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

Čj. UOOU-04568/20-43
Praha 13. ledna 2022

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) 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), (dále jen „nařízení (EU) 2016/679“) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon č. 110/2019 Sb.“).

Kontrolující:

Mgr. Eva Cupáková – pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole z 29. ledna 2021 a vedoucí kontrolní skupiny na základě plné moci z 10. ledna 2022;

Mgr. Barbora Šnajderová, pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], jako vedoucí kontrolní skupiny na základě pověření ke kontrole ze dne 29. ledna 2021, které bylo ukončeno dne 10. ledna 2022;

Mgr. Marek Šnajdr – pověřený zaměstnanec Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole z 29. ledna 2021;

Bc. Jaromír Kuba – přizvaná osoba, soudní znalec v oboru kybernetika, odvětví výpočetní technika, specializace informační technologie, na základě pověření ke kontrole z 13. dubna 2021, informatika a telekomunikace;

(dále jen „kontrolující“).

Kontrolovaná osoba:

[redacted], se sídlem [redacted], [redacted], [redacted] – [redacted], [redacted] (dále jen „kontrolovaná osoba“).

Místo provedení kontroly: sídlo Úřadu
sídlo kontrolované osoby

Předmět kontroly:
Předmětem kontroly je (i) dodržování zásad dle čl. 5 nařízení (EU) 2016/679 při zpracování osobních údajů získaných z trackovacích odkazů, (ii) dodržování čl. 6 nařízení (EU) 2016/679 při zpracování osobních údajů získaných z trackovacích odkazů, (iii) dodržování čl. 7 nařízení (EU) 2016/679 při zpracování osobních údajů získaných trackovacími odkazy, (iv) dodržování povinností v souladu čl. 13 nařízení (EU) 2016/679 s ohledem na používání trackovacích odkazů, (v) dodržování povinností při uzavírání smluv dle čl. 28 bod 3 nařízení (EU) 2016/679, pokud jsou osobní údaje získané z trackovacích odkazů předmětem těchto smluv, (vi) dodržování povinností dle čl. 30 bod 1 nařízení (EU) 2016/679 s ohledem na zpracování osobních údajů trackovacích odkazů, (vii) dodržování povinností dle čl. 32 nařízení (EU) 2016/679 při zabezpečování osobních údajů získaných z trackovacích odkazů a (viii) dodržování povinností dle čl. 44 nařízení (EU) 2016/679 při předávání osobních údajů získaných z trackovacích odkazů.

První kontrolní úkon:
Doručení oznámení o zahájení kontroly kontrolované osobě 21. prosince 2020 (čj. UOOU-04568/20-4).

Poslední kontrolní úkon:
Vypracování úředního záznamu ze 4. ledna 2022 o kontrole webové stránky kontrolované v souvislosti s novelizací zákona č. 127/2005 Sb., o elektronických komunikacích (čj. UOOU-04568/20-41).

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Stížnost z 15. října 2020 (čj. UOOU-04568/20-1), počet listů 1;
    1.1. Příloha – snímek obrazovky (obchodní sdělení eRouška), počet listů 1;
    1.2. Příloha – snímek obrazovky (obchodní sdělení eRouška), počet listů 1;
    1.3. Příloha – snímek obrazovky (obchodní sdělení eRouška), počet listů 1;
    1.4. Příloha – snímek obrazovky (obchodní sdělení eRouška), počet listů 1;
    1.5. Příloha – snímek obrazovky (obchodní sdělení eRouška), počet listů 1;
2. Postoupení k dalším dozorovým opatřením z 15. října 2020 (čj. UOOU-04568/20-2), počet listů 3;
3. Pověření ke kontrole z 15. prosince 2020 (čj. UOOU-04568/20-3), počet listů 1;
4. Oznámení o zahájení kontroly z 18. prosince 2020 (čj. UOOU-04568/20-4), počet listů 3;

