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-00341/21-46
Praha 1. června 2021

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], jako vedoucí kontrolní skupiny na základě pověření ke kontrole z 29. ledna 2021;

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

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

Mgr. Barbora Šnajderová, pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze dne 29. ledna 2021;
(dále jen „kontrolující“).

Kontrolovaná osoba:
[redacted], [redacted], [redacted], **:** [redacted] (dále jen „kontrolovaná osoba“).

Místo provedení kontroly: sídlo Úřadu

Předmět kontroly:
Předmětem kontroly je zpracování osobních údajů při provozování internetového portálu zaměřeného na rezervaci termínů očkování proti onemocnění COVID-19, zejména podle čl. 5-7, čl. 12-22, čl. 28-29, čl. 32-34 a čl. 44-49 nařízení (EU) 2016/679, a to jak v rozsahu podání, tak v oblasti dodržování nařízení (EU) 2016/679 s ohledem na databázi klientů kontrolované osoby.

První kontrolní úkon:
Doručení oznámení o zahájení kontroly kontrolované osobě dne 1. února 2021 (čj. UOOU-00341/21-13).

Poslední kontrolní úkon:
Vypracování úředního záznamu poskytovaných rezervačních systémů na stránkách kontrolované osoby (čj. UOOU-00341/21-45), dne 31. května 2021.

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. Podnět („Podnět k prošetření“) ze dne 15. ledna 2021 [redacted], počet listů 1;
2. Průvodní dopis – e-mail („Podnět k zahájení správního řízení“) ze dne 15. ledna 2021 [redacted], počet listů 1;
   2.1. Příloha – „Podnět k zahájení správního řízení“, počet listů 1;
3. Žádost o výmaz osobních údajů („[redacted] – [redacted], počet listů 1;
4. Stížnost ze dne 17. ledna 2021 [redacted], počet listů 1;
5. Podnět („Podání k prošetření“) ze dne 17. ledna 2021 [redacted], počet listů 1;
6. Stížnost ze dne 18. ledna 2021 [redacted], počet listů 1;
7. Stížnost („Stížnost na správce osobních údajů Ministerstvo zdravotnictví ČR podle článku 77, odst. 1“) ze dne 15. ledna 2021 [redacted], počet listů 3;
8. Odpověď společnosti [redacted], na žádost o výmaz osobních údajů [redacted] – [redacted] ze dne 18. ledna 2021 [redacted], počet listů 1;
9. Ohlášení porušení zabezpečení dle GDPR ze dne 18. ledna 2021 (čj. UOOU-00379/21-1), počet listů 1;
   9.1. Příloha – formulář Ohlášení porušení zabezpečení dle GDPR, počet listů 4;
10. Postoupení věci – „Bezpečnostní incident? Nezabezpečená osobní data při rezervaci“ na očkování ze dne 25. ledna 2021 (čj. UOOU-00341/21-10), počet listů 1;
    10.1. Příloha – podnět (*„bezpečnostní incident?“)* ze dne 20. ledna 2021, počet listů 1;
11. Úřední záznam ze dne 29. ledna 2021 (čj. UOOU-00341/21-11), počet listů 1;
    11.1. Příloha – Cookie scan record ze dne 26. ledna 2021, počet listů 2;
    11.2. Příloha – odkazy na objednávku očkování ze dne 27. ledna 2021, počet listů 2;

12. Pověření ke kontrole ze dne 29. ledna 2021 (čj. UOOU-00341/21-12), počet listů 1;
13. Oznámení o zahájení kontroly ze dne 29. ledna 2021 (čj. UOOU-00341/21-13), doručené kontrolované osobě dne 1. února 2021, počet listů 2;
14. Žádost o vyjádření ze dne 1. února 2021 (čj. UOOU-00341/21-14), počet listů 2;
15. Stížnost [„Podání stížnosti subjektu údajů v souladu s článkem 77 Nařízení EP a Rady č. 2016/679 (dále jen GDPR)“] ze dne 17. ledna 2021 (čj. UOOU-00341/21-15), počet listů 1;
16. Doplnění podnětu („Re: Úřad pro ochranu osobních údajů“) ze dne 10. února 2021 (čj. UOOU-00341/21-21), počet listů 1;
    16.1. Příloha – odpověď společnosti  (výmaz údajů) ze dne 18. ledna 2021, počet listů 1;
17. Odpověď Ministerstva zdravotnictví ČR ze dne 10. února 2021 (čj. UOOU-00341/21-22), počet listů 7;
    17.1. Příloha – Posouzení vlivu na ochranu osobních údajů ze dne 10. února 2021, počet listů 12;
    17.2. Příloha – Záznam o činnostech zpracování (2/2021), počet listů 5;
18. Odpověď ze dne 10. února 2021 na Oznámení o zahájení kontroly ze dne 29. ledna 2021 (čj. UOOU-00341/21-23), počet listů 3;
19. Doplnění stížnosti *(„Re: Úřad pro ochranu osobních údajů“)* ze dne 15. února 2021 (čj. UOOU-00341/21-25), počet listů 2;
    19.1. Příloha - Odpověď na „Stížnost na správce osobních údajů Ministerstvo zdravotnictví ČR podle článku 77, odst. 1“ ze dne 11. února 2021, počet listů 1;
    19.2. Příloha - Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ, počet listů 4;
20. Úřední záznam – analýza zpracovatelských smluv, rozbor doložených dokladů a analýza cookies týkajících se provozu rezervačního systému na očkování proti onemocnění COVID-19 ze dne 19. února 2021 (čj. UOOU-00341/21-26), počet listů 4;
    20.1. Příloha – Smlouva o poskytování softwarových, odborných a mobilních služeb - chytrá karanténa 2.0, počet listů 13;
    20.2. Příloha – Příloha č. 1 – Specifikace služby systému, Příloha č. 2 – Specifikace rolí, Příloha č. 3 – Akceptační protokol, Příloha č. 4 – SLA Služby systému, Příloha č. 5 – Bezpečnostní požadavky, počet listů 18;
    20.3. Příloha – Smlouva o poskytování softwarových a odborných služeb ze dne 8. října 2020, počet listů 16;
    20.4. Příloha – Dodatek č. 1 ke smlouvě o poskytování softwarových a odborných služeb, počet listů 2;
    20.5. Příloha – snímek obrazovky www.mzcr.cz/ochrana-osobnich-udaju/, počet listů 1;
    20.6. Příloha – Základní informace o zpracování osobních údajů Ministerstvem zdravotnictví, počet listů 2;
    20.7. Příloha – Centrální rezervační systém – Očkování proti COVID-19 registrace do systému ze dne 16. února 2021, počet listů 2;
    20.8. Příloha – Informace o zpracování osobních údajů v rámci Projektu: IT podpora očkování, počet listů 4;
    20.9. Příloha – Cookie scan report ze dne 16. února 2021, počet listů 2;
    20.10. Příloha – Zásady zpracování osobních údajů ze dne 16. února 2021, počet listů 8;

20.11. Příloha – snímek obrazovky [redacted], počet listů 1;

21. Výzva k doplnění podkladů ze dne 26. února 2021 (čj. UOOU-00341/21-27), počet listů 1;
22. Podnět („Formulář na očkování a Facebook“) ze dne 1. března 2021 (čj. UOOU-00341/21-30), počet listů 1;
23. Zpracovatelská smlouva č. [redacted] ze dne 25. srpna 2018 (čj. UOOU-00341/21-31), počet listů 5;
    23.1. Příloha – Odpověď ze dne 4. března 2021 k Výzvě k doplnění podkladů ze dne 26. února 2021, počet listů 2;
    23.2. Příloha – Smlouva o poskytování služeb pronájmu a připojení serveru [redacted] ze dne 13. března 2019, počet listů 3.
24. Úřední záznam ze dne 27. dubna 2021 (čj. UOOU-00341/21-32), analýza zpracovatelské smlouvy „Smlouva o poskytování softwarových a odborných služeb“ uzavřené mezi NAKIT a kontrolovanou osobou, vč. jejích následných dodatků a příloh, počet listů 4;
    24.1. Příloha – Smlouva o poskytování softwarových a odborných služeb ze dne 8. října 2020, vč. Přílohy č. 1 Specifikace Předmětu plnění, Přílohy č. 2 Specifikace podpory Služby a sankce za nedodržení SLA, Přílohy č. 3 Specifikace rolí a ceník jednotkových cen rolí, Přílohy č. 4 Vzor akceptační protokol a výkazu, Příloha 5 Bezpečnostní požadavky, počet listů 32;
    24.2. Příloha – Dodatek č. 1 ke smlouvě o poskytování softwarových a odborných služeb, počet listů 3;
    24.3. Příloha – Dodatek č. 2 ke smlouvě o poskytování softwarových a odborných služeb, počet listů 11;
    24.4. Příloha – PrtScr rozboru smlouvy, počet listů 17;
25. Úřední záznam ze dne 28. dubna 2021 (čj. UOOU-00341/21-33), analýza zpracovatelské smlouvy „Smlouva o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“, počet listů 5;
    25.1. Příloha – PrtScr rozboru smlouvy, počet listů 9;
    25.2. Příloha – Příloha smlouvy č. 1 až 5 smlouvy, počet listů 36;
    25.3. Příloha – Smlouva o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“, počet listů 26;
    25.4. Příloha – Dodatek č. 3 ke Smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0, počet listů 51;
    25.5. Příloha – Dodatek č. 1 ke Smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0, počet listů 41;
        25.5.1. Podpříloha č. 3 a 4 Dodatku č. 1 ke Smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0, počet listů 8;
    25.6. Příloha – Dodatek č. 2 ke Smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0, počet listů 9;
26. Doplnění stížnosti ze dne 3. května 2021 (čj. UOOU-00341/21-41), počet listů 1.
27. Úřední záznam ze dne 18. května 2021 (čj. UOOU-00341/21-42), analýza informační povinnosti a její plnění kontrolovanou osobou, počet listů 21;
    27.1. Příloha 1 – printscreen https://www.mzcr.cz/ochrana-osobnich-udaju/, počet listů 1;
    27.2. Příloha 2 - Dokument s názvem Základní informace o zpracování osobních údajů Ministerstvem zdravotnictví. Informace je uveřejňována pro plnění povinnosti stanovené v článcích 12 až 14 Obecného nařízení o ochraně osobních údajů č. 2016/679 ze dne 27. dubna 2016 (dále jen „nařízení“). Tato informace může

být doplňována a upřesňována bližšími informacemi zveřejněnými nebo poskytnutými ke specifickým zpracováním, počet listů, počet listů 2;

27.3. Příloha 3 - printscreen , počet listů 1;
27.4. Příloha 4 - printscreen , počet listů 1;
27.5. Příloha 5 - printscreen , počet listů 1;
27.6. Příloha 6 - printscreen , počet listů 1;
27.7. Příloha 7 - printscreen , počet listů 1;
27.8. Příloha 8 – Dokument s názvem „*Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ“*, počet listů 3;
27.9. Příloha 9 - printscreen - rezervační systém, počet listů 1;
27.10. Příloha 10 - printscreen GDPR | , počet listů 1;
27.11. Příloha 11 - printscreen GDPR | , počet listů 1;
27.12. Příloha 12 - printscreen GDPR | , počet listů 1;
27.13. Příloha 13 - printscreen GDPR | , počet listů 1;
27.14. Příloha 14 - printscreen GDPR | , počet listů 1;
27.15. Příloha 15 - printscreen GDPR | , počet listů 1;
27.16. Příloha 16 - printscreen GDPR | , počet listů 1;
27.17. Příloha 17 - printscreen GDPR | , počet listů 1;
27.18. Příloha 18 - printscreen GDPR | , počet listů 1;
27.19. Příloha 19 - printscreen GDPR | , počet listů 1;
27.20. Příloha 20 - printscreen GDPR | , počet listů 1;
27.21. Příloha 21 - printscreen GDPR | , počet listů 1.

28. Úřední záznam ze dne 24. května 2021 (čj. UOOU-000341/21-43) Analýza cookies na stránkách , počet listů 4;
28.1. Příloha 1 – Cookiebot ze dne 18. května 2021, počet listů 3;
28.2. Příloha 2 – , počet listů 1;
28.3. Příloha 3 – , počet listů 1;
28.4. Příloha 4 – Nová rezervace – výstup, počet listů 1;
28.5. Příloha 5 – – předání, počet listů 1;
28.6. Příloha 6 – – předání, počet listů 1;
28.7. Příloha 7 – – předání, počet listů 1;
28.8. Příloha 8 – , počet listů 1;
28.9. Příloha 9 – , počet listů 1;
28.10. Příloha 10 – , počet listů 1.

29. Úřední záznam webových stránek kontrolované osoby – kontrola rezervačních systémů provozovaných kontrolovanou osobou (čj. UOOU-00341/21-45), počet listů 43;
29.1. Příloha – GDPR , počet listů 15.

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 ve dnech 19. ledna až 1. března 2021 obdržel celkem 10 stížností a podnětů týkajících se podezření na porušení právních předpisů na ochranu osobních údajů při zpracování osobních údajů v rámci on-line systému registrace na očkování proti nemoci COVD-19 (Centrální rezervační systém pro očkování proti COVID-19), (viz k tomu body 1., 2., 3., 4., 5., 6., 7., 8., 10., 15., 16.,19., 22. a 26 přehledu podkladů).

Podání č. 1 z 18. ledna 2021 (viz body 3, 8 a 16 přehledu podkladů)

Stěžovatel doložil e-mailovou zprávu, ze které je patrné, že dne 17. ledna 2021 z e-mailu [redacted] zaslal zprávu na e-mailovou adresu [redacted] kontrolované osoby, kdy žádal o okamžité vymazání svých osobních údajů v rámci registrace na rezervačním portálu kontrolované osoby a uvedl, že odebírá svůj souhlas s nakládáním s jeho osobními údaji.

Podání č. 2 z 18. ledna 2021 (viz bod 6 přehledu podkladů)

Stěžovatel zde uvádí, že po registraci rodičů zjistil (z veřejně dostupných webových stránek), že jsou údaje registrovaných vč. jejich rodných čísel sdíleny s Googlem, a to prostřednictvím URL adresy obsahující toto rodné číslo. Dále zde uvádí podezření, že kontrolovaná osoba má rovněž přístup k datům z URL adres.

Podání č. 3 z 18. ledna 2021 (viz bod 10 přehledu podkladů)

Stížnost postoupena z Ministerstva vnitra, jako příslušnému úřadu. Stěžovatel zde uvádí, že při zadání odkazu [redacted], se mu otevřely odkazy jednotlivých nemocnic.

Podání č. 4 z 17. ledna 2021 (viz bod 15 přehledu podkladů)

Stěžovatel uvádí, že při registraci očkování byla stránkami [redacted] přesměrována na stránky kontrolované osoby, přičemž ihned po přesměrování byly ukládány reklamní skripty Facebooku a Googlu a odesílány osobní údaje vč. rodného čísla.

Podání č. 5 z 15. ledna 2021 (viz body 7, 19 a 26 přehledu podkladů)

Stěžovatel v podání a jeho doplnění uvedl, že ze stránek kontrolované osoby vyplývá, že URL včetně rodných čísel byla zasílána do Google Analytics a přestože na stránce o cookies je nasáno, že se člověka nesnaží identifikovat, vyplňuje se rodné číslo, telefon a další položky.

