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-00341/21-76

Praha 28. ledna 2022

Vyřízení námitek proti kontrolním zjištěním uvedeným v dodatku k protokolu o kontrole čj. UOOU-00341/21-71 ze dne 17. září 2021

Úřad pro ochranu osobních údajů (dále jen „Úřad“) jako kontrolní orgán dle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), obdržel dne 5. října 2021 od společnosti [redacted] (dále jen „kontrolovaná“), 13 námitek proti všem kontrolním zjištěním uvedeným v dodatku k protokolu o kontrole čj. UOOU-00341/21-71 ze dne 17. září 2021 (dále jen „dodatek k protokolu 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 dodatku k protokolu o kontrole, kde je konstatováno, že v období od 1. února 2021 do 25. března 2021 nebylo zpracování osobních údajů kontrolovanou osobou k předmětu kontroly prováděno v souladu s nařízením 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, jelikož se toto zpracování řídilo smlouvou, aniž by tato smlouva naplňovala atributy čl. 28 odst. 3 uvedeného nařízení, **se zamítá.**

   V této souvislosti kontrolovaná sdělila, že smluvní vztah mezi ní a Národní agenturou pro komunikační a informační technologie, s. p., se sídlem Kodaňská 1441/46, 101 00 Praha 10 - Vršovice (dále jen „NAKIT“), vždy obsahoval článek o ochraně osobních údajů, který lze považovat za řádnou zpracovatelskou smlouvu podle čl. 28 nařízení (EU) 2016/679, a měl stejnou formu jako smluvní vztah od 25. března 2021, přičemž dozorový orgán uznal, že od 25. března 2021 má tento smluvní vztah všechny dostačující náležitosti. Fakt, že se kontrolovaná vždy nacházela v postavení dalšího zpracovatele a řídila se smluvním vztahem a pokyny správce, potvrdil předseda Úřadu v rámci vyřízení námitek

proti protokolu o kontrole čj. UOOU-00341/20-50 ze dne 23. srpna 2021. Pokud byl smluvní vztah vzhledem k okolnostem celosvětové pandemie neúplně definován, ale obsahoval důležité aspekty určení role správce a zpracovatele a dalších povinností, nelze tento fakt zcela opomíjet.

K tomu uvádím, že kontrolovaná uzavřela s NAKIT smlouvu o poskytování softwarových a odborných služeb čj. [redacted] ze dne 8. října 2020, která se týká zajištění rezervačního systému pro rezervaci termínů na testování na COVID-19. Rezervační systém termínů na očkování byl spuštěn 15. ledna 2021, avšak teprve dodatkem č. 2 ze dne 26. března 2021 byl rozšířen předmět smlouvy o možnost rezervace termínů na očkování. Zpracování zpracovatelem se podle čl. 28 nařízení (EU) 2016/679 řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Pokud zpracovatel zapojí dalšího zpracovatele, musí být tomuto dalšímu zpracovateli uloženy stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem. Jak bylo konstatováno již ve vyřízení námitek proti protokolu o kontrole čj. UOOU-00341/20-50 ze dne 23. srpna 2021 kontrolovaná byla od počátku zpracování osobních údajů zájemců o očkování, tj. od 15. ledna 2021, v postavení dalšího zpracovatele, nicméně do 25. března 2021 (do uzavření dodatku č. 2) neměla zpracovatelská smlouva uzavřená mezi ní a NAKIT veškeré náležitosti podle čl. 28 odst. 3 nařízení (EU) 2016/679, zejména v ní nebyl upraven účel zpracování osobních údajů.

2. **Námitka** směřující proti kontrolnímu zjištění č. 2 dodatku k protokolu o kontrole, kde se konstatuje, že v období od 1. února 2021 do 25. března 2021 zpracovávala kontrolovaná osobní údaje k předmětu kontroly, aniž doložila pokyny, podle kterých tyto údaje zpracovávala, čímž porušila čl. 29 nařízení (EU) 2016/679, tedy povinnost zpracovatele zpracovávat osobní údaje pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu, **se vyřizuje tak, že na jejím základě bude v souladu s § 21 odst. 2 kontrolního řádu provedeno došetření.**

V této souvislosti kontrolovaná sdělila, že dostávala pokyny cestou zpracovatele (NAKIT) od správce Ministerstva zdravotnictví České republiky (dále jen „Ministerstvo zdravotnictví“), které provádí činnosti pro Centrální rezervační systém v kontextu pokynů Integrovaného centrálního řídícího týmu (dále jen „ICŘT“). Před spuštěním Centrálního rezervačního systému – očkování proti COVID-19 proběhlo dne 8. ledna 2021 v prostorách Armády České republiky společné jednání některých subjektů ICŘT a dalších subjektů, kde bylo mimo jiné představeno řízení projektu Chytré karantény 2.0. včetně jeho součástí, jako například pravidelné pracovní skupiny [redacted] (dále jen [redacted]. Dále ICŘT definoval operativní agilní informování a řízení pomocí systému [redacted] a základní evidenci požadavků v systému [redacted], o čemž kontrolovaná informovala kontrolující v průběhu místního šetření ve dnech 25. a 26. srpna 2021. Současně kontrolovaná informovala o tom, že nedisponuje administračními právy do těchto systémů a o získání přístupu je třeba požádat NAKIT, což kontrolující dle jí dostupných informací neučinili. Členy [redacted] jsou [redacted] (další zpracovatelé osobních

[redacted], [redacted]. Uvedený postup lze dle názoru kontrolované zcela bez pochyby uznat za předávání pokynů. Jednotlivé pokyny (například zápisy ze [redacted] byly kontrolujícím předány, avšak byly zcela přehlédnuty. Další pokyny jsou v systémech [redacted] a [redacted] a část pokynů dostávala kontrolovaná prostřednictvím e-mailové a další elektronické komunikace od pověřenců správce i zpracovatele.

K tomu uvádím, že z protokolu z ústního jednání a místního šetření ze dne 25. srpna 2021 čj. UOOU-00341/21-52 vyplývá, že kontrolující vyzvali kontrolovanou k doložení pokynů, které ke zpracování dostala od NAKIT, případně Ministerstva zdravotnictví nebo od kohokoli. K tomu kontrolovaná sdělila, že původní návrhy byly jiné, neboť se systém týkal pouze rezervace termínů na testování a rezervace termínů na očkování byla požadována až později. Komunikace dle kontrolované probíhá elektronickou formou podle požadavků a urgence, a to většinou skrze pravidelné porady [redacted], formou [redacted], e-mailu a telefonu. Obecná představa pocházela vždy od Ministerstva zdravotnictví a s kontrolovanou komunikoval NAKIT, přičemž vždy byl vznesen požadavek na kýžený výsledek zadané činnosti, a rozsah a prostředky určila kontrolovaná. Dále z uvedeného protokolu vyplývá, že kontrolovaná předložila flash disk s řadou dokumentů a současně sdělila, že předložené podklady neobsahují veškeré pokyny, které od NAKIT obdržela, a že další pokyny jsou v e-mailech, projektovém systému [redacted] a systému [redacted]. Držitelem licencí na tyto systémy je dle kontrolované NAKIT, proto doporučila kontrolujícím obrátit se na NAKIT.

V protokolu z ústního jednání a místního šetření ze dne 26. srpna 2021 čj. UOOU-00341/21-53 je uvedeno, že kontrolovaná předala kontrolujícím další flash disky s tím, že *„případné další vyžadované dokumenty a skutečnosti budou případně doplněny na základě výzvy/seznamu požadavků, jelikož společnost* [redacted] *s.r.o. nebyla o ústním jednání řádně informována dle správního řádu“*. Dále kontrolovaná opětovně uvedla, že exporty, které jsou ve formě odkazu na portál, kam není přístup [redacted] a [redacted], si mají kontrolující vyžádat u NAKIT.