5. Vyjádření v rámci státní kontroly z 20. ledna 2021 (čj. UOOU-04568/20-9), počet listů 6;
   5.1. Smlouva o zpracování osobních údajů [redacted] správce) č. 8000019240 z 5. října 2018 vč. příloh č. 1 a 2, počet listů 22;
   5.2. Žádost o spolupráci z 12. září 2020, počet listů 2;
   5.3. Směrnice [redacted] Ochrana informací z 5. června 2019 vč. přílohy 1 až 3, počet listů 25;
   5.4. Směrnice [redacted] Administrátorský bezpečnostní manuál z 18. července 2019, počet listů 32;
   5.5. Směrnice [redacted] Bezpečnostní požadavky na databázové systémy z 5. června 2018, počet listů 15;
6. Úřední záznam z 1. února 2021 (čj. UOOU-04568/20-11), počet listů 1;
   6.1. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.2. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.3. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.4. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.5. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.6. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.7. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.8. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.9. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.10. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.11. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.12. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.13. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.14. Příloha - Zásady zpracování osobních údajů - [redacted] (printscreen), počet listů 1;
   6.15. Příloha - Informace o mimořádném zpracování osobních údajů osob nakažených koronavirem SARS-CoV-2 – [redacted] (printscreen), počet listů 1;
   6.16. Příloha - Informace o mimořádném zpracování osobních údajů osob nakažených koronavirem SARS-CoV-2 – [redacted] (printscreen), počet listů 1;
   6.17. Příloha - Informace o mimořádném zpracování osobních údajů osob nakažených koronavirem SARS-CoV-2 – [redacted] (printscreen), počet listů 1;
   6.18. Příloha - Seznam zpracovatelů osobních údajů – [redacted] (printscreen), počet listů 1;
   6.19. Příloha - Seznam zpracovatelů osobních údajů – [redacted] (printscreen), počet listů 1;
   6.20. Příloha - Seznam zpracovatelů osobních údajů – [redacted] (printscreen), počet listů 1;
   6.21. Příloha - Seznam zpracovatelů osobních údajů – [redacted] (printscreen), počet listů 1;
   6.22. Příloha - Seznam zpracovatelů osobních údajů – [redacted] (printscreen), počet listů 1;
   6.23. Příloha - Cookie scan record z 1. února 2021 [redacted], počet listů 11;
   6.24. Příloha - Zásady zpracování osobních údajů, počet listů 11;
   6.25. Příloha - Informace o mimořádném zpracování osobních údajů osob nakažených koronavirem SARS-CoV-2, počet listů 3;
   6.26. Příloha - Cookies, počet listů 5;

7. Protokol z ústního jednání a místního šetření z 10. února 2021 (čj. UOOU-04568/20-13), počet listů 4;
8. Výzva k doložení tvrzení uvedených ve stížnosti z 10. února 2021 (čj. UOOU-04568/20-14), počet listů 1;
9. Žádost o součinnost z 10. února 2021 (čj. UOOU-04568/20-15), počet listů 2;
10. Žádost o vyjádření z 11. února 2021 (čj. UOOU-04568/20-16), počet listů 2;
11. RE:Výzva k doložení tvrzení uvedených ve stížnosti k čj. UOOU-04568/20 (čj. UOOU-04568/20-17), počet listů 1;
12. Úřední záznam z 15. února 2021 (čj. UOOU-04568/20-18), počet listů 1;
    12.1. Příloha - RE: Čj. UOOU-04568/20-12, stanovení termínu ústního jednání a místního šetření z 8. února 2021, počet listů 1;
13. Odpověď na dopis z 13. října 2020 (čj. UOOU-04568/20-19), počet listů 2;
    13.1. Příloha - Odpověď na žádost o vyjádření z 15. února 2021, počet listů 2;
14. Úřední záznam z 18. února 2021 (čj. UOOU-04568/20-21), počet listů 2;
    14.1. Příloha - SMS vyzývající k instalaci eRoušky jsou kybernetickou hrozbou. Ta od  navíc může narušit soukromí, počet listů 6;
    14.2. Příloha - Dekodér odkazu  na eRoušku, počet listů 1;
    14.3. Příloha - Dekódovaný odkaz  , počet listů 1;
    14.4. Příloha - Dekódovaný odkaz  , počet listů 1;
    14.5. Příloha - Dekódovaný odkaz  , počet listů 1;
    14.6. Příloha - Dekódovaný odkaz  , počet listů 1;
    14.7. Příloha - Dekódovaný odkaz  , počet listů 1;
    14.8. Příloha - Nefunkční odkaz _____, počet listů 1;
    14.9. Příloha - Vyjádření stěžovatele – spojení odkazů s telefonními čísly, počet listů 1;
15. Odpověď na Žádost o součinnost UOOU informační SMS  z 11. března 2021 (čj. UOOU-04568/20-27), počet listů 1;
    15.1. Příloha - Dopis Asociace provozovatelů mobilních sítí hlavní hygieničce ČR z 13. října 2020, počet listů 2;
16. Doplnění vyjádření v rámci státní kontroly k čj. 4568/20 z 19. března 2021 (čj. UOOU 04568/20-29), počet listů 8;
17. Pověření ke kontrole z dne 13. dubna 2021 (čj. UOOU-04568/20-30), počet listů 1;
18. Protokol z ústního jednání a místního šetření z 5. května 2021 (čj. UOOU-04568/20-35), počet listů 8;
    18.1. Příloha – Pověření  , počet listů 4;
    18.2. Příloha – Nová rozesílka (printscreeny), počet listů 6;
    18.3. Příloha – Detail aplikace (printscreeny), počet listů 9;
    18.4. Příloha – Směrnice SM000168 z 26. května 2020, počet listů 20
19. Doložení rozhodnutí slovenského UOOU z 15. června 2021 (čj. UOOU-04568/20-36), počet listů 1;
    19.1. Příloha - Rozhodnutie o rozklade z 29 listopadu 2019, počet listů 20;
20. Úřední záznam ze 14. června 2021 o analýze IT systémů umožňujících zpracování osobních údajů v souvislosti s hromadnou rozesílkou SMS e-Rouška (čj. UOOU-04568/20-37), počet listů 4;
    20.1. Příloha – Dekodér odkazu  na eRoušku, počet listů 1;
    20.2. Příloha – Generátor odkazu  na eRoušku, počet listů 1;

20.3. Příloha - Výstupy z programu v textových souborech [redacted], [redacted], počet listů 1+1;
20.4. Příloha – Soubor s příkazy, které byly zadány do programu curl (prikazy.txt), počet listů 1;
20.5. Příloha - Výsledek komunikace s adresou [redacted], včetně zachycených HTTP hlaviček (presmerovani.txt, hlavicka.txt), počet listů 1+1;
20.6. Příloha – Výsledek komunikace s adresou [redacted], včetně zachycených HTTP hlaviček [redacted], počet listů 1+1.