Podání č. 6 z 15. ledna 2021 viz bod 2 přehled podkladů)

Podatel pod názvem „*Podnět k zahájení správního řízení*“ ve svém podání uvádí, že byl 15. ledna 2021 Ministerstvem zdravotnictví spuštěn registrační portál pro očkování proti nemoci COVID-19, přičemž ve druhé fázi je využíváno serveru kontrolované osoby. Uvádí, že v průběhu registrace na očkování bylo na serveru kontrolované osoby rodné číslo přímou součástí veřejné URL adresy. Součástí tohoto podání je PrtScr. obrazovky při registraci, ze které je patrné, že zadávané číslo pojištěnce (rodné číslo fyzické osoby) se při zadávání do kolonky pro vyplňování zároveň přepisuje do URL adresy.

Podání č. 7 ze 17. ledna 2021 (viz bod 4 přehledu podkladů)

Podnět k prošetření možného spáchání přestupku, kdy MZ na doménách registrace.mzce.cz a crs.uzis.cz určenou k registraci očkování proti nemoci COVID-19 umístilo sledovací skripty služeb Facebook, Google Analytics a Seznam.cz.

Podání č. 8 ze 17. ledna 2021 (viz bod 5 přehledu podkladů)

Podatel ve svém e-mailu zaslal několik odkazů týkajících se reservačního systému, kdy v těchto odkazech jsou uvedeny informace o zasílání dat reklamním gigantům, a to rodných čísel (čísel pojištěnců).

Podání č. 9 z 1. března 2021 (viz bod 22 přehledu podkladů)

Podatel žádá o sdělení, s jakým závěrem byl prověřen web [redacted], který dle stěžovatele obsahuje Jawascripty Facebook.

Podání č. 10 z 15. ledna 2021 (viz bod 1 přehledu podkladů)
V podání je uvedeno, že: *„Centrální rezervační systém pro objednávání na antigenní testování posílá část informací o uživatelích také reklamním společnostem. Zjistil to web iRozhlas. Stejná firma bude dodávat i objednávkový registr pro očkování proti koronaviru.“* Součástí podání je odkaz:

V rámci tohoto článku je upozorněno na *„systémy třetích stran“.*

Podání se tedy týkala podezření na neoprávněné předávání osobních údajů třetím stranám (kdy tato podezření vyplývala ze samotného názoru stěžovatelů a podatelů, ale i na základě informací z veřejných v médií), na nedostatečné zabezpečení osobních údajů a neplnění práv subjektů údajů.

Z podnětů a vlastní činností kontrolující zjistili, že odborná zařízení (nemocnice), která poskytují očkování, na svých vlastních webových stránkách nabízejí rezervační systém očkování proti nemoci COVID-19, přičemž návštěvou webových stránek nemocnic a následným kliknutím na odkaz pro rezervaci je klient přesměrován na stránky kontrolované osoby (viz příloha č. 11.2 bodu 11. přehledu podkladů). Zpracování osobních údajů v rámci rezervačního systému očkování tak probíhá prostřednictvím webových stránek kontrolované osoby.

Porušení zabezpečení ohlášené úřadu
Úřad 20. ledna 2021 obdržel rovněž ohlášení porušení zabezpečení ochrany osobních údajů od Ministerstva zdravotnictví České republiky, se sídlem Palackého náměstí 375/4, 128 01 Praha 2 (dále jen „MZ“ nebo také „Ministerstvo zdravotnictví“) a Národní agentury pro komunikační a informační technologie, s.p., se sídlem Kodaňská 1441/46, 101 00 Praha 10 - Vršovice (dále jen „NAKIT“), ve kterém je uvedeno, že došlo k chybě ve funkcionalitě systému webových stránek kontrolované osoby, která umožnila zobrazení čísla pojištěnce a jeho následný přenos do systému Google Analytics (dalšího zpracovatele) a sdílení se společností Google (dále jen „Google“), a to, jak je uvedeno v ohlášení, *„za účelem zlepšování služeb*“ (viz k tomu bod 9. přehledu podkladů). Oznamovatelé v ohlášení o porušení zabezpečení dále uvedli, že v rámci přijatých opatření došlo k odstranění vadné funkcionality zobrazení čísla pojištěnce, zastavení sdílení dat se společností Google pro účely zlepšování služeb a byl zajištěn výmaz dat ze serverů Google Analytics, kdy byla veškerá přenesená data smazána. Oznamovatelé dále uvedli, že se jednalo přibližně o 80 tisíc čísel (přičemž číslo pojištěnce je rodné číslo fyzické osoby) a danou situaci vyhodnotili tak, že se jedná o mírné riziko a z tohoto důvodu nepřistoupili k oznámení o porušení zabezpečení subjektům údajů.

Předkontrolní zjištění o webových stránkách 
Pro ověření situace kontrolující provedli kontrolu funkčních cookies kontrolované osoby na webových stránkách  a formou úředního záznamu jej 29. ledna 2021 vložili do spisu (viz bod 11 přehledu podkladů, příloha 11.1.). Zjištěno bylo, že ke dni 26. ledna 2021 jsou nadále v rámci registrace užívány cookies, které sbírají data o klientech a užívají je mimo jiné i k cílení reklamy, že tyto cookies spravuje Google a dochází nadále k přenosu dat do USA, jak je popsáno níže.
Z výše uvedeného prověření vyplynulo podezření, že kontrolovaná osoba o přenosu dat neinformovala, kdy na jejích webových stránkách nebyla plněna ani povinnost informovat

o zpracování osobních údajů, které probíhá v rámci tohoto systému. Klienti neměli možnost ovlivnit přenos vlastních dat, jelikož webové stránky a užitý systém neumožňoval nesouhlasit s tímto přenosem a ke zpracování osobních údajů docházelo automaticky již návštěvou uvedených stránek.

Na základě výše uvedených faktů Úřad 1. února 2021 zahájil kontrolu u kontrolované osoby doručením oznámení o zahájení kontroly (viz bod 13 přehledu podkladů).

Průběh kontroly:
Na počátku kontroly, 1. února 2021, kontrolující požádali o vyjádření Ministerstvo zdravotnictví (viz bod 14 přehledu podkladů). Na základě odpovědí a dokumentů doložených ve vyjádření Ministerstva zdravotnictví, doručených 11. února 2021 (viz bod 17 přehledu podkladů, vč. příloh 17.1 a 17.2) a odpovědí a podkladů kontrolované osoby doručených 12. února 2021 (viz bod 18 přehledu podkladů), byl 19. února 2021 proveden rozbor zpracovatelských smluv, cookies týkajících se provozu rezervačního portálu a dalších doložených podkladů (viz bod 20 přehledu podkladů vč. příloh č. 20.1 až 20.11). Dne 26. února 2021 byla kontrolovaná osoba vyzvána k doplnění neúplných podkladů (viz bod 21 přehledu podkladů. Odpověď kontrolované osoby byla doručena 4. března 2021 (viz bod 23 přehledu podkladů vč. příloha 23.1 a 23.2).

Z dodaných materiálů a navazující vlastní činností kontrolujících bylo zjištěno že:

III. Kontrolní zjištění:
Z důvodu krizového vývoje epidemiologické situace na území České republiky spojené s výskytem koronaviru SARS-CoV-2, který vyvolává onemocnění COVID-19, bylo rozhodnuto o plošném dobrovolném očkování obyvatelstva České republiky proti COVID-19, resp. zabránění šíření tohoto infekčního a hromadně se vyskytujícího onemocnění. Z tohoto důvodu MZ vypracovalo projekt: *IT podpora očkování,* který vychází z dokumentu *„Strategie očkování proti covid-19 v České republice“* (vzata na vědomí vládou 7. prosince 2020 s aktualizací 22. prosince 2020). Projekt byl vypracován v návaznosti na implementaci zákona č. 569/2020 Sb., o distribuci léčivých přípravků obsahujících očkovací látku pro očkování proti onemocnění COIVID-19, o náhradě újmy způsobené očkovaným osobám těmito léčivými přípravky a o změně zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů a dále v návaznosti na zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

Projekt se sestává ze tří bloků:

1. centrální rezervační systém, který svými komponentami plní role registrace a rezervace,
2. ISIN/vakcinační modul OČKO, který svými komponentami plní role evidence provedeného očkování a vystavení certifikátu o provedeném očkování a
3. aplikace a systémy podporující řídící a logistické procesy, jedná o systémy a aplikace projektu Chytrá karanténa.

Pro danou oblast kontroly je relevantní blok č. 1, kdy kontrolovaná osoba svými činnostmi zabezpečuje plnění rolí registračních a rezervačních činností, přičemž jak je popsáno níže, tuto

činnost prováděla jako správce osobních údajů a to do 25. března 2021 a dále jako zpracovatel (další zpracovatel) osobních údajů od data 26. března 2021.

V rámci těchto činností (v obou obdobích) kontrolovaná osoba vykonávala a dosud vykonává elektronické rezervace termínu očkování pro plátce pojištění v ČR, plánování prvních a druhých termínů očkování, správu a administraci rezervací a kapacitní plánování očkování vč. navazující technické podpory pro tyto činnosti a její činnost tak přímo navazuje na další činnosti veřejných subjektů.

O kontrolované osobě:
Kontrolovaná osoba, obchodní společnost [redacted].
Společnost je vedena pod spisovou značkou [redacted] u [redacted].

Předmětem podnikání je

- výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona a
- vývoj a poskytování práva užití počítačových programů (software) pro objednávání klientů a poskytování služeb s tím souvisejících.

Společnost má dle výpisu z obchodního rejstříku v současnosti dva jednatele (ti jsou současně jedinými společníky), kteří za společnost jednají společně.

Kontrolovaná osoba ve své *Odpovědi na Oznámení o zahájení kontroly ze dne 29. ledna 2021* (viz bod 18 přehledu podkladů), která byla doručena dne 10. února 2021 sdělila, že se nachází v postavení dalšího zpracovatele osobních údajů, a to pro správce Ministerstvo zdravotnictví, prostřednictvím zpracovatele, kterým je NAKIT. K bližšímu zaslala odkaz (bod 2 písm. b. odpovědi) na smlouvu zveřejněnou v Registru smluv na webových stránkách [redacted].

Identickou informaci zaslalo rovněž Ministerstvo zdravotnictví ve své odpovědi ze dne 10. února 2021 (viz bod 17 přehledu podkladů vč. příloh č. 17.1 a 17.2). V ní potvrdilo řetězení zpracovatelů, tedy že se NAKIT nachází v postavení zpracovatele a kontrolovaná osoba je v postavení dalšího zpracovatele pro MZ, v pozici správce. V bodu 6) této odpovědi vložilo odkazy na předmětné smlouvy, a to zpracovatelskou smlouvu uzavřenou mezi MZ a NAKIT: [redacted] a navazující zpracovatelskou smlouvu zavřenou mezi NAKIT a kontrolovanou osobou: [redacted].

Pro kontrolu tvrzeného postavení kontrolované osoby kontrolující provedli 19. února 2021 rozbor zpracovatelských smluv týkajících se provozu rezervačního systému na očkování proti onemocnění COVID-19 a tento rozbor byl vložen do spisu kontroly (viz bod 20 a přílohy 20.1 až 20.8 sezamu podkladů).

Pod č. smlouvy 13430376 (odkaz https://smlouvy.gov.cz/smlouva/13430376) se nachází Smlouva o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“, uzavřená mezi NAKIT a Ministerstvem zdravotnictví, kdy podle čl. 4.1 je účinnost smlouvy stanovena na den zveřejnění v registru smluv, kterým je 31. červenec 2020. V článku 1 odst. 2 smlouvy je specifikován předmět zpracování, sestávající ze:

a) zpřístupnění a poskytování nástrojů služby Chytrá karanténa, jejichž specifikace je uvedena v příloze č. 1 této Smlouvy, včetně oprávnění užít tyto nástroje a s nimi

související služby dle podmínek uvedených v této Smlouvě a jejích přílohách, přičemž se jedná o následující nástroje a služby:

- webové aplikace pro vizualizaci dat o průběhu pandemie COVID-19 v České republice i ve vybraných státech světa (EPI Dashboard), blíže specifikované v části A přílohy č. 1,
- komunikační nástroje kontaktního centra, blíže specifikované v části B přílohy č. 1,
- vzpomínkové mapy sloužící k vizualizaci a k analýze dat nad mapovým podkladem, vč. nástrojů pro datovou integraci, blíže specifikované v části C přílohy č. 1,
- mobilní aplikace pro chytré telefony trasující kontakty, s nimiž v poslední době nakažení přišli do styku a u nichž je vysoké riziko nákazy (eRouška) blíže specifikované v části D přílohy č. 1,
- integrace mobilní aplikace Mapy.cz (Mapy.cz) trasující pohyby nakažených, blíže specifikované v části E přílohy č. 1,
- služby pro správu a rozvoj modelu enterprise architektury (EA) systému Chytrá karanténa 2.0 a systému správy grafových dat (objektové databáze), včetně podpory řízení katalogu požadavků na různé komponenty systému a jejich funkce, blíže specifikované v části F přílohy č.1,
- COVID mobilní info karta sloužící k informování veřejnosti o stavu epidemie a k propagaci mobilní aplikace eRouška, blíže specifikované v části G přílohy č.1, (vše dohromady dále jako „Služba Systému" nebo samostatně jako „Aplikace"),

b) poskytování odborných služeb na základě požadavku Objednatele, souvisejících zejména se Službou Systému a/nebo jednotlivých Aplikací zahrnující i jejich rozvoj, a s účelem této Smlouvy, prostřednictvím rolí uvedených v příloze č. 2 této Smlouvy (dále jen „Odborné služby"),

c) odchozích telefonních hovorů z kontaktního centra a odchozích SMS z kontaktního centra (dále jen „Mobilní služby"), specifikovaných v příloze č. 1 Smlouvy,

d) provedení nezávislého posouzení Chytré karantény 2.0, jehož předmětem je:

- nákres a popis datových toků, a to v rozsahu nezbytném pro posouzení dostatečnosti personálního zabezpečení. Popis bude obsahovat seznam a obsah datových toků, jejich frekvence a formu předávání,
- provedení testování vzorku obsahu dat, zda odpovídá popisu a formě předání,
- popis účelu dat a návazných procesů a vyhodnocení jejich kritičnosti,
- analýza procesního řízení v oblasti zpracování osobních údajů s cílem identifikovat odchylky od požadavků regulace GDPR a vypracování přehledu nesouladů včetně jejich prioritizace.

Kontrolující tak konstatovali, že předmět kontroly, tj. provozování internetového portálu zaměřeného na rezervaci termínů očkování proti onemocnění COVID-19 nelze jednoznačně zařadit k žádnému z uvedených bodů.

Kontrolou dalšího odkazu a v něm umístěné smlouvy č. [redacted] (odkaz [redacted]) bylo zjištěno, že se zde nachází Smlouva o poskytování softwarových a odborných služeb uzavřená mezi NAKIT a kontrolovanou osobou, ze dne 8. října 2020 (datum určeno dle digitálního podpisu na dokumentu a zároveň datum zveřejnění v registru smluv).