Obecně lze v souladu s čl. 28 odst. 3 písm. a) a čl. 29 nařízení (EU) 2016/679 konstatovat, že zpracovatel je oprávněn nakládat s osobními údaji pouze na základě doložených pokynů správce. Výstižně jsou pokyny správce popsány v komentáři Uřičař, M., Rámiš, V. a kol. Obecné nařízení o ochraně osobních údajů. 1. vydání. Praha: C. H. Beck, 2021, str. 695, kde je uvedeno, že *„základní pokyny ohledně zpracování obsahuje zpravidla zpracovatelská smlouva, která je písemná, ale následně lze dávat pokyny ad hoc dle potřeby a dohodnutého způsobu komunikace (v souladu se smlouvou a povahou zpracování). Může se jednat o písemné instrukce, včetně elektronických, ale i jiné, dají-li se zpětně prokázat (například nahrávka telefonátu). Pokud zpracovatel obdrží z nenadálých důvodů pokyn v ústní formě, je vhodné o takovém pokynu provést spolu se správcem zápis, nebo jej alespoň zpětně potvrdit třeba e-mailem.*“. K otázce konkrétnosti pokynů je ve výše citovaném komentáři na str. 712 uvedeno, že *„ta bude muset být určena vždy s ohledem na veškeré relevantní okolnosti. Pokud správce bude udělovat pokyny svým zaměstnancům, bude se obvykle jednat o konkrétnější pokyny než pokyny udělené zpracovateli, který bude provádět zpracování ve svém systému určeném pro velké množství správců, kde budou pokyny správce spíše obecnější a směřující k tomu, jakého výsledku má být dosaženo, než aby se zabývaly jednotlivými dílčími operacemi zpracování.*“.

V dodatku k protokolu o kontrole je konstatováno, že podle článku 2 bodu A3 smlouvy o poskytování softwarových a odborných služeb čj. [redacted] ze dne 8. října 2020 měly být další dílčí objednávky odborných služeb zadávány písemně a komunikovány výhradně mezi kontaktními osobami uvedenými v bodě 10 této smlouvy. Sdělení kontrolované, že pokyny související se zpracováním osobních údajů zájemců o očkování prostřednictvím rezervačního systému byly předávány formou [redacted], e-mailem, telefonem a v rámci porad [redacted], je dle kontrolujících jednoznačně v rozporu s výše uvedenou smlouvou. Je však otázkou, zda dalšími dílčími objednávkami odborných služeb je myšleno předávání pokynů ke zpracování osobních údajů. Z uvedeného bodu A3 smlouvy vyplývá, že požadavek (dílčí objednávka) musí obsahovat detailní specifikaci zamýšleného obsahu a rozsahu, včetně očekávané pracnosti, je vyhodnocován vliv na cenu služby a poskytovatel (kontrolovaná) může požadavek odmítnout, což nasvědčuje spíše tomu, že další dílčí objednávkou je myšleno rozšíření poskytované služby a nikoli předávání pokynů ve smyslu čl. 28 odst. 3 písm. a) a 29 nařízení (EU) 2016/679.

Evropský sbor pro ochranu osobních údajů ve svých pokynech 7/2020 k pojmům správce a zpracovatele podle GDPR přijatých dne 7. července 2021 v bodě 118 ve vztahu k doložitelnosti pokynů správce doporučuje, aby byl postup pro udělování dalších pokynů uveden v příloze smlouvy, alternativně mohou být pokyny poskytnuty v jakékoli písemné formě (např. e-mail), jakož i v jakékoli jiné dokumentované formě, pokud je možné o takových pokynech vést záznamy. Z uvedeného v souladu s výše citovaným komentářem vyplývá, že za pokyn může být považován i pokyn udělený na poradě pracovní skupiny, je-li o něm učiněn záznam, pokyn udělený prostřednictvím e-mailu a není vyloučena ani možnost udělení pokynu elektronicky prostřednictvím nějakého systému, jsou-li tyto pokyny doložitelné.

Kontrolovaná v průběhu ústního jednání a místního šetření ve dnech 25. a 26. srpna 2021 (dále jen „místní šetření“) předložila velké množství dokumentů, které dle jejího vyjádření obsahují pokyny správce ve vztahu k předmětu kontroly. Řada těchto dokumentů však jakékoli pokyny správce neobsahuje. Předložené zápisy z porady pracovní skupiny SSM jsou z období od 26. února do 25. srpna 2021. Zde je třeba připomenout, že předmětem kontroly byla mimo jiné kontrola dodržování povinností stanovených nařízením (EU) 2016/679, v souvislosti s podáními doručenými Úřadu, v nichž je upozorňováno na možné porušení zabezpečení osobních údajů, jelikož v průběhu rezervace termínu očkování bylo dne 15. ledna 2021 na serveru kontrolované přímou součástí veřejné URL rodné číslo, přičemž URL adresa obsahující rodné číslo byla zasílána do Google Analytics. Jelikož uvedený únik dat nebyl kontrolou řádně prošetřen, bylo na základě vyřízení námitek provedeno došetření. Kontrolovaná však kontrolujícím nepředložila pokyny správce, které by se týkaly zpracování osobních údajů v souvislosti s předmětným bezpečnostním incidentem, ke kterému došlo 15. ledna 2021 (zejm. pokyn k převzetí formátu URL z modulu registrace, pokyn k využití Google Analytics, ke smazání logů a k využití systému [redacted].

Jak již bylo uvedeno výše, kontrolovaná v rámci místního šetření sdělila, že pokyny od správce jsou udělovány prostřednictvím systémů [redacted] a [redacted], přičemž k přístupu do těchto systémů si kontrolující měli vyžádat přístup u NAKIT. Kontrolovaná je povinna podle § 10 odst. 2 kontrolního řádu poskytovat kontrolujícím potřebnou součinnost. Nelze

tedy akceptovat názor kontrolované, že si kontrolující měli vyžádat přístupové údaje u jiného subjektu (NAKIT) a v systémech si potřebné údaje vyhledat. Je to totiž kontrolovaná, která má povinnost obdržené pokyny od správce doložit a měla by tedy vědět, kde jsou uloženy (v systémech, e-mailech, zápisech z porad, záznamech z telefonních hovorů atd). Současně je však třeba připomenout, že kontrolovaná v průběhu místního šetření sdělila, že na základě výzvy (seznamu požadavků) kontrolujících doloží další dokumenty a skutečnosti, avšak kontrolující doložení dalších pokynů nepožadovali.

Pouze na základě skutečnosti, že kontrolovaná na základě žádosti o předložení všech pokynů vznesené při místním šetření hned nepředložila veškeré pokyny (přičemž sama informovala, že předkládané pokyny nejsou kompletní), nelze učinit jednoznačný závěr, že porušila povinnost zpracovávat osobní údaje pouze na pokyn správce vyplývající z čl. 29 nařízení (EU) 2016/679. V případě, že kontrolující za dané situace považovali dokumenty předložené kontrolovanou při místním šetření za nedostatečné ke zjištění skutečného stavu, měli si předložení dalších (konkrétních) dokumentů vyžádat (což např. v případě smlouvy se [redacted] učinili a kontrolovaná požadovanou smlouvu doložila). Pokud tedy kontrolovaná v námitkách proti dodatku k protokolu o kontrole uvádí, že jednala na pokyn správce, je třeba, aby pokyny v rámci došetření doložila.

3. **Námitka** směřující proti kontrolnímu zjištění č. 3 dodatku k protokolu o kontrole, kde se konstatuje, že kontrolovaná se v období od 1. února 2021 do vydání dodatku tohoto protokolu o kontrole, k předmětu kontroly, v souvislosti s nastavením a zpracováním cookies při provozování portálu určeného pro rezervace očkovacích míst, nachází v postavení správce ve smyslu čl. 4 bod 7 nařízení (EU) 2016/679, **se vyřizuje tak, že na jejím základě bude v souladu s § 21 odst. 2 kontrolního řádu provedeno došetření.**

Kontrolovaná v této souvislosti uvedla, že se v rámci vývoje a provozování Centrálního rezervačního systému nikdy nenacházela v pozici správce a cookies rovněž využívala na pokyn správce pro jím stanovené účely. Kontrolovaná dle svého vyjádření dostává pokyny od správce na využívání cookies pro jím stanovené účely a stejně tak na využívání externích nástrojů, což kontrolovaná uvedla již při místním šetření. Dále kontrolovaná uvedla, že kontrolující vycházeli pouze z podkladů předložených v časové nouzi během místního šetření, o kterém kontrolovaná nebyla s předstihem informována. Kontrolující přitom byli informováni o předávání pokynů prostřednictvím systémů [redacted] a [redacted] i o tom, že si mohou doplnění dalších podkladů vyžádat.