21. Úřední záznam ze 4. ledna 2022 o kontrole webu v souvislosti s novelizací zákona č. 127/2005 Sb., o elektronických komunikacích (čj. UOOU-04568/20-41);
22. Pověření ke kontrole z 10. ledna 2022 (čj. UOOU-04568/20-42).

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly a ledaže je níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod a průběh kontroly:

Úřad 15. října 2020 obdržel stížnost týkající se podezření na porušení právních předpisů na ochranu osobních údajů při zpracování osobních údajů v rámci zasílání rozesílání SMS s výzvou k instalaci aplikace eRouška ze strany kontrolované osoby (viz k tomu bod 1 vč. příloh 1 až 5 přehledu podkladů).

Stěžovatel uvedl, že kontrolovaná osoba v těchto SMS uvedla sledovací (trackovací) odkaz. Dle jeho názoru kontrolovaná osoba neplnila informační povinnost (ohledně trackovacího odkazu) a též zřejmě nedisponovala žádným platným právním titulem pro takové zpracování. Ke stížnosti bylo doloženo celkem pět snímků obrazovky mobilního telefonu s textem: *„Prosime nainstalujte si na vas chytry telefon aplikaci eRouska ZDE:* [redacted] *Aplikace nezna Vasi identitu ani polohu, ale muze upozornit na setkani s COVID nakazenym. Dekuji. Jarmila Razova, hlavni hygienicka CR (sic)“.*

Na základě výše uvedených informací Úřad 21. prosince 2020 zahájil kontrolu u kontrolované osoby doručením oznámení o zahájení kontroly (viz bod 4 přehledu podkladů).

III. Kontrolní zjištění:

Svým dopisem z 12. září 2020, čj. MZDR 43616/2020-1/NH oslovilo Ministerstvo zdravotnictví České republiky, resp. náměstkyně ministra pro ochranu a podporu veřejného zdraví a hlavní hygienička ČR (dále jen „Hlavní hygienička“) Asociaci provozovatelů mobilních sítí, se sídlem Kodaňská 1441/46, 101 00 Praha 10, IČO: 751 18 891 (dále jen „Asociace provozovatelů mobilních sítí“) se žádostí o spolupráci jejích členů ve věci boje se šířením viru SARS-CoV-2 a ochrany zdraví obyvatel ČR (viz bod 5., příloha 5.2. přehledu podkladů). Konkrétně žádala o rozesílku informačních SMS na všechny zákazníky členů Asociace provozovatelů mobilních

sítí a to: *„V rámci vyhlášeného nouzového stavu bez ohledu na to, zda udělili či neudělili marketingový souhlas pro rozesílku informačních sdělení.“*
Ve své žádosti Hlavní hygienička specifikovala typy rozesílané SMS zprávy: 1. SMS pro zákazníky s telefonem typu smartphone s operačním systémem podporujícím aplikaci eRouška, kde by byli zákazníci vyzváni k přímému stažení aplikace eRouška ve verzi pro iOS či Android, 2. SMS pro zákazníky s telefonem typu smartphone, jejichž operační systém nepodporuje instalaci aplikace eRouška, kde SMS zpráva kromě výzvy ke stažení aplikace obsahovala rovněž sdělení nutnosti updatu operačního systému nebo 3. SMS pro zákazníky, kteří nemají telefon typu smartphone, kdy kromě výzvy ke stažení aplikace měli být informováni, jak si jednoduše opatřit telefon typu smartphone. Rozhodnutí o použití typu zprávy 2. či 3. nechala na jejích členech (telefonních operátorech). Současně je v žádosti uvedeno: „V*lastní obsah SMS si dovolujeme přenechat na jednotlivých operátorech.“*

SMS zpráva kontrolované osoby obsahující trackovací odkaz (unikátní analytický skript)
Kontrolovaná osoba k tomu ve svém vyjádření z 20. ledna 2021 (viz bod 5. přehledu podkladů) uvedla, že jako člen Asociace provozovatelů mobilních sítí žádosti hlavní hygieničky vyhověla, přičemž o podobě textace SMS, včetně formátu odkazů na stažení aplikace eRouška informovala Ministerstvo zdravotnictví ČR (dále jen „Ministerstvo zdravotnictví“). Uvádí, že unikátní odkaz „*vložila do SMS jako samostatný správce osobních údajů získaných na základě analytických skriptů umístěných pod odkazem unikátním pro každou rozeslanou sms za účelem evidování počtu unikátních prokliků na stránky, kde bylo možné stáhnout aplikaci eRouška. Smyslem této evidence bylo předejít opakování rozesílky na účastníky, kteří si již aplikaci stáhli, a rovněž mít v budoucnu možnost minimalizovat náklady s rozesílkou v případě, že by došlo k opakované žádosti o předmětnou rozesílku ze strany Ministerstva zdravotnictví…“.*