Jako předmět smlouvy v čl. 1 je zde uvedeno:

a) zpřístupnění a poskytování služby rezervační komponenty portálu centrálního rezervačního systému pro 150 odběrných míst COVID-19, který obsahuje funkce elektronické rezervace termínu odběru testů COVID-19 indikovaných pacientů a samoplátců, kapacitní reporty rezervací, uživatelské funkce předvyplnění rezervace z aplikace eŽádanka (indikovaní) a založení rezervace z aplikace eŽádanka pro samoplátce v rámci projektu Chytrá karanténa 2.0 jehož specifikace je uvedena v příloze č. 1 smlouvy, včetně oprávnění užít tento nástroj dle podmínek uvedených ve smlouvě a v jejich přílohách a včetně podpory výrobce (Služba, která sestává ze souvisejících služeb, ze standardizovaného software a z personalizace jádra služby prostřednictvím implementačních, integračních, customizačních, konfiguračních a konzultačních prací, kdy podpora poskytovatele služby je uvedena v příloze č. 2 smlouvy),
b) poskytování odborných služeb souvisejících zejména se službou zahrnující i jejich rozvoj a s účelem smlouvy, prostřednictvím rolí uvedených v příloze č. 3 smlouvy,
c) poskytnutí oprávnění k výkonu dílo užít za podmínek sjednaných smlouvou vč. dodání veškeré související dokumentace a komentovaných zdrojových kódů za podmínek sjednaných smlouvou.

K tomu kontrolující konstatují, že smlouva se netýká rezervačního systému na očkování (tedy předmětu kontroly), nýbrž rezervačního systému na testování. Tento závěr potvrzuje rovněž výčet zpracovávaných osobních údajů v propojení se subjektem údajů, kterým může být samoplátce, potencionálně nakažený či nakažený.

Kompletní rozbor smluv vč. jejich příloh je vložen do spisu (viz bod 20 přehledu podkladů).

Vzhledem k absenci návaznosti smluv k předmětu kontroly byla kontrolovaná osoba přípisem ze dne 26. února 2021 vyzvána k doložení podkladů, a to možných navazujících smluv či jejich dodatků ve smyslu řetězení zpracovatelů (viz bod 21 přehledu podkladů), popř. k rozšíření účelů uvedených ve smlouvách.

Dne 4. března 2021 byla kontrolovanou osobou zaslána odpověď (viz bod 23 přehledu podkladů vč. příloh 23.1 a 23.2). V uvedeném dokumentu jsou vloženy odkazy, týkající se

- Smlouvy uzavřené mezi Ministerstvem zdravotnictví a NAKIT: https://smlouvy.gov.cz/smlouva/13430376,
- Dodatku č. 1 smlouvy: https://smlouvy.gov.cz/smlouva/14075272 a
- Dodatku č. 2 smlouvy: https://smlouvy.gov.cz/smlouva/14934078.

V návaznosti na to provedli kontrolující novou analýzu zpracovatelských smluv.

Úřední záznam analýzy zpracovatelské smlouvy „Smlouva o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“ uzavřené mezi MZ a NAKIT byl vypracován a vložen do spisu kontroly dne 28. dubna 2021 (viz bod 25 přehledu podkladů, vč. příloh 25.1 až 25.6). K dané smlouvě byly kontrolovanou poskytnuty výše uvedené odkazy.

První z odkazů (*https://smlouvy.gov.cz/smlouva/13430376*) vedl k otevření smlouvy v portálu smlouvy.gov.cz, ze kterého je patrné, že smlouva byla vložena 31. července 2020 a v části „Soubory“ se nacházely dvě přílohy smlouvy:

Prvním ze souborů, vloženým pod názvem *„Přílohy.pdf“,* je soubor skládající se z příloh č. 1 až 5:

- Příloha č. 1 – *Specifikace Služby Systému* je rozdělena do částí:
  - A EPI Dashboard[1]
  - B Komunikační nástroj kontaktního centra
  - C Vzpomínkové mapy a datové integrace
  - D eRouška
  - E Integrace Mapy.cz
  - F Nástroje EA[2]
  - G COVID mobilní info karta[3]
  - H Mobilní služby, kdy u modulů A až G jsou dále pododstavce:
    - ✓ 1 Funkcionalita
    - ✓ 2 Uživatelé
    - ✓ 3 Architektura rozhraní
    - ✓ 4 Zpracování osobních údajů
    - ✓ 5 Rozsah provozních služeb
- Příloha č. 2 – *Specifikace Rolí* s dělením do částí:
  - A Role zajištěné interními zdroji NAKIT
  - B role zajištěné subdodavateli
    - ✓ B.1 Specifikace rolí Keboola
    - ✓ B.2 Specifikace rolí Daktela
    - ✓ B.3 Specifikace rolí Intelligent Technologies
  - C Popis rolí
    - ✓ C.1 Role zajištěné interními zdroji NAKIT
    - ✓ C.2 Role zajištěné externími zdroji
- Příloha č. 3 – *Akceptační protokol*
- Příloha č. 4 – *SLA Služby systému* s rozdělením do částí:
  - A EPI Dashboard
  - B Komunikační nástroj kontaktního centra
  - C Vzpomínkové mapy a datové integrace
  - **Chybějící str. 4 - chybí popis D**
  - E Integrace Mapy.cz
  - F Nástroje EA
  - G COVID mobilní info karta
- Příloha č. 5 – *Bezpečnostní požadavky*

Druhým ze souborů je dokument pod názvem *„ISRS 1005-20.pdf“,* kde je uložen text celé hlavní smlouvy (*Smlouva o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2,0*). Tato smlouva byla již předmětem zkoumání, viz výše (viz bod 20 přehledu podkladů) se závěrem, že provozování internetového portálu zaměřeného na rezervaci termínů očkování proti onemocnění COVID-19 nelze jednoznačně zařadit k žádnému z předmětů zpracování, uvedeném v čl. 1 odst. 2 smlouvy. Výčet zpracovávaných osobních údajů je sice konkretizován v příloze č. 1 smlouvy, nicméně k předmětu kontroly žádné

[1] Aplikace EPI Dashboard je webová aplikace pro analýzu dat a sdílení informací na jednom místě v reálném čase.
[2] Aplikace pro správu modelu enterprise architektury (EA) celého řešení Chytré karantény 2.0 a systému správy grafových dat, včetně podpory řízení katalogu požadavků na různé komponenty systému a jejich funkce
[3] Aplikace pro operační systémy Android a iOS

konkrétní uvedené nejsou. Povaha a účel zpracování jsou stanoveny v čl. 3 odst. 13 a v příloze č. 1, avšak ve vztahu k předmětu kontroly se v této smlouvě nenachází žádné stanovení účelu tomu odpovídající.

Dodatek č. 1 Smlouvy o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0:
Dodatek č. 1 nebyl vložen do portálu www.smlouvy.gov jako návazná smlouva k hlavní smlouvě. Na základě žádosti o doložení navazujících dodatků smluv, které nebyly vloženy jako smlouvy návazné k hlavní smlouvě, byly dne 4. března 2021 kontrolovanou osobou zaslány odkazy na Dodatek č. 1 a Dodatek č. 2 hlavní smlouvy.
Odkazem https://smlouvy.gov.cz/smlouva/14075272 se otevřela stránka, kde v části *„Soubory"* byly nalezeny dva soubory.
V souboru pod názvem *„ISRS 1207-20.pdf"* se nachází *„Dodatek č. 1. ke smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0"* ze dne 8. října 2020, (viz bod 25, příloha 25.1. přehledu podkladů).
Další přílohou je dokument s názvem *„přílohy 3 a 4.pdf"*, které byly do systému smlouvy.gov.cz vloženy dne 9. října 2020.

Předmětem Dodatku č. 1 je rozšíření předmětu plnění o další služby (IT služby, call centrum, propagační video).

Dodatek č. 2 Smlouvy o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0:
Dodatek č. 2 také nebyl vložen do portálu www.smlouvy.gov jako návazná smlouva k hlavní smlouvě. Na základě žádosti o doložení navazujících dodatků smluv, které nebyly vloženy jako smlouvy návazné k hlavní smlouvě, byly dne 4. března 2021 kontrolovanou osobou zaslány odkazy na Dodatek č. 1 a Dodatek č. 2 hlavní smlouvy.
Odkazem https://smlouvy.gov.cz/smlouva/14934078 se otevřela stránka, kde v části *„Soubory"* byly nalezeny tři soubory.
V souboru pod názvem *„1479-20.pdf"* se nachází *„Dodatek č. 2. ke smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0"* ze dne 16. prosince 2020, (viz bod 25 příloha 25.6. přehledu podkladů.

Dalšími soubory téhož zápisu je dokument *„P1_MZDR_NAKIT-dodatek2.pdf"* ze dne 17. prosince 2020, vel. 157.12 kB (viz příloha 6.1.) a *„P2_MZDR_NAKIT_dodatek_2.pdf"* ze dne 17. prosince 2020, vel. 164.61 kB, (viz příloha 6.2.).

Předmětem Dodatku č. 2 je: rozšíření Předmětu plnění, navýšení uživatelů aplikace „komunikační nástroj kontaktního centra", prodloužení účinnosti smlouvy do 31. prosince 2012 (konkrétně se jednalo o vložení textu *„zprostředkování a doručení na odběrné místo k provádění odběrů pro následné vyhodnocení testu na virus SARS – CoV-2, tj. odběr vzorků ze stěru sliznice nosohltanu, dále jen „COVID testy").*

Jak je uvedeno výše, ani jedním z uvedených dodatků, na které kontrolovaná osoba zaslala odkaz, neobsahoval rozšíření předmětu plnění o provozování internetového portálu zaměřeného na rezervaci termínů očkování proti onemocnění COVID-19 (předmět kontroly).

Kontrolující v rámci svých činností prozkoumali webový odkaz https://smlouvy.gov.cz/smlouva/13430376, který je odkazem i pro hlavní smlouvu a který je zpřístupněn s výše uvedenými přílohami (hlavní smlouva „Poskytování softwarových nástrojů služby Chytrá karanténa, včetně poskytování provozní podpory“ a příloha č. 1 až 5) a zjistili, že se v části *„Návazné smlouvy“* nachází smlouva s identifikačním číslem 14796355, kdy číslo smlouvy je rovněž interaktivním odkazem na tuto smlouvu. V rámci hlavní smlouvy se jedná o jedinou smlouvu, která je uvedena jako návazná a která je dalším dodatkem smlouvy:

Dodatek č. 3 Smlouvy o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0:
Otevřením interaktivního odkazu (https://smlouvy.gov.cz/smlouva/13430376, část „Návazné smlouvy“) se otevřela stránka https://smlouvy.gov.cz/smlouva/15913407 s názvem *„Národní agentura pro komunikační a informační technologie, s.p. – Úprava poskytovaného rozsahu služeb“.*
V části *„Soubory“,* je vložena jedna příloha s názvem *„2020_106 NAKIT Dodatek č. 3.pdf“,* kdy název je zároveň interaktivním odkazem dané smlouvy. Otevřením se zpřístupní *„Dodatek č. 3 ke smlouvě o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“.* Z vlastní vložené smlouvy, respektive Dodatku č. 3 není patrné, kdy smlouva nabyla účinnosti, jelikož údaje s daty jsou anonymizovány. Účinnost lze tedy dovodit od data vložení tohoto dodatku do portálu smlouvy.gov.cz, které je 19. března 2021.

Jedním z předmětů tohoto dodatku, v části 2.1, odst. a), 6. odkaz je uvedeno, že je zde zahrnut centrální rezervační systém (CRS) pro neomezený počet odběrových a očkovacích míst na COVID-19, přičemž bližší specifikace je uvedena v části E přílohy č. 1 tohoto dodatku.
V části *„E Centrální rezervační systém odběrových a očkovacích míst“,* je v části E.4, kategorii subjektů údajů uvedeno, že se mj. jedná o občana se zájmem o testování či očkování v rámci boje proti pandemii COVID-19 a to v rámci vlastního rozhodnutí, dále jako vyhledaný rizikový kontakt v rámci trasování a také z rozhodnutí krajské hygienické stanice nebo praktického lékaře. U typu osobních údajů je uvedeno: jméno, příjmení, číslo pojištěnce = rodné číslo, telefonní číslo a adresa jako údaje povinné, dále e-mailová adresa jako údaj nepovinný a profese a informace o zdravotním stavu, které jsou navázány na přednostní práva očkování a informace specifické pro prioritizaci očkování.

Jak je patrné z výše uvedeného, kontrolující zjistili, že ke dni 19. března 2021 došlo k rozšíření předmětu Smlouvy o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0“ uzavřené mezi MZ a NAKIT, a to změnou čl. 1 odst. 1 písm. a) a písm. b) prostřednictvím Dodatku č. 3 smlouvy, kdy je v předmětu dodatku doplněna rezervace pro očkování. Od tohoto data, vzhledem k předmětu kontroly, se NAKIT nachází v postavení zpracovatele osobních údajů pro správce Ministerstvo zdravotnictví.

Úřední záznam analýzy zpracovatelské smlouvy „Smlouva o poskytování softwarových a odborných služeb“ uzavřené mezi NAKIT a kontrolovanou osobou byl vypracován a vložen do spisu kontroly dne 27. dubna 2021 (viz bod 24 přehledu podkladů, vč. příloh 24.1 až 24.4). Analýza byla zaměřena na dodatky či změny smlouvy. Kontrolující podotýkají, že kontrolovaná osoba ve své *„Odpovědi k Výzvě k doplnění podkladů ze dne 26. února 2021“* (viz bod 23 přehledu podkladů) uvedla, že:

„Všechny zveřejněné smlouvy jsou dostupné v systému smlouvy.gov.cz: Národní agentura pro komunikační a informační technologie, s.p. – [redacted] Smlouva – [redacted], Dodatek č. 1 –

Na odkazu [redacted] se otevřela stránka portálu smluv s názvem *„Národní agentura pro komunikační a informační technologie, s.p. – Odborné služby a paušál v rámci projektu Chytrá karanténa“*, kde v části soubory byly uvedené dvě přílohy:
<u>první z odkazů</u> (3610003036 M.pdf) vedl k otevření e-mailové korespondence týkající se objednávky,
<u>druhý z odkazů</u> (3610003036.pdf) vedl k otevření Objednávky č. 3610003036, ze dne 8. února 2021.
Vzhledem k tomu, že ani jeden z odkazů poskytnutých kontrolovanou osobou nevedl přímo ke smlouvě, jak bylo kontrolovanou v odkazu tvrzeno, provedl Úřad samostatně kontrolu na portálu smlouvy.gov.cz.

Původní smlouva je zveřejněna na [redacted] pod názvem „Zajištění centrálního rezervačního systému“. Otevřením přiložené smlouvy se otevře „Smlouva o poskytování softwarových a odborných služeb“ uzavřená mezi kontrolovanou osobou a NAKIT pod č.j. [redacted], ze dne 8. října 2020.
Tato smlouva byla již Úřadem podrobena kontrole (viz výše), a to ve smyslu splnění požadavků dle čl. 28 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“), (viz bod 20 přehledu podkladů).