K tomu uvádím, že v dodatku k protokolu o kontrole je konstatováno, že přistoupením na stránky [redacted] dochází k nastavení cookies systému [redacted] (k tomu blíže viz námitka č. 9). Dále z něho vyplývá, že Google Analytics získával do 15. ledna 2021 informace o zájemcích o termín očkování, kteří v rámci procesu registrace k očkování dokončili registrační část a zahájili rezervaci konkrétního termínu. Dále kontrolující konstatují, že je-li zájemce o očkování přesměrován z registračního modulu Chytré karantény 2.0 přímo na stránku [redacted], nedochází ke dni vydání dodatku k protokolu o kontrole automaticky k nastavení cookies Google Analytics ani k načítání souvisejících skriptů. Tyto jsou však nastaveny, a to i před odsouhlasením cookie lišty, v případě, došlo-li k návštěvě stránky proklikem z hlavní stránky [redacted]. Je tedy třeba odlišit stránku

[redacted], kde je možné rezervovat termín na očkování, od stránky [redacted], která slouží k běžným obchodním činnostem kontrolované (lze provést rezervaci termínu např. na úřadě, ve zdravotnickém zařízení nebo u poskytovatelů různých služeb), zároveň lze z této stránky pokračovat na registraci termínu očkování proti COVID-19. V případě stránek [redacted] kontrolovaná zpracovává cookies v rámci svých obchodních činností, sama stanovila účel a prostředky, proto se v rámci tohoto zpracování nachází v postavení správce. Ohledně stránek [redacted], na nichž je provozován Centrální rezervační systém, přičemž kontrolovaná se nachází v pozici dalšího zpracovatele, je třeba zkoumat, zda k nasazení cookies došlo na pokyn správce.

Kontrolovaná v rámci této námitky odkazuje na dokument *Základní specifikace CRS – Očkování 2021 (Specifikace požadavků na vývoj a procesy v rezervační komponentě CRS –* [redacted] (čj. UOOU-00341/21-52 příloha 1.5.1.), jehož je autorem. V dokumentu je zmínka o cookies na str. 29 v bodě 13, avšak tento text je přeškrtnut a není tedy patrné, zda informace platí či nikoli. Jak bylo uvedeno výše, pokyny ke zpracování osobních údajů může správce udělit různými způsoby, vždy však musí být doložitelné. Ústně udělený pokyn (např. při jednání) proto musí být písemně zaznamenán. Obecně nelze vyloučit, aby písemný záznam učinil zpracovatel, resp. další zpracovatel, zejména v případě, kdy je zpracovatel odborník, který má více informací o technické specifikaci dodávané služby, nicméně k prokázání toho, že se jednalo o pokyn správce je potřeba, aby tento zápis správce potvrdil. Kontrolovaná dále v rámci této námitky odkazuje na pokyny udělované prostřednictvím systémů [redacted] a [redacted], případně na možnost kontrolujících vyžádat si další podklady. V této souvislosti odkazuji na vyřízení námitky č. 2. Kontrolou nebylo zjištěno, zda kontrolovaná v souvislosti s využitím cookies (např. systému [redacted] na stránkách [redacted] jednala v souladu s pokyny správce a nelze tedy jednoznačně určit, zda se nachází v postavení správce či zpracovatele, z tohoto důvodu je třeba provést došetření.

Ke Google Analytics je třeba doplnit, že posouzení vlivu na ochranu osobních údajů „Projekt: IT podpora OČKOVÁNÍ“ verze 2 ze dne 10. února 2021 (DPIA správce) obsahuje v bodě 6.5 a 6.6 informaci o využití Google Analytics v rámci registrace i rezervace (verze 1 ze dne 9. ledna 2021 informaci o cookies neobsahuje). Stejná informace je uvedena i v Záznamu o činnostech zpracování z února 2021, který předložilo Ministerstvo zdravotnictví. Od února 2021 Ministerstvo zdravotnictví zmiňuje využití Google Analytics v průběhu registrace a rezervace ve svých dokumentech, tedy lze usuzovat na existenci pokynu k nasazení cookies vůči kontrolované. Od února 2021 se tak kontrolovaná ve vztahu ke cookies služby Google Analytics na stránkách [redacted] pravděpodobně nacházela v postavení zpracovatele. Zda správce udělil kontrolované pokyn k využívání Google Analytics již dříve, nebylo zjištěno.

4. **Námitka** směřující proti kontrolnímu zjištění č. 4 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná v postavení správce osobních údajů pro zpracování osobních údajů prostřednictvím analytických cookies v případě přistoupení k rezervaci termínu očkování přímo ze stránky kontrolované osoby, v období od 1. února 2021 do vydání tohoto dodatku protokolu o kontrole porušuje čl. 6 odst. 1 nařízení (EU) 2016/679 tím, že

předmětné zpracování není prováděno na základě některého z právních titulů definovaných pod čl. 6 nařízení 2016/679, **se zamítá.**

K tomu kontrolovaná uvedla, že nasazené cookies provozovala pouze na pokyn správce, analytická data sloužila a slouží pouze správci a kontrolovaná pro tento druh zpracování neurčuje jeho účel. Kontrolovaná dle svého vyjádření zpracovává cookies v rámci svých běžných obchodních činností na doméně [redacted], o čemž řádně informuje na svých webových stránkách. Centrální rezervační systém probíhá na [redacted] a zde nasazené cookies jsou zpracovány pro potřeby správce. Obecně je tedy Centrální rezervační systém oddělen od komerčního provozu kontrolované.

K tomu uvádím, že kontrolou bylo zjištěno, že vstupem na stránky [redacted] dochází k nastavení analytických a dalších cookies (úřední záznam čj. UOOU-00341/21-43 ze dne 24. května 2021). Zájemci o očkování, který si chce rezervovat termín a přichází na stránky [redacted] (a následně klikne na odkaz „Očkování Covid-19“), jsou nastaveny cookies. K nastavení cookies tedy dochází na stránkách kontrolované, které slouží k jejím komerčním účelům. Jak bylo konstatováno výše, zde se kontrolovaná nachází v pozici správce, na kterého se mimo jiné vztahuje povinnost zpracovávat osobní údaje na základě některého právního titulu podle čl. 6 odst. 1 nařízení (EU) 2016/679.

Kontrolovaná na svých internetových stránkách prostřednictvím cookies lišty poskytovala informaci „*Abychom Vám mohli poskytovat služby sociálních sítí, používáme na tomto webu soubory cookie. Používáním našich služeb vyjadřujete souhlas s používáním souborů cookies.*“. Vedle této informace je tlačítko „souhlasím“ (viz příloha č. 11 úředního záznamu čj. UOOU-00341/21-26 ze dne 19. února 2021). Kontrolovaná tedy stanovila jako právní titul zpracování osobních údajů prostřednictvím cookies souhlas, tj. provádí zpracování podle čl. 6 odst. 1 písm. a) nařízení 2016/679. Cookies jsou však do prohlížeče uživatele uloženy i bez interakce s cookies lištou, tedy bez kliknutí na tlačítko souhlasu (viz. úřední záznam čj. UOOU-00341/21-65 ze dne 16. září 2021). Takto udělený souhlas nelze považovat za souhlas podle čl. 4 odst. 11 nařízení (EU) 2016/679, zejména z důvodu, že není svobodný ani informovaný.

Dále kontrolovaná informuje o cookies na svých stránkách [redacted] (úřední záznam čj. uoou-00341/21-61 ze dne 13. září 2021), kde uvádí, že sběr cookies lze považovat za zpracování osobních údajů, které je možné, s výjimkou marketingových cookies, na základě oprávněného zájmu kontrolované dle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679. Marketingové cookies kontrolovaná zpracovává na základě souhlasu subjektů údajů podle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679, který subjekt údajů uděluje prostřednictvím nastavení internetového prohlížeče. Informace v cookie liště se tedy neshodují s informací uvedenou na internetových stránkách kontrolované, jelikož cookie lišta hovoří pouze o souhlasu a nikoli o oprávněném zájmu. Jak uvádí sama kontrolovaná „*většina internetových prohlížečů cookies automaticky přijímá již ve výchozím nastavení*“, proto nelze souhlas udělený prostřednictvím prohlížeče považovat za souhlas podle nařízení (EU) 2016/679, neboť zde absentuje jakýkoli projev vůle ze strany subjektů údajů. Skutečnost, že lze nastavením prohlížeče souhlas následně odvolat, na situaci nic nemění, jelikož ke zpracování údajů již došlo, a to bez souhlasu subjektu údajů,

a navíc změna nastavení internetového prohlížeče není pro běžného uživatele jednoduchá. Lze tedy v souladu s kontrolním zjištěním č. 4 konstatovat, že kontrolovaná zpracovávala předmětné osobní údaje bez právního titulu.

