníka, zda se s nimi seznámí. V bodě A.5 Zásad nazvaném Ostatní údaje generované v souvislosti s poskytováním služeb, je uvedeno, že „*tyto údaje vznikají při poskytování služeb, které nejsou službami elektronických komunikací, při využívání aplikací společnosti* [redacted]*, prohlížení internetových stránek* [redacted] *či internetových stránek, na které je odkazováno v rozesílkách* [redacted] *(analytické skripty), nebo při poskytování služeb elektronických komunikací nad rámec údajů potřebných pro přenos zprávy. Údaje generované sítěmi při poskytování služeb elektronických komunikací nad rámec provozních a provozních lokalizačních údajů jsou nezbytné pro řešení sporů týkajících se kvality služby, vyhodnocování a zvyšování kvality sítí a služeb a údržbu sítí*“. V bodě B.1 Zásad je jako jeden z mnoha účelů zpracování

uvedena „*analýza návštěvnosti internetových stránek [redacted] či internetových stránek, na které je odkazováno v rozesílkách [redacted] (oprávněný zájem společnosti [redacted]*. Kontrolovaná tedy své zákazníky informuje o tom, že na základě svého oprávněného zájmu zpracovává údaje za účelem analýzy návštěvnosti internetových stránek, a že k tomu využívá analytické skripty. K rozsahu zpracovávaných údajů kontrolovaná uvádí, že ten závisí na účelu zpracování.

Informace o zpracování osobních údajů má být podle čl. 12 nařízení (EU) 2016/679 správcem poskytována stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. V pokynech WP 29 k transparentnosti podle nařízení 2016/679 v revidovaném znění ze dne 11. dubna 2018 (odst. 9) je uvedeno, že „*požadavek na „srozumitelné" informace znamená, že by jim měla porozumět i průměrná osoba v cílové skupině. Srozumitelnost úzce souvisí s požadavkem na použití jasných a jednoduchých jazykových prostředků. Odpovědný správce údajů má znalosti o lidech, o nichž shromažďuje informace, které může využít, aby určil, jakým jazykovým prostředkům daná cílová skupina pravděpodobně porozumí. Například správce shromažďující osobní údaje pracujících odborníků může předpokládat, že jeho cílová skupina má vyšší úroveň porozumění než cílová skupina správce shromažďujícího osobní údaje dětí*". Je tedy nezbytné, aby správce v rámci plnění informační povinnosti posoudil úroveň porozumění adresátů této informace. Ačkoli má kontrolovaná za to, že všichni její zákazníci jsou schopni dedukce, že budou zpracovávány údaje o tom, že klikli na odkaz v zaslané SMS, je třeba konstatovat, že výše citovaná informace není pro průměrného uživatele dostatečně srozumitelná, navíc není zřejmé, jaké údaje budou zpracovávány ani po jakou dobu. Ve výroční zprávě za rok 2021 (ze dne 1. března 2022, str. 11) kontrolovaná uvádí, že je největším telekomunikačním operátorem na českém trhu; hlasové, internetové a datové služby poskytuje zákazníkům od domácností přes malé a střední firmy až po velké korporace. Kontrolovaná tedy poskytuje své služby širokému spektru uživatelů, včetně dětí a seniorů, které lze podle Pokynů WP 29[1] považovat za zranitelné subjekty, vůči nimž by měl správce postupovat při poskytování informací se zvláštní péčí kladoucí důraz na srozumitelnost a jednoduchost. Nelze tedy souhlasit s kontrolovanou, že všichni její zákazníci jsou schopni výše citovanou informaci pochopit. Současně poukazuji na to, že v případě poskytování informací elektronickými prostředky je vhodné, pro větší přehlednost, zobrazovat informaci vrstevnatě (detailnější informace o zpracování zobrazit po kliknutí na základní informaci).

Na základě výše uvedeného konstatuji, že kontrolovaná sice informuje své zákazníky o tom, že zpracovává jejich osobní údaje za účelem analýzy návštěvnosti internetových stránek, na které je odkazováno v rozesílkách kontrolované, avšak poskytovaná informace není dostatečně srozumitelná pro průměrného adresáta zpráv, proto nelze považovat plnění informační povinnosti za dostatečné. Nadto lze jednoznačně doporučit, aby v případě obdobných masových kampaní kontrolovaná na svých internetových stránkách transparentně informovala o tom, že dochází ke zpracování osobních údajů a za jakým účelem, aby tato informace byla adresátům zpráv snadno dostupná.

[1] Pokyny WP29 pro posouzení vlivu na ochranu údajů a stanovení zda „*je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*" pro účely nařízení 2016/679 ze dne 4. dubna 2017 v aktualizovaném znění (WP 248 rev.01 str. 12)

3. **Námitce** směřující proti kontrolnímu zjištění č. 3 protokolu o kontrole, v němž je konstatováno, že kontrolovaná osoba porušila čl. 32 odst. 1 nařízení (EU) 2016/679, protože neprokázala provedení vhodných technických a organizačních opatření při zpracování osobních údajů příjemců SMS zprávy rozeslané kontrolovanou osobou dle tohoto ustanovení, **se vyhovuje.**