Účelem této smlouvy (viz poslední odstavec čl. 1) *<u>„je poskytnutí předmětu plnění pro vzájemnou spolupráci objednatele s koncovým zákazníkem (MZ) na provozu uživatelsky komfortním rezervačním systému pro výběr termínu na odběr testu na nemoc COVID-19</u>, který bude zajišťovat vysokou dostupnost blízkého odběrového místa COVID-19 s minimální čekací dobou. Tento rezervační systém je určený jak pro osoby indikované na základě chytré karantény, tak i pro osoby, které chtějí podstoupit test dobrovolně (samoplátce)“.*

Vzhledem k závěru, že smlouva jako taková neřeší rezervační systém na očkování, nýbrž reservační systém na testování, a ani z dalšího textu smlouvy, především z výčtu zpracovávaných osobních údajů, není možné vyvodit souvislost smlouvy se systémem rezervací očkování a také vzhledem k tomu, že na základě výzvy kontrolované osobě, kdy byla zažádána o poskytnutí dalších dodatků smluv „Výzvou k doplnění podkladů“ ze dne 26. února 2021 (viz bod 21 přehledu podkladů), kontrolovaná osoba k předmětné smlouvě uzavřené s NAKITEM poskytla pouze odkaz na Dodatek č. 1, kontrolující vyhledali předmětné dodatky na portálu smlouvy.gov.cz. Pod odkazem [redacted] je v registru smluv umístěna smlouva „Národní agentura pro komunikační a informační technologie, s. p. - Zajištění centrálního rezervačního systému“. V sekci „Navázané záznamy“ nalezeny čtyři (4) ID navázané smlouvy, a to ID č. [redacted], [redacted], [redacted] a [redacted], které jsou dále podrobně rozebrány.

1. **Návazná smlouva ID č.** [redacted]
   - Název: „Zpřístupnění a poskytování služby rezervační komponenty portálu centrálního rezervačního systému“
   - Příloha: e-mailová korespondence týkající se objednávky ze dne 24. listopadu 2020 (viz příloha č. 2.1. tohoto úředního záznamu)
   - Další příloha: Objednávka NAKIT č. [redacted] vůči kontrolované osobě

   Obsahem objednávky je zpřístupnění a poskytování služby rezervační komponenty portálu centrálního rezervačního systému v rámci projektu Chytrá karanténa s odkazem na původní smlouvu.

2. **Návazná smlouva ID č.** [redacted]
   - Název: „Navýšení celkové ceny Předmětu plnění Smlouvy o 376 000,- Kč“
   - Příloha: „Dodatek č. 1 ke smlouvě o poskytování softwarových a odborných služeb“ ze dne 17. prosince 2020 (den účinnosti smlouvy je odvozen od data publikace v rámci portálu smlouvy.gov.cz, kdy na samotné smlouvě je datum podpisu či účinnosti smlouvy buď začerněno, nebo není uvedeno), (viz bod 24 příloha 24.2. přehledu podkladů).

   Předmětem tohoto dodatku je navýšení celkové částky plnění smlouvy, a to s ohledem na to, že: „*ke dni uzavření Smlouvy předpokládaly* (smluvní strany) *do budoucna realizaci záměru Vlády ČR celoplošně testovat obyvatelstvo ČR ve vazbě na počet odběrných míst, dohodly na opravě čl. 1 odst. 1 písm. a) tak, že Služba je ke dni uzavření Smlouvy, tj. ke dni 8. října 2020 poskytována pro neomezený počet odběrných míst…“*

3. **Návazná smlouva ID č.** [redacted]

   Verze smlouvy 1 ze dne 8. února 2021:
   - Název: „Odborné služby a paušál v rámci projektu Chytrá karanténa“
   - Příloha: Objednávka NAKIT č. 3610003036/8.2.2021 vůči společnosti [redacted]
   - Další příloha: e-mailová korespondence týkající se objednávky ze dne 8. února 2021

   Verze smlouvy 2 ze dne 25. března 2021:
   - Název: „Odborné služby a paušál v rámci projektu Chytrá karanténa“
   - Hlavní příloha: e-mailová korespondence týkající se objednávky ze dne 8. února 2021
   - Další příloha: Objednávka NAKIT č. [redacted] vůči kontrolované osobě
   - Další příloha: Objednávka NAKIT č. [redacted] vůči kontrolované osobě

4. **Návazná smlouva ID č.** [redacted]
   - Název: „Dodatek č. 2 ke smlouvě o poskytování softwarových a odborných služeb“ (viz bod 24 příloha 24.3. přehledu podkladů)
   - Předmět dodatku: „*Předmětem Dodatku č. 2 ke smlouvě* [redacted] *je změna čl. 1 odst. 1 písm. a) a b) Smlouvy a čl. 6 písm. A odst. 3 Smlouvy:*
   - Příloha: Dodatek č. 2 ke smlouvě o poskytování softwarových a odborných služeb ze dne 26. března 2021 (datum je odvozeno od data publikace v portálu smlouvy.gov.cz, jelikož samotná smlouva neobsahuje datum podpisu ani účinnosti dodatku).
   - V úvodním ustanovení je uvedeno, že: *„Vzhledem k realizaci záměru Vlády ČR očkovat obyvatelstvo České republiky vznikla potřeba rozšíření rezervačního systému používaného pro provádění PCR a antigenních testů o možnost rezervace na očkování pro plátce pojištění (občany) ČR a cizince se zdravotním pojištěním na území ČR“.*

- Předmětem smlouvy je, jak je uvedeno výše, změna čl. 1 odst. 1 písm. a) a b) a čl. 6 písm. A odst. 3 smlouvy.

Jedním z předmětů tohoto dodatku, uvedeným v čl. č. 2, odst. 2.1, pododst. a) bodu 2) je:
„2) elektronická rezervace termínu očkování pro plátce pojištění v ČR včetně integračních vazeb API rozhraní na systém registrací zájemců o očkování a agendový informační systém infekčních nemocí (ISIN), včetně funkcí podpory plánování prvních a druhých termínů očkování“
Výčet zpracovávaných osobních údajů je součástí tohoto dodatku a s ohledem na předmět kontroly rozdělen do částí *„Registrační modul pro očkování“, „Rezervační modul pro očkování“ a „Následné rozšířené registrace pro očkování“.*
V rámci těchto částí jsou zpracovávány osobní údaje: jméno, příjmení, číslo pojištěnce, číslo pojišťovny, místo trvalého pobytu, telefon, preferované očkovací centrum, dosažená věková hranice (u osob nad 80 let), profesní příslušnost (týkající se pouze zdravotnického personálu) a jako variantní k číslu telefonu je uveden e-mail.

Kontrola daných smluv a jejich návaznost byla zpracována a formou úředního záznamu založena do spisu kontroly (viz bod 24 příloha 24.4. přehledu podkladů).

Kde dni 26. března 2021 došlo k rozšíření předmětu Smlouvy o poskytování softwarových a odborných služeb uzavřené mezi NAKIT a kontrolovanou osobou, a to změnou čl. 1 odst. 1 písm. a) a písm. b), kdy je v předmětu dodatku doplněna mj. i elektronická rezervace pro očkování, integrační vazby API rozhraní na systém registrací zájemců o očkování, a agendový informační systém infekčních nemocí, vč. funkcí podpory plánování prvních a druhých termínů očkování.
Od tohoto data se kontrolovaná osoba nachází v postavení zpracovatele, kdy správcem osobních údajů je Ministerstvo zdravotnictví a zpracovatelem je NAKIT, jelikož zpracovatelská smlouva mezi správcem MZ a zpracovatelem NAKIT byla o systém rezervací očkování COVID-19 rozšířena od data 19. března 2021, jak je uvedeno výše. Vzhledem k tomu, že v době uzavření dodatku zpracovatelské smlouvy mezi zpracovatelem NAKIT a kontrolovanou osobou, ke dni 26. března 2021, již byla zpracovatelská smlouva mezi MZ a NAKIT účinná, od data 26. března platí: MZ je v pozici správce osobních údajů, NAKIT je v pozici zpracovatele a kontrolovaná osoba je ve smyslu řetězení zpracovatelů v postavení dalšího zpracovatele.

Kontrolující provedli kontrolu *Smlouvy o poskytování softwarových a odborných služeb* uzavřené mezi NAKIT a kontrolovanou osobou, (dále jen „Smlouva“), (viz bod 24 příloha 24.1. přehledu podkladů) vč. Dodatku č. 1 (viz bod 24 příloha 24.2. přehledu podkladů) a Dodatku č. 2 (viz bod 24 příloha 24.3. přehledu podkladů), kdy zkoumali obsahy těchto dokumentů, především zda jsou plněny podmínky čl. 28 odst. 3 nařízení (EU) 2016/679:

- **předmět** (čl. 1 Smlouvy), z hlediska předmětu kontroly (čl. 2 Dodatku č. 2)
- **účel zpracování** (čl. 1, odst. 1, pododstavec bez označení písmene Smlouvy); uvedeno je zde, že účelem je *„…poskytnutí Předmětu plnění pro vzájemnou spolupráci Objednatele s koncovým zákazníkem Ministerstvo zdravotnictví na provozu uživatelsky komfortním rezervačním systému pro výběr termínu na odběr testu na nemoc COVID-19, který bude zajišťovat vysokou dostupnost blízkého odběrového místa COVID-19 s minimální čekací dobou. Tento rezervační systém bude určený jak pro osoby indikované na základě chytré karantény, tak i pro osoby, které chtějí podstoupit test dobrovolně (samoplátce)“;* z daného vyplývá, že účel uvedený ve Smlouvě se váže výhradně k rezervačnímu portálu pro

rezervace odběrů testů; účel zpracování vzhledem k předmětu kontroly není konkrétně uveden ani ve Smlouvě ani v předmětném Dodatku č. 2., z dodatku lze pouze vyčíst, v souvislosti s rozsahem zpracovávaných osobních údajů účel – poskytování předmětu plnění (registrace pro očkování). Kontrolující tedy mají za to, že účelem je právě poskytování předmětu plnění, který je v rámci Dodatku č. 2 definován článkem č. 2;

- **povaha služby** je definována jako služba poskytovaná formou vzdáleného přístupu přes webové rozhraní a je provozována na serveru umístěném v prostředí kontrolované osoby, přičemž NAKIT je oprávněn přístupové údaje ke službě šířit, kopírovat nebo jiným způsobem umožnit její užívání (čl. 2, část A2, odst. 1 až 4 Smlouvy);
- **typ zpracovávaných osobních** údajů (odst. 2.2. Dodatku č. 2) je uveden přesným výčtem zpracovávaných osobních údajů rozdělených na fáze zpracování: a to zpracování pro registrační modul, zpracování pro rezervační modul a následné zpracování pro rozšířené registrace očkování; souhrnem jde o jméno, příjmení, číslo pojištěnce, číslo pojišťovny, místo trvalého pobytu, telefon (variantně s e-mailem), preferované očkovací centrum, pro zjištění přednosti v očkování rovněž věková hranice, profesní příslušnost a zdravotní stav žadatele;
- **kategorie subjektů údajů** – zatím co je tento údaj uveden v Dodatku č. 2 u změn týkajících se registrací pro testování (bod 2.2. Dodatku č. 2, kdy u výčtu zpracovávaných osobních údajů je v závorkách uveden rovněž výčet subjektů údajů, jichž se zpracování týká), u nového zpracování týkajícího se rezervací očkování tento výčet není uveden, kdy subjekty údajů, jichž se rezervační systém na očkování týká, je možné nepřímo zjistit z Dodatku č. 2 (čl. 1 bod 1.2.), kde je uvedeno, že: *„Vzhledem k realizaci záměru Vlády ČR očkovat obyvatelstvo České republiky, vznikla potřeba rozšíření rezervačního systému používaného pro provádění PCR a antigenních testů o možnost rezervace na očkování pro plátce pojištění (občany) ČR a cizince se zdravotním pojištěním na území ČR“.* Kontrolující tedy za subjekty údajů považují osoby takto vyjádřené;
- **povinnosti a práva kontrolované osoby a NAKIT** jsou upravena v několika částech Smlouvy. Patří k nim ustanovení, že kontrolovaná osoba bez souhlasu NAKIT neposkytne informace třetím stranám (čl. 6, část A, odst. 4), kontrolovaná osoba bude zpracování provádět jen dle pokynů NAKIT, přičemž Smlouva je považována rovněž za smlouvu o zpracování osobních údajů (čl. 6 část C., odst. 1), kontrolovaná osoba při zpracování musí postupovat s řádnou péčí (čl. 6 část C, odst. 7), kontrolovaná osoba při zpracování bude zohledňovat povahu zpracování, bude nápomocna při vyřizování žádostí subjektů údajů, bude nápomocna v plnění povinností při zabezpečení osobních údajů a NAKIT poskytne veškeré informace k doložení skutečnosti, že byly splněny povinnosti podle čl. 28 nařízení (EU) 2016/679, umožní audity a inspekce NAKITU či jím pověřeným osobám a poskytne jim řádnou součinnost (čl. 6 část C, odst. 7), provede výmaz osobních údajů ve lhůtách stanovených zpracovatelem (čl. 6 část C, odst. 8), při ukončení smlouvy předá NAKIT protokolárně všechny nosiče obsahující osobní údaje a vymaže všechny v elektronické podobě, pokud nedostane jiné pokyny (čl. 6, část C, odst. 9), kontrolovaná osoba dbá, aby žádný ze subjektů údajů neutrpěl újmu na svých právech (čl. 6 část C, odst. 10), povinnost mlčenlivosti (čl. 6 část A, odst. 1), povinnost kontrolované zabezpečit řádnou technickou a organizační ochranu zpracovávaných osobních údajů a přijat opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajů, jejich úplné nebo částečné změně, zničení či ztrátě a neoprávněných přenosům atd. (čl. 6 část C, odst. 16 až 18), přístup k osobním údajům budou mít jen pověřené osoby (čl. 6 část C, odst. 19.1 a 19.2), dále je zde řešeno uložení na zabezpečených serverech, ve fyzické osobě uchováván

zabezpečené (čl. 6 část C, odst. 19.3 až 19.5). V neposlední řadě je třeba zdůraznit povinnost kontrolované osoby zpracovat a zdokumentovat přijatá a provedená technickoorganizační opatření (čl. 6 část C, odst. 20), povinnost přijmout opatření k zabezpečení zpracování včetně schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systému (čl. 6 část B, odst. 25 a násl.), povinnost vypracovat plán postupu pro případ porušení zabezpečení, vést podrobnou evidenci veškerých případů porušení zabezpečení bez ohledu na to, zda představují riziko pro práva a svobody fyzických osob s uvedením skutečností o daném porušení, jeho účinků a přijatých nápravných opatření (čl. 6 část C, odst. 31. až 32.).

Z daného lze konstatovat, že zpracovatelská smlouva obsahuje náležitosti stanovené čl. 28 odst. 3 nařízení (EU) 2016/679.