5. **Námitce** směřující proti kontrolnímu zjištění č. 5 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná v období od 1. února 2021 do vydání tohoto dodatku protokolu o kontrole porušuje ustanovení čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 (zásada korektnosti) tím, že informace poskytnuté subjektům údajů prostřednictvím webových stránek kontrolované jsou pro subjekty údajů v rámci rezervačního systému zmatečné z důvodu, že je zde kontrolovaná uvedena v pozici správce, přičemž tento vztah se těchto subjektů údajů netýká, což v dokumentu není uvedeno a zároveň zde nejsou přímo dostupné informace týkající se zpracování osobních údajů zájemců o rezervaci termínu očkování COVID-19, čímž není plněna zásada korektnosti, **se částečně vyhovuje.**

   V této souvislosti kontrolovaná uvedla, že každý zájemce o rezervaci termínu očkování pomocí Centrálního rezervačního systému je od jeho spuštění dne 15. ledna 2021 řádně informován o budoucím zpracování osobních údajů, přičemž kontrolovaná odkazuje na informaci zveřejněnou na stránkách https://registrace.mzcr.cz, kde je kontrolovaná uvedena jako další zpracovatel. Kontrolovaná má za to, že osobní údaje jsou v rámci Centrálního rezervačního systému ve vztahu k subjektu údajů zpracovávány korektně a zákonným způsobem. Dále kontrolovaná opakuje argumenty, které uvedla již dříve a současně poukazuje na nesprávné údaje, které jsou dle jejího názoru na internetových stránkách Úřadu.

   K tomu uvádím, že pokud chce zájemce o očkování rezervovat termín očkování, nejprve se registruje na stránkách https://registrace.mzcr.cz. K provedení registrace je třeba, aby subjekt údajů zaškrtnul souhlas se zpracováním osobních údajů. Informace k souhlasu jsou uvedeny pod tímto zaškrtávacím políčkem a obsahují i interaktivní odkaz na detailní informace o zpracování osobních údajů. Po jeho rozkliknutí se zobrazí dokument „Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ (Centrální rezervační systém – očkování proti covid-19)“, ve kterém jsou uvedeny základní informace o zpracování osobních údajů, a to důvod a účel zpracování, výčet zpracovávaných osobních údajů, výčet zpracovatelů, doba uchování osobních údajů, výčet práv subjektu údajů a způsob, jak tato práva uplatnit. Zájemcům o očkování jsou tedy informace o zpracování osobních údajů poskytnuty již při registraci. Teprve po úspěšné registraci a po obdržení PIN2 uživatel přechází na internetové stránky kontrolované k provedení rezervace termínu očkování. Povinnost poskytnout subjektu údajů transparentní informace o zpracování je uložena správci, přičemž podle čl. 13 odst. 4 nařízení (EU) 2016/679 informace subjektu údajů poskytovat nemusí, pokud subjekt údajů uvedené informace má, a do té míry, v níž je má.

   Poskytované informace mají být snadno přístupné. Mezi registrací a rezervací termínu očkování může uplynout delší doba, případně se subjekt údajů může chtít k informacím dostat kdykoli později a vzhledem k tomu, že rezervace termínu je prováděna na stránkách kontrolované, může subjekt tyto informace vyhledávat a očekávat právě tam. Z tohoto důvodu je vhodné, aby tyto informace byly umístěny i na stránkách kontrolované, a to třeba i formou odkazu na stránky správce. Kontrolovaná na svých stránkách odkazuje na informaci

zveřejněnou na https://registrace.mzcr.cz, avšak na tyto stránky odkazuje v souvislosti s tím, že je nejprve nutné na těchto stránkách provést registraci a teprve poté termín rezervovat na stránkách kontrolované. Zmíněný odkaz tak není výslovně uveden jako zdroj informací o zpracování osobních údajů, nicméně lze konstatovat (na rozdíl od závěrů kontrolujících), že tento odkaz vede přímo k informacím o zpracování. Je sice třeba se rolováním myší posunout na stránce o něco níž, kde jsou uvedeny základní informace, a následně je možné rozkliknout odkaz na podrobnější informace, avšak informace není třeba nijak složitě vyhledávat. Z výše uvedených důvodů se námitce kontrolované částečně vyhovuje.

Nad rámec námitky kontrolované ke konstatování kontrolujících, že ve výčtu práv subjektů údajů uvedených v informacích zveřejněných na https://registrace.mzcr.cz absentuje právo být informován ohledně opravy, výmazu či omezení zpracování podle čl. 19 nařízení (EU) 2016/679 uvádím, že obsah informační povinnosti správce je upraven v čl. 13 a 14 nařízení (EU) 2016/679, přičemž povinnost informovat subjekt údajů ohledně opravy, výmazu či omezení zpracování zde uvedena není. Neuvedení této informace v rámci plnění informační povinnosti tak nelze považovat za porušení nařízení (EU) 2016/679.

Na stránkách  nejsou přímo uvedeny informace o zpracování osobních údajů zájemců o očkování. Kontrolovaná tedy pouze odkazuje na stránky správce, avšak, jak bylo zmíněno výše, tento odkaz není označen jako místo, kde je plněna informační povinnost správce. Pokud tedy kdokoli, kdo přijde na stránky kontrolované, bude hledat informace o zpracování osobních údajů zájemců o očkování, pak jediným odkazem, který k těmto informacím jednoznačně vede, je interaktivní odkaz „Zásady zpracování osobních údajů“ umístěný v patičce webu kontrolované. Na tomto místě jsou však poskytovány informace týkající se obchodních činností kontrolované, kde je kontrolovaná označena jako správce osobních údajů, přičemž zájemce o očkování o komerční činnosti kontrolované nemusí vůbec vědět. Informace poskytované kontrolovanou na jejích webových stránkách jsou tedy zmatečné, jak je konstatováno v kontrolním zjištění č. 5.

Námitka kontrolované ohledně zpracování osobních údajů Úřadem nijak nesouvisí s kontrolním zjištěním č. 5 a ani nemá vliv na plnění povinností vyplývajících z nařízení (EU) 2016/679 kontrolovanou.

6. **Námitce** směřující proti kontrolnímu zjištění č. 6 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná v postavení správce osobních údajů pro oblast zpracování osobních údajů prostřednictvím cookies v rámci prováděných rezervací na očkování COVID-19 přímo ze stránek kontrolované osoby porušuje ustanovení čl. 13 až 22 nařízení (EU) 2016/679, neboť řádně neplní informační povinnosti a nezabezpečuje výkon práv subjektů údajů; v souvislosti s tím porušuje rovněž ustanovení čl. 12 odst. 2 nařízení (EU) 2016/679, neboť neusnadňuje výkon práv subjektů údajů**, se částečně vyhovuje.**

Kontrolovaná k tomu uvádí, že je pouze technický realizátor. O způsobu nasazení prostředků, jejich rozsahu a využití vždy rozhoduje správce, který také za tímto účelem plní informační povinnost. Osobní údaje, které zpracovává v rámci svých běžných obchodních činností jsou odděleny, o čemž řádně informuje na svém webu

[redacted]. Přesto kontrolovaná proaktivně detailněji rozpracovala dokument „Zásady zpracování osobních údajů“, včetně informací o cookies.

Předně je třeba konstatovat, že kontrolní zjištění č. 6 se týká používání cookies na stránkách [redacted], tedy na stránkách, kde dochází ke zpracování osobních údajů v rámci obchodních činností kontrolované, kde se kontrolovaná nachází v postavení správce. Ohledně cookies kontrolovaná na stránkách [redacted] (úřední záznam čj. UOOU-00341/21-61 ze dne 13. září 2021) v souladu s čl. 13 nařízení (EU) 2016/679 informuje o tom, že je správcem, o účelech zpracování, právním titulu i o dalších zpracovatelích, dále pak vyjmenovává práva subjektů údajů podle čl. 15-18 a čl. 20 a 21 a informuje o právu podat stížnost Úřadu. Absentuje zde však informace zejména o době uložení údajů, o jednotlivých zpracovávaných cookies, o předávání údajů do třetích zemí a o profilování podle čl. 22 nařízení (EU) 2019/679. Kontrolovaná tak neplní informační povinnost podle čl. 13 nařízení (EU) 2016/679 v plném rozsahu.

