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-00490/21-49
Praha 9. února 2022

Protokol o kontrole

Kontrolní orgán:

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

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „nařízení (EU) 2016/679“) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

Mgr. et Mgr. Božena Čajková (vedoucí kontrolní skupiny) jako vrchní rada odboru dozoru pověřená na základě pověření ke kontrole ze dne 1. září 2021

Bc. Hana Imiolková – pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze dne 1. září 2021;

Mgr. Zuzana Jeřábková – pověřená zaměstnankyně Úřadu, č. průkazu: [redacted], na základě pověření ke kontrole ze dne 1. září 2021;

Ing. David Mrňák, DiS – pověřený zaměstnanec Úřadu, č. průkazu: [redacted], pověření ke kontrole ze dne 1. září 2021 (protokol o kontrole není pověřeným zaměstnancem podepsán pro dlouhodobou nepřítomnost);

Bc. Jaromír Kuba – soudní znalec v oboru kybernetika, odvětví výpočetní technika, specializace informační technologie, informatika a telekomunikace, pověření ke kontrole ze dne 1. září 2021.

Kontrolovaná osoba:

Ministerstvo zdravotnictví České republiky, se sídlem Palackého náměstí 375/4, 128 01 Praha 2 – Nové Město, IČO: 00024341,
(dále také „kontrolovaná osoba“, „MZ“ nebo „Ministerstvo zdravotnictví ČR“)
zastoupená Mgr. Robertem Vávrou, DiS., pověřencem pro ochranu osobních údajů.

Předmět kontroly:

Předmětem kontroly je dodržování povinností MZ při zpracování osobních údajů subjektu údajů v souvislosti s elektronickým certifikátem EU COVID-19, zpřístupněném na očkovacím portálu https://ocko.uzis.cz/, včetně aplikací „Tečka“ a „čTečka“, a to zejména kontrola plnění povinností podle čl. 5, 6, 12-14, 15-21 a čl. 32 nařízení (EU) 2016/679.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-00490/21-19, ze dne 10. září 2021.

Poslední kontrolní úkon:

Úřední záznam o pořízení dokumentace čj. UOOU-00490/21-48, ze dne 31. ledna 2022.

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. Oznámení o zahájení kontroly ze dne 10. září 2021, čj. UOOU-00490/21-19, počet stran 2;
   1.1. Příloha – pověření ke kontrole, počet stran 1;
2. Podnět č. 1 ze dne 22. ledna 2021, čj. UOOU-00490/21-1, počet stran 1;
3. Vyjádření ÚZIS (reakce na podnět č. 1 ze dne 22. ledna 2021, čj. UOOU-00490/21-1) ze dne 22. ledna 2021, čj. UOOU-00490/21-2, počet stran 2;
4. Vyjádření ÚZIS (reakce na žádost o součinnost) ze dne 18. května 2021, čj. UOOU-00490/21-6, počet stran 3;
5. Podnět č. 2 ze dne 16. dubna 2021, čj. UOOU-01958/21-1, počet stran 1;
6. Podnět č. 3 ze dne 4. května 2021, čj. UOOU-02354/21-1, počet stran 2;
   6.1. Příloha – aktuální stránka, která se zobrazí po otevření odkazu načteného z QR code;
7. Vyjádření kontrolované osoby ze dne 30. července 2021, čj. UOOU-00490/21-14, počet stran 9;
   7.1. Příloha – ISIN Dotazník zpracování osobních údajů CHK 2. 0., počet stran 7;
   7.2. Příloha – DPIA – Projekt: IT podpora OČKOVÁNÍ, počet stran 40;
      7.2.1. Metodický pokyn pro očkovací kampaň Plán provedení (1_DPIA_Metodický_pokyn_pro_očkovací_kampaň_Plán_provedení), počet stran 10;

7.2.2. Dodatek 1 Přílohy 1 – Prioritizace cílových skupin (2_DPIA_Dodatek_1_Přílohy_1_Prioritizace_cílových_skupin), počet stran 3;
7.2.3. Dodatek 1 Přílohy 2 – Metodika práce v CFA (3_DPIA_Dodatek_1_Přílohy_2_Metodika_práce_v_CFA), počet stran 3;
7.2.4. Dodatek 1 Přílohy 4 – Očkovací modul OČKO (4_DPIA_Dodatek_1_Přílohy_4_Očkovací_modul_OČKO), počet stran 11;
7.2.5. Dodatek 1 Přílohy 5 – Komunikační schéma Centrálního komunikační (5_DPIA_Dodatek_1_Přílohy_5_Komunikační_schéma_Centrálního_komunikační), počet stran 1;
7.2.6. Dodatek 2 Přílohy 1 – Organizace očkování 1 (6_DPIA_Dodatek_2_Přílohy_1_Organizace_očkování_1), počet stran 19;
7.2.7. Dodatek 2 Přílohy 4 – Informační podpora očkovacích míst (7_DPIA_Dodatek_2_Přílohy_4_Informační_podpora_očkovacích_míst) počet stran 9;
7.2.8. Dodatek 3 Přílohy 1 – Pokyn k vedení zdravotnické dokumentace (8_DPIA_Dodatek_3_Přílohy_1_Pokyn_k_vedení_zdravotnické_dokumentace), počet stran 3;
7.2.9. Dotazník před očkováním proti COVID 19 (9_DPIA_Dotazník_před_očkováním_proti_COVID_19), počet stran 1;
7.2.10. Dotazník před očkováním proti onemocnění COVID 19 pro nezletilé (10_DPIA_Dotazník_před_očkováním_proti_onemocnění_COVID_19_pro_nezletilé_), počet stran 1;
7.2.11. Příloha 1 – Popis procesu očkování (11_DPIA_Příloha_1_Popis_procesu_očkování), počet stran 10;
7.2.12. Příloha 2 – Logistické zabezpečení (12_DPIA_Příloha_2_Logistické_zabezpečení), počet stran 11;
7.2.13. Příloha 3 – Finanční zabezpečení 13_DPIA_Příloha_3_Finanční_zabezpečení), počet stran 6;
7.2.14. Příloha 4 – IT podpora (14_DPIA_Příloha_4_IT_podpora), počet stran 36;
7.2.15. Příloha 5 – Mediální a informační podpora (15_DPIA_Příloha_5_Mediální_a_informační_podpora), počet stran 5;
7.2.16. Vzor certifikátu (16_DPIA_Vzor_certifikátu), počet stran 4;

7.3. Příloha – Informační povinnost CRS očkování, počet stran 8;
7.4. Příloha – Popis systémů, procesů a zpracování [redacted], počet stran 70;

8. Podnět č. 4 ze dne 28. června 2021, čj. UOOU-03059/21-1, počet stran 1;
   8.1. Příloha – Certifikát o provedeném testu, počet stran 1;
9. Úřední záznam o úkonech předcházejících kontrole ze dne 19. srpna 2021, čj. UOOU-00490/21-17, počet stran 2;
   9.1. Příloha – výtisk internetové stránky Validační aplikace Tečka a čTečka – Aktuální informace o COVID-19, počet stran 2;
   9.2. Příloha – výtisk internetové stránky Nápověda pro aplikaci Tečka – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 17;
   9.3. Příloha – výtisk internetové stránky Nápověda pro aplikaci čTečka – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 10;

9.4. Příloha – výtisk internetové stránky Často kladené dotazy k aplikacím čTečka a Tečka – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 5;
9.5. Příloha – výtisk internetové stránky _Tečka v App Storu, počet stran 4;
9.6. Příloha – snímek obrazovky 1 [internetové stránky _Tečka v App Storu];
9.7. Příloha – snímek obrazovky 2 [internetové stránky _Tečka v App Storu];
9.8. Příloha – výtisk internetové stránky čTečka on the App Store, počet stran 3;
9.9. Příloha – snímek obrazovky 1 [internetové stránky čTečka on the App Store];
9.10. Příloha – snímek obrazovky 2 [internetové stránky čTečka on the App Store];
9.11. Příloha – výtisk internetové stránky Podmínky používání – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 3;
9.12. Příloha – výtisk internetové stránky Podmínky používání – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 4;
9.13. Příloha – výtisk internetové stránky Digitální COVID certifikáty – základní informace – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 4;
9.14. Příloha – výtisk internetové stránky Často kladené obecné dotazy k certifikátům a jejich obsahu – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 2;
9.15. Příloha – výtisk internetové stránky Často kladené dotazy k vystavení a platnosti Digitálních COVID certifikátů v ČR – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 2;
9.16. Příloha – výtisk internetové stránky Často kladené dotazy k ověřování certifikátů a osobním údajům – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 2;
9.17. Příloha – výtisk internetové stránky Často kladené dotazy k použití Digitálního COVID certifikátu při cestování – Portál nápovědy pro nástroje Chytré karantény a Očkovací portál občana, počet stran 2;
9.18. Příloha – snímek obrazovky app čtečka po stažení 1;
9.19. Příloha – snímek obrazovky app čtečka po stažení 2;
9.20. Příloha – snímek obrazovky app čtečka neplatný certifikát  ;
9.21. Příloha – snímek obrazovky app čtečka neplatný certifikát  ;
9.22. Příloha – snímek obrazovky app čtečka neplatný certifikát  ;
9.23. Příloha – snímek obrazovky app čtečka neplatný certifikát  ;
9.24. Příloha – snímek obrazovky app čtečka neplatný certifikát  ;
9.25. Příloha – snímek obrazovky app čtečka platný certifikát  ;
9.26. Příloha – snímek obrazovky app čtečka platný certifikát  ;
9.27. Příloha – snímek obrazovky app čtečka platný certifikát  ;

10. Úřední záznam o úkonech předcházejících kontrole ze dne 10. září 2021, čj. UOOU-00490/21-20, počet stran 1;
    10.1. Příloha – snímek obrazovky app Tečka – Novinka – Sdílení certifikátů s externími službami;
11. Protokol z ústního jednání a místního šetření ze dne 21. září 2021, čj. UOOU-00490/21-21, počet stran 6;
12. Vyjádření kontrolované osoby ze dne 4. listopadu 2021, čj. UOOU-00490/21-23, počet stran 9;

12.1. Příloha – Příloha č. 7 – Smlouvy se zpracovateli k očkovacímu portálu – Dodatek č. 1 k Rámcové smlouvě na poskytování služeb (Dodatek_č_1_ICZ_a_s_Služby_eREG_Z2017_029592_část_28_CUD), počet stran 17;
12.2. Příloha – Příloha č. 8 – Vzory certifikátů – Certifikát o provedeném testu (COVIDTestCertifikat_disease), počet stran 1;
12.3. Příloha – Příloha č. 8 – Vzory certifikátů – Certifikát o provedené vakcinaci (CZ_Vaccine), počet stran 1;
12.4. Příloha – Příloha č. 8 – Vzory certifikátů – Certifikát o prodělané nemoci (CZ_test_NAAT), počet stran 1;
12.5. Příloha – Příloha č. 9 – Dokument – „Politika systému řízení bezpečnosti informací MZČR“ (05_00_Politika_systému_řízení_bezpečnosti_informací_MZ_ČR), počet stran 7;

13. Vyjádření kontrolované osoby ze dne 4. listopadu 2021, čj. UOOU-00490/21-24, počet stran 9;
13.1. Příloha – Příloha č. 1 – Podklad pro jednání porady vedení „Realizace vakcinačního modulu“ (Realizace_vakcinačního_modulu_v_prostředí_rezortních_registrů_Ministerstva_zdravotnictví_Informačního_systému_infekčních_nemocí_a_centrálního_), počet stran 8;
13.2. Příloha – Příloha č. 2 – Zápis z porady vedení č. 48 ze dne 8. 12. 2020 (2020_48_zapis_Ockovani_v_ISIN_003_), počet stran 21;
13.3. Příloha – Příloha č. 3 – Zápis z porady vedení č. 50 ze dne 29.12. 2020 (2020_50_zápis), počet stran 14;
13.4. Příloha – Příloha č. 4 – Zřizovací listina ÚZIS (zrizovaci_listina), počet stran 6;
13.5. Příloha – Příloha č. 5 – Dokument-Informační povinnost k očkování (Informacni_povinnost_CRS_ockovani), počet stran 8;
13.6. Příloha – Vakcinace COVID-19
13.7. Příloha – Základní popis pro tvorbu vakcinačního modulu v Centrálním úložišti dat/ISIN (příloha_č1_analýza_Vakcinace_final_1_), počet stran 17;

14. Vyjádření kontrolované osoby ze dne 8. listopadu 2021, čj. UOOU-00490/21-25, počet stran 1;
14.1. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 4. června 2021, počet stran 1;
14.2. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 10. června 2021, počet stran 1;
14.3. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 6. června 2021, počet stran 1;
14.4. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 9. června 2021, počet stran 1;
14.5. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 21. července 2021, počet stran 1;
14.6. Příloha – Příloha č. 6 – Žádosti uplatňující práva subjektu údajů – 19. května 2021, počet stran 1;

15. Vyjádření kontrolované osoby ze dne 8. listopadu 2021, čj. UOOU-00490/21-26, počet stran 1;

15.1. Příloha – Příloha č. 7 – Smlouvy se zpracovateli k očkovacímu portálu – Rámcová smlouva na poskytování služeb (Smlouva_ICZ_eREG_část_28_CUD_test), počet stran 75;

16. Úřední záznam o pořízení dokumentace ze dne 11. listopadu 2021, čj. UOOU-00490/21-27, počet stran 1;
    16.1. Příloha – výpis ze spisové služby Úřadu – Oznámení pověřence pro ochranu osobních údajů kontrolované osoby ze dne 26. března 2021, čj. UOOU-00005/21-385;
17. Protokol z ústního jednání a místního šetření ze dne 23. listopadu 2021, čj. UOOU-00490/21-29, počet stran 4;
18. Úřední záznam o pořízení dokumentace ze dne 23. listopadu 2021 čj. UOOU-00490/21-30, počet stran 1;
    18.1. Očkovací portál občana – ocko.uzis.cz., počet stran 10;
19. Úřední záznam o pořízení dokumentace ze dne 2. prosince 2021 čj. UOOU-00490/21-31, počet stran 1;
    19.1. snímek obrazovky z aplikace čTečka Platný certifikát [redacted] (úvodní zobrazení)
    19.2. snímek obrazovky z aplikace čTečka Platný certifikát [redacted] (podrobnosti I.)
    19.3. snímek obrazovky z aplikace čTečka Platný certifikát [redacted] (podrobnosti II.)
    19.4. snímek obrazovky z aplikace čTečka Neplatný certifikát [redacted] (úvodní zobrazení)
    19.5. snímek obrazovky z aplikace čTečka Neplatný certifikát [redacted] (podrobnosti I.)
    19.6. snímek obrazovky z aplikace čTečka Neplatný certifikát [redacted] (podrobnosti II.)
    19.7. snímek obrazovky z aplikace čTečka Neplatný certifikát [redacted] (úvodní zobrazení)
    19.8. snímek obrazovky z aplikace čTečka Neplatný certifikát [redacted] (podrobnosti)
20. Úřední záznam o pořízení dokumentace ze dne 3. prosince 2021 čj. UOOU-00490/21-32, počet stran 1;
    20.1. Doporučení pro bezpečné nakládání s e-identitou, počet stran 49;
    20.2. Zaznamenání očkování proti onemocnění COVID-19 v informačním systému infekčních nemocí ISIN (COVID-19-ockovani-isin-manual-v-5-4), počet stran 25;
21. Vyjádření kontrolované osoby ze dne 3. prosince 2021, čj. UOOU-00490/21-33, počet stran 4;
    21.1. Příloha č. 1 – Očkovací portál občana – manuál, počet stran 10;
    21.2. Příloha č. 2 – ocko log, počet stran 4;
    21.3. Příloha č. 3 – Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ (Centrální rezervační systém-očkování proti COVID-19), počet stran 8;
    21.4. Příloha č. 4 – Technický popis generování URL, počet stran 1;
    21.5. Příloha č. 5 – Charakteristika služebního místa [redacted], počet stran 4;
    21.6. Příloha č. 6 – Informační povinnost CRS očkování, počet stran 8;
22. Vyjádření kontrolované osoby ze dne 7. prosince 2021, čj. UOOU-00490/21-34, počet stran 5;

22.1. Smlouva mezi MZ a NAKIT, s. p.;
22.2. Dodatek č. 1 ke smlouvě mezi MZ a NAKIT, s. p.;
22.3. Dodatek č. 2 ke smlouvě mezi MZ a NAKIT, s. p.;
22.4. Příloha 1 Dodatku č. 2 ke smlouvě mezi MZ a NAKIT, s. p.;
22.5. Příloha 2 Dodatku č. 2 ke smlouvě mezi MZ a NAKIT, s. p.;
22.6. Dodatek č. 3 ke smlouvě mezi MZ a NAKIT, s. p.;
22.7. Dodatek č. 4 ke smlouvě mezi MZ a NAKIT, s. p.;
22.8. Dodatek č. 5 ke smlouvě mezi MZ a NAKIT, s. p.;

23. Vyjádření kontrolované osoby ze dne 16. prosince 2021, čj. UOOU-00490/21-35, počet stran 2;
23.1. Záznam o činnostech zpracování – CRS, počet stran 4;

24. Úřední záznam o pořízení dokumentace ze dne 16. prosince 2021 čj. UOOU-00490/21-36, počet stran 5;
24.1. „Najdi stát“ pro URL ocko.uzis.cz s výstupy programu „Najdi stát“ pro analyzované stránky, počet stran 2;
24.2. Screenshot stránky Tečka – [redacted];
24.3. Screenshot stránky Tečka – [redacted];
24.4. Screenshot stránky Tečka – [redacted];
24.5. Screenshot stránky čTečka ctecka-[redacted];
24.6. Screenshot stránky čTečka-[redacted]
24.7. Screenshot stránky Očkovací portál občana – portál očkování, ocko.uzis.cz;
24.8. Screenshot stránky Ústav zdravotnických informací a statistiky ČR – úvodní strana www.uzis.cz;
24.9. Screenshot stránky Informace o souborech cookie a jejich využívání, www.uzis.cz/cookies;
24.10. Screenshot stránky ocko.uzis.cz dokládající nastavené cookies;
24.11. Screenshot stránky www.uzis.cz/cookies dokládající nastavené cookies;
24.12. Screenshot stránky ocko.uzis.cz, dokládající načítání externího obsahu;

25. Úřední záznam o pořízení dokumentace ze dne 3. ledna 2022 čj. UOOU-00490/21-38, počet stran 1;
25.1. snímek obrazovky z aplikace čTečka zobrazit i neplatné certifikáty 1;
25.2. snímek obrazovky z aplikace čTečka zobrazit i neplatné certifikáty 2;

26. Podnět č. 5 ze dne 2. listopadu 2021, čj. UOOU-00490/21-40, počet stran 1;

27. Úřední záznam o pořízení dokumentace ze dne 3. ledna 2022, čj. UOOU-00490/21-42, počet stran 1;
27.1. snímek obrazovky z aplikace Tečka Soukromí;
27.2. snímek obrazovky z aplikace Tečka Podpora certifikátů kontraindikace;
27.3. snímek obrazovky z aplikace Tečka Přidat certifikát – Identita občana;
27.4. snímek obrazovky z aplikace Tečka Souhlas ÚZISu část 1;
27.5. snímek obrazovky z aplikace Tečka Souhlas ÚZISu část 2;

28. Protokol z ústního jednání ze dne 11. ledna 2022, čj. UOOU-00490/21-44, počet stran 6;

29. Vyjádření kontrolované osoby ze dne 19. ledna 2022, čj. UOOU-00490/21-45, počet stran 2;
29.1. Metodický pokyn k implementaci Obecného nařízení o ochraně osobních údajů – GDPR na Ministerstvu zdravotnictví ČR, počet stran 10;
29.2. Smlouva o spolupráci k ISIN mezi MZ a ÚZIS, počet stran 52;

30. Úřední záznam o pořízení dokumentace ze dne 24. ledna 2022, čj. UOOU-00490/21-46, počet stran 1;
    30.1. výtisk internetové stránky Očkovací portál občana – manuál, počet stran 10;
    30.2. výtisk internetové stránky Zaznamenání očkování proti onemocnění COVID-19 v informačním systému infekčních nemocí ISIN, počet stran 34
31. Vyjádření kontrolované osoby ze dne 20. ledna 2022, čj. UOOU-00490/21-47, počet stran 2;
    31.1. Záznam o činnostech zpracování, počet stran 5.
32. Úřední záznam o pořízení dokumentace ze dne 31. ledna 2022, čj. UOOU-00490/21-48, počet stran 1;
    32.1. Mimořádné opatření ze dne 28. června 2021, č. j.: MZDR 1595/2021-5/MIN/KAN, počet stran 4;
    32.2. Mimořádné opatření ze dne 2. července 2021, č. j.: MZDR 1595/2021-7/MIN/KAN, počet stran 1.

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 kontroly:

Kontrola byla zahájena na základě podnětů doručených Úřadu. Z jejich obsahu vyplývalo možné porušení nařízení (EU) 2016/679, zejména při ověřování platnosti certifikátu EU COVID-19 (dále jen „certifikát“). K tomuto porušení mělo dojít při načtení QR kódu z certifikátu, který obsahoval URL adresu pro ověření jeho platnosti. *URL adresa měla obsahovat jméno, příjmení, číslo pojištěnce, číslo občanského průkazu, číslo cestovního dokladu, datum narození, datum vakcinace a datum vystavení a tyto osobní údaje majitele certifikátu tak byly zpřístupněny kontrolující osobě ve větším rozsahu, než bylo potřeba pro ověření jeho platnosti.* Stěžovatelé se dále domnívali, že při ověření platnosti certifikátu se mohou informace automaticky uložit do historie prohlížeče či paměti čtečky a také byl namítán rozsah údajů, které jsou prostřednictvím očkovacího portálu občana zpracovány. (podklad č. 2., 5., 6., 8.)

Z výše uvedených důvodů se kontrolující zaměřili především na dodržování zásad zpracování osobních údajů dle čl. 5, zákonnosti zpracování osobních údajů podle čl. 6, poskytování informací subjektům údajů podle čl. 12-14, plnění povinnosti při uplatňování práv subjektů údajů stanovených čl. 15-17 a 21 (právo na informace, opravu, výmaz, vznést námitku) a zabezpečení osobních údajů dle čl. 32 nařízení (EU) 2016/679, a to v rámci provozu očkovacího portálu občana na https://ocko.uzis.cz (dále jen „OČKO“) a aplikace Tečka, jejichž prostřednictvím subjekt údajů získává svůj certifikát a aplikace čTečka, jejímž prostřednictvím je povinnými subjekty kontrolována validita těchto certifikátů.

III. Kontrolní zjištění:

Za účelem možnosti vyzvednutí certifikátů o provedeném očkování, testu či prodělaném onemocnění, vytvořil Ústav zdravotnických informací a statistiky ČR (dále jen „ÚZIS“), na pokyn MZ, OČKO, prostřednictvím kterého si může každý subjekt údajů ověřit svá zaznamenaná očkování a provedené testy.

Na uvedeném portálu jsou tak zpřístupňovány certifikáty (o očkování, prodělané nemoci či provedené antigenní testy (dále jen „AG testy“) a testy polymerázové řetězové reakce (dále jen „PCR testy")). Certifikát má elektronickou a/nebo tištěnou podobu, je založen na standardu EU a umožňuje i mezinárodní použití – od 1. července 2021 je prostřednictvím nařízení Evropského parlamentu a Rady (EU) 2021/953 ze dne 14. června 2021 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 za účelem usnadnění volného pohybu během pandemie COVID-19 (dále jen „nařízení (EU) 2021/953“) stanovena povinnost států EU uznávat certifikáty. (podklad č. 9.13., 31.1.)

1. června 2021 se změnil vzhled do tohoto data vydávaných certifikátů (na jednotný vzhled certifikátů EU) a pro subjekty údajů i možnosti jeho vyzvednutí. Po přechodnou dobu (do 7. června 2021) probíhalo také automatické odeslání všech nově vydaných vakcinačních certifikátů po podání první i druhé dávky. Od 7. června 2021 bylo ukončeno automatické odesílání všech nově vydaných certifikátů po podání první i druhé dávky prostřednictvím e-mailů. Od tohoto data jsou pro vyzvednutí očkovacích certifikátů používány pouze OČKO nebo aplikace Tečka. (podklad č. 20.2.)

Metody získání certifikátu:

- Certifikát lze vyzvednout na OČKO. Po proběhlém očkování přijde každému informační e-mail s odkazem na tento web a postupem, jak certifikát stáhnout.
- Od 1. července 2021 je k dispozici také mobilní aplikace Tečka, která má stejné funkce jako OČKO, a umožňuje stahovat certifikáty do mobilního telefonu. V této aplikaci dochází k automatickému načítání nových certifikátů.
- Na vyžádání na testovacích a očkovacích místech, kde mohou vytisknout papírovou verzi certifikátu, nebo na vyžádání odeslat certifikát e-mailem.
- Praktický lékař může na vyžádání vytisknout nebo odeslat e-mailem certifikát pacientovi. (podklad č. 9.13.)

Aplikace Tečka je určena držitelům certifikátů, jejím účelem je zobrazení platných i neplatných certifikátů držitele, nebo jiné osoby (např. člena rodiny). Po stažení aplikace do zařízení je držitel vyzván k přihlášení (ztotožnění), které probíhá přes OČKO, později se již aplikace připojuje automaticky. Vstup do aplikace je chráněn PINem, který si subjekt zvolí po ztotožnění, nebo rozpoznáním obličeje nebo otiskem prstu.

Naproti tomu aplikace čTečka je určena pro kontrolu certifikátů, tj. zejména pro státní orgány a pro provozovatele služeb a akcí, kterým kontrolu certifikátů ukládá aktuální ochranné opatření MZ. (podklad č. 9.4.) čTečka umí přečíst QR kód z Tečky, ale i z papírového certifikátu nebo z certifikátu staženého do mobilního zařízení. Běžné mobilní aplikace na čtení QR kódů mohou přečíst datovou strukturu QR kódu na certifikátu, ale nedokáží ji interpretovat a ověřit

elektronický podpis. Pro plnohodnotnou kontrolu QR kódů je nezbytné použít aplikaci čTečka. (podklad č. 9.)

čTečka certifikát zobrazí na displeji mobilu pouze dočasně, neuchovává ani nikam neodesílá osobní údaje kontrolovaných osob, pravidelně (cca 1x za 24 hodin) aktualizuje svoje parametry – validační pravidla a podpisové certifikáty států EU. (podklad č. 9.)

Posledním krokem pro kompletní ověření je ověření totožnosti držitele certifikátu, např. kontrolou jeho dokladů, jestli jde o stejnou osobu, pro kterou byl vystaven certifikát (kontrola podle jména a data narození). (podklad č. 9.)

Kontrolní zjištění č. 1:

Kontrolující předně posuzovali, zda informace, které kontrolovaná osoba v souvislosti s certifikátem zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1, případně též osobní údaje zvláštní kategorie podle čl. 9 odst. 1 nařízení (EU) 2016(679.

Zdrojem dat pro vydávání certifikátů je Informační systém infekčních nemocí a tzv. vakcinační modul OČKO, který byl na pokyn MZ, navržen jako rozšíření modulu tohoto informačního systému infekčních nemocí (dále jen „ISIN“).

ISIN byl zřízen za účelem získávání informací o výskytu infekčních onemocnění, k posouzení vývoje epidemiologické situace na území ČR, ke sledování zdravotního stavu obyvatelstva a k řízení poskytovaní zdravotní péče, [redacted]. (podklad č. 7.)

Základní funkce ISIN v rámci předmětné kontroly:

- Zaznamenání vakcinace;
- Vytvoření „průkazu“ očkování (potvrzení o provedeném očkování);
- Notifikace lékařům a pacientům (subjektům údajů) o termínech vícefázového očkování;
- Napojení na služby eGovernmentu – NIA a portál občana;
- Tvorba veřejného webového portálu za účelem ověření proočkovanosti osoby jinou osobou na základě souhlasu ověřované osoby;
- Napojení na obdobné služby EU, případně mezinárodní, k prokazování očkování subjektu údajů při cestování do jiných zemí.
- Ztotožňování osob probíhá vůči základním registrům. (podklad č. 13.1., 13.2.)

Po provedení očkování či testu jsou v ISIN oprávněnými osobami (poskytovatelé zdravotních služeb) podle § 2 zákona č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) shromažďovány osobní údaje subjektu údajů. OČKO, je komponentou informačního systému ISIN (modul náhledu pouze pro daného uživatele), který komunikuje výhradně s ISIN. (podklad č. 12.)

Po přihlášení do OČKO je subjektu údajů v náhledu přístupná tzv. osobní karta s informacemi v následujícím rozsahu: jméno a příjmení; číslo pojištěnce; datum narození; číslo občanského průkazu; číslo pasu; číslo mobilního telefonu; e-mail.

V osobní kartě se sekce „*Vakcinace*“ COVID-19 dělí na další pododdíly dle počtu absolvovaných dávek (Dávka 1/2 Dávka 2/2, Dávka 3/3) s následujícími osobními údaji: datum vakcinace; vakcinace ukončena; původce, proti kterému byla vakcinace provedena; typ očkovací látky; název produktu; držitel rozhodnutí o registraci; šarže; dávka/celkový počet dávek; zařízení název; zařízení IČO, PČZ. V sekci „*Testy*“ se zobrazují pododdíly (PCR test negativní (případně PCR test pozitivní), Průkaz antigenu / Detection of antigen test) vždy se dvěma údaji: výsledek testu a datum provedení. V sekci „*Kontraindikace“* (je např. s poznámka: „*Nemáte evidovanou žádnou kontraindikaci*“).

V jednotlivých sekcích se zobrazuje možnost stáhnout si certifikát o podstoupeném očkování „*Očkovací certifikát*“, u negativních výsledků testů „*Certifikát testu*“, v případě pozitivního PCR testu *„Certifikát o prodělaném onemocnění“*.

V případě, kdy se subjekt údajů přihlašuje do OČKO mobilním telefonem prostřednictvím aplikace Tečka, je na osobní kartě uveden i „*Název zařízení*“ jeho telefonu.

Údaje shodně uvedené na jednotlivých certifikátech:

- Základní identifikační informace držitele – jméno, příjmení, datum narození;
- QR kód (obsahuje elektronický podpis a údaje, které jsou viditelné na certifikátech);
- Členský stát, vydavatel certifikátu a unikátní identifikátor certifikátu;
- Detailní informace o provedeném očkování nebo testu:

  Na certifikátu o provedeném testu:

  původce, který byl testován; typ testu; název testu (volitelné pro PCR); datum a čas odběru vzorku; datum a čas vystavení certifikátu (volitelné pro antigen); výsledek testu; testovací středisko nebo zařízení.

  Na certifikátu o provedené vakcinaci:

  cílená nemoc nebo agens; vakcína; výrobce nebo držitel rozhodnutí o registraci vakcíny; pořadové číslo dávky / počet dávek; datum vakcinace.

  Na certifikátu o prodělané nemoci:

  nemoc, ze které se občan zotavil; datum prvního pozitivního výsledku; certifikát platný od; certifikát platný do (ne více než 180 dní po datu prvního pozitivního výsledku). (podklad č. 3., 7., 9.13., 9.14., 12.2., 12.3., 12.4.)

Údaje subjektů údajů na certifikátech (o provedené vakcinaci, testu či prodělané nemoci COVID-19) jsou zpracovávány (shromažďovány a zpřístupňovány) z ISIN, do kterého vkládají data o daném subjektu údajů konkrétní poskytovatelé zdravotních služeb, kteří vykonali vakcinaci či test např. praktičtí lékaři, očkovací místa, zdravotnické laboratoře. (podklad č. 3., 7., 31.1.)

Dle výše uvedeného jsou v souvislosti se zpřístupňováním a vydáváním certifikátů zpracovávány nepochybně osobní údaje, včetně údajů o zdravotním stavu subjektu údajů (údaje o vakcinaci, výsledku testu na onemocnění COVID-19 či jeho prodělání – tedy informace

o zdravotním stavu fyzické osoby), které patří podle čl. 9 odst. 1 nařízení (EU) 2016/679 do tzv. zvláštní kategorie osobních údajů, zasluhují zvláštní ochranu a možnost jejich zpracování je výrazně omezena.

Kontrolující proto vyhodnotili zjištěný stav věci tak, že informace, které kontrolovaná osoba o subjektech údajů zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 a čl. 9 odst. 1 nařízení (EU) 2016/679.

Soubory operací, které jsou u kontrolované osoby prováděny s osobními údaji subjektů údajů (jako např. shromažďování, ukládání, oprava, zpřístupnění, uchovávání, likvidace), jsou nepochybně zpracováním osobních údajů, včetně zpracování údajů zvláštní kategorie ve smyslu definice uvedené v čl. 4 odst. 2 nařízení (EU) 2016/679.

Kontrolní zjištění č. 2:

Kontrolující následně posuzovali postavení kontrolované osoby ve vztahu k čl. 4 bodu 7 nařízení (EU) 2016/679, dle kterého se správcem rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.“*

MZ je ústředním orgánem státní správy pro rezort zdravotnictví, který v souvislosti s výkonem státní správy plní úkoly v oblasti ochrany a podpory veřejného zdraví.

V podkladech k předmětné kontrole je v záznamech o činnostech zpracování osobních údajů uvedeno, že problematika prokazování o platném očkování proti nemoci COVID-19, nebo jejím prodělání či potvrzení o negativní či pozitivním výsledku testu je řešena společně s národními subjekty v oblasti ochrany veřejného zdraví a dalšími subjekty (technickými integrátory) v rámci pracovní skupiny Evropské komise – eHealth. Ti se nachází v pozici společných správců. (podklad č. 31.1.)

Na úrovni Evropské unie, je agenda certifikátů upravena nařízením (EU) 2021/953), dále pak prováděcím předpisem Rozhodnutím komise (EU) 2021/1073, kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro certifikáty stanovené uvedeným nařízením Evropského parlamentu.

Podle čl. 8 Rozhodnutí komise (EU) 2021/1073 se orgány nebo jiné určené subjekty odpovědné za vydávání certifikátů v průběhu procesu vydávání ve své roli zpracovatelů osobních údajů považují za správce ve smyslu čl. 4 odst. 7 nařízení (EU) 2016/679.

Na národní úrovni je vydávání certifikátů spojeno s prokazováním tzv. bezinfekčnosti subjektu údajů v souladu s podmínkami, které jsou upraveny Mimořádnými opatřeními vydávanými v souvislosti s pandemií nemoci COVID-19 v ČR (č. j.: MZDR 1595/2021-5/MIN/KAN, a další platné mimořádné nařízení MZ).

V souvislosti s přetrvávající epidemií spojenou s výskytem onemocnění COVID-19, způsobeného novým koronavirem s označením SARS-CoV-2 v Evropě a zejména v České

republice, vydalo MZ jako správní úřad příslušný podle § 80 odst. 1 písm. g) zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon č. 258/2000 Sb.“), postupem podle § 69 odst. 1 písm. i) a odst. 2 zákona č. 258/2000 Sb. k ochraně obyvatelstva a prevenci nebezpečí vzniku a rozšíření onemocnění COVID-19, mimořádné opatření č. j.: MZDR 1595/2021-5/MIN/KAN ze dne 28. června 2021, vydané v návaznosti na publikování nařízení (EU) 2021/953 v Úředním věstníku Evropské unie.

V dokumentu „*DPIA – Projekt: IT Podpora očkování*“ (podklad č. 7.2.) je uvedeno, že OČKO je komponentou informačního systému ISIN, jehož účelem je získávání informací o výskytu infekčních onemocnění, k posouzení vývoje epidemiologické situace na území ČR, ke sledování zdravotního stavu obyvatelstva a k řízení poskytování zdravotní péče. Je dostupný na webové adrese http://ocko.uzis.cz/. Na základě rozhodnutí ministra zdravotnictví a hlavní hygieničky ČR ze dne 2. prosince 2020 byl ÚZIS pověřen realizací nového registru očkování – vakcinačního modulu, který je součástí ISIN [redacted]. (podklad č. 13.1.) MZ stanovilo v *„Zápisu z porady vedení č. 48 ze dne 8. prosince 2020*“ a jeho příloze č. 3, že realizace elektronické evidence očkování – *„registr očkování bude veden v rámci systému ISIN“ „pro ztotožňování osob vůči základním registrům v registru ISIN* [redacted]*, včetně osob spřažených, tedy agendu Zdravotních služeb“.* (podklad č. 12.,13.2.)

Na základě výše uvedeného, ÚZIS na pokyn MZ, vytvořil v souvislosti s vydáváním certifikátů OČKO, kde si každý subjekt údajů může ověřit svá zaznamenaná očkování a provedené testy na webové stránce https://ocko.uzis.cz. Zdrojem osobních údajů v certifikátu je informační systém ISIN. (viz kontrolní zjištění č. 1)

S odkazem na ustanovení uvedené v čl. 8 Rozhodnutí komise (EU) a vydaný pokyn MZ, lze konstatovat, že MZ v souvislosti s vydáváním certifikátů stanovilo účel, způsob a prostředky zpracování osobních údajů subjektu údajů.

Kontrolující s ohledem na výše uvedené konstatují, že MZ je v postavení správce podle čl. 4 bodu 7 nařízení (EU) 2016/679, neboť určilo účel a prostředky předmětného zpracování osobních údajů.

Kontrolní zjištění č. 3:

Kontrolující se zabývali skutečností, zda zpracování osobních údajů, které je předmětem této kontroly, probíhá v souladu s čl. 6 nařízení (EU) 2016/679, podle kterého musí správce osobních údajů vždy disponovat legitimním právním titulem pro zpracování osobních údajů a čl. 9 odst. 1 nařízení (EU) 2016/679 podle kterého se zakazuje zpracování osobních údajů vypovídajících o zdravotním stavu, pokud není splněna jedna z výjimek uvedená ve druhém odstavci tohoto ustanovení.

Ustanovení uvedená v čl. 6 reflektují jednu ze základních zásad zpracování osobních údajů, která je uvedena v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, tedy zásadu zákonnosti – *„Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“)“.*

Problematika prokazování o platném očkování proti nemoci COVID-19, nebo jejím prodělání či potvrzení o negativním či pozitivním výsledku testu je řešena společně s národními subjekty v oblasti ochrany veřejného zdraví a dalších subjektů (technických integrátorů) v rámci pracovní skupiny Evropské komise – eHealth (pod vedením European Commission, Directorate-General for Health and Food Safety). Ti se nachází v postavení společných správců (Joint Controllers). Na úrovni Evropské unie je agenda certifikátů mimo jiné upravena nařízením (EU) 2021/953, prováděcím Rozhodnutím komise (EU) 2021/1073, kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro digitální certifikát EU COVID-19 stanoveného nařízením (EU) 2021/953.

Na národní úrovni se v souladu s výše uvedeným nařízením (EU) 2021/953 řídí prokazování bezinfekčnosti Mimořádným opatřením Ministerstva zdravotnictví č. j.: MZDR 1595/2021-8/MIN/KAN v aktuálním znění, případně v dané době platnými mimořádnými nařízeními MZ.

V podkladech k předmětné kontrole je v záznamech o činnostech zpracování uvedena následující zákonnost zpracování osobních údajů v ISIN a certifikátech (podklad č. 31.1.):

- Zákonnost pro zpracování osobních údajů v ISIN se řídí čl. 6 odst. 1 písm. e) nařízení (EU) 2016/679 – zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, v souladu s ustanovením § 62, § 79 zákon č. 258/2000 Sb.
- Osobní údaje na certifikátech jsou zpracovávány podle čl. 6 odst. 1 písm. c), e) a čl. 9 odst. 2 písm. i), nařízení (EU) 2016/679 (čl. 3 odst. 2 nařízení (EU) 2021/953 a Mimořádné opatření Ministerstva zdravotnictví č. j.: MZDR 1595/2021-8/MIN/KAN v aktuálním znění).

Primárně je nutno rozlišit účely, pro které jsou osobní údaje z ISIN využívány. (viz kontrolní zjištění č. 1 a 2). Jedním z důvodů zpřístupňování a vydávání certifikátů, které obsahují údaje o provedeném očkování, testování nebo prodělání nemoci COVID-19, je umožnění přeshraničního pohybu osob v rámci prostoru EU dle nařízení (EU) 2021/953 během pandemie COVID-19. Uvedené nařízení v recitálu 48 uvádí: „*Toto nařízení stanoví právní základ pro zpracování osobních údajů ve smyslu čl. 6 odst. 1 písm. c) a čl. 9 odst. 2 písm. g) nařízení (EU) 2016/679, nezbytné pro vydávání a ověřování interoperabilních certifikátů stanovených v tomto nařízení. Neupravuje zpracování osobních údajů týkajících se dokumentace o očkování, testování nebo zotavení pro jiné účely, například pro účely farmakovigilance nebo vedení osobních zdravotních záznamů. Členské státy mohou osobní údaje pro jiné účely zpracovávat, pokud je právní základ pro zpracování těchto údajů pro jiné účely, včetně souvisejících lhůt pro jejich uchovávání, stanoven ve vnitrostátním právu, které musí být v souladu s právními předpisy Unie na ochranu údajů a se zásadami účinnosti, nezbytnosti a proporcionality a které by mělo obsahovat ustanovení, jež jasně stanoví oblast a rozsah zpracování, konkrétní účel, kategorie subjektů, které mohou certifikát ověřit, a příslušné záruky pro předcházení diskriminaci a zneužívání, s přihlédnutím k rizikům pro práva a svobody subjektů údajů. Pokud se certifikát používá pro jiné než lékařské účely, osobní údaje zpřístupněné během procesu ověřování se nesmí uchovávat, jak je stanoveno v tomto nařízení.*“

V souladu s výše uvedeným lze konstatovat, že zpracování certifikátů pro účely usnadnění volného pohybu v prostoru EU při přeshraničním pohybu subjektu údajů mezi jednotlivými členskými státy nachází oporu v právu Unie. **Dochází tedy ke zpracování osobních údajů ve smyslu čl. 6 odst. 1 písm. c) a výjimky ze zákazu zpracování zvláštní kategorie osobních údajů ve smyslu čl. 9 odst. 2 písm. g) nařízení (EU) 2016/679.**

Druhým účelem je prokazování tzv. „bezinfekčnosti" při vstupu do vybraných uzavřených prostor, kulturních akcí, poskytování služeb apod. K tomuto účelu MZ jako správce umožňuje využít certifikáty v papírové podobě/ elektronické podobě (Tečka) a ověření jejich validity prostřednictvím čTečky.

V souvislosti s vývojem pandemie nemoci COVID-19, je MZ správním úřadem příslušným podle § 80 odst. 1 písm. g) zákona č. 258/2000 Sb., k ochraně a podpoře veřejného zdraví s ohledem na aktuální pandemickou situaci postupem podle § 69 odst. 1 písm. i) a odst. 2 zákona č. 258/2000 Sb. k ochraně obyvatelstva a prevenci nebezpečí vzniku a rozšíření onemocnění COVID-19, k vydávání mimořádných opatření. Mimořádná opatření (v aktuálním znění) nařizují provozovatelům obchodů a služeb, ale i jiným subjektům kontrolovat při vstupu do jejich zařízení subjekty údajů, splňující podmínky pro jejich vstup.

Jako potvrzení o provedeném očkování/testu na COVID-19, nebo prodělání nemoci je ke dni shromáždění podkladů (k 31. lednu 2021, čj. UOOU-00490/21-48) z Tečky a portálu OČKO přístupný mezinárodní elektronický certifikát odpovídající požadavkům nařízení (EU) 2021/953. Podle čl. IV. odst. 2 bodu a) mimořádného opatření MZ č. j.: MZDR 42085/2021-1/MIN/KAN ze dne 20. listopadu 2021 mohou zaměstnanci prokazovat svoji bezinfekčnost: „*národním certifikátem o provedeném očkování nebo certifikátem o provedeném očkování vydávaným podle nařízení Evropské unie o digitálním certifikátu EU COVID; za národní certifikát o provedeném očkování se považuje písemné potvrzení vydané alespoň v anglickém jazyce oprávněnou osobou působící v třetí zemi, jehož vzor je zveřejněn v seznamu uznaných národních certifikátů na internetových stránkách Ministerstva zdravotnictví; písemné potvrzení musí obsahovat údaje o očkované osobě, podanému typu vakcíny, datu podání vakcíny, identifikaci osoby, která potvrzení vydala, a tyto údaje musí být možné ověřit dálkovým přístupem přímo z písemného potvrzení, za předpokladu, že očkování bylo provedeno."* V „*DPIA – Projekt: IT Podpora očkování*" ve verzi ze dne 29. července 2021 (podklad č. 7.2.) správce uvádí, že údaje o očkování/testu na COVID-19 či prodělání nemoci jsou v ISIN zpracovávány v souladu s čl. 6 odst. 1 písm. e) nařízení (EU) 2016/679 a výjimky ze zákazu zpracování zvláštní kategorie dle čl. 9 odst. 2 písm. i) nařízení (EU) 2016/679. Správce shledává, že toto zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu, tedy k ochraně veřejného zdraví a ochrany před vážnými přeshraničními hrozbami. Právní základ správce spatřuje v zákoně č. 258/2000 Sb., stejný právní titul správce uvádí také v dokumentu „*Záznamy o činnostech – Centrální rezervační systém očkování proti COVID-19*" (podklad č. 31.1.), tento právní titul se vztahuje také na zpracování osobních údajů v rámci portálu OČKO, které je komponentou systému ISIN a aplikace Tečka.

Ve výše uvedeném případě tedy jde o zpracování v souladu s čl. 6 odst. 1 písm. e) (zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu při výkonu veřejné moci) a výjimky podle čl. 9 odst. 2 písm. i) (zpracování je nezbytné z důvodů veřejného zájmu

v oblasti veřejného zdraví) nařízení (EU) 2016/679, jelikož je prováděno na základě vydaných mimořádných opatření MZ v aktuálním znění v souladu se zákonem č. 258/2000 Sb., a to za účelem splnění úkolu prováděného ve veřejném zájmu.

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaná osoba **neporušila** povinnost stanovenou v čl. 6 a čl. 9 nařízení (EU) 2016/679, zpracování osobních údajů je založeno na legitimních právních titulech.

Nadto je třeba uvést, že zpracování, které je předmětem této kontroly, se týká osobních údajů velkého množství subjektů údajů, zároveň se jedná o zpracování zvláštní kategorie osobních údajů, a jejich zpracováním dochází k významnému zásahu do práv těchto subjektů. Subjekt údajů nemá možnost takové zpracování odmítnout a při zachování běžného života se mu nemůže ani vyhnout. MZ toto zpracování provádí na základě právního titulu, který vyplývá z obecného zmocnění MZ v zákoně č. 258/2000 Sb., prostřednictvím vydaných mimořádných opatření v aktuálním znění. Mimořádná opatření vycházejí z určitého stavu a potřeby ochrany obyvatelstva a prevence před onemocněním, pro daný časový úsek. Kontrolující v tomto případě vzali v potaz, že k vytvoření certifikátů MZ přistoupilo na základě aktuální potřeby urychleně řešit problematiku prokazování prodělaného očkování/testu/nemoci COVID-19, a to ať už v souvislosti s přeshraničním pohybem osob, tak i v souvislosti s prokázáním bezinfekčnosti ve vnitrostátním styku. Je však nutné uvést, že by mimořádné opatření jako právní titul pro takto rozsáhlé zpracování zvláštní kategorie osobních údajů mělo sloužit pouze jako dočasný právní titul a mělo by být nahrazeno právním titulem, který bude vycházet ze zákona, jak předpokládá i recitál 48 nařízení (EU) 2021/953, který uvádí, že členské státy mohou osobní údaje pro jiné účely než je vydání certifikátu určeného pro usnadnění volného pohybu mezi zeměmi EU zpracovávat, pokud je právní základ pro zpracování těchto údajů pro jiné účely, včetně souvisejících lhůt pro jejich uchovávání, stanoven ve vnitrostátním právu, které musí být v souladu s právními předpisy Unie na ochranu údajů a se zásadami účinnosti, nezbytnosti a proporcionality a které by mělo obsahovat ustanovení, jež jasně stanoví oblast a rozsah zpracování, konkrétní účel, kategorie subjektů, které mohou certifikát ověřit, a příslušné záruky pro předcházení diskriminaci a zneužívání, s přihlédnutím k rizikům pro práva a svobody subjektů údajů.

V úvodu výše uvedeného recitálu je také uvedeno, že „Na zpracování osobních údajů při provádění tohoto nařízení se použije nařízení Evropského parlamentu a Rady (EU) 2016/679“. Z toho vyplývá, že toto nařízení je pouze právním základem pro zpracování a jednotliví správci mají povinnost při provádění tohoto nařízení dodržovat povinnosti stanovené v nařízení (EU) 2016/679.

Ostatně sám správce doložil dokumentem „Vakcinace COVID-19“ (podklad č. 13.6.), který nabízí dvě východiska k možnosti vytvoření vakcinačního modulu OČKO jako součást ISIN (viz kontrolní zjištění č. 1). Prvním je zavedení vakcinačního modulu OČKA bez legislativních změn, a to na podkladě rozhodnutí MZ. Druhým východiskem pro možnost vytvoření vakcinačního modulu OČKA jsou legislativní úpravy zákona o ochraně veřejného zdraví a zákona č. 378/2007 Sb., zákon o léčivech a o změnách některých souvisejících zákonů. MZ uvedlo, že zvláštní kategorii osobních údajů zpracovává ve vakcinačním modulu OČKO dle čl. 9 odst. 2 písm. i) nařízení (EU) 2016/679.

Dále je třeba upozornit, že před takovým zpracováním osobních údajů je nezbytné nepochybně splnit povinnost MZ jako správce vycházející z čl. 35 a 36 nařízení (EU) 2016/679 – zejména v této souvislosti provést předchozí konzultace s dozorovým úřadem, jestliže je pravděpodobné, že určitý druh zpracování, především při použití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob.

Kontrolní zjištění č. 4:

Kontrolující taktéž posuzovali, jakým způsobem při předmětném zpracování dochází k naplňování zásad ve smyslu čl. 5 odst. 1, konkrétně písm. a), c) - e) nařízení (EU) 2016/679.

Zásada čl. 5 odst. 1 písm. a) je jedním z hlavních projevů zásady zákonnosti (správce může osobní údaje zpracovávat pouze v případě, že k tomu má alespoň jeden z právních titulů, které jsou stanoveny v čl. 6 odst. 1 písm. a) - f) nařízení (EU) 2016/679. Dle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 *„Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost"). Jak kontrolující konstatovali v kontrolním zjištění č. 3 kontrolovaná osoba tuto povinnost splnila".*

V souvislosti se zásadou minimalizace údajů (čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679) kontrolující zhodnotili rozsah osobních údajů, které kontrolovaná osoba zpracovává v souvislosti s vydávaným certifikátem, zpřístupněným na OČKO, včetně Tečky a čTečky. (II. Důvod kontroly)

Rozsah zpracovávaných osobních údajů je řešen na centrální úrovni EU, kdy je stanoven předpisy EU. Jedná se např. o:

- Nařízení (EU) 2021/953;
- eHealth Network OUTLINE Interoperability of health certificates Trust framework V.1.0 ze dne 2021-03-12;
- Guidelines on verifiable vaccination certificates – basic interoperability elements, Release 2 ze dne 2021-03-12; (podklad č. 12.)

Dále jsou vydány standardy pro vývoj a provozování aplikací, aby jednotlivé členské státy mohly koordinovaně tyto standardy implementovat. MZ i Národní agentura pro komunikační a informační technologie, s. p., (dále jen „NAKIT") se pravidelně účastní jednání a spolupráce s ostatními členskými státy EU v rámci pracovní skupiny eHealth Network – European Commision. (podklad č. 12.)

Jak bylo uvedeno výše, certifikáty nejsou využívány pouze pro účely predikované v nařízení (EU) 2021/953, ale také pro účely prokázání očkování/testu na COVID-19, či prodělané nemoci v rámci vnitrostátního styku. Po posouzení rozsahu údajů zpracovávaných v certifikátech a s přihlédnutím k vyjádření MZ které uvedlo, že údaje o šarži a výrobci vakcíny na certifikátu o očkování slouží pro případ, kdy by držitel certifikátu např. podstoupil očkování druhou dávkou očkovací látky v jiné zemi, než kde mu byla aplikována první (podklad č. 12.), dospěli kontrolující k závěru, že v případě certifikátu o prodělaném očkování na COVID-19 použitého

v rámci vnitrostátního styku, jsou údaje o šarži a výrobci vakcíny nadbytečné. Kontrolující však přihlédli k faktu, že zpracováním těchto údajů nedochází k významnému zásahu do práv a svobod držitele certifikátů a že by rozlišování dvou certifikátů o očkování pro vnitrostátní a mezinárodní použití, kde by jediným rozdílem bylo vynechání výše uvedených údajů bylo pro držitele certifikátu matoucí.

V souvislosti se zásadou minimalizace údajů (čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679) kontrolující zhodnotili rozsah zpracování osobních údajů, které kontrolovaná osoba zpracovává v souvislosti s certifikátem, zpřístupněným na OČKO, včetně Tečky a čTečky. Kontrolující konstatují, že rozsah osobních údajů, zpracovávaných v souvislosti s certifikátem je **přiměřený**, kontrolovaná osoba tedy **dodržela** povinnost stanovenou v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 a tudíž **neporušila** uvedené ustanovení. (viz kontrolní zjištění č. 1 a 2).

V souvislosti se zásadou přesnosti (čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679) bylo kontrolou ověřeno, že primárně jsou osobní údaje aktualizovány z ROB. Kontaktní údaje aktualizuje Poskytovatel zdravotní péče, ten, koho aktualizací pověří MZ, aktuálně jde o cca 30 přístupů pro operátory linky 1221, kterým přístupy byly schváleny hlavní hygieničkou MZ a samotným subjektem údajů, který může provést změny kontaktních a identifikačních údajů prostřednictvím OČKO. (podklad č. 12.)

Postup provádění aktualizace údajů: ÚZIS pověřuje své zaměstnance pro přijímání informací o nepřesných údajích, zejména kontaktní údaje typu e mail, telefonní číslo. Část subjektů údajů se obrací přímo na pověřence pro ochranu osobních údajů ÚZIS. Tyto informace o nepřesných údajích jsou dále předávány helpdesku, který prověřuje, kde k dané chybě došlo, následně ÚZIS odkazuje např. na poskytovatele zdravotnických služeb, který má povinnost jako pověřený editor povinnost opravu údajů provést. Případně výše zmínění pověření zaměstnanci ÚZIS po ověření údajů a totožnosti subjektů údajů mohou také provést opravu. (podklad č. 11.)

Kontrolující konstatují, že MZ jako správce osobních údajů, **dodržel** povinnosti stanovené v čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679 a tudíž **neporušil** uvedené ustanovení.

Dle čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 by měly být osobní údaje uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Neplatné certifikáty jsou automaticky smazány nebo nejdou stáhnout. (podklad č. 12.) MZ určilo v průběhu kontroly v záznamech o činnostech (podklad č. 31.1.) dobu uchování osobních údajů v ISIN. Předmětné osobní údaje budou ukládány pouze po dobu nezbytně nutnou, ke splnění úkolů v oblasti zjišťování získávání informací o výskytu infekčních onemocnění k posouzení vývoje epidemiologické situace na území ČR, ke sledování zdravotního stavu obyvatelstva a k řízení poskytovaní zdravotní péče a souvisejících úkonů. Na OČKO má držitel certifikátu ve své osobní kartě přístup vždy pouze k poslednímu certifikátu v dané sekci. V aplikaci Tečka má mimo těchto údajů přístup i k certifikátům, které do aplikace sám naskenoval prostřednictvím QR kódu.

Kontrolující konstatují, že MZ jako správce osobních údajů, **dodržel** povinnosti stanovené v čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679 a tudíž **neporušil** uvedené ustanovení.

Kontrolní zjištění č. 5:

Kontrolující se dále zaměřili na posouzení plnění povinnosti uvedené v ustanovení čl. 12 nařízení (EU) 2016/679, v rozsahu informace dle čl. 13 a 14 tohoto nařízení. Uvedená ustanovení upravují povinnost správce informovat subjekt údajů o všech podstatných parametrech zpracování osobních údajů, a to včetně jeho práv, která mu ve vztahu k tomuto zpracování vznikají.

Pro splnění informační povinnosti je rozhodná skutečnost, zda osobní údaje byly správci osobních údajů poskytnuty přímo subjektem údajů (čl. 13), nebo je správce získal od jiného než od subjektu údajů (čl. 14). Vzhledem k tomu, že MZ získává osobní údaje přímo od subjektu údajů), je povinna mu podat informace o zpracování jeho osobních údajů dle čl. 13 nařízení (EU) 2016/679.

Kontrolovaná osoba má vypracovanou informační povinnost k Tečce a čTečce, kterou zveřejňuje na webových stránkách https://ockodoc.mzcr.cz/napoveda/tecka/cz/podminky-pouzivani/ (*„Podmínky používání“, „Informace o zpracování osobních údajů v rámci mobilní aplikace Tečka (EU digital COVID Certificate Wallet app)“*) pro uživatele Tečky a https://ockodoc.mzcr.cz/napoveda/ctecka/cz/podminky-pouzivani/ (*„Podmínky používání“, „Informace o zpracování osobních údajů v rámci mobilní aplikace čTečka (EU digital COVID Certificate Verifier app)“*) pro uživatele čTečky. Oba tyto dokumenty poskytují podobné informace o zpracování osobních údajů. Seznámení s těmito dokumenty je také nutno potvrdit před prvním použitím Tečky či čTečky. (podklad č. 9., 9.11., 9.12.)

- Z dokumentů vyplývá, že MZ je správcem osobních údajů, v dokumentech je uveden i kontakt na pověřence pro ochranu osobních údajů MZČR, pro případ uplatnění práv dle čl. 15-22 nařízení (EU) 2016/679 jedná se o e-mailovou a poštovní adresu.
- V dokumentech je uveden rozsah zpracovávaných osobních údajů uživatelů aplikace, tedy v případě uživatele Tečky jde o jméno, příjmení, datum narození, informace o provedeném očkování/testu (typ a výrobce vakcíny nebo testu, počet a data aplikace dávek vakcíny, výsledek testu), nebo informace o prodělaném onemocnění COVID-19 (datum prvního pozitivního testu). V případě uživatele Tečky i čTečky jsou to pak zpracovávány informace spojené s fungováním aplikace, údaje jsou zpracovávány prostřednictvím standartních nástrojů od společnosti Google (Firebase Crashlytics a Google Analytics), tyto údaje by neměli obsahovat osobní údaje, nemělo by být možno tyto údaje spojit s konkrétním zařízením, na kterém je aplikace nainstalována.
- V dokumentech je uvedeno, že osobní údaje Digitálních COVID-19 Certifikátů jsou zpracovávány za účelem jejich kontroly osobami oprávněným na základě nařízení EU, mimořádných opatření MZ nebo na dobrovolné bázi.
- Jako zdroj osobních údajů držitelů COVID-19 Certifikátů je uveden informační systém MZ a ÚZIS, určené pro řízení testování proti COVID-19 (ežádanka) a očkování proti COVID-19 (ISIN modul OČKO). V dokumentech je uveden jednoduchý popis zpracování osobních údajů COVID-19 Certifikátů, dále informace o správci, zpracovatelích a organizační a technické zabezpečení těchto údajů.

Informace o zpracování osobních údajů v certifikátu lze dále zjistit:

- V rámci registrace k očkování (https://registrace.mzcr.cz/#consent) – informace o zpracování osobních údajů zapisovaných do registračního systému;
- *„Informace o zpracování osobních údajů v rámci Projektu: IT podpora OČKOVÁNÍ (Centrální rezervační systém – očkování proti COVID-19)*“ (podklad č. 21.3.) (odkaz dostupný z výše uvedené stránky) – zpracování osobních údajů zejména během registrace k očkování, rezervace termínu očkování a po absolvování očkování. Pokud se jedná o informace o zpracování osobních údajů po očkování je zde uveden rozsah osobních údajů zpracovávaných v certifikátu, který prokazuje prodělané očkování či nemoc, rozsah osobních údajů zpracovávaných v ISIN modul OČKO. Jako právní titul pro zpracování osobních údajů je uveden souhlas a právní zmocnění, není však rozlišeno, jaké osobní údaje jsou zpracovávány na základě, jakého právního titulu, dále je tu definován správce osobních údajů, tedy MZ a kontakt na pověřence pro ochranu osobních údajů;
- *„Otázky a odpovědi k certifikátům a testování*“ https://koronavirus.mzcr.cz/caste-otazky-a-odpovedi/) – kde jsou uvedeny informace o tom, jak získat certifikát o prodělaném očkování, nemoci či testu. V dokumentu je uvedeno, že certifikát je možné získat na webových stránkách http://ocko.uzis.cz/, popis, jak přes tyto webové stránky získat certifikát, návod, jak změnit kontaktní údaje subjektu údajů, jednoduchý popis funkce Tečky a čTečky a další informace týkající se zejména platnosti certifikátů.
- *„Digitální COVID certifikáty – základní informace*“ (https://ockodoc.mzcr.cz/digitalni-zelene-certifikaty-informace/) – informace o tom, co je digitální COVID-19 certifikát, jak je možné jej získat, jaké osobní údaje jsou na něm uvedeny, jak probíhá jeho kontrola a na základě jakých právních předpisů je vydáván.

MZ plní informační povinnost stanovenou v čl. 12-14 nařízení (EU) 2016/679, kdy subjekty osobních údajů informuje zejména o tom, za jakým účelem a na jakém právním základě budou jejich osobní údaje zpracovávány, rozsah jejich zpracování, včetně popisu technicko-organizačních opatření při zabezpečení údajů. Tuto povinnost plní v několika dokumentech, které je možné najít pod různými odkazy na webových stránkách MZ. Odkazy a dokumenty jsou však pojmenovány tak, že na první pohled není zřejmý obsah informace o zpracování osobních údajů.

Kontrolující proto vyhodnotili zjištěný stav tak, že kontrolovaná osoba **neporušila** povinnost stanovenou v čl. 12 nařízení (EU) 2016/679, v rozsahu čl. 13 a 14 tohoto nařízení.

Přesto kontrolující v zájmu zachování podmínky transparentnosti doporučují MZ přejmenování odkazů a dokumentů obsahujících informace o zpracování osobních údajů tak, aby z jejich názvu vyplývalo, že obsahují i informace o zpracování osobních údajů.

Kontrolní zjištění č. 6:

Kontrolující hodnotili rovněž splnění povinnosti stanovené v čl. 15-21 nařízení (EU) 2016/679. Podle těchto ustanovení má subjekt údajů právo na přístup k osobním údajům, tj. právo žádat a získat relevantní informace o zpracování jeho osobních údajů a rovněž právo vznést námitku.

Věcně příslušnou osobou pro vyřizování žádostí o výkon práv subjektů údajů je pověřenec pro ochranu osobních údajů, jak MZ stanovilo interním předpisem *„Metodický pokyn k implementaci Obecného nařízení o ochraně osobních údajů – GDPR na Ministerstvu zdravotnictví ČR*“, konkrétně v článku IV. jednou z činností pověřence je komunikace se subjekty údajů, které se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem práv dle tohoto pokynu v souladu s nařízením (EU) 2016/679. V uvedeném dokumentu je v článku XII. definován postup při vyřizování žádostí subjektů údajů (při podání žádosti prokázat svou totožnost, prokázaní skutečností tvrzených v žádosti, předání žádosti k vyřízení příslušnému odboru, zaslání odpovědi žadateli). V případě opravy nebo výmazu osobních údajů nebo omezení zpracování informuje pověřenec o těchto změnách příjemce v souladu s čl. 19 nařízení (EU) 2016/679. (podklad č. 29.1.)

Informace k uplatnění práv subjektu údajů dle čl. 15-21 nařízení (EU) 2016/679 je poskytována obecně na webových stránkách MZ na https://www.mzcr.cz/ochrana-osobnich-udaju/ odkaz na dokument *„Základní informace o zpracování osobních údajů Ministerstvem zdravotnictví“* (https://www.mzcr.cz/wp-content/uploads/2019/06/Zakladni-informace-o-zpracovani-osobnich-udaju-Ministerstvem-zdravotnictvi.pdf) a dále na webových stránkách https://ockodoc.mzcr.cz/napoveda/tecka/cz/podminky-pouzivani/ (*„Podmínky používání“, „Informace o zpracování osobních údajů v rámci mobilní aplikace Tečka (EU digital COVID Certificate Wallet app)“*) a https://ockodoc.mzcr.cz/napoveda/ctecka/cz/podminky-pouzivani/ (*„Podmínky používání“, „Informace o zpracování osobních údajů v rámci mobilní aplikace čTečka (EU digital COVID Certificate Verifier app)“*). (podklad č. 9.11., 9.12.)

MZ obdrželo prostřednictvím pověřence pro ochranu osobních údajů od 26. prosince 2020 do 31. října 2021 celkem 18 žádostí na uplatnění práv subjektu údajů dle čl. 15-17 a 21 nařízení (EU) 2016/679 dotýkající se problematiky certifikátů zpřístupněných na OČKO nebo v Tečce a čTečce, rezervace či registrace k očkování. (podklad č. 12., 28.)

V rámci kontroly MZ doložilo 5 žádostí na uplatnění práv subjektu údajů ve vztahu k předmětu kontroly. Dvě z nich se týkaly práva subjektu údajů na přístup k osobním údajům dle čl. 15 nařízení (EU) 2016/679 (podklad č. 14.1., 14.2., 14.4.) Další dvě z podaných žádostí se týkaly odvolání souhlasu dle čl. 17 nařízení (EU) 2016/679, kterým bylo vyhověno a odvolání ze strany MZ potvrzeno. (podklad č. 14.3., 14.5.) Poslední doložená žádost se týkala uplatnění práva vznést námitku dle čl. 21 nařízení (EU) 2016/679. (podklad č. 14.6.)

Postup zpracování požadavků subjektů údajů MZ byl kontrolujícím doložen jako e-mailová komunikace týkající se uplatněného nároku a způsobu řešení, prostřednictvím e-mailové adresy OIA@mzcr.cz pověřence pro ochranu osobních údajů. (podklad č. 14.1., 14.2., 14.3., 14.4., 14.5., 14.6.)

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaná osoba **neporušila** povinnost stanovenou v čl. 15-21 nařízení (EU) 2016/679, tedy že má nastavený postup pro vyřizování žádostí na výkon práv subjektu údajů a tyto jsou vyřizovány.

Kontrolní zjištění č. 7:

Kontrolující rovněž zjišťovali podle čl. 28 nařízení (EU) 2016/679, kdo v MZ zpracovává předmětné osobní údaje, případně zda využívá služeb zpracovatele a v této souvislosti má uzavřenu příslušnou smlouvu, pokud mu zpracovatele nestanoví konkrétní zákon.

Jak bylo uvedeno v kontrolním zjištění č. 1 a 2, ÚZIS na základě pokynu MZ vytvořil vakcinační modul, který je komponentou k ISIN a ten je zdrojem dat pro zpřístupňování a vydávání certifikátů.

Provoz samotného informačního systému ISIN byl založen na základě „*Smlouvy o spolupráci*" (podklad č. 29.2.) (dále jen „Smlouva") ze dne 7. března 2018, která byla uzavřena mezi MZ, ÚZIS, Státním zdravotním ústavem (dále jen „SZÚ") a Krajskými hygienickými stanicemi (dále jen „KHS"). ÚZIS a SZÚ jsou dle této Smlouvy v roli zpracovatelů dle čl. 4 odst. 8 nařízení, nicméně v rámci předmětného zpracování je na základě pokynu MZ ÚZIS v roli zpracovatele dle nařízení (EU) 2016/679.

Jelikož zdrojem předmětného zpracování osobních údajů je právě ISIN, lze uzavřenou Smlouvu považovat za zpracovatelskou smlouvu podle ustanovení čl. 28 odst. 3 dle nařízení (EU) 2016/679. Smlouva byla uzavřena ještě v době platnosti zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, tedy před účinností nařízení (EU) 2016/679, nicméně v ustanovení čl. 10 je pak uvedeno, že se Smlouva s účinností nařízení považuje za smlouvu dle čl. 28 tohoto nařízení.

Podle této Smlouvy jsou KHS společnými správci a MZ jako ústřední orgán státní správy pro rezort zdravotnictví a v souladu s výkonem státní správy a plnění úkolů v ochraně a podpoře veřejného zdraví podle zákona č. 258/2000 Sb., centrálním správcem osobních údajů a údajů zvláštní kategorie vedených v systému ISIN.

Předmětem Smlouvy je závazek ÚZIS vytvořit ISIN a řádně jej s projektovou dokumentací předat k užívání MZ, zajistit následnou podporu, rozvoj a provoz ISIN. Rozsah osobních údajů, vedených v ISIN je uveden v příloze č. 4 smlouvy „*Popis položek v ISIN*".

ÚZIS ve Smlouvě prohlašuje, že je organizační složkou státu v přímé řídící působnosti MZ, splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené. Předmětem činností je mimo jiné technické zajištění tvorby a provozu informačních systémů ve zdravotnictví, jak je vymezeno v jeho zřizovací listině vydané ministrem zdravotnictví dne 10. května 2007. (podklad č. 13.4.)

V článku 10 smlouvy „*Ochrana osobních údajů*" je ujednání o zpracování osobních údajů subjektů údajů evidovaných v ISIN dle § 6 zákona č. 101/2000 Sb., MZ jako centrálním správcem, KHS jako společnými správci a ÚZIS jako zpracovatelem I a SZÚ jako zpracovatelem II, jež bude s účinností nařízení (EU) 2016/679 považováno za smlouvu dle čl. 28 tohoto nařízení. Od data účinnosti nařízení pak musí zpracovatelé plnit závazek a pokyny uvedené v této Smlouvě (např. povinnost zachovávat mlčenlivost, povinností ÚZIS a SZÚ je zajištění, že jejich zaměstnanci a jiné osoby, které budou zpracovávat osobní údaje na základě Smlouvy, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu stanoveném a odpovídajícím

této Smlouvě). ÚZIS napomáhá při vyřizování žádostí subjektu údajů dle čl. 15-21 a při plnění povinností dle čl. 32 až 36 nařízení (EU) 2016/679; umožňuje audity, včetně inspekcí prováděných centrálním správcem či jím pověřenou osobou a poskytnout součinnost u těchto auditů. Případní poddodavatelé mají povinnost poskytovat smluvně dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování osobních údajů splňovalo požadavky zákona č. 101/2000 Sb. a od data účinnosti nařízení (EU) 2016/679).

Povinnosti ÚZIS týkající se ochrany osobních údajů se zavazují plnit po dobu účinnosti Smlouvy, pokud z ustanovení Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti.

ÚZIS je povinen postupovat při zpracování osobních údajů v souladu s touto Smlouvou a zákonem č. 101/2000 Sb. a od data jeho účinnosti nařízení (EU) 2016/679 a zpracovávat osobní údaje výlučně pro účel a v rozsahu, ve kterém jim byly předány.

ÚZIS se zavazuje zajistit taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování v rozporu s touto Smlouvou. ÚZIS a SZÚ zároveň přijmou taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

Přístup k osobním údajům je umožněn výlučně pověřeným osobám. Při zpracování osobních údajů jsou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě. Při zpracování osobních údajů v jiné, než elektronické podobě jsou osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby.

ÚZIS se zavazuje zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem č. 101/2000 Sb. (a od data jeho účinnosti nařízení (EU) 2016/679), přičemž zajišťují, kontrolují a odpovídají zejména za:

a) plnění pokynů pro zpracování osobních údajů pověřenými osobami, které mají bezprostřední přístup k osobním údajům;
b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování;
c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje;
d) opatření, která umožní určit a ověřit, jak byly osobní údaje zpracovány.

V případě zjištění porušení záruk dle Smlouvy je ÚZIS povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušují, nejpozději však do 3 pracovních dnů poté, co je k tomu MZ vyzván.

V oblasti automatizovaného zpracování osobních údajů je ÚZIS povinen také pořizovat a uchovávat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a na vyžádání MZ či KHS tyto záznamy poskytnout a zabránit neoprávněnému přístupu k datovým nosičům.

ÚZIS se dle této Smlouvy zavazuje, že přijme všechna opatření k zabezpečení zpracování, případně včetně:

a) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
b) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
c) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Ukončení účinnosti Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení Smlouvy týkajících se ochrany osobních údajů a jejich účinnost přetrvá i po ukončení její účinnosti. V případě ukončení Smlouvy je ÚZIS povinen předat MZ protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li od MZ písemně jiné pokyny. (podklad č. 29.2.)

Po zhodnocení obsahu předložené Smlouvy a pokynů, které MZ vydalo v souvislosti se zřízením vakcinačního modulu (podklad č. 13.1, 13.2., 13.3., 29.2.) kontrolující konstatují, že spolupráce správce a zpracovatele je nastavena způsobem, který odpovídá požadavkům čl. 28 odst. 3 nařízení (EU) 2016/679, čímž je dán i předpoklad k závěru, že nedochází k porušení základní povinnosti vyjádřené v odst. 1 citovaného nařízení.

Kontrolující proto vyhodnotili zjištěný stav tak, že MZ **neporušilo** povinnost stanovenou v čl. 28 nařízení (EU) 2016/679.

Kontrolní zjištění č. 8:

Kontrolující dále ověřili plnění povinnosti, která MZ vyplývá z čl. 30 odst. 1 nařízení (EU) 2016/679, tj. povinnost vést záznamy o činnostech zpracování.

MZ předložilo záznamy o činnostech zpracování, které jsou vedeny jak v písemné, tak i elektronické formě dle čl. 30, odst. 3 tohoto nařízení. K předmětnému zpracování byly v záznamech uvedeny následující skutečnosti:

- jméno a kontaktní údaje správce i pověřence pro ochranu osobních údajů;
- účely zpracování;
  - problematika prokazování o platném očkování proti nemoci COVID-19, nebo jejím prodělání či potvrzení o negativní či pozitivním výsledku testu je řešena společně s národními subjekty v oblasti ochrany veřejného zdraví a dalších subjektů (technických integrátorů) v rámci pracovní skupiny Evropské komise – eHealth.
  - na národní úrovni je vydávání certifikátů spojeno s prokazováním bezinfekčnosti občana v souladu s podmínkami, které jsou upraveny Mimořádnými opatřeními vydávanými v souvislosti s pandemií nemocí COVID-19 v ČR (č.j.: MZDR 1595/2021-8/MIN/KAN, a další platné mimořádné nařízení Ministerstva zdravotnictví ČR).
- popis kategorií subjektů údajů a kategorií osobních údajů;

- Fyzická osoba, která cestou centrálního rezervačního systému hodlá podstoupit očkování proti COVID-19, nebo jej hodlá využít pro jinou osobu (např. rodič pro dítě), nebo prodělala nemoc COVID-19, nebo se nechala na tuto nemoc testovat.
- Certifikát obsahuje tyto kategorie osobních údajů:
  - totožnost držitele (kontaktní a identifikační údaje žadatele o certifikát);
  - informace o podané očkovací látce proti onemocnění COVID-19 a počtu dávek podaných držiteli; nebo informace o testu NAAT nebo rychlém testu na antigen, který držitel podstoupil; nebo informace o prodělané infekci SARS-CoV-2 držitelem po pozitivním výsledku testu;

  metadata certifikátu, jako je vydavatel certifikátu nebo jedinečný identifikátor certifikátu

- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
  Síť očkovacích míst tvoří:
  - Distribuční očkovací místa;
  - Očkovací místa;
  - Velkokapacitní očkovací místa;
  - Ordinace, tedy poskytovatelé zdravotních služeb v oboru všeobecného praktického lékařství;
  - Mobilní očkovací týmy;
  - Další poskytovatelé zdravotních služeb.
- plánované lhůty pro výmaz jednotlivých kategorií údajů;
  - ISIN: Osobní údaje jsou a budou ukládány pouze po dobu nezbytně nutnou, ke splnění úkolů v oblasti zjišťování získávání informací o výskytu infekčních onemocnění k posouzení vývoje epidemiologické situace na území ČR, ke sledování zdravotního stavu obyvatelstva a k řízení poskytovaní zdravotní péče a souvisejících úkonů.
  - OČKO: Osobní údaje jsou ukládány po dobu přihlášení do náhledové aplikace a její využívání (jedná se o průběhovou paměť, data se neukládají).
  - Certifikát: Osobní údaje obsažené v certifikátech se zpracovávají pouze po nezbytnou dobu přijetí opatření ke zvládnutí pandemie COVID-19 v souladu s legislativou EU, stanovisek WHO a národních opatření v souvislosti se zvládnutím pandemie.
- obecný popis technických a organizačních bezpečnostních opatření (viz kontrolní zjištění č. 9) uvedených v čl. 32 odst. 1.

Kontrolou bylo zjištěno, že MZ v pozici správce v rámci předmětné kontroly zpracovává záznamy o činnostech zpracování, které obsahují informace uvedené v čl. 30 odst. 1 písm. a) - g) nařízení (EU) 2016/679.

S ohledem na uvedené kontrolující konstatují, že kontrolovaná osoba povinnost stanovenou v čl. 30 odst. 1 nařízení (EU) 2016/679 **splnila**.

Kontrolní zjištění č. 9:

Kontrolující dále s ohledem na předmět kontroly hodnotili, zda a do jaké míry kontrolovaná osoba plní povinnosti týkající se zabezpečení osobních údajů v souvislosti s certifikátem, zpřístupněným na OČKO, včetně aplikací Tečky a čTečky, jak je její povinností podle čl. 32 nařízení (EU) 2016/679. Předmětem analýzy byly uvedené aplikace pro platformu Android, neboť mobilní telefony na této platformě jsou v rámci České republiky výrazně rozšířenější a zkoumání aplikací pro tuto platformu je výhodnější z hlediska času i technické náročnosti.

V *„Záznamech o činnosti zpracování – Centrální rezervační systém očkování proti onemocnění COVID-19*“ (podklad č. 31.1.) je uvedeno, že MZ je ústředním orgánem státní správy pro zdravotní služby, ochranu veřejného zdraví, zdravotnickou vědeckovýzkumnou činnost, poskytovatele zdravotních služeb v přímé řídící působnosti, zacházení s návykovými látkami, přípravky, prekursory a pomocnými látkami, vyhledávání, ochranu a využívání přírodních léčivých zdrojů, přírodních léčebných lázní a zdrojů přírodních minerálních vod, léčiva a prostředky zdravotnické techniky pro prevenci, diagnostiku a léčení lidí, zdravotní pojištění a zdravotnický informační systém, pro používání biocidních přípravků a uvádění biocidních přípravků a účinných látek na trh. Jako takové vyhlašuje zásady bezpečnosti informací platné pro resort zdravotnictví pro uplatnění vhodných technických a organizačních opatření.

MZ má v obecné rovině, v souvislosti s implementací zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákona č. 181/2014 Sb.“), přijatou *„Politiku systému řízení bezpečnosti informací s účinností od 27. března 2019“* (podklad č. 12.5.). Záměrem vedení MZ je udržovat přiměřenou ochranu osobních údajů v souladu se zákony a jinými právními předpisy ČR, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na spolupracující organizace. Uvedená politika je závazná pro všechny zaměstnance dotčených organizací resortu MZ a spolupracující organizace. Jednotlivé dotčené organizace v rámci resortu mohou vytvářet vlastní verzi této politiky, ta však musí být vždy v souladu s Bezpečnostní politikou informací MZ a dalšími závaznými dokumenty. Politika podléhá revizi nejméně jedenkrát ročně, upravuje pravidla a postupy pro řízení dokumentace, pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací, pravidla a postupy pro prováděná auditů kybernetické bezpečnosti a pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

S ochranou osobních údajů, zejména technicko-organizačními opatřeními, souvisí také *„Metodický pokyn k implementaci Obecného nařízení o ochraně osobních údajů – GDPR na Ministerstvu zdravotnictví ČR“* (podklad č. 29.1.), ve kterém jsou nastavena např. tato opatření:

- V článku III. *„Osoby odpovědné za ochranu osobních údajů“* se uvádí, že za dodržování zásad, pravidel a postupů při zpracování osobních údajů realizovaných na jednotlivých sekcích, odborech a odděleních MZ odpovídají příslušní představení a osoba odpovědná za příslušnou činnost zpracování dle záznamů v rozsahu svých kompetencí. Oprávněné osoby mohou zpracovávat osobní údaje vždy jen v rozsahu podmínek realizace/typového řešení příslušného zpracování údajů odpovědná za příslušnou činnost. S osobními údaji mohou přicházet do styku:
  a) oprávněné osoby, které osobní údaje využívají k plnění svých služebních a pracovních úkolů, zejména osoby:

- provádějící zpracování osobních údajů,
- provádějící provoz technické infrastruktury pro zpracování osobních údajů;
- provádějící likvidaci osobních údajů;

b) další osoby ustanovené na základě vnitřních předpisů nebo smlouvy s MZ za podmínky, že byly předem průkazně seznámení s tímto pokynem, nařízením (EU) 2016/679 a dalšími relevantními obecně závaznými právními předpisy.

Osoby uvedené výše jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po ukončení služebního nebo pracovního poměru nebo smlouvy s MZ.

- V článku VIII. *„Opatření na ochranu osobních údajů“* je popsáno, že osobní údaje jsou uchovávány tak, aby bylo zajištěno správné a zabezpečené nakládání s osobními údaji papírové evidence v neoznačených uzamčených skříních a boxech; elektronické evidence v informačních systémech a prostředcích s řízeným přístupem a provozním monitoringem zabezpečujícím průkaznou dohledatelnost každé provedené operace s osobními údaji.

  Osobní údaje zaměstnanec nezveřejňuje bez ověření, že takový postup je možný a nezpřístupňuje je osobám, které neprokáží právo s nimi nakládat.

  Písemnosti a mobilní/externí/přenosné technické nosiče informací, jimiž disponuje MZ a které obsahují osobní údaje chráněné podle tohoto pokynu, musí být uchovávány pouze v neoznačených uzamykatelných skříních a boxech na pracovištích.

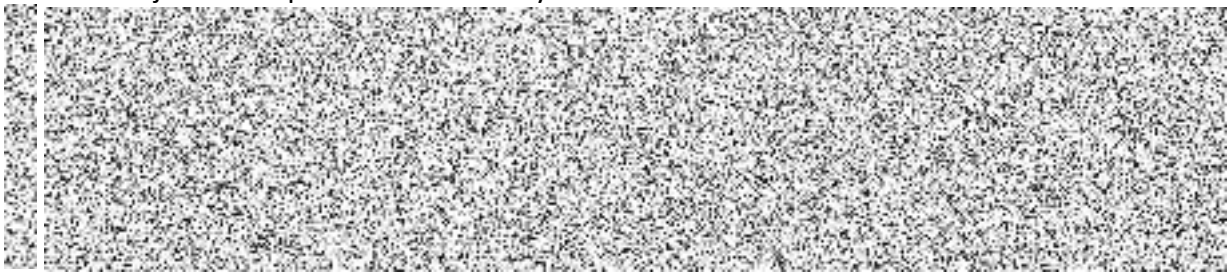
  V případě, že zaměstnanec zjistí, že zabezpečení osobních údajů, je nedostatečné, uvědomí o této skutečnosti bez zbytečného odkladu pověřence a svého přímého nadřízeného. Na základě tohoto oznámení učiní přímý nadřízený kroky potřebné ke zjednání nápravy.

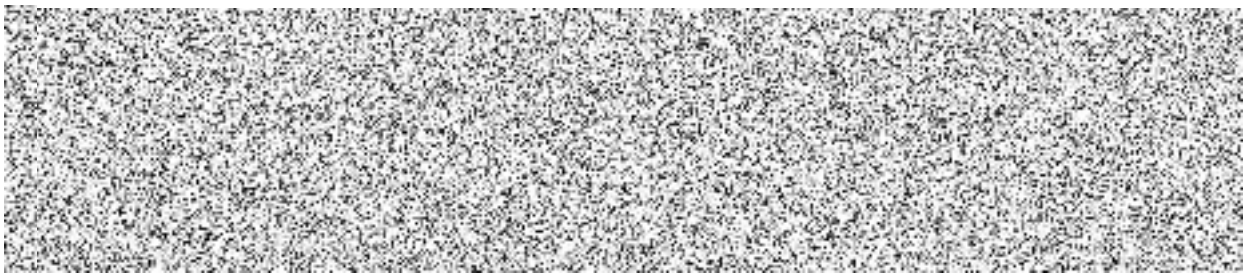
  Alespoň jednou ročně provede pověřenec ve spolupráci s právním odborem zhodnocení postupů, technických a organizačních při nakládání a zpracování osobních údajů. O zhodnocení postupů bude sepsán zápis.

- V článku XIII. *„Porušení zabezpečení osobních údajů“*:

  V případě zjištění porušení zabezpečení osobních údajů kontaktuje osoba, jež toto porušení zjistila neprodleně pověřence. O porušení zabezpečení vyrozumí rovněž svého přímého nadřízeného a v případě, že došlo porušení zajištění osobních údajů v elektronické evidenci i odbor informatiky. Pověřenec případ porušení bez zbytečného odkladu vyšetří a podnikne kroky stanovené čl. 33 a 34 nařízení (EU) 2016/679. V případě porušení zajištění osobních údajů v elektronické evidenci poskytne odbor informatiky pověřenci veškeré informace potřebné k učinění oznámení dle těchto ustanovení. Pověřenec vede evidenci veškerých případů porušení zabezpečení osobních údajů dle čl. 33 odst. 5 nařízení (EU) 2016/679.

Z vyjádření MZ kontrolující zdůrazňují níže uvedené informace, významné z hlediska ochrany osobních údajů v rámci předmětné kontroly:

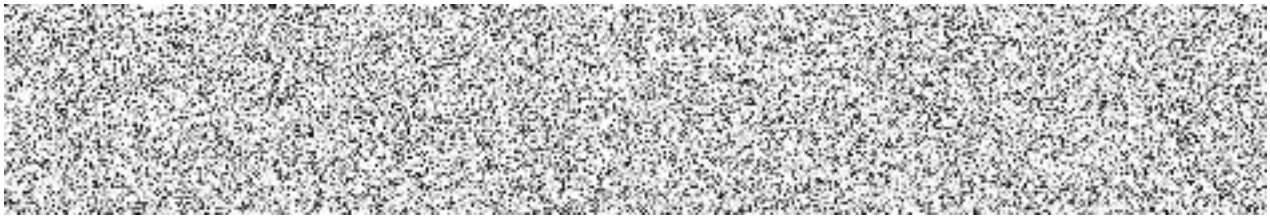




Přihlášení do OČKO je možné třemi způsoby ověření:

- Přihlášením pomocí účtu NIA – eIdentity. Tedy přihlášení pomocí elektronického občanského průkazu opatřeného čipem a aktivovanou komponentou pro komunikaci s veřejnou správou, nebo vytvořeným účtem NIA, případně bankovní identitou. Ověření přes bankovní identitu je možné pouze pro osoby, které jsou ověřeny přes registr obyvatel (ROB).
- Přihlášením pomocí rodného čísla a občanského průkazu. Jedná se o variantu pro osoby české národnosti, které jsou v registru obyvatel (ROB). Přihlášení je možné pouze pro osoby, které absolvovaly očkování, či test a uvedly číslo mobilního telefonu. Na telefonní číslo obdrží SMS zprávu s jednorázovým kódem, který během přihlašovacího procesu opíšou.
- Přihlášením pomocí čísla mobilního telefonu, e-mailu a data narození. Jedná se o variantu, kterou mohou využít i cizinci a děti bez občanského průkazu. Tento způsob přihlášení lze využít pro osoby, které absolvovaly očkování, či test a uvedly číslo mobilního telefonu. Na telefonní číslo obdrží SMS zprávu s jednorázovým kódem, který během přihlašovacího procesu opíšou. (podklad č. 21.1.)

Po přihlášení na OČKO má subjekt údajů možnost stáhnout jednotlivé certifikáty, nikdo jiný k nim přistoupit nemůže. Veškeré přístupy subjektu údajů jsou evidovány dle zákona č. 181/2014 Sb. . (podklad č. 12.)



OČKO neobsahuje cookie lištu, neboť nedochází k nastavování netechnických cookies. Z technických cookies je významná cookie „*cookiesession1*“, obsahující unikátní identifikátor, který má roční platnost. Na OČKO (webové stránce MZ) je umístěn odkaz „*Práce s cookie*“. Proklikem na tento odkaz subjekt údajů získá informace o cookies, které se však týkají webových stránek ÚZIS, nikoliv cookies na OČKO. Subjekt údajů je prostřednictvím zmiňovaného odkazu např. informován, že dochází k použití netechnických cookies, které ale OČKO aktuálně nevyužívá a které by vyžadovaly nasazení vhodné cookie lišty. (podklad č. 24.)

Aplikace Tečka je určena držitelům certifikátů a funguje jako „*peněženka*“, do které je možné načíst certifikát. Certifikáty jsou v aplikaci uloženy v zabezpečené formě. Po stažení aplikace do zařízení je držitel vyzván k přihlášení (ztotožnění), které probíhá přes OČKO, později se již aplikace připojuje automaticky. Vstup do aplikace je chráněn PINem, který si subjekt zvolí po ztotožnění, nebo rozpoznáním obličeje nebo otiskem prstu. V případě ztráty PINu je třeba

aplikaci odinstalovat, nainstalovat znovu a provést opětovné nahrání certifikátů. (podklad č. 24.)

Aplikace nabízí 3 možnosti načtení certifikátu.

1. Jedním z identifikačních prostředků eidentity.cz, propojit aplikaci s OČKO, odkud načte aktuální certifikáty a automaticky pak bude stahovat i všechny budoucí aktualizace. (Pokud chce subjekt údajů načíst certifikát do Tečky z OČKO, pomocí eidentity.cz, je nutné mít aktivovaný alespoň jeden z identifikačních prostředků eidentita.cz.)
2. Pomocí SMS kódu, který lze získat po přihlášení prostřednictvím zadání rodného čísla a čísla občanského průkazu, nebo zadání čísla mobilního telefonu, e-mailu a data narození, lze propojit aplikaci s OČKO odkud načte aktuální certifikáty a automaticky pak bude stahovat i všechny budoucí aktualizace.
3. Načtení QR kódu z papírového či jiného formátu certifikátu pomocí fotoaparátu nebo mobilního zařízení. (podklad č. 9.)

Tyto možnosti načtení lze zvolit i pro načtení certifikátů jiných držitelů, např. dětí, nebo jiných rodinných příslušníků. V aplikaci může subjekt údajů v nastavení upravit to, zda aplikace zobrazuje pouze platné, nebo i neplatné certifikáty. Jsou-li certifikáty načteny prostřednictvím QR kódů, nejsou tyto automaticky aktualizovány a v aplikaci se automaticky neprojeví např. nový certifikát o posilující dávce očkování. (podklad č. 24.)

Komunikace aplikace Tečky s OČKO probíhá šifrovaně, protokolem HTTPS. Aplikace umožňuje QR kód sdílet, a to buď ve formě obrázku či ve formátu HCERT. Je-li provedeno spárování aplikace Tečky s OČKO, je možné stáhnout i certifikát v PDF formátu. Aplikace Tečka rovněž umožňuje provádět screenshoty. Exporty a screenshoty uložených údajů je možné provádět až po ověření a exporty je nutné v aplikaci potvrdit (je vyžadován souhlas). Z dalších funkcí je významná funkce validace uložených certifikátů, díky čemuž má uživatel přehled o platnosti a možném použití uložených certifikátů k vybraným účelům. (podklad č. 24.)

Aplikace čTečka slouží k validaci certifikátů prostřednictvím načtení QR kódu, který je součástí certifikátu. Obě aplikace vyvíjí NAKIT. Jsou k dispozici pro mobilní telefony na platformách Android a iOS. (podklad č. 24.)

Kontrolující ověřili, že čTečka neukládá ověřované certifikáty v mobilním telefonu ani je nikam neposílá k ověření. V čTečce není v rámci validace zobrazen QR kód, pouze informace o držiteli certifikátu a informace o očkování / výsledku testu / prodělané nemoci a ověření – platný/neplatný certifikát. V této souvislosti kontrolující upozorňují, že z aplikace je možné provádět screenshoty, aplikace jejich pořizování sama nijak aktivně nebrání. Toto chování je v rozporu s primárním účelem aplikace, která má sloužit k ověření platnosti certifikátů, bez zanechání elektronické stopy s osobními údaji o tomto ověření. čTečka zároveň uchovává informace o počtu certifikátů, které byly ověřeny, s rozdělením na platné/neplatné. Tato funkce se chová jako počítadlo a neobsahuje bližší informace o certifikátech. (podklad č. 24.)

QR kód je tvořen složitou datovou strukturou, slouží pro ověření platnosti certifikátu pomocí mobilní aplikace (čTečka: https://ockodoc.mzcr.cz/napoveda/ctecka/cz/). QR kód na certifikátu obsahuje zašifrované informace, které nelze přečíst normální aplikací. Obsahuje informace o identifikaci osoby (jméno, příjmení, datum narození) a také informace o testu

či očkování. Po načtení QR kódu z certifikátu dochází ke spojení [redacted] a ověřují se aktuálně nastavená validační pravidla a na základě jejich vyhodnocení zobrazí aplikace informaci o stavu certifikátu (platný/neplatný). (podklad č. 3., 7., 12.)

K načtení QR kódu z certifikátu potřebuje čTečka přístup k fotoaparátu mobilního telefonu. Následně je možné načíst certifikáty do aplikace, která okamžitě po načtení provede validaci certifikátu, která probíhá bez připojení k internetu, výjimkou jsou certifikáty v původním formátu (vydávané do 1. června 2021). U těchto certifikátů je provedena automatická náhrada certifikátem v novém formátu, ta vyžaduje komunikaci s OČKO kvůli jeho stažení. Kontrolující ověřili, že automaticky je aktualizován jen certifikát, který byl skutečně vydán a funkci není možné použít k vydávání falešných certifikátů. Komunikace s OČKO je opět šifrovaná (protokol HTTPS). (podklad č. 24.)

Kontrolující upozorňují, že původní certifikáty obsahují v QR kódu URL adresu, prostřednictvím které je možné kdykoliv stáhnout certifikát v aktuálním formátu. V rámci přístupu ke stažení aktuální verze certifikátu nedochází k žádné formě ověření identity a certifikát je přístupný komukoliv, kdo je schopen získat či dovodit URL adresu pro aktualizaci certifikátu. Tato URL adresa rovněž obsahuje číslo pojištěnce ve formátu rodného čísla. Kontrolující upozorňují, že je-li QR kód v původním formátu přečten běžnou čtečkou QR kódů, tato ve většině případů nabídne načtení URL adresy v internetovém prohlížeči. Číslo pojištěnce tak může zůstávat v zařízení, konkrétně v historii navštívených stránek, a to v nechráněné podobě. (podklad č. 24.)

Aplikace Tečka a čTečka v pravidelných časových intervalech aktualizují informace o způsobu vyhodnocování platnosti certifikátů. Z informačního hlediska je významný hlavně seznam aktuálních podpisových certifikátů, prostřednictvím kterých jednotlivé státy podepisují informace, obsažené v QR kódech certifikátů a také informace o platnosti a validitě jednotlivých typů QR certifikátů. Tyto informace jsou následně uloženy v mobilním telefonu pro další použití. Aktualizace probíhá v denních intervalech, jsou-li aplikace spuštěny. Aktualizace je možné ručně vyvolat i častěji. (podklad č. 24.)

Obě aplikace pracují s veřejnými informacemi – seznamem podpisových klíčů členských států EU a definicemi validačních pravidel jednotlivých členských států EU. Pracují s údaji o fungování aplikace (např. záznamy o pádech aplikace a používání aplikace) a používají k tomu standardní nástroje [redacted]. S takto získanými údaji pracují maximálně po dobu 180 dní. (podklad č. 9.)

Aplikace komunikují jak [redacted], [redacted], [redacted]. Analýzou komunikace bylo zjištěno, že rozsah komunikace neodpovídá informacím o zpracování osobních údajů zmíněných aplikací. Konkrétně jsou uživatelé aplikace Tečka v informační povinnosti informováni o komunikaci se službou Firebase takto: „*Data odesílaná aplikací do těchto služeb neobsahují identifikátory vlastníka mobilního telefonu ani mobilního telefonu (jako je např. tel. číslo, IMEI, AdvertisingID) a zpracováváme je pouze za účelem vyhledávání a odstraňování kritických chyb, evidenci aktualizací aplikace a statistického zmapování používání aplikace uživateli. Aplikace nezná osobní údaje uživatele a tato telemetrická data tak nelze žádným způsobem navázat na jeho osobu.*“ (podklad č. 9.11., 9.12.)

Nicméně analýzou komunikace byly identifikovány následující údaje, které byly zaslány na servery [redacted]:

- Device model – informace o modelu mobilního telefonu;
- Os-build-version – informace o verzi operačního systému;
- Installation-id – unikátní identifikátor instalace aplikace. (podklad č. 24.)

Kontrolující konstatují, že kombinace těchto tří faktorů dává dohromady dostatečně podrobný souhrn dat, aby bylo možné na jejich základě jednoznačně identifikovat konkrétní mobilní zařízení, kde je aplikace identifikována. Dále byla zachycena informace o modelu mobilního telefonu, přenášená na OČKO. (podklad č. 24.

V rámci komunikace aplikace čTečka byl zachycen obsah spojení se službou Firebase Remote Config, o čemž není uživatel aplikace v informační povinnosti k aplikaci čTečka informován. V informační povinnosti se hovoří pouze o Firebase Crashlytics. Konkrétně je přenášen např. unikátní identifikátor instalace aplikace. (podklad č. 24.)

Na základě výše uvedených skutečností dospěli kontrolující k závěru, že kontrolovaný **neplní** povinnosti dle čl. 32 nařízení (EU) 2016/679, jelikož:

- v souvislosti s vydáváním původních certifikátů docházelo při načtení QR kódu čtečkou v mobilním zařízení ke zpřístupnění údaje o číslu pojištěnce držitele certifikátu;
- v aplikaci čTečka nebylo znemožněno pořizování screenshotu displeje, což je v rozporu se smyslem aplikace, tedy ověření platnosti certifikátů, bez zanechání elektronické stopy s osobními údaji o tomto ověření;
- informační povinnost k aplikacím Tečka a čTečka dostatečně nerozlišuje rozdíl mezi službami Firebase Crashlytics a Firebase Remote Config, subjekt údajů je informován pouze o první jmenované službě. (podklad č. 24.)

Kontrolní zjištění č. 10:

Kontrolující prověřili naplnění čl. 37 nařízení (EU) 2016/679, tj. povinnost správce jmenovat pověřence pro ochranu osobních údajů a tuto skutečnost oznámit Úřadu.

Úřadu byl dne 26. března 2021 řádně oznámen jmenovaný pověřenec pro ochranu osobních údajů. (podklad č. 16.)

V dokumentu „*Charakteristika služebního místa*“, je uvedeno, že zaměstnanec plní úkoly pověřence pro ochranu osobních údajů dle nařízení EU) 2016/679 pro MZ, jehož funkce je stanovena a popsána v článku IV. v „*Metodickém pokynu k implementaci Obecného nařízení o ochraně osobních údajů – GDPR na Ministerstvu zdravotnictví ČR*“. (podklad č. 21.5., 29.1.) Jsou zde vyjmenovány činnosti pověřence, konkrétně:

a) komunikuje se subjekty údajů, které se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv dle tohoto pokynu a nařízení (EU) 2016/679;
b) je informován o nedostatečném zabezpečení v oblasti ochrany a zpracování osobních údajů;

c) přijímá oznámení o případech porušení zabezpečení osobních údajů, prošetřuje a ohlašuje je dozorovému úřadu dle čl. 33 nařízení (EU) 2016/679 a oznamuje případy porušení ochrany osobních údajů subjektu údajů dle čl. 34 tohoto nařízení;
d) schvaluje návrhy na zahájení nového, resp. změnu dosavadního zpracování osobních údajů a zaujímá k takovýmto návrhům stanoviska;
e) plní další úkoly vyplývající pro jeho pozici z nařízení (EU) 2016/679, obecně závazných právních předpisů, tohoto pokynu nebo ostatních vnitřních předpisů MZ.

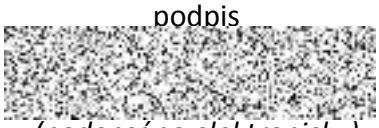
Kontrolující proto vyhodnotili zjištěný stav tak, že MZ jako správce **splnil** povinnost stanovenou v čl. 37 nařízení (EU) 2016/679.

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. et Mgr. Božena Čajková	vrchní rada odboru dozoru Úřadu	*(podepsáno elektronicky)* podpis
Bc. Hana Imiolková	pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis
Mgr. Zuzana Jeřábková	pověřená zaměstnankyně Úřadu	*(podepsáno elektronicky)* podpis
Ing. David Mrňák, DiS	pověřený zaměstnanec Úřadu	*(podepsáno elektronicky)* podpis
Bc. Jaromír Kuba	pověřený zaměstnanec Úřadu	 *(podepsáno elektronicky)* podpis