Jak je patrné z přípisu Ministerstva zdravotnictví z 22. února 2021 (viz bod 15 přehledu podkladů) a dále z přípisu Asociace provozovatelů mobilních sítí z 15. února 2021 (viz bod 13 přehledu podkladů), kontrolovaná osoba přesnou textaci, a především obsah unikátního kódu v textaci SMS zprávy, se žádnou z uvedených institucí nekonzultovala.

Znění SMS zprávy kontrolované osoby bylo předmětem podnětu (viz bod 1 přehledu podkladů), kdy původce podnětu upozorňuje na fakt, že ačkoli společnost tvrdí, že nezná identitu subjektu údajů, trackovací (sledovací) odkaz toto tvrzení vyvrací. Dle podnětu jsou klienti kontrolované osoby bezdůvodně monitorováni a nejsou o tomto faktu nikterak informováni. Součástí podnětu bylo několik SMS z unikátními kódy, které kontrolovaná osoba rozeslala.

Osobní údaje zpracovávané prostřednictvím trackovacího odkazu
Kontrolující předmětné kódy částečně dekódovali (viz bod 14 přehledu podkladů vč. příloh) a zjistili, že v části před lomítkem je zakódováno telefonní číslo. Následně si 10. února 2021 od původce podnětu vyžádali doplnění jeho podání (viz bod 8 přehledu podkladů) a to informaci, na jaká telefonní čísla byly zaslány předmětné odkazy. Podatel ve své odpovědi z 12. února 2021 (viz bod 11 přehledu podkladů) doplnil k jednotlivým kódům rovněž telefonní

čísla telefonů, na které byly kódy zaslány. Kódy jednotlivých odkazů se pak shodovali s částí odkazu před lomítkem, kterou kontrolující dekódovali.

Kontrolovaná osoba ve své odpovědi z 20. ledna 2021 (viz bod 5 přehledu podkladů) uvedla, že SMS obsahovala analytický skript, prostřednictvím kterého byla schopna zjistit, že: *„..uživatel příslušného telefonního čísla klikl na příslušný odkaz a následně byl přesměrován na odkaz, kde bylo možné stáhnout aplikaci eRouška. U uživatelů, kteří na příslušný odkaz SMS klikli, bylo tedy zpracováno telefonní číslo a informace o prokliku..“* Dále kontrolovaná osoba při místním šetření a ústním jednání 5. května 2021 (viz bod 18 přehledu podkladů, dotaz č. 1) uvedla, že pokud by uživatel (subjekt údajů) neklikl na unikátní analytický skript, nedostal by se touto cestou k aplikaci eRouška, musel by tak učinit pouze vlastní iniciativou přímo na webových stránkách Ministerstva zdravotnictví. Jinými slovy, po zaslání SMS zprávy, pokud si uživatel chtěl na základě výzvy hlavní hygieničky stáhnout aplikaci eRouška touto cestou, musel kliknout na tento unikátní analytický skript.
Tento fakt nekoresponduje s tvrzením kontrolované osoby (viz bod 18 přehledu podkladů, otázka č. 2), kdy kontrolovaná uvedla, že vložení analytického skriptu bylo provedeno na základě požadavku hlavní hygieničky k rozeslání masové a efektivní SMS zprávy vedoucí k instalaci aplikace eRouška, za účelem možné opakované výzvy u osob, které neklikly při první výzvě na odkaz vedoucí k aplikaci eRoušky.
Kontrolovaná osoba uvedla (viz bod 5 přehledu podkladů, otázka v), že osobní údaje zpracovávané prostřednictvím trackovacího odkazu jsou zpracovávány v systému MAMP, který je ve vlastnictví kontrolované osoby (nedochází tak ke zpracování osobních údajů prostřednictvím jiného subjektu – zpracovatele). Při místním šetření (viz bod 18 přehledu podkladů, otázka 5) k tomu dále kontrolovaná osoba doplnila, že systém [redacted] je přístupný [redacted]. Nástroj umožňuje nastavování a rozesílku kampaní a práva k systému jsou realizována přes [redacted]. Při místním šetření pak kontrolovaná osoba předvedla tento systém, který byl pro rozesílání zpráv využit a jeho funkcionalitu prezentovala odesláním zprávy s unikátním odkazem. Zpráva byla následně kontrolujícími ověřena (viz bod 20 přehledu podkladů) a zjištěny byly tyto skutečnosti:

- URL adresa, obsažená v testovací zprávě, byla [redacted]
- po návštěvě došlo k přesměrování na adresu [redacted]
- a následně k přesměrování na [redacted].