Zpracovávané osobní údaje:
K předmětnému období do počátku účinnosti zpracovatelské smlouvy (26. března 2021) uzavřené s NAKITEM kontrolovaná ve své *Odpovědi na oznámení o zahájení kontroly ze dne 29. ledna 2021 (*viz bod 18 přehledu podkladů) uvádí, že v rámci rezervačního systému jsou zpracovávány osobní údaje: číslo pojištěnce = rodné číslo fyzické osoby, jméno, příjmení, adresa trvalého pobytu, číslo pojišťovny, vybrané očkovací místo, telefon a nepovinným údajem je zde uveden rovněž e-mail.

Z důvodu prošetření obsahu stížností bylo v rámci předkontrolních úkonů prověřeno, zda webové stránky kontrolované osoby, které primárně slouží ke zpracování osobních údajů (jejich získávání v rámci registrace), užívají cookies či jiné sledovací skripty prostřednictvím kterých by mohlo dále docházet ke zpracování osobních údajů.

Cookies:
První kontrola funkčních cookies byla provedena 26. ledna 2021 (viz bod 11 přehledu podkladů vč. přílohy 11.1.). Z provedeného testu stránek [redacted], prostřednictvím systému Cookiebot k uvedenému datu bylo zjištěno, že již při návštěvě daných stránek se uživateli nahrají do koncového zařízení následující cookies:

- [redacted] jsou zařazeny do kategorie „Nezbytné (Necessary)“, přičemž slouží k rozlišení mezi lidmi a tzv. boty (automatický systém využívající umělou inteligenci), dále je zde uvedeno, že data jsou zasílána do USA (poskytovatelem jsou stránky google.com); první z uvedených cookies je trvalá, tedy je s neomezenou dobou uchování;
- [redacted] jsou řazeny mezi „Statistické (Statistics)“, poskytovatelem je zde [redacted], data směřují do USA, z analýzy je u všech zřejmé propojení se službou Google Analytics; doba uchování těchto cookies je v rozmezí od jednoho dne až po dva roky;
- [redacted] patří do kategorie „Statistické (Statistics)“ a zasílá data o zařízení a chování návštěvníka stránek službě Google Analytics, ta jsou zasílána do USA (poskytovatelem google-analytics.com);
- [redacted] nástroj analyzuje jako „Marketingové (Marketing)“, první ze jmenovaných využívá služba Google AdWords pro marketingové

účely, účelem druhé je cílení reklamy, data směřují do USA (poskytovatel google.com); doba uchování je stanovena na 6 měsíců;

- [redacted], [redacted] jsou zařazeny do kategorie „Neklasifikované (Unclassified)“, jejich funkce není blíže popsána, data zůstávají v České republice (poskytovatel [redacted]; doba expirace je 1 den.

Druhá kontrola funkčních cookies byla provedena 16. února 2021 (viz bod 20 přehledu podkladů, příloha 20.9). Z provedeného testu stránek [redacted], prostřednictvím systému Cookiebot k uvedenému datu bylo zjištěno, že již při návštěvě daných stránek se uživateli nahrají do koncového zařízení následující cookies:

- nezbytné (necessary) cookies: původní cookies, uvedené rovněž v první kontrole, [redacted], [redacted], [redacted] , které byly zjištěny i v rámci druhé kontroly, byly rozšířeny o cookies:
    - [redacted], [redacted], [redacted] poskytovatele [redacted]. Jedná se o cookies s identickým posláním, předáním údajů do USA s rozdílným nastavením délky uchovávání, kdy první z nich je na dobu nezbytně nutnou při návštěvě stránek a druhá z nich je na dobu 1 roku;
- statistické cookies zůstaly beze změny, jedná se o cookies [redacted], [redacted], [redacted], [redacted], [redacted], [redacted];
- marketingové cookies naznaly změnu, kdy původní cookies uvedené v první kontrole nahradily cookies:
    - [redacted], [redacted] poskytovatele [redacted], které shromažďují informace o chování uživatelů na více webových stránkách a tyto informace jsou užívány k optimalizaci reklamy (cílení reklamy). Údaje jsou předávány do USA a jejich nastavení je omezeno na 1 den;
    - [redacted] poskytovatele Google.com. Přesné určení není jasné, údaje jsou předávány do USA a doba uchování je nastavena na 1 rok;
- neklasifikovatelné cookies jsou identické jako u první kontroly, kdy se jedná o [redacted], a [redacted].

Třetí, poslední, kontrola funkčních cookies byla provedena 18. května 2021 (viz bod 43 přehledu podkladů, příloha 43.1). Z provedeného testu na stránce [redacted], prostřednictvím systému Cookiebot k uvedenému datu bylo zjištěno, že již při návštěvě daných stránek se uživateli nahrají do koncového zařízení následující cookies:

- nezbytné cookies nenaznaly změnu od kontroly č. 2, jsou to , [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted].
- statistické cookies zůstaly beze změny, jedná se o cookies [redacted], [redacted], [redacted] **a** [redacted], [redacted];
- v rámci marketingových cookies zde zůstala pouze [redacted], [redacted];
- neklasifikovatelné cookies jsou identické jako u první i druhé kontroly, kdy se jedná o [redacted], a [redacted] **typu http.**

Na základě výsledků testů Cookiebotu bylo prověřeno chování stránek [redacted] ve vztahu k funkčním cookies (viz bod 43 přehledu podkladů, přílohy 43.2 až 43.11), přičemž k testu bylo využito objednání PCR testu pro samoplátce poskytovatele [redacted], která systém na stránkách užívá.

K danému kontrolující použili počítač s Windows 10 64bit (20H2), prohlížeč MS Edge. V prohlížeči byly vypnuté funkce pro prevenci sledování, aby nebyly ovlivněny funkce analyzované stránky. Prohlížeč byl spuštěn s parametry [redacted], aby mohl program [redacted].
Dále byl použit program [redacted] související [redacted] (dále jen „Program“). Pro analýzu síťové komunikace byl použit program [redacted].

Vzhledem k množství nastavovaných cookies byly aktivně zkoumány pouze ty, které se jeví významné z pohledu ochrany osobních údajů a/nebo předávání osobních údajů mimo EU, jejichž platnost je více než 24 hodin. (Ostatní cookies včetně hodnot jsou k dispozici ve screenshotu, který je součástí analýzy). Screenshot byl pořízen po načtení zkoumané stránky v doméně [redacted]. Analýzou stránky byly zjištěny následující skutečnosti:

- dochází k nastavování cookies s platností až na 2 roky;
- je načítán obsah z domén:
  [redacted]
- z některých výše uvedených domén dochází k nastavování cookies, což je patrné z přiloženého screenshotu. Z domény [redacted] není cookies nastavena ve všech případech přístupů, proto zde není uvedena.

Kontrolující dále níže uvádějí cookies, které se jeví jako významné. Časové formáty jsou pro úplnost ponechány v původním formátu, první je rok, za pomlčkou měsíc a den, následovaný časem a informací o časovém pásmu (Z).

[redacted]
Byla nastavena cookie [redacted] s hodnotou [redacted] a platností do [redacted]. Cookie je, vzhledem k platnosti a unikátnosti, unikátním identifikátorem. Dle výstupu Programu je protistrana komunikace umístěna v USA, dochází tak k předávání unikátního identifikátoru do USA.

[redacted]
Byly nastaveny následující významné cookies:
[redacted] s hodnotou [redacted] a platností do [redacted]. Nastavuje unikátní identifikátor.
[redacted] s hodnotou [redacted] a platností do [redacted]. Nastavuje unikátní identifikátor.

Dle výstupu Programu je protistrana komunikace umístěna v USA, dochází tak k předávání unikátních identifikátorů do USA. Protistranou je v těchto případech míněna doména

google-analytics.com, ze které je stránkou načítán JavaScriptový kód, který dané cookies obsluhuje.
Závěrem lze konstatovat, že dochází k nastavení unikátních cookies s dlouhou platností. Dochází ke komunikaci s celou řadou domén, jejichž provozovatelé tak mají k dispozici minimálně údaj o IP adrese návštěvníků stránky [redacted] a v některých případech i unikátní řetězec znaků v cookie.

Dle výstupu programu [redacted] dochází v případě komunikace s doménami [redacted] k předání osobních údajů do USA, neboť výstup Programu ukazuje na provoz stránek na území USA a zmíněné weby zjevně mají informaci minimálně o IP adrese návštěvníka stránek [redacted].

Registrační formulář
Dále bylo kontrolujícími prověřeno, zda URL adresy registračního formuláře neobsahují informace o rodném číslu. Systémy pro analýzu návštěv mají přehled o kompletních URL adresách, touto cestou by tak mohlo dojít k předání zmíněného osobního údaje do zahraničí. V době prováděné analýzy rodné číslo nebylo coby parametr URL adresy užito. URL adresa obsahuje převážně provozní údaje a také údaj o požadovaném datu rezervace na PCR tes. Příklad URL adresy:

[redacted]

Rodné číslo bylo předáváno systému [redacted] v rámci požadavku POST (adresa [redacted], spolu se jménem a dalšími osobními údaji, které žadatel o registraci k testování zadal do formuláře. Předávaná data rovněž obsahují položku [redacted], což dokládá, že součástí formuláře je i odpověď od systému pro prevenci formulářového spamu. Nebylo zjištěno, že by některý ze skriptů pro analýzu návštěvníků webu k těmto informacím přistupoval.

Zpracovávané osobní údaje v období od účinnosti zpracovatelské smlouvy z 26. března 2021 jsou uvedeny v Dodatku č. 2 Smlouvy a jedná se o: jméno, příjmení, číslo pojištěnce, číslo pojišťovny, místo trvalého pobytu, telefon (alternativně e-mail), preferované očkovací centrum a pro registrační modul a následnou rozšířenou registraci rovněž dosažená věková hranice, profesní příslušnost a zdravotní stav (z důvodu zjištění přednosti a urgentnosti očkování).

Z výše uvedeného lze tedy konstatovat, že kromě osobních údajů uvedených v podkladech kontrolované osoby, jsou rovněž zpracovávány osobní údaje prostřednictvím cookies, a to přinejmenším IP adresa subjektu údajů, který se přihlásí (nebo je automaticky přesměrován) na stránky [redacted], kontrolované osoby, přičemž dochází k předání do USA.

Právní titul zpracování:
Kontrolovaná osoba ve své *Odpovědi na Oznámení o zahájení kontroly ze dne 29. ledna 2021* (viz bod 13 přehledu podkladů), v bodu 3 uvádí, že jediným titulem pro všechna zpracování osobních údajů, která probíhají v rámci rezervačního systému očkování COVID-19, je souhlas subjektu údajů.
V předmětném období do 25. března 2021 tak kontrolovaná jako správce osobních údajů zpracovávala osobní údaje subjektů údajů, kteří se prostřednictvím stránek poskytovatelů očkování (proklikem na odkaz registrace na těchto stránkách), ocitli na stránkách kontrolované osoby, kde dle instrukcí měli provést registraci (viz bod 11 přehledu podkladů). Při tomto po subjektech údajů nebyl vyžadován žádný aktivní souhlas a již samotné přihlášení či přesměrování z důvodu provedení registrace pak kontrolovaná osoba patrně považovala za dostatečný akt svobodné vůle subjektu údajů, založený na dobrovolnosti, aby samotné přihlášení s přesměrováním bez dalšího, tedy i informaci, že k danému přesměrování dojde, mohla zařadit pod zákonné zpracování podle čl. 6 odst. 1 písm. a) souhlas subjektu údajů.
K tomu kontrolující upozorňují, že k samotnému zpracování osobních údajů nedocházelo pouze způsobem, kdy samotné subjekty údajů své osobní údaje uvedly do formulářů prostřednictvím rezervačního portálu, ale rovněž již samotným přístupem na webové stránky kontrolované osoby (přesměrováním bez možnosti ovlivnění), a to prostřednictvím cookies, umístěných na stránkách kontrolované osoby.

Z materiálů předložených kontrolovanou osobou není možné pro období do 25. března 2021 dovodit ani všechny skutečné účely, pro které se v daném období zpracování provádělo, jelikož kontrolovaná pro dané období žádné takové relevantní podklady neposkytla a ani v rámci informační povinnosti, jak je popsáno níže, takové údaje nebyly přístupné.

S přihlédnutím k podobnému rozsahu a účelům zpracování uvedených v Dodatku č. 2 Smlouvy o poskytování softwarových a odborných služeb (na základě kterého se kontrolovaná osoba dostala do postavení zpracovatele), vzhledem k tomu, že se jednalo o totožné probíhající zpracování, kdy kontrolovaná v rámci téže činnosti a téhož procesu pouze změnila své postavení, bylo zjištěno, že v rámci rezervačního systému jsou údaje zpracovávány minimálně za účelem rezervace očkování, účelem vyhodnocení případné přednosti v očkování, rezervace místa očkování, pozvánce k očkování a poskytnutí potvrzení o provedeném očkování a že je tedy souhlas, který kontrolovaná vyžaduje, vztahován na všechny tyto účely.

Jak je uvedeno výše, v období do 25. března 2021 docházelo k automatickému přesměrování zájemců o očkování (a jejich případných zástupců) ze stránek poskytovatelů očkování na stránky kontrolované osoby bez existence jakékoli přesně stanovené vazby na tuto osobu (poskytovatele očkování). V této době se kontrolovaná nacházela v postavení správce a osoby, které se za účelem rezervace termínu na očkování přihlásily na odkaz u jednotlivých poskytovatelů, se tak bez nejmenšího tušení ocitly na stránkách kontrolované osoby, kde byly jejich osobní údaje zpracovány i pro další, jiné účely, mimo jiné i pro účely marketingu (prostřednictvím marketingových cookies).

Je-li kontrolujícími posuzován samotný souhlas se zpracováním osobních údajů, jakožto užitého zákonného titulu zpracování, pak je nutné konstatovat, že souhlas podléhá režimu ve smyslu čl. 4 bod 11 nařízení (EU) 2016/679 a to i souhlas se zpracováním osobních údajů prostřednictvím cookies ve smyslu čl. 5 odst. 3 Směrnice č. 2002/58/ES, kdy se musí jednat

o projev vůle, který je svobodný, konkrétní, informovaný a jednoznačný a je učiněn prohlášením nebo jiným zjevným potvrzením. Správce osobních údajů (myšleno i jeho zpracovatelé či další zpracovatelé) pak musí dodržet podmínky stanovené čl. 7 nařízení (EU) 2016/679, kdy musí prokázat souhlas se zpracováním, a to po celou dobu zpracování.

Pro období do 25. března tak kontrolující konstatují, že zpracování na základě souhlasů osob dotčených zpracování (subjektů údajů) tyto požadavky nesplňuje. Souhlas se totiž váže k více účelům, subjekty údajů nejsou informovány o tomto zpracování a jeho délce, zpracování probíhá bez přičinění samotných subjektů údajů již po automatickém přesměrování ze stránek poskytovatelů očkování, tedy bez prokazatelného projevu vůle subjektu údajů.

Plnění informační povinnosti a plnění práv subjektů údajů

S ohledem na to, co je uvedeno v kontrolním zjištění č. 1, se posuzování plnění informační povinnosti rozděluje na dvě (2) období:

A) od 1. února 2021 (datum zahájení kontroly[4]) do 25. března 2021 (včetně tohoto dne), a
B) od 26. března 2021 (včetně tohoto dne) do dne vyhotovení tohoto protokolu.