Kontrolovaná dále v souladu s čl. 13 odst. 2 písm. b) nařízení (EU) 2016/679 informuje o právu požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i právu na přenositelnost údajů. Současně kontrolovaná informuje, že proti zpracování cookies lze vznést námitku na e-mail [redacted], přičemž tento e-mail lze využít i v případě jakýchkoli dotazů či připomínek. Kontrolovaná tedy neporušuje čl. 15 až 21 nařízení (EU) 2016/679. Vzhledem k tomu, že osobní údaje jsou získávány od subjektů údajů, povinnost informovat subjekty podle čl. 14 nařízení (EU) 2016/679 se na kontrolovanou nevztahuje. Kontrolovaná tedy neporušuje ani čl. 14 nařízení (EU) 2016/679. Z uvedených důvodů se námitce kontrolované částečně vyhovuje.

7. **Námitka** směřující proti kontrolnímu zjištění č. 7 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná porušila čl. 32 odst. 1 písm. b) nařízení (EU) 2016/679 tím, že nezajistila neustálou důvěrnost, integritu, dostupnost a odolnost systému tím, že přebírala URL adresu obsahující CPOJ a tuto zpracovávala za současného použití služby Google Analytics, přičemž tímto došlo k úniku URL adres včetně CPOJ v rozsahu cca 800 tisíc subjektů údajů**, se zamítá.**

V této souvislosti kontrolovaná zopakovala, že nástroj Google Analytics využila na základě potřeb a pokynů správce, přičemž zpracování osobních údajů v nástrojích společnosti Google nemůže být dle jejího názoru bráno jako porušení jejich ochrany. Služba Google Analytics byla podle kontrolované řádně zasmluvněna a společnost Google byla jako zpracovatel uvedena zájemcům ještě před jejich registrací (např. na stránkách [redacted] nebo v DPIA správce). Po upozornění ze strany médií bylo zpracování prošetřeno pověřenci Ministerstva zdravotnictví a NAKIT, kteří shledali zpracování čísla pojištěnce v URL jako nevhodné a neopodstatněné, proto správce vydal pokyn kontrolované k zastavení zpracování URL s číslem pojištěnce souběžně s nástrojem Google Analytics a k provedení výmazu veškerých údajů předaných v rámci nástroje Google Analytics. Toto bylo provedeno, zdokumentováno a správcem doloženo kontrolujícím. I přes nízkou míru rizika byl incident pro možné porušení zabezpečení ohlášen Úřadu. Kontrolovaná dále uvedla, že jednala na pokyn správce, proto se porušení čl. 32 odst. 1 písm. b) nařízení (EU) 2016/679 nemohla dopustit. Dále kontrolovaná sdělila, že ohlášení se

týkalo 80 000 čísel pojištěnců, nikoli 800 000, jak je uvedeno v napadeném kontrolním zjištění.

K tomu uvádím, že k úniku dat došlo dne 15. ledna 2021, proto je třeba posuzovat veškeré poskytnuté informace a pokyny předcházející tomuto datu. Před provedením registrace k očkování na stránkách https://registrace.mzcr.cz nebyly subjekty údajů o využití Google Analytics předem informovány. Posouzení vlivu na ochranu osobních údajů „Projekt: IT podpora OČKOVÁNÍ" verze 1 ze dne 9. ledna 2021 (DPIA správce) informaci o cookies neobsahuje. Informace o využití Google Analytics je uvedena až ve verzi 2 ze dne 10. února 2021, kde je mimo jiné uvedeno, že „v URL není sbíráno RČ". Stejná informace ohledně rodného čísla v URL je uvedena i v Záznamu o činnostech zpracování z února 2021, který předložilo Ministerstvo zdravotnictví. Oba tyto dokumenty jsou datovány k únoru 2021, vznikly tedy až po předmětném úniku dat a informace o rodném čísle v URL je v nich zřejmě uvedena právě v souvislosti s tímto incidentem. Od února 2021 Ministerstvo zdravotnictví zmiňuje využití Google Analytics v průběhu registrace a rezervace ve svých dokumentech, z čehož lze usuzovat na existenci pokynu k nasazení cookies vůči kontrolované. Zda správce udělil pokyn k převzetí rodného čísla v URL (před 15. lednem 2021), případně jak zněl, nebylo kontrolou zjištěno.

Skutečnosti, že k úniku dat došlo, si zřejmě byla vědoma sama kontrolovaná (na základě podnětu z médií), když událost oznámila správci, resp. NAKIT. Stejně tak situaci (existenci rizika) vyhodnotili pověřenci správce a zpracovatele, když incident oznámili Úřadu. Je třeba si uvědomit, že do Google Analytics nebyly předány pouze údaje o IP adrese, nebo o chování uživatele na internetu, ale zcela jednoznačný identifikátor fyzické osoby, proto nelze tuto situaci srovnávat s běžným využitím Google Analytics.

Zpracovatel, resp. další zpracovatel má dle čl. 28 odst. 3 písm. h) nařízení (EU) 2016/679 povinnost neprodleně informovat správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů. Tato povinnost kontrolované vyplývá i ze smlouvy s NAKIT čj. [redacted] ze dne 8. října 2020, kde je v čl. 6 písm. C bod 12 uvedeno *„Pokud poskytovatel zjistí, že Objednatel porušuje povinnosti stanovené GDPR, je povinen na to Objednatele neprodleně upozornit.".*

Pokyny k přebírání URL obsahující čísla pojištěnců a k využití Google Analytics budou předmětem došetření (viz vyřízení námitky č. 2). Ačkoli existence těchto pokynů nemá vliv na to, zda došlo k porušení čl. 32 odst. 1 písm. b) nařízení (EU) 2016/679, má vliv na míru odpovědnosti kontrolované. Pokud by kontrolovaná jednala svévolně bez pokynu správce, byla by za únik dat sama zcela odpovědná. V případě, že jednala na pokyn správce, byla by spoluodpovědná, jelikož jej měla upozornit, že požadované zpracování není v souladu s nařízením (EU) 2016/679.

Počet uniklých čísel pojištěnců 800 000 uvedený v kontrolním zjištění č. 7 je zjevnou chybou v psaní (správně je 80 000). K úniku dat došlo dne 15. ledna 2021, přičemž z veřejně dostupných zdrojů vyplývá, že v tento první den spuštění registrace k očkování se registrovalo něco přes 100 000 osob. Zároveň se k tomuto datu mohly registrovat pouze osoby starší 80 let, kterých bylo, podle dat dostupných na internetových stránkách Českého

statistického úřadu ke dni 1. ledna 2020, cca 450 000. V tomto kontextu je zřejmé, že číslo 800 000 je pouze chybou v psaní.

8. **Námitka** směřující proti kontrolnímu zjištění č. 8 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná porušila ustanovení čl. 29 (EU) 2016/679 tím, že smazala logy týkající se databreach, v rozporu se smlouvou o poskytování softwarových a odborných služeb čj. [redacted], **se vyřizuje tak, že na jejím základě bude v souladu s § 21 odst. 2 kontrolního řádu provedeno došetření.**

   K tomu kontrolovaná sdělila, že dne 15. ledna 2021 obdržela od správce, prostřednictvím zpracovatele, požadavek na prošetření a nápravu stavu ohledně předávání a přebírání dat v URL obsahujících číslo pojištěnce a následné předávání do nástroje Google Analytics včetně ukládání údajů do logů serverů. Po konzultacích mezi zástupci správce, zpracovatele a kontrolované, bylo požádáno o výmaz logů obsahujících uvedené osobní údaje a zajištění automatické anonymizace dat v logu v případě požadavku na server obsahující číslo pojištěnce. Kontrolovaná tak v souladu s rozhodnutím správce podle čl. 28 odst. 3 písm. g) nařízení (EU) 2016/679 osobní údaje vymazala. Zároveň kontrolovaná postupovala v souladu s článkem 6 písm. C bodem 8 smlouvy čj. [redacted] ze dne 8. října 2020, kde je uvedeno, že „*Poskytovatel se zavazuje zajistit výmaz osobních údajů ve lhůtách stanovených Zpracovatelem*“.