Během komunikace s první z výše uvedených adres byly nastaveny cookies [redacted] a [redacted], jejichž platnost byla po dobu relace. Nejedná se tak o dlouhodobý unikátní identifikátor.

Kontrolující k tomu poznamenávají, že prvotní prověřování bylo provedeno již během místního šetření 5. května 2021 v sídle kontrolované osoby (viz bod 18. a bod 20. přehledu podkladů), kontrolovaná osoba pak zjištěné skutečnosti nijak nerozporovala. Dle jejího vyjádření se prezentovaná SMS technicky neliší od rozeslané SMS s žádostí o instalaci eRoušky, až na použitý protokol v odkazu (HTTPS) a slovíčko „vzor“ v adrese URL.

[1] [redacted]

V původní zprávě unikátní identifikátor následoval přímo po adrese info.o2.cz a byl použit protokol HTTP. Užití protokolu HTTP kontrolovaná osoba zdůvodnila tím, že po kliknutí na odkaz v mobilním telefonu je komunikace vedena přes síť O2, která je již sama o sobě dostatečnou zárukou bezpečnosti přenosu. Zabezpečení zpracování osobních údajů je dále uvedeno níže v části Zabezpečení zpracování.

Kontrolovaná osoba ve svém přípisu (viz bod 18 přehledu podkladů, otázka č. 2) sice uvedla, že vložení analytického skriptu bylo provedeno na základě požadavku hlavní hygieničky k rozeslání masové a efektivní SMS zprávy vedoucí k instalaci aplikace eRouška, za účelem možné opakované výzvy u osob, které neklikly při první výzvě na odkaz vedoucí k aplikaci eRoušky. Tento fakt však kontrolovaná nedoložila.

Kontrolující tak konstatují, že k předmětnému zpracování osobních údajů v rozsahu telefonního čísla a údaje o kliknutí na webovou stránku vedoucí k aplikaci eRoušky se kontrolovaná osoba nachází v postavení správce osobních údajů ve smyslu čl. 4 bodu 7) nařízení (EU) 2016/679, neboť sama určila účel, kterým je vedení přehledu o provedení prokliku na stránku vedoucí k aplikaci eRouška ve spojení s konkrétním telefonním číslem a určila prostředek zpracování, kterým je vlastní systém pro rozesílku reklamních a dalších sdělení klientům (viz bod 20. přehledu podkladů). Osobní údaje zpracovávané ve smyslu čl. 4 bodu 2) nařízení (EU) 2016/679 jsou osobními údaji ve smyslu čl. 4 bod 1) nařízení (EU) 2016/3679.

Zákonnost zpracování

Ve svém přípisu z 20. ledna 2021 (viz bod 5 přehledu podkladů) kontrolovaná osoba uvádí, že z pozice správce osobních údajů umístila do každé rozeslané SMS s informací o stažení aplikace eRouška odkaz na stránku s unikátním analytickým skriptem, který jí umožnil získat informace o tom, že uživatel daného telefonního čísla *„klikl na příslušný odkaz a následně byl přesměrován na odkaz, kde bylo možné stáhnout aplikaci eRouška. U uživatelů, kteří na příslušný odkaz v SMS klikli, bylo tedy zpracováno telefonní číslo a informace o prokliku. Uvedené zpracování bylo v souladu s čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 nezbytné pro účely dosažení oprávněného zájmu společnosti* [redacted] *v podobě informace o uživatelích, kterým není nutné v případě opakované žádosti Ministerstva zdravotnictví o předmětnou rozesílku informační SMS zasílat, a to z důvodu snížení případných budoucích nákladů a dále z důvodu snahy neobtěžovat opakovaně uživatele, kterým již nemělo smysl opakovanou informační SMS zasílat z důvodu její irelevance pro ně. Informace získané prostřednictvím tohoto skriptu slouží výhradně k uvedenému účelu a nejsou a nebyly předány žádnému dalšímu správci osobních údajů.“*

K požadavku doložení balančních testů, pokud je zpracování založeno na oprávněném zájmu, tj. čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679 kontrolovaná osoba uvedla: *„Co se týče balančního testu, tento byl proveden před započetím předmětného zpracování a je 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..“.*

K tomu kontrolující podotýkají, že existenci oprávněného zájmu je v každém případě třeba pečlivě posoudit, a to nejprve z hlediska, zda předmětné zpracování a užité prostředky tohoto

zpracování jsou schopné sloužit vytčenému cíli (stanovenému účelu), dále zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít.

Kontrolující k věci poznamenávají, že pokud správce zpracovává osobní údaje na základě právního důvodu oprávněného zájmu správce, musí nejdříve (před zahájením zpracování) vyhodnotit, zda nad jeho oprávněným zájmem nepřevažují zájmy (práva a svobody) subjektu údajů. Správce musí posoudit přiměřenost zpracování, a to s ohledem na správcem stanovený účel takového zpracování.
S ohledem na fakt, že kontrolovaná osoba nepředložila k předmětnému zpracování písemný balanční test, kdy kontrolující nebyli schopni posoudit, zda kontrolovaná zvažovala všechny aspekty takového zpracování, jako je zvážení rizik pro subjekty údajů, faktu, zda je možné takové zpracování předpokládat, míru zabezpečení zpracování a celkové vyhodnocení všech těchto atributů, vycházeli kontrolující z podkladů a faktů uvedených kontrolovanou osobou.