Ad A)

V tomto období se kontrolovaná osoba nacházela v postavení správce (viz výše). Dle čl. 12 bod 1 nařízení (EU) 2016/679 správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učiní veškerá sdělení podle článků 15 až 22 a 4 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti.

Na otázku kontrolujících „*Sdělte a doložte, jak plníte své povinnosti a práva subjektů údajů dle čl. 12 až 22 nařízení (EU) 2016/679 při zpracovávání osobních údajů v rámci Centrálního rezervačního systému pro očkování proti COVID-19 na výše uvedené doméně*“ kontrolovaná osoba ve své odpovědi ze dne 10. února 2021 (viz bod 18. přehledu podkladů) uvedla, že informace k uplatnění práv subjektů osobních údajů dle čl. 12-22 nařízení (EU) 2016/679 jsou zpracovávány v první vrstvě na stránkách (i) https://www.mzcr.cz/ochrana-osobnich-udaju/ a ve druhé vrstvě na stránkách (ii) https://registrace.mzcr.cz/#consent, https://registrace.mzcr.cz/assets/Informacni_povinnost_CRS_ockovani.pdf.

Ad (i) „první vrstva“

Po kliku na tyto stránky se uživatel dostane na web Ministerstva zdravotnictví České republiky. Je zde uveden kontakt na pověřence pro ochranu osobních údajů Ministerstva zdravotnictví České republiky pana Mgr. Roberta Vávru, DiS. a je zde také interaktivní odkaz s názvem „*Základní informace o zpracování osobních údajů Ministerstvem zdravotnictví*“. Po prokliku na něj se zobrazí čtyř (4) stránkový PDF nazvaný „*Základní informace o zpracování osobních údajů Ministerstvem zdravotnictví. Informace je uveřejňována pro plnění povinnosti stanovené v článcích 12 až 14 Obecného nařízení o ochraně osobních údajů č. 2016/679 ze dne*

[4] Doručení oznámení o zahájení kontroly do datové schránky kontrolované osoby [srov. § 5 odst. 2 písm. b) kontrolního řádu].

27. dubna 2016 (dále jen „nařízení“). Tato informace může být doplňována a upřesňována bližšími informacemi zveřejněnými nebo poskytnutými ke specifickým zpracováním.“ Tento dokument v obecné rovině popisuje informační povinnost Ministerstva zdravotnictví České republiky a nejedná se o informační povinnost poskytovanou v rámci registrace na očkování proti onemocnění COVID-19[5].

Ze shora popsaného vyplývá, že a) jedná se o plnění informační povinnosti jiného správce (tj. Ministerstva zdravotnictví České republiky), nikoliv kontrolované osoby, b) tyto informace se netýkají informování subjektů v rámci registrace na očkování proti onemocnění COVID-19.

Ad (ii) „druhá vrstva“
Po prokliku na stránky https://registrace.mzcr.cz/#consent se uživatel dostane na stránky Ministerstva zdravotnictví České republiky s názvem *„Centrální rezervační systém - Očkování proti COVID-19 registrace do systému*“. V dolní části se nachází text *„Detailní informace o zpracování vašich osobních údajů naleznete zde*“. Po prokliku na *„zde*“ se zobrazí osmi (8) stránkový PDF dokument s názvem *„Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ*“ (dále jen „Informace o zpracování“). K tomuto dokumentu se lze rovnou dostat přes proklik na https://registrace.mzcr.cz/assets/Informacni_povinnost_CRS_ockovani.pdf (viz bod 27. přehledu podkladů). Informace o zpracování se týkají plnění informační povinnosti vůči subjektů údajů v rámci registrace očkování proti onemocnění COVID-19.

V bodu 4. Informací o zpracování je uvedeno, že správcem osobních údajů je Ministerstvo zdravotnictví České republiky. Kontrolovaná osoba je zde uvedena jako další zpracovatel. Kontrolující shrnují, že „první“ i „druhá“ vrstva je plněním informační povinnosti jiného správce (tj. Ministerstva zdravotnictví České republiky). Nezbývá než uzavřít, že v období od 1. února 2021 do 25. března 2021 kontrolovaná osoba neplnila informační povinnost vůbec.

Ad B)
Jak je uvedeno v kontrolním zjištění č. 1, kontrolovaná osoba se od 26. března 2021 nachází v postavení dalšího zpracovatele vůči Ministerstvu zdravotnictví České republiky a v postavení zpracovatele vůči NAKIT. Kontrolující tedy posuzovali plnění informační povinnosti a plnění práv subjektů údajů kontrolovanou osobou od 26. března 2021 jako zpracovatele.

I v tomto období je nutno vycházet z odpovědi kontrolované osoby ze dne 10. února 2021 (viz bod 18. přehledu podkladů)[6], kde uvedla, že informace k uplatnění práv subjektů osobních údajů dle čl. 12-22 nařízení (EU) 2016/679 jsou zpracovávány v první vrstvě na stránkách (i) https://www.mzcr.cz/ochrana-osobnich-udaju/ a ve druhé vrstvě na stránkách

[5] K informační povinnosti viz úřední záznam ze dne 19. února 2021 (viz bod 20 přehledu podkladů, strana 5 a 6) a úřední záznam ze dne 18. května 2021 (viz bod 27. přehledu podkladů).

[6] A to z důvodu, že nic jiného k informační povinnosti, vyjma odpovědi ze dne 4. března 2021, kontrolovaná neuvedla.

(ii)https://registrace.mzcr.cz/#consent,
ttps://registrace.mzcr.cz/assets/Informacni_povinnost_CRS_ockovani.pdf.

Jelikož dokument popsaný v odstavci (i) obsahuje obecné informace ke zpracování osobních údajů, zaměřili se kontrolující na druhou vrstvu, tedy dokument, který se týká informační povinnosti ve vztahu k registraci na očkování proti onemocnění COVID-19 (ii).
Klíčové z hlediska posuzování plnění informační povinnosti a plnění práv subjektů údajů kontrolovanou osobou dle čl. 12 až 22 nařízení (EU) s ohledem na registraci na očkování proti onemocnění COVID-19 jsou tedy *„Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ“* (dále také jen „Informace o zpracování“).
Kontrolující prověřovali, zda Informace o zpracování obsahují podstatné náležitosti dle nařízení (EU). Informace o zpracování v souladu s čl. 13 bod 1 nařízení (EU) 2016/679 zahrnují: totožnost a kontaktní údaje správce (bod 4.), kontaktní údaj na pověřence pro ochranu osobních údajů (bod 7.), účely zpracovávání osobních údajů (bod 3.), právní základ zpracování (bod 3., kterými jsou souhlas a plnění zákonné povinnosti), příjemci osobních údajů (bod 4.).

V Informacích o zpracování je dále v souladu s čl. 13 bod 2 psím. a) nařízení (EU) 2016/679 uvedena doba, po kterou jsou osobní údaje zpracovávány (bod 5.). Konkrétně se zde stanoví, že *„Vaše osobní údaje uchováváme po dobu Vámi uděleného souhlasu…“,* z čehož není vůbec zřejmé, na jak dlouho se souhlas uděluje a po jakou dobu hodlá správce osobní údaje uchovávat. Dále se zde stanoví, že *„Po jeho provedení* (myšleno po souhlasu) *jsou údaje uloženy v ISIN v souladu se zákonem č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a souvisejících právních předpisů*.“

Kontrolující shrnují, že u souhlasu není uvedeno, na jak dlouho se uděluje. Doba udělování souhlasu není citována ani na základní stránce https://registrace.mzcr.cz/#consent (viz bod 27.6 přehledu podkladů), přičemž kontrolující upozorňují, že informace o době musí být formulována takovým způsobem, aby měl subjekt údajů jistotu, kdy bude zpracování ukončeno, resp. budou data předána správci či smazána.

V Informacích o zpracování je dále v souladu s čl. 13 bod 2 psím. b) nařízení (EU) 2016/679 zahrnuto právo na přístup k osobním údajům (bod 6.), v souladu s písm. d) citovaného ustanovení právo podat stížnost u dozorového úřadu (bod 7.), v souladu s písm. c) citovaného ustanovení právo souhlas odvolat, v souladu s písm. f) citovaného ustanovení právo na lidský zásah ze strany správce. Dále jsou zde podle čl. 12 bod 1 nařízení (EU) 2016/679 uvedena tato práva: na opravu (čl. 16 nařízení (EU) 2016/679), výmaz (čl. 17 nařízení (EU) 2016/679), omezení zpracování (čl. 18 nařízení (EU) 2016/679), přenositelnost (čl. 20 nařízení (EU) 2016/679). Tato práva jsou uvedena také přímo na stránkách https://registrace.mzcr.cz/#consent (viz bod 27.6 přehledu podkladů).

Kontrolující také ověřovali, jaké informace lze najít přímo na po prokliku na stránky https://registrace.mzcr.cz/#consent (viz bod 27.6 přehledu podkladů). Nachází se zde informace ve smyslu čl. 12 a 13 nařízení (EU) 2016/679, tj. informace o správci (tj. Ministerstvo zdravotnictví České republiky), účelu zpracování osobních údajů pomocí registračního formuláře na očkování, právním titulu - souhlas dle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679, o možnosti souhlas odvolat dle čl. 7 bod 3 nařízení (EU) 2016/679. Zde kontrolující akcentují fakt, že zde není uvedeno, jakým způsobem lze souhlas odvolat, což není v souladu

s nařízením (EU) 2016/679. Dále se zde stanoví, že se zpracovávají o biometrické údaje dle čl. 9 nařízení (EU) 2016/679 a že je od 1. února 2021 v rámci zpracování osobních údajů využíváno automatizované rozhodování[7] dle č. 22 nařízení (EU) 2016/679 pro prioritizaci osob v rámci očkování. Na tomto místě je třeba uvést, že pokud správce provádí automatizované rozhodování dle výjimky čl. 22 bod 3 nařízení (EU) 2016/679, musí plnit vůči subjektům údajů mimo jiné i informační povinnost dle čl. 13 odst. 2 písm. f) nebo čl. 14 odst. 2 písm. g) nařízení (EU) 2016/679. Správce by tak měl informovat (v souladu s čl. 13 odst. 2 písm. f) nařízení (EU) 2016/679) nejen o automatizovaném rozhodování pro prioritizaci, ale měl by uvádět i relevantní informace ohledně použitého postupu pro prioritizaci a také informaci o významu a předpokládaných důsledcích takového zpracování pro subjekt údajů, což v daném případě chybí. Pouze v bodě 3. Informací o zpracování (první věta) se uvádí, že osobní údaje jsou zpracovávány za účelem efektivně zajistit objednání termínu očkování a „*určit pořadí očkovaných, v návaznosti na jejich zdravotní stav a rizika, která jim hrozí*“, což dle kontrolujících nenaplňuje požadavky uvedené v předchozí větě.

Plnění práv subjektů údajů

Kontrolovaná osoba ve své odpovědi ze 4. března 2021 (viz bod 23.1 přehledu podkladů) uvedla u bodu 2., že „*V případě, že se subjekty obrací přímo na společnost [redacted] kontaktujeme a řešíme tyto záležitosti přímo se správcem. Tento postup je v souladu s informační povinností a následně konáme dle pokynu správce*.“

Kontrolovaná osoba však neuvedla konkrétní postup, jak řeší plnění práv subjektů údajů, v jakých lhůtách kontaktuje správce, v jakých lhůtách pak reaguje správce na žádosti kontrolované osoby o reakci a následně kontrolovaná osoba na žádosti subjektů údajů. Nebyly doloženy žádné informace nebo např. vnitřní předpisy o vyřizování žádostí subjektů údajů dle čl. 15 až 22 nařízení (EU) 2016/679. K danému tématu kontrolující konstatují, že subjekty jsou sice informováni o svých právech, ale není doložen a přesně popsán proces při řešení uplatňování práv subjektů údajů dle čl. 15 až 22 nařízení (EU) 2016/679.

Zabezpečení zpracování

A) Pro období od 1. února 2021 do 25. března 2021, kdy se kontrolovaná osoba nacházela v pozici správce osobních údajů (viz kontrolní zjištění č. 1.1)

Vzhledem k zaměření kontroly kontrolující v *Oznámení o zahájení kontroly* doručeném kontrolované osobě 1. února 2021 (viz bod č. 13, str. 2 přehledu podkladů) požádali kontrolovanou osobu o sdělení technických a organizačních opatření pro zabezpečení zpracovávaných osobních údajů v rámci Centrálního rezervačního systému pro očkování proti COVID-19 na internetové doméně [redacted].

Kontrolovaná osoba v rámci *Odpovědi na Oznámení o zahájení kontroly ze dne 29. ledna 2021* (viz bod č. 18, str. 4 přehledu podkladů) poskytla 10. února 2021 následující odpověď:

[7] Pokud správce provádí automatizované rozhodování dle výjimky čl. 22 bod 3 nařízení (EU) 2016/679, musí plnit vůči subjektům údajů mimo jiné i informační povinnost správce dle čl. 13 odst. 2 písm. f) nebo čl. 14 odst. 2 písm. g) nařízení (EU) 2016/679.

„Bezpečnostní dokumentace, výsledky penetračních a zátěžových testů a další technická dokumentace byla poskytnuta správci, z důvodu kybernetické bezpečnosti tyto dokumenty nezasíláme. V případě požadavku o doložení žádáme o zajištění souhlasu ze strany správce. Daná dokumentace může být z bezpečnostních důvodů poskytnuta pouze pro nahlédnutí a nemůže být zasílána jakoukoliv formou."

Kontrolující vzhledem ke skutečnostem popsaným v kontrolním zjištění č. 1.1 ve *Výzvě k doplnění podkladů* (viz bod č. 21, str. 1 přehledu podkladů) doručené kontrolované osobě 26. února 2021 znovu požádali kontrolovanou osobu o sdělení technických a organizačních opatření pro zabezpečení zpracovávaných osobních údajů, která v rámci *Odpovědi k Výzvě k doplnění podkladů ze dne 26. února 2021* (viz bod č. 23.1, str. 2 přehledu podkladů) sdělila 4. března 2021 následující:

„Jak jsme již uvedli v původní odpovědi, jedná se o neveřejné dokumenty, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Uvedené dokumenty, mimo jiné, obsahují např. výsledky penetračních a zátěžových testů. V souladu s interními předpisy a s ohledem na klasifikaci předmětných dokumentů a v návaznosti na výše uvedené nemůže být dokumentace zasílána jakoukoliv formou. Uvedená dokumentace může být poskytnuta pouze pro nahlédnutí v prostorách společnosti.

Z obecného hlediska sdělujeme, že mimo jiné máme aktuálně zpracovány tyto dokumenty:

- Výsledky penetračních testů
- Výsledky zátěžových testů
- Komplexní bezpečnostní dokumentaci
- Interní bezpečnostní procesy
- A další".

S odkazem na kontrolní zjištění č. 1.1 kontrolující uvádějí, že v době do 25. března 2021 nebyly kontrolovanou osobou, jakožto správcem osobních údajů, dostatečně doloženy informace a podklady, které by s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob prokazovaly provedení vhodných technických a organizačních opatření k zajištění úrovně zabezpečení odpovídající danému riziku dle čl. 32 odst. 1 nařízení (EU) 2016/679.