   Z dodatku k protokolu o kontrole vyplývá, že kontrolovaná „*nedoložila žádné instrukce vedoucí k vymazání logů týkajících se databreach, z čehož kontrolující vyvodili, že k odstranění logů přistoupila z vlastní iniciativy, čímž došlo k jednání v rozporu se Smlouvou o poskytování softwarových a odborných služeb čj.* [redacted] *(viz č. 26.3. přehledu podkladů, bod 24.3), kde je uvedeno, že je kontrolovaná osoba povinna pořizovat a uchovávat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány*“. K posouzení, zda kontrolovaná porušila čl. 29 nařízení (EU) je zásadní, zda jednala z pokynu správce, či z vlastní iniciativy. Ohledně doložení pokynů plně odkazuji na vyřízení námitky č. 2.

   Nad rámec námitky kontrolované je třeba doplnit, že pokud existovalo podezření z porušení zabezpečení osobních údajů, neměla kontrolovaná logy smazat (ani z pokynu správce), jelikož tím došlo ke smazání důkazů o tom, jak k předmětnému porušení zabezpečení došlo.

9. **Námitka** směřující proti kontrolnímu zjištění č. 9 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná, jako zpracovatel osobních údajů, v období od 1. února 2021 minimálně do 10. září 2021 porušovala ustanovení čl. 44 nařízení (EU) 2016/679, tím, že prostřednictvím systému [redacted] předávala osobní údaje uživatelů stránek [redacted] do třetích zemí (USA), aniž by plnila podmínky ustanovení čl. 44 a následujících nařízení (EU) 2016/679**, se vyřizuje tak, že na jejím základě bude v souladu s § 21 odst. 2 kontrolního řádu provedeno došetření.**

   K tomu kontrolovaná uvedla, že postupovala podle pokynů správce, neboť požadavek na systém [redacted] z důvodu zajištění vysoké míry bezpečnosti dat byl předmětem prvotní nabídky a celého výběrového řízení a současně byl tento systém nutnou podmínkou pro provoz platební brány systému [redacted]. Nástroj byl dle názoru kontrolované řádně

zajištěn smluvními podmínkami, které jsou plně v souladu s právním řádem Evropské unie a České republiky včetně ochrany osobních údajů. Pokud má Úřad za to, že společnost [redacted] provozuje své nástroje v rozporu s legislativou Evropské unie, měl zahájit kontrolu této společnosti. Dále kontrolovaná sdělila (shodně se svým doplněním ke spisu ze dne 14. září 2021), že na základě konzultace s ICŘT bylo vyhodnoceno, že systém bezpečnostních kontrol poskytovaný společností [redacted] byl adekvátně nahrazen pravidelnými bezpečnostními a zátěžovými testy zajišťovanými zpracovatelem a současně byl platební systém [redacted] nahrazen systémem [redacted], proto bylo používání systému [redacted] ukončeno.

Při předávání osobních údajů do třetích zemí musí správce vybrat pouze takové zpracovatele, kteří poskytnou vhodné záruky, že předaným osobním údajům ve třetí zemi bude zajištěna v zásadě rovnocenná ochrana, jako je poskytovaná nařízením (EU) 2016/679. Ze smluvních podmínek společnosti [redacted] zveřejněných na stránkách [redacted] vyplývá, že tato společnost poskytuje záruky pro zpracování osobních údajů na základě své certifikace k tzv. Štítu EU-USA (dále jen „Štít soukromí“) na ochranu soukromí. Prováděcí rozhodnutí komise (EU) 2016/1250 ze dne 12. července 2016 o odpovídající úrovni ochrany poskytované Štítem soukromí bylo prohlášeno za neplatné rozsudkem Soudního dvora Evropské unie ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) ze dne 16. července 2020. Nadále tak již není možné předávat osobní údaje do USA na základě Štítu soukromí. Společnost [redacted] tak nezajišťuje dostatečnou ochranu předávaným údajům ani účinnou právní ochranu subjektům údajů. K předávání údajů do USA navíc dochází, aniž by o tom byly subjekty údajů informovány. V případě, že k využití systému [redacted] dal kontrolované pokyn správce, měla jej kontrolovaná upozornit, že pokyn porušuje nařízení (EU) 2016/679.

Nad rámec argumentů uvedených kontrolovanou v rámci této námitky je třeba konstatovat, že kontrolovanou nebyl doložen pokyn k nasazení systému [redacted] a není tedy zřejmé, proč v tomto případě kontrolující považují kontrolovanou za zpracovatele, což současně nekoresponduje s kontrolním zjištěním č. 3, kde je kontrolovaná v souvislosti s nastavením cookies při provozování portálu určeného pro rezervace očkovacích míst považována za správce. V souladu s vyřízením námitky č. 3 je třeba provést došetření.

10. **Námitka** směřující proti kontrolnímu zjištění č. 10 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná, jako zpracovatel osobních údajů pro rezervační systém zájemců o očkování COVID-19, v období od 1. února 2021 do vydání tohoto dodatku protokolu o kontrole, porušuje čl. 37 odst. 1 nařízení (EU) 2016/679, neboť pro předmětné zpracování nejmenovala pověřence pro ochranu osobních údajů**, se zamítá.**

Kontrolovaná k tomu uvedla, že je přesvědčena, že není povinnou osobou podle čl. 37 nařízení (EU) 2016/679. Dále kontrolovaná konstatuje, že zmíněné nařízení nedefinuje, co znamená rozsáhlé zpracování, přičemž vychází z příkladů zpracování velkého rozsahu uvedených v pokynech Evropského sboru pro ochranu osobních údajů WP 243 ze dne 13. prosince 2016 (rev. dne 5 dubna 2017) týkajících se pověřenců pro ochranu osobních údajů (dále jen „Pokyny WP 243“). Informace nutné k prioritizaci osob, jež by mohly být klasifikovány jako osobní údaje zvláštní kategorie, byly podle kontrolované správcem

vyžadovány pouze v počátku Centrálního rezervačního systému a pouze v malém množství. Samotné údaje o prioritizaci sice obsahují prvky citlivosti, ale dle vyjádření kontrolované se nejedná o zvláštní kategorie osobních údajů podle čl. 9 nařízení (EU) 2016/679. Dále k tomuto kontrolovaná uvedla, že rizika v souvislosti se zpracováním osobních údajů jsou ze strany správce a zpracovatele (včetně kontrolované) pravidelně posuzována a to i s přihlédnutím k rozšiřování funkcionality Centrálního rezervačního systému a množství zpracovávaných osobních údajů a dalších dat. Následně jsou rizika i opatření implementována mimo jiné do DPIA, které je pravidelně aktualizováno. Závěrem kontrolovaná uvedla, že i přes výše uvedené ke dni 5. října 2021 dobrovolně pověřence pro ochranu osobních údajů jmenovala.

K tomu uvádím, že správce a zpracovatel jmenují pověřence pro ochranu osobních údajů ve smyslu čl. 37 odst. 1 nařízení (EU) 2016/679 v případě, že a) zpracování provádí orgán veřejné moci či veřejný subjekt, nebo b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 uvedeného nařízení.

V dodatku k protokolu o kontrole je konstatováno, že vzhledem ke skutečnosti, že do zpracování je zapojen orgán veřejné moci (Ministerstvo zdravotnictví) a dále k tomu, že dochází k rozsáhlému zpracování zvláštní kategorie údajů, vznikla kontrolované povinnost jmenovat pověřence pro ochranu osobních údajů. Zde je třeba v souladu s Pokyny WP 243 (str. 11) zmínit, že správcem je sice orgán veřejné moci, avšak „*i když správce splňuje kritéria pro povinné jmenování, jeho zpracovatel není nutně povinen jmenovat pověřence pro ochranu osobních údajů*“. Skutečnost, že zpracování osobních údajů provádí orgán veřejné moci, nemusí nutně znamenat, že veškeré další subjekty zapojené do zpracování musí jmenovat pověřence pro ochranu osobních údajů.

Ke zpracování zvláštní kategorie údajů je třeba konstatovat, že údaje o zdravotním stavu do této kategorie bezesporu spadají. V případě kontrolované se nejedná pouze o informaci o diagnóze uváděnou v případě prioritizace, ale i samotná informace o tom, zda je subjekt údajů očkovaný, je zvláštní kategorií osobních údajů podle čl. 9 nařízení (EU) 2016/679.

Ohledně pojmu „rozsáhlé zpracování“ je v Pokynech WP 243 doporučeno, aby byly při určování toho, zda je zpracování prováděno ve velkém rozsahu, vzaty v úvahu především tyto faktory: počet dotčených subjektů (buď jako konkrétní číslo, nebo jako podíl příslušné skupiny obyvatelstva), objem údajů a/nebo škála různých údajových položek, trvání nebo stálost činnosti zpracování údajů a zeměpisný rozsah činnosti zpracování. V Metodickém pokynu pro očkovací kampaň Plán provedení vydaném Ministerstvem zdravotnictví se v čl. 1 písm. C uvádí, že požadovaný konečný stav v rámci procesu očkování je dosáhnout minimálně 60 % proočkovanosti cílové populace České republiky. V záznamech o činnostech zpracování správce je v bodě 11 uvedeno, že přibližný celkový plánovaný počet osob v systému je 8 až 10 milionů (k datu 9. září 2021 byl počet unikátních čísel pojištěnců, kteří měli vytvořenou rezervaci na očkování, celkem 4 629 802 – viz vyjádření kontrolované ze dne 10. září 2021). Od počátku zpracování tak bylo zřejmé, že bude docházet ke zpracování údajů milionů subjektů údajů, což jistě je rozsáhlé zpracování. Ke stejnému závěru ostatně

dospěl i sám správce, který v Posouzení vlivu na ochranu osobních údajů „Projekt: IT podpora OČKOVÁNÍ“ ze dne 9. ledna 2021 (DPIA správce) v čl. 4 uvedl, že „*se jedná o **rozsáhlé zpracování zvláštní kategorie údajů** dle č. 9 odst. 1 GDPR (čl. 35 odst. 3 b)*“, což byl ostatně jeden z důvodů, proč správce posouzení vlivu na ochranu osobních údajů prováděl.

Zbývá tedy v souvislosti s čl. 37 odst. 1 písm. c) nařízení (EU) 2016/679 posoudit, zda se jedná o hlavní činnost kontrolované. Opět lze vycházet z Pokynů WP 243, podle kterých za hlavní činnosti mohou být považovány klíčové operace nezbytné pro dosažení cílů správce nebo zpracovatele. Dále je na tomto místě uvedeno, že hlavní činnosti by neměly být vykládány tak, že vylučují činnosti, při nichž zpracování údajů tvoří neoddělitelnou část činnosti správce nebo zpracovatele. Předmětem činnosti kontrolované je, podle výpisu z obchodního rejstříku, vývoj a poskytování práva užití počítačových programů (software) pro objednávání klientů a poskytování služeb s tím souvisejících. Kontrolovaná tedy vyvíjí a provozuje software, jehož nedílnou součástí je zpracování osobních údajů, což lze považovat za hlavní činnost.

Vzhledem k rozsahu zpracovávaných citlivých údajů (přes 4,5 milionu subjektů údajů) je zřejmé, že hlavní činnosti kontrolované spočívají v rozsáhlém zpracování zvláštních kategorií údajů. Na základě výše uvedeného je třeba konstatovat, že kontrolovaná měla povinnost jmenovat pověřence pro ochranu osobních údajů podle čl. 37 odst. 1 písm. c) nařízení (EU) 2016/679. Tuto povinnost kontrolovaná splnila až dne 5. října 2021, na základě zjištění uvedeného v dodatku k protokolu o kontrole.

11. Námitce směřující proti kontrolnímu zjištění č. 11 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná minimálně v období od 1. února 2021 do 5. září 2021 porušovala čl. 30 odst. 1 a 2 nařízení (EU) 2016/679 tím, že nevedla žádné záznamy o činnostech zpracování týkající se rezervací termínů očkování COVID-19, **se částečně vyhovuje.**

Kontrolovaná v této souvislosti sdělila, že správce vedl od počátku zpracování záznamy o činnostech zpracování, které využívala i kontrolovaná. Od počátku provozování Centrálního rezervačního systému měla kontrolovaná také v papírové podobě zpracovány „Záznamy o kategoriích činností“, které obsahují všechny atributy podle čl. 30 odst. 2 nařízení (EU) 2016/679. Oba dokumenty byly kontrolujícím předloženy. Kontrolovaná dále uvedla, že odkaz na záznamy o činnostech zpracování a jejich popis je uveden také v interních metodikách kontrolované, konkrétně v dokumentu „2020-09-28 Interní směrnice pro práci s osobními údaji NAKIT [redacted], který byl kontrolujícím rovněž předložen. Dále se kontrolovaná ohrazuje vůči konstatovanému porušení čl. 30 odst. 1 nařízení (EU) 2016/679, kterého se nemohla dopustit, jelikož se nenacházela v postavení správce.

K tomu uvádím, že kontrolovaná ve svém vyjádření ze dne 10. února 2021 sdělila, že „je pouze subzpracovatel, Záznam o činnostech zpracování má správce osobních údajů“. Z této věty lze vyvodit, že kontrolovaná sama záznamy o činnostech zpracování nevede, nicméně ví o tom, že je vede správce. Ačkoli povinnost vést záznamy o činnostech zpracování je uložena jak správci, tak zpracovateli, příp. dalšímu zpracovateli, v zásadě není vyloučeno,

aby záznamy vedli společně, pokud budou splňovat veškeré náležitosti čl. 30 nařízení (EU) 2016/679. Z výše citovaného vyjádření kontrolované však nelze jednoznačně dovodit, zda záznamy vedené správcem využívala také kontrolovaná či nikoli. Dokument kontrolované „2020-09-28 Interní směrnice pro práci s osobními údaji NAKIT [redacted], na který kontrolovaná v souvislosti se záznamy o činnostech zpracování odkazuje, žádné informace o záznamech ve smyslu čl. 30 nařízení (EU) 2016/679 neobsahuje.

V rámci místního šetření dne 26. srpna 2021 kontrolovaná na dotaz, zda má vlastní záznamy o činnostech zpracování týkající se rezervace očkování, uvedla, že nemá vytvořeny vlastní záznamy o zpracování, že jsou používány záznamy správce. Následně dne 6. září 2021 zaslala kontrolovaná návrh na doplnění kontrolního spisu, v němž uvedla, že dotaz ohledně záznamů o činnostech zpracování položený při místním šetření mylně pochopila (vinou absence právního zástupce) a za účelem doplnění otázky doložila Záznamy o kategoriích činností zpracování prováděných pro správce, tedy záznamy o činnostech zpracování podle čl. 30 odst. 2 nařízení (EU) 2016/679. Předložený dokument není datován. Je v něm však uveden pověřenec pro ochranu osobních údajů správce Robert Vávra, který byl dle sdělení Ministerstva zdravotnictví ze dne 26. března 2021 (čj. UOOU-00005/21-385) jmenován s účinností od 15. března 2021, a předložené záznamy tak byly vytvořeny po tomto datu. Kontrolou se však nepodařilo zjistit, od kdy kontrolovaná záznamy o činnostech zpracování vede. Současně kontrolou nebylo dostatečně prokázáno, zda kontrolovaná využívala záznamy o činnostech zpracování vedené správcem společně s ním. Na základě zásady *in dubio pro reo* bylo námitce vyhověno.

Ohledně možného porušení čl. 30 odst. 1 nařízení (EU) 2016/679 uvádím, že kontrolou bude v souladu s vyřízením námitky č. 2 došetřeno, zda kontrolovaná v rámci provozování systému pro rezervaci termínů očkování vždy jednala pouze na pokyn správce. S tím poté souvisí posouzení, zda se ve vztahu k jednotlivým částem tohoto zpracování nacházela nebo nachází v pozici správce či zpracovatele. Teprve poté, dojdou-li kontrolující k závěru, že kontrolovaná je správcem, lze posoudit plnění povinností podle čl. 30 odst. 1 nařízení (EU) 2016/679, jelikož povinnosti vyplývající z tohoto odstavce jsou uloženy správci.

12. **Námitka** směřující proti kontrolnímu zjištění č. 12 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná, v pozici správce osobních údajů v oblasti cookies, v období od 6. září 2021 minimálně do dne vyhotovení dodatku protokolu o kontrole, porušuje čl. 30 odst. 1 nařízení (EU) 2016/679 tím, že k předmětnému zpracování nevede záznamy o činnostech zpracování, **se zamítá.**

V této souvislosti kontrolovaná uvedla, že vzhledem ke skutečnostem, že se jedná o cookies, které podle vyhodnocení rizik kontrolované nepředstavují riziko pro práva a svobody subjektů údajů a kontrolovaná nemá více než 250 zaměstnanců, není povinna vést záznamy o činnostech zpracování podle čl. 30 nařízení (EU) 2016/679.

K tomu uvádím, že podle čl. 30 odst. 5 nařízení (EU) 2016/679 se povinnost vést záznamy o činnostech zpracování nevztahuje na podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže prováděné zpracování pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů. Kontrolovaná sice podle svého vyjádření nemá více než 250

zaměstnanců, avšak jí prováděné zpracování není příležitostné. Údaje zpracovávané prostřednictvím cookies kontrolované jsou zpracovávány systematicky za kontrolovanou definovanými účely. Výjimku z povinnosti vést záznamy o činnostech zpracování tak nelze aplikovat.

13. **Námitka** směřující proti kontrolnímu zjištění č. 13 dodatku k protokolu o kontrole, kde je konstatováno, že kontrolovaná postupovala v souladu s ustanovením čl. 33 odst. 2 nařízení (EU) 2016/679 tím, že bez zbytečného odkladu (15. ledna 2021) oznámila správci porušení zabezpečení (databreach), **se zamítá.**

V této souvislosti kontrolovaná sdělila, že možné porušení zabezpečení osobních údajů oznámil Úřadu správce prostřednictvím zpracovatele dne 18. ledna 2021 na základě podnětu z médií. Dále kontrolovaná uvedla, že se nenacházela v postavení správce, který by se dopustil přestupku podle zákona č. 110/2019 Sb., o zpracování osobních údajů, naopak byl správci nápomocen při zajišťování souladu s povinnostmi podle čl. 32 až 36 nařízení (EU) 2016/679 a má za to, že dostál svých povinností.

K tomu uvádím, že zpracovatel, jakmile zjistí porušení zabezpečení osobních údajů, je povinen tuto skutečnost bez zbytečného odkladu ohlásit správci. Kontrolním zjištěním č. 13 dodatku k protokolu o kontrole je konstatováno, že kontrolovaná tuto svoji povinnost vyplývající z čl. 33 odst. 2 nařízení (EU) 2016/679 splnila. Z protokolu z ústního jednání a místního šetření čj. UOOU-00341/21-52 ze dne 25. srpna 2021 vyplývá, že kontrolovaná se o bezpečnostním incidentu dozvěděla z médií dne 15. ledna 2021 a hned ten den jej ohlásila zpracovateli, tj. NAKIT. Ten následně dne 18. ledna 2021 ve spolupráci s Ministerstvem zdravotnictví ohlásil porušení zabezpečení Úřadu. Uvedeným kontrolním zjištěním tak není konstatováno porušení povinnosti kontrolované.

V rámci podaných námitek kontrolovaná na několika místech uvedla, že ve dnech 25. a 26. srpna 2021 proběhlo u kontrolované místní šetření, o kterém nebyla s dostatečným předstihem informována (a to i s ohledem na termín dovolených) a neměla tak možnost zajistit přítomnost potřebných osob. Zároveň neměla dostatek času na přípravu všech podkladů vyžadovaných kontrolujícími, přičemž kontrolující neuložili kontrolované povinnost doložit další dokumenty a vycházeli tak pouze z dokumentů předaných v časové nouzi, což je dle kontrolované v rozporu se zásadou zákonnosti ve spojení se zásadou materiální pravdy. Dále kontrolované nebylo umožněno dle § 36 zákona č. 500/2004 Sb., správní řád, navrhovat důkazy a činit jiné návrhy, neboť dne 17. září 2021 žádala o prodloužení termínu kontroly, aby mohla prostudovat závěry soudního znalce (úřední záznam čj. UOOU-00341/21-65 ze dne 16. září 2021) a vyjádřit se k nim. Pokud by měla kontrolovaná možnost se k úřednímu záznamu vyjádřit, mělo by to vliv na směřování výsledku kontroly. Kontrolovaná se tedy domnívá, že jednáním kontrolujících byla podstatným způsobem poškozena na svých právech.

Kontrolní řád je lex specialis vůči správnímu řádu a správní řád se tak při kontrole nepoužije v celém rozsahu. V komentáři k § 10 kontrolního řádu (J. Jelínková, Kontrolní řád: Praktický komentář, ASPI, právní stav komentáře ke dni 3.1.2019) je uvedeno, že kontrolovaná osoba *„však např. nemá práva obdobná procesním právům účastníků správního řízení podle § 36 správního řádu, zejména právo vyjádřit se k podkladům před vydáním rozhodnutí (§ 36*

odst. 3), v případě kontroly tedy protokolu o kontrole, právo na to, aby se kontrolující v protokolu o kontrole vypořádal s případnými návrhy a námitkami kontrolované osoby a vyjádřeními ke kontrolním podkladům (analogie k § 68 odst. 2 správního řádu); třebaže to kontrolující v praxi leckdy do jisté míry do protokolu o kontrole uvádějí. Kontrola je mnohem jednostrannější proces než správní řízení.". Kontrolující jsou rovněž oprávněni provést místní šetření bez předchozího ohlášení kontrolované.

Z důvodové zprávy ke kontrolnímu řádu vyplývá, že pojem „kontrola" je obecně „definován tak, aby zahrnoval jakoukoli kontrolní činnost, jejímž předmětem je zkoumání skutečného stavu a jeho porovnání se stavem žádoucím, jenž je vymezen stanovením příslušných povinností". Kontrolujícím pak z § 9 písm. a) kontrolního řádu vyplývá povinnost zjistit (faktický) stav věci v rozsahu nezbytném pro dosažení účelu kontroly a v závislosti na povaze kontroly doložit kontrolní zjištění potřebnými podklady. Přestože kontrolovaná nemá veškerá práva podle správního řádu (a o právu podle § 36 správního řádu byla kontrolujícími nesprávně poučena), mají kontrolující postupovat v souladu se zásadou materiální pravdy tak, aby byl zjištěn stav věci, o němž nejsou důvodné pochybnosti. Současně má kontrolovaná možnost se ke kontrolním zjištěním uvedeným v protokolu o kontrole vyjádřit v rámci podaných námitek, přičemž je na kontrolované, aby svá tvrzení (např. o existenci pokynů) doložila.

Kontrolovaná dále namítá, že měl-li Úřad pochybnosti o fungování Centrálního rezervačního systému, měl své námitky uplatnit ještě před jeho spuštěním, neboť na základě jednání (které proběhlo dne 8. ledna 2021 v prostorách Armády České republiky) a Posouzení vlivu na ochranu osobních údajů předloženého dne 13. ledna 2021 Úřadu ke konzultaci, Úřad prokazatelně disponoval informacemi k posouzení jeho fungování. Na jednání dne 8. ledna 2021 však proběhla pouze neformální diskuse, kde bylo zdůrazněno, že Úřad je dozorový a nikoli schvalovací orgán, a že za zpracování osobních údajů primárně odpovídá správce. Dále bylo na tomto místě sděleno, že pokud Úřad obdrží oficiální žádost o konzultaci, pak ji posoudí. Dne 13. ledna 2021 (dva dny před spuštěním systému) byla Úřadu doručena žádost Ministerstva zdravotnictví, jejímž předmětem bylo poskytnutí konzultace ve smyslu čl. 36 odst. 1 a čl. 57 odst. 1 písm. c) nařízení (EU) 2016/679 ve věci Projekt: IT podpora OČKOVÁNÍ. Součástí této žádosti bylo posouzení vlivu na ochranu osobních údajů vypracované Ministerstvem zdravotnictví k dané oblasti. Úřad ve svém vyjádření ze dne 4. února 2021 čj. UOOU-00314/21-2 konstatoval, že žádost je neúplná a předložené informace nejsou pro danou konzultaci dostačující, přičemž předloženému posouzení vlivu vytkl řadu nedostatků. Kontrolovaná se tedy nemůže odvolávat na to, že předmětné zpracování bylo s Úřadem řádně konzultováno ještě před jeho započetím.

Mgr. Jiří Kaucký
předseda
(podepsáno elektronicky)