V této souvislosti kontrolovaná osoba uvedla, že kontrolní zjištění, které vychází z tvrzení, že po kliknutí na odkaz v SMS probíhá komunikace vždy výhradně v rámci sítě [redacted], je věcně nesprávné. Kontrolovaná nikdy nepočítala s tím, že komunikace bude probíhat vždy výhradně prostřednictvím sítě [redacted], což je zřejmé z bodu IV. jejího vyjádření ze dne 19. března 2021. Chybné je podle kontrolované i konstatování kontrolujících, že v případě, kdy došlo k přenosu předmětného odkazu prostřednictvím externí wifi sítě (doma, v kavárně, ve vlaku), tento byl přenášen v nezašifrované podobě, neboť nebyl využit protokol HTTPS, z čehož pak kontrolující chybně dovodili porušení čl. 32 nařízení (EU) 2016/679. Podle kontrolované byl již samotný odkaz šifrou a síla použité šifry byla zcela odpovídající riziku zpracování; pokud by tomu tak nebylo, Bc. Jaromír Kuba (Úřadem přizvaná osoba a soudní znalec v oboru kybernetika, odvětví výpočetní technika, specializace informační technologie) by toto zcela nepochybně zmínil v rámci místního šetření dne 5. května 2021 nebo v rámci úředního záznamu ze dne 14. června 2021 čj. UOOU-04568/20-37. Výsledkem případného úspěšného napadení (které by samo o sobě bylo trestným činem) by bylo toliko zjištění telefonního čísla.

K tomu uvádím, že kontrolovaná ve svém vyjádření ze dne 19. března 2021 uvedla, že „*uživatel by musel kliknout na odkaz v SMS v momentu připojení na nezabezpečenou wifi síť (tedy doma, v kavárně apod.). Pokud použije standardní mobilní datové připojení přes mobilní síť operátora, pak není možné údaje útočníkem odposlechnout – protože síť je proti těmto útokům chráněna*“. Konstatování uvedené v protokolu o kontrole, že podle kontrolované po kliknutí na odkaz probíhá komunikace vždy výhradně v rámci sítě [redacted], tak neodpovídá tomu, co kontrolovaná v průběhu kontroly sdělila. Z výše citovaného vyjádření kontrolované vyplývá, že si byla vědoma toho, že komunikace může probíhat nejen prostřednictvím její mobilní sítě, ale i prostřednictvím nezabezpečených wifi sítí.

Podle kontrolované se při zpracování telefonního čísla a údaje o kliknutí na odkaz nejednalo o osobní údaje, jejichž případné zneužití by mělo za následek vysoké riziko pro práva a svobody fyzických osob, a zvolené technicko-organizační opatření pro dosažení zabezpečení odpovídajícího riziku zpracování (zakódování telefonního čísla prostřednictvím šifrovací funkce) považuje za adekvátní. Pokud došlo k přenosu dat prostřednictvím externí wifi sítě, nebyl využit protokol HTTPS, ale podle kontrolované byl samotný odkaz šifrou, jejíž síla zcela odpovídala riziku zpracování. Z úředního záznamu ze dne 14. června 2021 čj. UOOU-04568/20-37 vyplývá, že použitá šifra (algoritmus zakódování telefonního čísla v adrese odkazu) je příliš jednoduchá na to, aby bylo možné konstatovat faktickou ochranu přenášeného telefonního čísla. Autor výše zmíněného článku v Hospodářských Novinách vytvořil a umístil na internetové stránky [redacted] webovou aplikaci, pomocí které lze dekódovat zašifrované telefonní číslo do numerického formátu. Dešifrovat tak telefonní číslo z kódu za lomítkem v odkazu zaslaném v předmětných SMS lze velmi snadno. K využití dekodéru je však potřeba mít k dispozici daný odkaz. Pokud dekodér využije adresát předmětné SMS, pak získá pouze své telefonní číslo. V případě

přeposlání SMS obsahující odkaz někomu jinému, se příjemce této zprávy telefonní číslo dozví, aniž by musel cokoli dekódovat. Pokud by došlo k neoprávněnému odposlechu obsahu přenášené zprávy, útočník by podle kontrolované zjistil telefonní číslo už z čísla adresáta zprávy a nemusel by informace obsažené v zaslaném odkazu dešifrovat. Útočník by tak mohl získat telefonní číslo, které si ovšem může podle kontrolované kdokoli vygenerovat náhodným generátorem čísel při znalosti vyhlášky č. 117/2007 Sb., o číslovacích plánech sítí a služeb elektronických komunikací, a veřejně dostupné databáze Českého telekomunikačního úřadu o přidělených rozsazích čísel jednotlivým operátorům.

Správce a zpracovatel podle čl. 32 nařízení (EU) 2016/679 provedou vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, a to 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. Kontrolovaná zpracovávala prostřednictvím odkazu zaslaného v SMS telefonní číslo a údaj o tom, zda uživatel tohoto čísla na zaslaný link klikl. Údaj o tom, zda adresát SMS klikl na odkaz vedoucí k instalaci aplikace eRouška, nevypovídá o tom, zda si aplikaci nainstaloval nebo ji využíval. Z tohoto údaje lze vyvodit pouze to, že uživatel na odkaz klikl, což nemůže zasáhnout do jeho soukromí. Zjištění samotného telefonního čísla, bez dalších údajů, rovněž nepředstavuje zásah do soukromí subjektu údajů, přičemž telefonní čísla lze získat různými (legálními) způsoby, např. vygenerováním, vyhledáním na internetu, v telefonním seznamu atd. Jak kontrolovaná sama zmínila, uživatel mohl kliknout na odkaz v SMS v momentě připojení na nezabezpečenou wifi síť a případný útočník mohl přenášené údaje odposlechnout. Útočník by takto získal jedno telefonní číslo. Kontrolovaná měla povinnost zabezpečit osobní údaje tak, aby přijatá opatření odpovídala možnému riziku. Je velmi nepravděpodobné, a to právě s ohledem na zpracovávané údaje, že by případný neoprávněný přístup k nim představoval zvýšené riziko pro práva a svobody fyzických osob. Na základě výše uvedeného lze konstatovat, že využití protokolu HTTPS nebylo nezbytné a kontrolovanou přijatá opatření v posuzovaném případě odpovídala danému riziku.

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)