B) Pro období od 26. března 2021 do data vyhotovení kontrolního protokolu, kdy se kontrolovaná osoba nacházela v pozici dalšího zpracovatele osobních údajů (viz kontrolní zjištění č. 1.2)

V rámci *Odpovědi Ministerstva zdravotnictví ČR* (viz bod č. 17, str. 7-11 přehledu podkladů) ze 10. února 2021 bylo ze strany MZ sděleno a doloženo opatření – odstranění funkcionality zobrazení čísla pojištěnce v URL, zastavení sdílení dat se zpracovatelem Google a výmaz ze serverů Google Analytics (viz též *Ohlášení porušení zabezpečení osobních údajů dle GDPR*, bod 9 přehledu podkladů vč. přílohy 9.1). MZ dle svého vyjádření vzneslo požadavek k okamžitému zastavení předávání čísla pojištěnce v URL rezervace do informačního systému kontrolované osoby a zakázání příjmu těchto dat na straně kontrolované osoby, jakožto dalšího

zpracovatele. MZ dále uvedlo, že rovněž vzneslo požadavek na službu Google Analytics o výmaz zaslaných dat (žádost, odpověď a záznam o smazání byly doloženy přiloženými snímky obrazovky a ověřeny kontrolujícími) a dále nechalo vymazat informace v souborech s logy (včetně záloh) obsahující číslo pojištěnce a PIN2. Pro zabránění sdílení dat v budoucnu (např. při uložení původní URL v oblíbených položkách či úmyslném pokusu) provedla kontrolovaná osoba následující opatření při volání dopadové stránky [redacted] s parametrem [redacted] (číslo pojištěnce) v [redacted]:

„a. [redacted]

b. Při zjištění URL adresy s parametrem CPOJ není volána vůbec služba Google Analytics

c. Dojde k přesměrování na dopadovou stránku [redacted] bez uvedených parametrů v URL“.

MZ poté tento bezpečnostní incident ohlásilo Úřadu (viz bod 9 přehledu podkladů vč. přílohy 9.1). Dále bylo ze strany MZ sděleno, že data nebyla před vymazáním volně uložena ve veřejném úložišti a dle prošetření ze strany MZ nedošlo k jejich zneužití, přičemž data v URL byla chráněna protokolem HTTPS[8]. K výmazu dat společností Google došlo k 16. lednu 2021 (doloženo přiloženým snímkem obrazovky).

V *Záznamu o činnostech zpracování (2/2021)* (viz bod č. 17.2, str. 5-6 přehledu podkladů) MZ uvádí, že data vztahující se k předmětu kontroly jsou uložena v České republice. [redacted]

Smlouva o poskytování softwarových a odborných služeb uzavřená 8. října 2020 mezi NAKIT a kontrolovanou osobou (viz bod č. 20.3, str. 3, 9-16 přehledu podkladů) ukládá kontrolované osobě povinnosti v souvislosti se zabezpečením osobních údajů.

Dle čl. 2, A2) bod 3 kontrolovaná osoba zajistí, že přístupové údaje budou uchovávány v tajnosti. Čl. 2, A2) bod 5 stanoví, že kontrolovaná osoba bude pravidelně provádět zálohu dat. Čl. 6, A, bod 1 zavazuje kontrolovanou osobu k mlčenlivosti o skutečnostech a informacích při plnění smlouvy, a to až do doby, kdy se stanou obecně známými, přičemž dle čl. 6, A, bodu 7 povinnost mlčenlivosti trvá bez ohledu na ukončení platnosti smlouvy. Dle čl. 6, A, bodu 9 pak při zpracování údajů podléhajících režimu zvláštní ochrany dle nařízení (EU) 2016/679 a zákona č. 110/2019 Sb. budou smluvní strany dodržovat důvěrnost a tajnost těchto údajů.

Čl. 6, B, body 1-4 stanoví požadavky na kybernetickou bezpečnost. Informační systém provozovaný na základě této smlouvy musí splňovat bezpečnostní požadavky, které jsou aplikovány při provozu významných informačních systémů dle zákona č. 181/2014 Sb.,

[8] Bezpečná verze protokolu http, který používá protokol SSL/TLS protokol pro šifrování a autentizaci.

[9] [redacted]

[10] [redacted] *a* [redacted]

[11] [redacted]

[12] [redacted]

o kybernetické bezpečnosti a o změně souvisejících zákonů, a kontrolovaná osoba se stává významným dodavatelem ve smyslu tohoto zákona. Dále musí kontrolovaná osoba dodržovat bezpečnostní opatření stanovená vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, a to minimálně po dobu platnosti smlouvy. Dále je zde odkázáno na přílohu č. 5 této smlouvy, která mj. stanoví, že všechny úspěšné i neúspěšné přístupy ke službě provozované na základě této smlouvy musí být logovány a neúspěšné pokusy monitorovány s odpovídají akcí v případě vícero neúspěšných pokusů. Veškeré změny dat musí být logovány tak, aby bylo možné zjistit kdo, kdy, jak a která data modifikoval. U smazaných záznamů nesmí dojít k trvalému odstranění dat, ale pouze k logickému zneplatnění záznamu, přičemž musí být zřejmé, kdo, kdy a v jakém stavu záznam logicky zneplatnil.

Dle čl. 6, C, bod 6 musí kontrolovaná osoba dodržovat povinnosti týkající se ochrany osobních údajů po dobu účinnosti smlouvy, pokud není stanoveno jinak. Dle čl. 6, C, bodu 14 nesmí kontrolovaná osoba obdržené osobní údaje ukládat, kopírovat tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud to není nezbytné pro plnění povinností dle smlouvy. Čl. 16 pak umožňuje NAKIT na vyžádání provést kontrolu dodržování povinností týkající se povinností v čl. 6., zejména se jedná o přístup do prostor, kde jsou osobní údaje uchovávány, a předložení seznamu osob, které mají přístup k osobním údajům.

Čl. 6, C, body 16-25 pak stanovují záruky technického a organizačního zabezpečení osobních údajů subjektů údajů. Kontrolovaná osoba je zejména povinna zavést vhodná technická a organizační opatření splňující požadavky nařízení (EU) 2016/679. Nesmí dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničeni či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování. Přístup k osobním údajům bude umožněn výlučně pověřeným osobám povinným dodržovat mlčenlivost. Zpracování musí probíhat pouze za podmínek a v rozsahu stanoveném smlouvou a nařízením (EU) 2016/679. Osobní údaje budou uchovávány pouze na zabezpečených serverech nebo na zabezpečených nosičích dat. Jiné, než elektronické osobní údaje, budou uchovány v místnostech s náležitou úrovní zabezpečení, kam budou mít přístup jen pověřené osoby. Kontrolovaná osoba musí zpracovat a zdokumentovat přijatá a provedená technickoorganizační opatření. Musí uvést místa a prostředí zpracování, v případě předávání do třetích zemí musí být plněny podmínky dle čl. 44 a 46 nařízení (EU) 2016/679. V případě porušení těchto záruk musí být zajištěn odpovídající stav neprodleně, nejpozději do tří pracovních dnů poté, co je ze strany NAKIT vyzván. V případě automatizovaného zpracování musí být zajištěno, aby předmětné systémy byly přístupné pouze na základě zvláštních uživatelských oprávnění a pouze pověřenými osobami, přičemž musí být pořizovány a uchovávány elektronické záznamy a dále musí být zabráněno neoprávněnému přístupu k datovým nosičům. Kontrolovaná osoba musí zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, obnovit dostupnost osobních údajů v případě fyzických či technických incidentů a pravidelně testovat, posuzovat a hodnotit účinnost zavedených opatření.

Dle čl. 6, C, bodů 26-32 pak musí kontrolovaná osoba nejpozději do 24 hodin oznámit NAKIT všechna porušeních zabezpečení osobních údajů dle čl. 33 a 34 nařízení (EU) 2016/679 s poskytnutím všech předepsaných informací. Dále musí být součinná při poskytování dodatečných informacím Úřadu. Pro případ porušení zabezpečení musí být vypracován plán, který NAKIT na vyžádání obdrží. Musí být vedena podrobná evidence všech případů porušení

zabezpečení v minimálním rozsahu stanoveném čl. 33 odst. 3 nařízení (EU) 2016/679 a na vyžádání předložena NAKIT.

Kontrolovaná osoba dále za účelem pověření dalšího, navazujícího zpracovatele osobních údajů uzavřela 25. srpna 2018 *Zpracovatelskou smlouvu č.* [redacted] se společností [redacted], [redacted], [redacted] – [redacted], [redacted]: [redacted] (viz bod č. 23, str. 3-4 přehledu podkladů). Čl. 6 této smlouvy se zabývá zabezpečením osobních údajů. Je zde stanoveno přijetí a udržování opatření k zabezpečení osobních údajů, které splňují požadavky čl. 32 nařízení (EU) 2016/679. Technická a organizační opatření musí zamezit neoprávněnému nebo nahodilému přístupu k osobním údajům, neoprávněné změně, zničení, ztrátě, zpracování či zneužití. Musí být předcházeno porušení zabezpečení osobních údajů, pokud k němu dojde, pak musí být do 48 hodin oznámeno kontrolované osobě.

Na základě výše uvedených důkazů o nápravě porušení zabezpečení osobních údajů, s přihlédnutím k šíři informací dostupných z výše uvedených dokumentů a k nepříznivé pandemické situaci kontrolující neprovedli ústní jednání a místní šetření v sídle kontrolované osoby, která s odkazem na zákon č. 181/2014 Sb., o kybernetické bezpečnosti, odmítla některé další dokumenty zpřístupnit formou jinou než osobním nahlédnutím (viz body č. 18, str. 4 a 23.1, str. 2 přehledu podkladů).

Kontrolující uzavírají, že od 26. března 2021 vzhledem k předmětu kontroly kontrolovaná osoba plní jako zpracovatel v součinnosti se správcem a dalšími zpracovateli povinnosti stanovené čl. 32 odst. 1 nařízení (EU) 2016/679 týkající se technických a organizačních opatření při zpracování osobních údajů.

Ohlášení porušení zabezpečení osobních údajů

Dne 18. ledna 2021 bylo Úřadu doručeno *Ohlášení porušení zabezpečení osobních údajů dle GDPR* (viz bod 9 přehledu podkladů vč. přílohy 9.1). Jako správce, u něhož došlo k porušení zabezpečení, je zde uvedeno Ministerstvo zdravotnictví, zpracovatelem pak dle údajů uvedených ve formuláři NAKIT. [redacted]. [redacted]. [redacted] [redacted].

Příčinou porušení měla být: [redacted], *která umožnila zobrazení čísla pojištěnce a jeho následný přenos do systému Google Analytics (dalšího zpracovatele) a sdílení se společností Google za účelem zlepšování služeb https://support.google.com/analytics/answer/3379636. Podle předběžných odhadů se jednalo o cca 80 tis. čísel. Data v URL byla chráněna HTTPS (Hypertext Transfer Protocol Secure)[13] jedná se o protokol, který umožňuje zabezpečenou komunikaci v počítačové síti".*

MZ zjistilo, že došlo k porušení důvěrnosti dat (neoprávněné nebo náhodné poskytnutí nebo zpřístupnění osobních údajů), přičemž dotčenými osobními údaji tedy byla čísla pojištěnců uživatelů rezervačního systému.

[13] Bezpečná verze protokolu http, který používá protokol SSL/TLS protokol pro šifrování a autentizaci.

Počet dotčených subjektů údajů a záznamů osobních údajů dle MZ nelze přesně určit, MZ uvádí, že se nemělo jednat o reálný útok, ale hrozbu, přičemž data mohla být spojena s dalšími informacemi. V rámci ohlášení porušení zabezpečení osobních údajů (viz bod 9 přehledu podkladů), jak je uvedeno výše, tak MZ uvedlo pouze přibližný počet čísel pojištěnce (rodných čísel), kterých se porušení týkalo, a to je 80 tisíc.

Před vznikem porušení zabezpečení MZ dle svého vyjádření (viz bod 17 přehledu podkladů) zavedlo opatření, mezi něž patřily vnitřní předpisy, závazné politiky správy a zabezpečení dat a informací. Dalšími opatřeními měly být: „Posouzení vlivu na ochranu osobních údajů dle čl. 35 Obecného nařízení, předchozí konzultace s dozorovým orgánem dle čl. 36 Obecného nařízení, zapojení zpracovatelů a dalších zpracovatelů je řádně smluvně upraveno dle čl. 28 Obecného nařízení, zabezpečení řešeno v souladu se standardy kybernetické bezpečnosti“. Osobní údaje byly, jak uvedlo MZ, zpracovávány prostředky [redacted].

K danému kontrolující poznamenávají, jak je uvedeno výše a vyplývá především z výsledků této kontroly, tvrzení MZ týkající se smluvního upravení zpracovatelů v souladu se čl. 28 nařízení (EU) 2016/679 je nepodložené, neboť ke smluvnímu uspořádání vztahů správce MZ a zpracovatelů NAKIT a kontrolované osoby došlo až na základě neustálých urgencí ze strany kontrolujících spočívajících ve vyžadování dodatků smluv, které smluvně pokrývají i předmět kontroly. Posouzení vlivu, které bylo MZ předloženo, je rovněž posouzeno ze strany kontrolujících jako nedostatečné. Informaci o předchozí konzultaci s dozorovým orgánem dle čl. 36 nařízení (EU) 2016/679 kontrolující ověřili se závěrem, že MZ o konzultaci ve skutečnosti nepožádalo, a tak mu ani nemohla být poskytnuta.

Dle MZ poté bylo přijato následující opatření: „Odstranění funkcionality zobrazení čísla pojištěnce v URL. Zastavení sdílení dat se zpracovatelem Google pro účely zlepšování služeb. Výmaz dat ze serverů Google Analytics (všechna přenesená data smazána)“.

V ohlášení byly dále uvedeny následující informace: [redacted]

Z výše uvedeného je zřejmé, že ohlášení případu porušení zabezpečení osobních údajů bylo Úřadu ohlášeno MZ, nikoliv kontrolovanou osobou, která je v textu zmíněna pouze jedenkrát, v informacích o prostředcích zpracování.

Jak je však uvedeno v kontrolním zjištění č. 1, kontrolovaná osoba se až do 25. března 2021 nacházela vzhledem k předmětu kontroly v postavení správce osobních údajů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679 a měla tedy povinnost dle čl. 33 odst. 1 nařízení (EU) 2016/679 bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se dozvěděla o jakémkoli porušení zabezpečení osobních údajů, ohlásit toto Úřadu, ledaže by bylo nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických

osob. Kontrolovaná osoba porušení neohlásila (vč. povinné informace příčiny zpoždění přes lhůtu 72 hodin).

Záznamy o činnostech zpracování

Dle čl. 30 nařízení (EU) 2016/679 mají správce i zpracovatel či jejich případní zástupci povinnost vést záznamy o zpracování osobních údajů, za které odpovídají, a dokumentovat tak důležité skutečnosti, které se ke zpracování osobních údajů vztahují. Záznamy musejí být vyhotovovány písemně, přičemž za písemnou formu se považuje i forma elektronická.