Oprávněný zájem kontrolovaná osoba odůvodnila tak, že účelem pro umístění trackovacího odkazu bylo vedení evidence počtu unikátních prokliků na stránky, kde bylo možné stáhnout aplikaci eRouška, kdy smyslem této evidence bylo předejít opakování rozesílky na účastníky, kteří si již aplikaci stáhli (viz bod 5. přehledu podkladů, str. 2). Kontrolovaná osoba dále uvedla (viz bod 18. přehledu podkladů, str. 3 a str. 5), že zpracovávala pouze informaci o tom, že uživatel (subjekt údajů) klikl na eRoušku, informaci o tom, zda byla aplikace stažena kontrolovaná osoba nezjistila.

Základem posouzení proporcionality vždy musí být posouzení kritéria vhodnosti, tedy zdali zvolený prostředek může sloužit vytyčenému účelu zpracování osobních údajů. Na základě uvedených podkladů pak kontrolující konstatují, že deklarovaného účelu kontrolovaná osoba nemohla zvoleným prostředkem dosáhnout. Kontrolovaná toliko evidovala informaci o prokliku na stránky, kde bylo možné stáhnout aplikaci eRouška, nikoli to, zda došlo ke stažení předmětné aplikace. Z tohoto důvodu tak nemohly být naplněny podmínky titulu pro zpracování osobních údajů dle čl. 6 nařízení (EU) 2016/679, neboť v takovém případě (nevhodnosti použitého prostředku k dosažení deklarovaného cíle) nelze mít z to, že převáží oprávněné zájmy kontrolované osoby nad zájmy a právy subjektů údajů.

Plnění informační povinnosti
Kontrolovaná osoba uvedla (viz bod 5 přehledu podkladů, str. 4), že plnění povinnosti dle čl. 13 nařízení (EU) 2016/679 s ohledem na zasílání trackovacích odkazů je řešeno skrze dokument „Zásady osobních údajů“, který je dostupný na [redacted] (viz bod 6.24 přehledu podkladů). Dále kontrolovaná osoba upřesnila, že vzhledem k předmětu zpracování jsou požadované informace uvedeny v části A.5 a dále v části B.1 (viz bod 18 přehledu podkladů, str. 5).

V těchto částech jsou uvedeny následující informace:
„5. Ostatní údaje generované v souvislosti s poskytováním služeb
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.“

A dále:
„B. Účely, právní důvody a doby zpracování osobních údajů
Rozsah zpracovávaných údajů závisí na účelu zpracování. Pro některé účely je možné zpracovávat údaje přímo na základě smlouvy, oprávněného zájmu nebo na základě zákona (bez souhlasu), pro jiné pouze na základě souhlasu.
1. Zpracovávání z důvodu plnění smlouvy, plnění zákonných povinností a z důvodu oprávněných zájmů
Poskytnutí osobních údajů nutných pro plnění smlouvy, plnění zákonných povinností a pro ochranu oprávněných zájmů je povinné. Bez poskytnutí osobních údajů k těmto účelům by nebylo možné služby poskytovat. Ke zpracování osobních údajů pro tyto účely nepotřebujeme souhlas, nicméně proti zpracování osobních údajů pro účely oprávněných zájmů společnosti O2 je možné podat námitku. Zpracování z důvodu plnění smlouvy a plnění zákonných povinností nelze odmítnout.
Jedná se zejména o tyto základní dílčí účely:
(…) analýza návštěvnosti internetových stránek či internetových stránek, na které je odkazováno v rozesílkách (oprávněný zájem společnosti (…)
(…) Osobní údaje pro tyto dílčí účely jsou zpracovány v rozsahu nutném pro naplnění těchto účelů a po dobu nutnou k jejich dosažení nebo po dobu přímo stanovenou právními předpisy. Poté jsou osobní údaje vymazány či anonymizovány. Základní lhůty pro zpracování osobních údajů jsou k dispozici níže. (…)“

Kontrolující k tomu uvádějí, že v citovaných odstavcích jsou uvedeny účely zpracování a právní základ pro zpracování vč. oprávněných zájmů správce a na jiných místech v tomto dokumentu lze dohledat další informace taxativně vymezené čl. 13 odst. 1 a 2 nařízení (EU) 2016/679. Dodávají však, že tyto informace jsou dostupné pouze na výše uvedené internetové adrese a subjekt údajů, který klikne na odkaz v příchozí SMS, je nemá v okamžiku získání osobních údajů kontrolovanou osobou k dispozici, ani na ně není nikterak odkázán. Není tedy splněn požadavek stanovený čl. 13 odst. 1. nařízení (EU) 2016/679.
Z textu samotné SMS zprávy nevyplývá a nelze ani dovodit, že skrze tento odkaz budou zpracovávány osobní údaje o prokliku na webovou stránku vedoucí k instalaci eRoušky ve spojení s konkrétním telefonním číslem, z čehož jasně vyplývá, že uživatel (subjekt údajů) je nedostatečně informován o skutečnosti, že k tomuto zpracování dochází.

Kontrolující konstatují, že nejsou plněny podmínky čl. 13 nařízení (EU) 2016/679 z důvodu, že kontrolovaná osoba neplnila informační povinnost ve smyslu tohoto ustanovení.

Zabezpečení zpracování
Osobní údaje subjektů údajů, které využily trackovací odkaz v předmětných SMS zprávách jsou dle vyjádření kontrolované osoby (viz bod 5 přehledu podkladů, str. 5-6) zpracovány výhradně v systému , jehož technologická úroveň zabezpečení má odpovídat riziku zpracování.

[2] . Kontrolující fungování ověřili na ústním jednání a místním

Společnost [redacted] je držitelem certifikátu [redacted] v oblasti informační bezpečnosti vydaného certifikačním místem [redacted]. Do technicko-organizačních opatření na zabezpečení systému [redacted] je kromě systému samotného zahrnuta i komponenta koncových stanic uživatelů tohoto systému. Podrobnosti o technicko-organizačních opatřeních pro jednotlivé komponenty jsou vedeny elektronicky v systému [redacted]. Pro všechny komponenty jsou provedeny analýzy rizik dle [redacted], výstupy těchto analýz jsou vedeny elektronicky v systému [redacted]. Shoda evidence a výsledků analýz rizik se všemi oblastmi uvedené normy je každoročně ověřována nezávislým externím auditem, který provádí společnost [redacted].

Jak dále uvedla kontrolovaná osoba, pro systém [redacted] a koncové stanice uživatelů byla přijata následující opatření:

- fyzický přístup ke komponentám informačních systémů je řízen vstupními kartami a recepcí v ústředí společnosti a ve větších pobočkách a regulován klíčovým režimem na značkových prodejnách,
- klíčové servery jsou umístěny v prostorách [redacted], [redacted] a [redacted],
- komponenty mají v provozně udržitelné míře [redacted], které se přenášejí do systému [redacted] společnosti, kde probíhá jejich vyhodnocování,
- všechny servery jsou dohledovány a periodicky kontrolovány na známé zranitelnosti,
- probíhá také nezbytné opravy bezpečnostních zranitelností,
- přístupy do systémů jsou zřizovány vždy na základě žádosti v [redacted] a jsou schvalovány,
- systém [redacted] zajišťuje neprodlené odebrání přístupových práv v případě odchodu, nebo změny pozice zaměstnance,
- případné incidenty z neoprávněných přístupů jsou vždy řešeny,
- všichni zaměstnanci jsou přiměřeně ke své pracovní pozici proškoleni v oblasti ochrany informací,

šetření, zjistili též, že skutečně nedochází k uchování informací o mobilním zařízení subjektu údajů, IP adrese či internetovém připojení (viz bod 18 přehledu podkladů, str. 5-6 a přílohy 18.2 a 18.3).

[3] Mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací, především pak řízení bezpečnosti důvěry informací pro zaměstnance, procesy, IT systémy a strategii firmy. Tyto normy určuje Mezinárodní organizace pro normalizaci, známá pod zkratkou ISO. Zaručuje soulad s aktuálními legislativními požadavky (především ochrana osobních údajů).

[4] [redacted] je [redacted], založen je na metodice [redacted]. Dotazníky hrozeb a zranitelností, knihovna protiopatření a postupy hodnocení rizik jsou integrovány do nástroje. Analyzuje všechny druhy informačních systémů, ve všech fázích jejich životního cyklu včetně hodnocení kritických procesů.

[5] https://cs.wikipedia.org/wiki/Security_Information_and_Event_Management je management bezpečnostních informací a událostí, která má dvě kategorie: SIM (Serurity Information Management), která se zabývá dlouhodobým ukládáním událostí, jejich analýzou a hlášením problémů a SEM (Security Event Management), která se zabývá monitoringem infrastruktury, korelacemi událostí a alertováním v reálném čase. SIEM umožňuje analýzu bezpečnostních alertů, které generují sítová zařízení a aplikace, řešení je postaveno na bázi aplikace, služeb a potřebného zařízení – tento základ konzumuje záznamy bezpečnostních dat (logy) a generuje reporty.

- přístup na koncové stanice je možný pouze na základě přihlášení uživatele; [redacted], jako opatření proti útoku škodlivým kódem,
- na koncových stanicích uživatelů je nasazeno [redacted],
- vybrané mobilní koncové stanice (notebooky) mají doplněno šifrování pevného disku,
- logy z koncových stanic se průběžně vyhodnocují,
- pro stanice je k dispozici náhradní koncová stanice pro případ výpadku,
- síťová infrastruktura je doplněna [redacted] pro zajištění odpovídající bezpečnosti perimetru a včasné detekce bezpečnostních hrozeb ve vnitřním prostředí.

Výše uvedená organizační opatření k zajištění ochrany osobních údajů byla stanovena na základě interních předpisů upravujících povinnosti zaměstnanců společnosti [redacted] oprávněných přistupovat do informačních systémů:

- [redacted],
- [redacted],
- [redacted] (viz body 5.3 až 5.5 přehledu podkladů).

Co se týče samotných rozesílaných SMS (k následujícím vyjádření kontrolované osoby viz bod 18 přehledu podkladů, str. 5-6), v [redacted] byl kontrolovanou osobou využit [redacted] – [redacted], parametrem byla zvolena adresa uvedená v SMS. Byl uložen výstup hlaviček, dochází k přesměrování na [redacted] a následně k přesměrování na stránku vedoucí k aplikaci eRoušky.

K 5. květnu 2021 byl odkaz zaslán celkem 1 787 616 klientům kontrolované osoby.

V souvislosti s tím kontrolující konstatují nepřesné informování o tvorbě unikátního kódu v URL adrese kontrolovanou osobou ve vyjádření z 19. března 2021 (viz bod 16 přehledu podkladů, str. 2-3). Postup není kompletní a nelze podle něj napsat funkční prototyp pro generování kódu v SMS a ověření poskytnuté informace. Funkční variantu lze získat (a také byla získána) úpravou kódu autora aplikace pro dekódování čísla (viz bod 14.2 přehledu podkladů) a funkčnost ověřit (bylo ověřeno) na zaslaných podkladech od stěžovatele (viz bod 11 přehledu podkladů). Původní kód pro dekódování byl pro výše uvedené ověření dále rozšířen, aby tento dekódoval i informaci o ID kampaně (viz bod 20 přehledu podkladů, vč. příloh 20.1-20.6). Rozpor lze spatřit i v tvrzení kontrolované osoby, že se má telefonní číslo a identifikátor kampaně spojit a z něj po modulo vydělení vygenerovat kód. Ke správným výsledkům lze však dospět, pokud se vygeneruje kód z telefonního čísla a ID kampaně zvlášť a tyto vygenerované kódy se následně spojí. O správnosti tohoto postupu svědčí i skutečnost, že první a poslední kód v URL, který zaslal stěžovatel (viz bod 11 přehledu podkladů), obsahují jako pět posledních znaků [redacted], což ukazuje na stejnou rozesílku. Stejně tak je ve výše uvedeném vyjádření uveden kód [redacted], který je použit i v jednom z kódů stěžovatele. V případě vygenerování kódu až po spojení telefonního čísla s identifikátorem kampaně a modulo vydělení číslem [redacted] by tento údaj zcela jistě nebyl stejný. Argumentace zmíněná

[redacted]

v předchozích dvou odstavcích byla provedena na základě analýzy provedené soudním znalcem v oboru kybernetika, odvětví výpočetní technika, specializace informační technologie, informatika a telekomunikace, který je součástí kontrolní skupiny (analýza řádně provedena v rámci úředního záznamu a příloh k tomuto dokumentu, viz bod 20 přehledu podkladů, vč. příloh 20.1–20.6).

Odkaz rozesílaný kontrolovanou osobou nevyužívá zabezpečený protokol HTTPS, což kontrolovaná osoba zdůvodnila tím, že se nejedná o zpracování osobních údajů, jejichž případné zneužití by mělo za následek vysoké riziko pro práva a svobody fyzických osob (viz bod 18. přehledu podkladů, str. 8), rovněž že se nejedná se o „citlivé“ údaje a bylo využito zakódování. Uvádí, že zpracovávané údaje jsou uloženy v systému [redacted] v databázi, na kterou je aplikován výše uvedený systém řízení přístupů uživatelů, že nedochází k uchování informací o mobilním zařízení, které přistoupilo na stránku, není uchovávána ani IP adresa. Na dotaz, proč byl použit HTTP protokol, kontrolovaná osoba uvedla, že po kliknutí na odkaz v mobilním telefonu je komunikace vedena přes síť [redacted], která je již sama o sobě dostatečnou zárukou bezpečnosti přenosu.

Dle názoru kontrolujících však není možné se ztotožnit s konstatováním, že po kliknutí na odkaz v SMS probíhá komunikace vždy výhradně v rámci sítě [redacted] a nehrozí tak únik přenášeného osobního údaje – mobilního telefonního čísla, které je součástí odkazu v SMS zprávě. Pokud má uživatel aktivní připojení k síti Wi-Fi (jiné externí sítě), telefonní číslo příjemce SMS může být po kliknutí na odkaz v SMS přenášeno přes internetovou síť třetí strany, tj. mimo kontrolu kontrolované osoby, a navíc v nešifrované podobě, protože nebyl použit protokol HTTPS.

<u>Souhrnem výše uvedeného kontrolující konstatují, že:</u>

Kontrolní zjištění č. 1:
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 (EU) 2016/679.

Kontrolní zjištění č. 2:
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.

Kontrolní zjištění č. 3:
Kontrolovaná osoba porušila článek 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.

IV. Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

Mgr. Eva Cupáková	vedoucí kontrolní skupiny	*(podepsáno elektronicky)* podpis
Mgr. Marek Šnajdr	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Bc. Jaromír Kuba	přizvaná osoba	 podpis