Kontrolovaná osoba ve své *Odpovědi na Oznámení o zahájení kontroly* (viz bod 18 přehledu podkladů) uvedla, že se nachází v postavení dalšího zpracovatele, přičemž záznamy o činnostech zpracování má správce osobních údajů, tj. Ministerstvo zdravotnictví.
Jak bylo zjištěno výše, kontrolovaná osoba se od 1. února2021 do 25. března 2021 nacházela v postavení správce osobních údajů a od data 26. března 2021 se nachází v postavení dalšího zpracovatele pro správce MZ, prostřednictvím zpracovatele NAKIT. Bez ohledu na postavení kontrolované osoby se na zpracování osobních údajů, které bylo v rámci této kontroly prověřováno, vztahuje povinnost vést záznamy o zpracování definovaná v čl. 30 nařízení (EU) 2016/679, kdy v odst. 1 či odst. 2 jsou přímo definovány povinné údaje těchto záznamů, a to podle postavení daného subjektu.
Kontrolující mají za to, že zpracování, které kontrolovaná osoba provádí, není příležitostné a vzhledem k jeho rozsáhlosti kontrolovaná osoba byla a je povinna vést záznamy o činnostech zpracování, a to pro obě fáze, tedy i pro období, kdy se nacházela v postavení správce, tak pro období, kdy se nachází v postavení dalšího zpracovatele (zpracovatele).

Ministerstvo zdravotnictví ve své *Odpovědi* ze dne 10. února 2021 (viz bod 17 přehledu podkladů), jako přílohu přiložilo *Záznamy o činnostech zpracování 2/2021,* vztahující se na *Centrální rezervační systém na očkování (Registrace a Rezervace)*, kde je kontrolovaná osoba uvedená v části „*Další zpracovatelé*“. Uvedené záznamy o činnostech zpracování jsou široce pojaty pro ne příliš jednoznačně určený účel, za situace, kdy v účelu ve smyslu čl. 30 odst. 1 písm. b) nařízení (EU) 2016/679 má být uveden přesný účel zpracování, jako je např. zajištění rezervací či zajištění registrací apod., zatímco správce MZ uvádí: *„Účelem IT podpory očkování je zabezpečit podporu procesů a provoz řídících a koordinačních struktur, a subjektů participujících na procesu očkování“.*
Z pohledu povinností kontrolované osoby nelze tyto záznamy o činnostech zpracování pokládat za splnění povinnosti „vést záznamy“ a to především z důvodu absence některých povinných náležitostí, jako jsou kategorie zpracování prováděného pro každého ze správců či informace o předání údajů do třetí země a doložení vhodných záruk.

Kontrolující konstatují, že kontrolovaná osoba v době od 1. února do 25. března 2021, kdy se nacházela v postavení správce osobních údajů vůči předmětu kontroly, nevedla záznamy o činnostech zpracování a záznamy o činnostech zpracování podle čl. 30 a pro období od 26. března 2021 záznamy, které byly kontrolujícím předloženy, neobsahují všechny náležitosti a informace, stanovené taxativním výčtem.

Posouzení vlivu na ochranu osobních údajů

V období do 25. března 2021, kdy se kontrolovaná osoba nacházela v postavení správce osobních údajů pro zpracování údajů zájemců o očkování COVID-19 v rámci jím provozovaného rezervačního systému, kontrolovaná dle názoru kontrolujících nezvážila závažnost zpracování, a to vzhledem k rozsáhlému, systematickému zpracování, které je částečně založeno na automatizovaném zpracování a na němž se zakládala rozhodnutí týkající se každého z dotčených subjektů údajů (například přednosti při očkování), povahu, rozsah, kontext a účel zpracování, a následkem toho nevypracovala posouzení vlivu na ochranu osobních údajů**,** jak jí to v těchto případech ukládá čl. 35 nařízení (EU) 2016/679. Kontrolující poznamenávají, že zpracování osobních údajů navazovalo na vývoj krizové situace v České republice spojené s výskytem nemoci SARS-CoV-2 a následné rozhodnutí o plošném očkování obyvatelstva a vzhledem k citlivosti a závažnosti situace mělo být, dle zvážení kontrolujících, vypracováno posouzení vlivu.

Kontrolujícím bylo sice v rámci vyjádření MZ z 10. února 2021 (viz bod 17 přehledu podkladů, příloha 17.1.) předloženo *Posouzení vlivu na ochranu osobních údajů DATA PROTECTION IMPACT ASSESMENT (DPIA) Projekt: IT podpora OČKOVÁNÍ*, ze dne 10. února 2021 (dále jen „Posouzení vlivu"), vypracované správcem osobních údajů Ministerstvem zdravotnictví, přičemž v tomto posouzení je kontrolovaná osoba uvedená v pozici dalšího zpracovatele, avšak toto posouzení na činnosti kontrolované osoby nelze aplikovat dříve, než v období od 26. března 2021, kdy tento zpracovatelský vztah reálně vznikl.

Pokud se týká posouzení vlivu, které předložilo MZ (viz příloha 17.1 bodu 17 přehledu podkladů) a které se vztahuje na činnosti kontrolované osoby v období od 26. března 2021, kdy se kontrolovaná osoba již nachází v postavení zpracovatele (dalšího zpracovatele) osobních údajů, musí kontrolující konstatovat, že posouzení vlivu je nedostatečné a neplní podmínky nařízení (EU) 2016/679.

K tomu závěru kontrolující došli porovnáním předloženého Posouzení vlivu (viz bod 17 přehledu podkladů, příloha 17.1.) s reálným zpracováním dle výše uvedených zjištěných skutečností a dále posoudili jeho obsah, přičemž došli ke zjištění značných nesrovnalostí a nedostatečností, například:

- v bodu *6.4 Doba uložení* není jasně a srozumitelně stanovena lhůta pro uložení (především vzhledem k možným zásahům ze strany jednotlivých odběrových míst) a absentuje zdůvodnění této lhůty;
- v bodu *6.5 Cookies* je uvedeno, že v rámci registračního procesu nejsou v aplikaci pro registraci vkládány žádné cookies, krom systémových cookies, přičemž výše uvedené závěry šetření užitých cookies tomu neodpovídají;
- v bodu *6.6 Využití Google Analytics* je uvedeno, že v URL není sbíráno rodné číslo, přičemž ze samotného ohlášení porušení zabezpečení (viz bod 9 přehledu podkladů) vyplývá, že k tomuto zpracování došlo a rovněž je prokázáno, že rodné číslo bylo předáváno do USA;
- v posouzení absentuje rozdělení míry ingerence a odpovědnosti správce a zpracovatelů pro jednotlivé části zpracování;
- v části *c Centrální rezervační systém (CRS)* absentuje popis operací zpracování a přesná specifikace osob, které zpracování mají provádět, a to i s dopadem na jednotlivé pozice správce – zpracovatel – další zpracovatel a další osud zpracovávaných osobních údajů, tj. jejich předávání apod.; v případě kontrolované osoby je to absence

informace o rozsahu a způsobu předávání osobních údajů z Centrálního rezervačního systému kontrolované osoby, která je odpovědná za vytvoření termínu pro očkování;
- nedostatečný způsob prokázání souhlasu se zpracováním a možnosti jeho odvolání.

Pověřenec pro ochranu osobních údajů

V období do 25. března 2021 byla kontrolovaná osoba v postavení správce osobních údajů, jak je popsáno výše. V této době zpracovávala osobní údaje zájemců o očkování proti nemoci COVID-19, a to prostřednictvím vlastních stránek a vlastní aplikace.

Vzhledem k tomu, že se dané zpracování týkalo potenciálně všech občanů České republiky starších 18 let, bylo technologicky i obsahově navázáno na další zpracování prováděná orgány veřejné moci a veřejnými subjekty (jak je uvedeno v úvodní části bodu *III. Kontrolní zjištění*) a vzhledem k delegaci výkonu činnosti veřejného subjektu na kontrolovanou osobu v období od 26. března 2021, a to tak, že tato zpracování prováděná kontrolovanou osobou jednak předcházela a také na ně navazovala a sběr dat byl prakticky prováděn pro celé území státu, a to souběžně s technologicky totožným zpracováním zajišťujícím rezervaci termínů očkování proti onemocnění COVID-19, které provádí jako rezervace termínů antigenního testování onemocnění COVID-19 nebo rezervace termínů na lékařské ošetření pro další poskytovatele zdravotních služeb, jak je zřejmé z jejích webových stránek (viz bod 29 přehledu podkladů), vznikla kontrolované osobě povinnost jmenovat pověřence pro ochranu osobních údajů ve smyslu čl. 37 odst. 1 písm. a) nařízení (EU) 2016/679, neboť do takového zpracování je vždy zapojen, tj. podílí se na něm, veřejný subjekt.

Jak je patrné z podkladů, kdy kontrolovaná osoba v rámci svých odpovědí odkazovala na stránky MZ a jejich pověřence a současně vzhledem ke skutečnosti, že o případném pověřenci pro ochranu osobních údajů není možné nalézt jakékoli informace na webových stránkách kontrolované osoby a kontrolovaná osoba nesdělila informace požadované v čl. 37 odst. 7 nařízení (EU) 2016/679 Úřadu, mají kontrolující za zřejmé, že kontrolovaná pověřence nejmenovala.

Souhrnem výše uvedeného kontrolující konstatují, že:

Kontrolní zjištění č. 1:

1.1. V období do 25. března 2021 se k předmětu kontroly, tedy zpracování osobních údajů při provozování internetového portálu zaměřeného na rezervaci termínů očkování proti onemocnění COVID-19, kontrolovaná osoba nacházela v postavení správce osobních údajů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679.

1.2. V době od 26. března 2021 se k předmětu kontroly kontrolovaná nachází v postavení dalšího zpracovatele (v rámci řetězení zpracovatelů) pro správce, Ministerstvo zdravotnictví ČR, prostřednictvím zpracovatele, Národní agentury pro komunikační a informační technologie, ve smyslu čl. 4 bodu 8) a smlouva uzavřená mezi Národní agenturou pro komunikační a informační technologie a kontrolovanou osobou má všechny náležitosti smlouvy ve smyslu čl. 28, odst. 3 a 4 nařízení (EU) 2016/679.

1.3. Osobní údaje, které kontrolovaná zpracovává ve smyslu čl. 4 odst. 2 nařízení (EU) 2016/679, jsou osobními údaji ve smyslu čl. 4 odst. 1 nařízení (EU) 2016/679 a zpracování odpovídá definici dle čl. 4 odst. 2 tohoto nařízení.

Kontrolní zjištění č. 2:

2.1. Kontrolovaná osoba porušila podmínku stanovenou čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679, kdy v období od 1. února do 25. března 2021 zpracovávala osobní údaje v rozsahu jméno, příjmení, adresa trvalého pobytu, číslo pojištěnce – rodné číslo, číslo pojišťovny, vybrané očkovací místo, telefon event. E-mail a IP adresu (tj. včetně údajů získaných skrze cookies) na základě tohoto právního titulu nezákonným způsobem, neboť nebyl doložen souhlas se zpracováním osobních údajů, který by splňoval podmínku dle čl. 7 nařízení (EU) 2016/679. V důsledku toho byly zpracovávány osobní údaje, v daném období, bez právního titulu.

Kontrolní zjištění č. 3:

3.1. V období od 1. února 2021 do 25. března 2021 kontrolovaná osoba, jako správce osobních údajů, porušovala čl. 12-22 nařízení (EU) 2016/679 tím, že neplnila informační povinnost ve smyslu těchto ustanovení a neměla nastaveny procesy pro výkon práv subjektů údajů dle čl. 15 až 22 nařízení (EU) 2016/679.

3.2. V období od 26. března 2021 do dne vyhotovení protokolu kontrolovaná osoba, jako zpracovatel osobních údajů, plnila informační povinnost dle čl. 12-22 nařízení (EU) 2016/679 prostřednictvím správce, tj. Ministerstva zdravotnictví České republiky, vůči kterému je v postavení dalšího zpracovatele (srov. kontrolní zjištění č. 1.2).

3.3 V období od 26. března 2021 do dne vyhotovení protokolu kontrolovaná osoba, jako zpracovatel osobních údajů, neplnila práva subjektů údajů dle čl. 15 až 22 nařízení (EU) 2016/679; subjekty jsou sice informováni o svých právech, ale není doložen a přesně popsán proces při řešení uplatňování práv subjektů údajů dle čl. 15 až 22 nařízení (EU) 2016/679.

Kontrolní zjištění č. 4:

4.1 Kontrolovaná porušila článek 32 odst. 1 nařízení (EU) 2016/679, protože k období do 25. března 2021, kdy se nacházela v postavení správce osobních údajů pro rezervační systém rezervací očkování proti nemoci COVID-19, neprokázala provedení vhodných technických a organizačních opatření dle tohoto ustanovení.

4.2 V období od 26. března 2021 do dne vyhotovení protokolu kontrolovaná osoba, jako zpracovatel osobních údajů, plnila povinnosti týkající se technického a organizačního zabezpečení zpracování osobních údajů dle článku 32 odst.1 nařízení (EU) 2016/679 v součinnosti se správcem, tj. Ministerstvem zdravotnictví České republiky, a dalšími zpracovateli osobních údajů zapojenými do zpracování v rozsahu kontroly.

Kontrolní zjištění č. 5:

5.1. Kontrolovaná porušila článek 33 odst. 1 nařízení (EU) 2016/679, protože neohlásila Úřadu porušení zabezpečení osobních údajů ze dne 15. ledna 2021, které se uskutečnilo

v období do 25. března 2021, kdy se nacházela v postavení správce osobních údajů pro rezervační systém rezervací očkování proti nemoci COVID-19.

Kontrolní zjištění č. 6:

6.1. Kontrolovaná porušila článek 30 nařízení 2016/679, neboť nedoložila řádné záznamy o činnostech zpracování, které by odpovídaly požadavkům tohoto článku a v některých případech (pro období od 1. února 2021 do 25. března 2021) nedoložila žádné záznamy o činnostech zpracování.

Kontrolní zjištění č. 7:

7.1. Kontrolovaná porušila článek 35 nařízení (EU) 2016/679, protože v období do 25. března 2021, kdy se nacházela v postavení správce osobních údajů pro rezervační systém rezervací očkování proti nemoci COVID-19, ač prováděla rozsáhlé zpracování naplňující podmínky článku 35 odst. 1 a odst. 2 písm. a), pro předmětné zpracování nevypracovala posouzení vlivu na ochranu osobních údajů.

7.2. Posouzení vlivu předložené MZ, které se vztahuje na zpracování osobních údajů kontrolované osoby v období od 26. března 2021, není vypracováno v souladu se článkem 35 nařízení (EU) 2016/679.

Kontrolní zjištění 8:

8.1. Kontrolovaná porušila článek 37 nařízení (EU) 2016/679, protože v období do 25. března 2021, kdy se nacházela v postavení správce osobních údajů pro rezervační systém rezervací očkování proti nemoci COVID-19, ač prováděla rozsáhlé zpracování naplňující podmínky článku 37 odst. 1 písm. a), pro předmětné období nejmenovala pověřence pro ochranu osobních údajů.

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
Josef Polák	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Mgr. Barbora Šnajderová	pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis