JUDr. Denisa Sudolská
advokátní kancelář

Soudní dvůr Evropské unie
Kancelář
L-2925 LUCEMBURK

elektronicky a souběžně poštovní službou

Dne 10. 2. 2023, Praha

Ve věci předběžné otázky C-659/22

Předkládající soud: Nejvyšší správní soud – Česká republika

Účastník řízení: [redacted]
zastoupený advokátkou JUDr. Denisou Sudolskou, ČAK se sídlem Italská 2, 120 00 Praha 2

*dále jen „**Účastník**“*

Vyjádření účastníka řízení k žádosti o rozhodnutí o předběžné otázce

Přílohy: *plná moc (spisem)*
dále dle seznamu příloh

AK Sudolská s.r.o. | Italská 1219/2, 120 00 Praha 2 | IČ 076 78 380
+420 777 122 208 | denisa.sudolska@aksudolska.cz | www.aksudolska.cz

Obsah vyjádření

I.
Úvod

[1] Navrhovateli byl dne 1. 12. 2022 doručen dokument „*Žádost o rozhodnutí o předběžné otázce C-659/22“,* ve kterém Kancelář Soudního dvoru Evropské unie vyzývá Účastníka řízení před původním vnitrostátním řízením před Nejvyšším správním soudem ČR, tamní sp. zn. 8 Ao 7/2022, tamního navrhovatele zrušení mimořádného opatření (opatření obecné povahy) Ministerstva zdravotnictví ze dne 29. 12. 2021, č.j. MZDR 14601/2021-34/MIN/KAN v rozsahu čl. I bodu 2 písm. b) a c), bodu 3 písm. b), bodu 6 písm. c) a d), bodu 7 písm. b), bodu 8 písm. a) a b), bodu 9 písm. a) a b), bodu 10 písm. a) a b), bodu 11 písm. b) a c), bodu 12 písm. c) a d), bodu 13 písm. b) a c), bodu 14 písm. c) a bodu 15 (dále jen „**Mimořádné opatření**“), k předložení písemného vyjádření k projednávané věci.

[2] V souladu se čl. 23 odstavcem druhým Statutu soudního dvora Evropské unie Účastník předkládá nadepsanému Soudními dvoru Evropské unie (dále jen „**Soudní dvůr**“) své vyjádření.

[3] Účastník tímto vyjádřením míní předložit své stanovisko k projednávané otázce zpracování osobních údajů s ohledem na východiska právní úpravy, indikativní odborná stanoviska a předběžně vyjádřené názory odborných institucí, v neposlední řadě s ohledem na potenciální dopady rozhodnutí Soudního dvora o předložené předběžné otázce.

II.
Podstata předběžné otázky

[4] V rámci vnitrostátního řízení před Nejvyšším správním soudem Účastník nynějšího řízení napadl Mimořádné opatření, které po občanech České republiky požadovalo (jako ostatně v řadě jiných zemí EU) prokázat provozovatelům rozličných podniků splnění podmínky tzv. bezinfekčnosti, a to za využití QR-kódu, který jednotliví provozovatelé kontrolovali v rámci české „národní" (vnitrostátní) aplikace „čTečka".

[5] Podstata kontroly národní aplikací „čTečka" je následující. Aplikace načte QR kód certifikátu kamerou mobilního telefonu. Následně zobrazí kontrolující osobě náhled na základní informace o certifikátu, tj. základní identifikační údaje držitele certifikátu (jméno, příjmení a datum narození) a stav platný/neplatný. Na vyžádání (kliknutí na tlačítko) aplikace zobrazí kompletní sadu informací uvedených v certifikátu (např. očkování, typ vakcíny, výrobce vakcíny, počet dávek, datum očkování, datum prvního pozitivního výsledku, členský stát EU, vydavatel certifikátu, identifikátor certifikátu). Aplikace tyto informace neuchovává a nikam neodesílá. Pouze je dočasně zobrazuje na obrazovce mobilního telefonu. Jde-li o ověření platnosti certifikátu, aplikace jednou za 24 hodin nebo na vyžádání stahuje veřejné klíče certifikátů členských států a validační pravidla členských států z rozhraní odpůrce. Aplikace při načtení QR kódu ověří veřejný klíč certifikátu a platnost certifikátu s ohledem na aktuálně platná validační pravidla.

*(celý proces kontroly dále označován jako „**Kontrola**")*

[6] Účastník Mimořádné opatření napadl z celé řady důvodů, pro které jej považoval za nesouladné s vnitrostátním právem zákonné i ústavní úrovně, mimo jiné kupř. pro absenci vnitrostátní pravomoci Ministerstva zdravotnictví České republiky, zároveň však (relevantně pro nynější řízení před Soudním dvorem) namítal, že užití aplikace „čTečka" za účelem Kontroly zasahuje nezákonným způsobem do práva na soukromí občanů České republiky. V odůvodnění Mimořádného opatření totiž absentuje jakékoliv zamyšlení nad rozsahem zpracovávaných údajů, jeho účelem, nebo nad způsobem jejich ochrany v rámci Kontroly.

[7] Nad rámec vnitrostátní úrovně Účastník dovodil, že napadené Mimořádné opatření je v rozporu s evropským komunitárním právem, konkrétně pak v rozporu s 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 též „**GDPR**").

[8] Soukromí a osobní údaje jsou na české vnitrostátní úrovni chráněny zákonem č. 2/1993 Sb., Listina základních práv a svobod (dále též „**LZPS**") konkrétně čl. 10 odst. 2 a 3, které stanoví, že „*Každý má právo na ochranu před neoprávněným zasahováním do soukromého*

a rodinného života“, a že „*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“.* Odpovídající úpravu ochrany soukromí obsahuje taktéž Listiny základních práv Evropské unie (dále též „**LZPEU**“), kdy konkrétně ve čl. 8 odst. 1 a 2 stanoví, že „*Každý má právo na ochranu osobních údajů, které se ho týkají.“*, a že „*Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“*.

[9] Účastník nemá žádných pochyb, že Mimořádné opatření je v rozporu s vnitrostátním právem ústavní úrovně, kdy je v rozporu s LZPS a v rozporu s nejzásadnější lidskoprávní úmluvou v oblasti ochrany lidských práv v Evropě , z důvodů, které uvedl již v původním návrhu na zrušení Mimořádného opatření před Nejvyšším správním soudem ČR.

[10] Bez ohledu na svojí technicistní textaci předběžná otázka předložená ESD nabývá do výše nastíněného lidskoprávního rozměru ochrany soukromí českých, a zprostředkovaně též evropských občanů, když zkoumá, zda při použití „národní“ aplikace „čTečka“ dochází k automatizovanému zpracování osobních údajů ve smyslu čl. 4 odrážky 2) GDPR.

[11] Lidskoprávní rozměr nařízení GDPR nicméně nepřikládá pouze Účastník tímto svým vyjádřením a všemi dosavadními vyjádřeními ve vnitrostátním řízení, ale učinil tak sám evropský zákonodárce, když v preambuli GDPR, v odůvodnění v bodě 1. GDPR vztahuje k základnímu právu na ochranu osobních údajů jako k právnímu východisku přijaté právní úpravy.

[12] **Nikoliv bezduše na tomto místě tedy Účastník uvádí, že odpověď na předloženou předběžnou otázku není jen a pouze technicistním ano / ne na téma věcné působnosti GDPR a je odpovědí z dalekosáhlým interpretačním přesahem pro původní úmysl evropského zákonodárce ochránit soukromí a osobní data evropských občanů.**

III.
Vyjádření

[13] Účastník na tomto místě transparentně předesílá, že stejně jako při podání návrhu na zrušení Mimořádného opatření před Nejvyšším správním soudem, i v nynějším řízení před Soudním dvorem zastává konzistentně stanovisko, že při „scanování" QR-kódů při ověřování platnosti interoperabilních certifikátů o očkování, testu a zotavení v souvislosti s onemocněním covid-19 vydávaných podle 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 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 (dále též „**Nařízení č. 2021/953**"), které jsou Českou republikou používány pro vnitrostátní účely, **dochází** k automatizovanému zpracování osobních údajů ve smyslu čl. 4 odrážky 2) GDPR.

[14] Toto Vyjádření Účastníka analyzuje následující oblasti, na základě čehož dochází k názoru, že v případě Kontroly dochází ke zpracování osobních údajů:

A. Východiska právní úpravy vyjádřené v preambuli (odůvodnění) GDPR;
B. Analýza věcné působnosti GDPR a definice zpracování ve smyslu čl. 4 odst. 2 GDPR;
C. Analýza článku 10 Nařízení 2021/953 ze dne 14. června 2021;
D. Užitelná prejudikatura evropských soudů a Soudního dvora ve věci zpracování ve smyslu čl. 4 odrážky 2) GDPR;
E. Relevantní stanoviska orgánů ochrany osobních údajů ve vztahu k digitálním certifikátům EU-COVID;
F. Srovnání verifikačních aplikací používaných v členských státech EU a jejich přístupu k GDPR-compliance;
G. Analýza dopadů rozhodnutí Soudního dvora o předběžné otázce na rozsah ochrany osobních údajů.

A.
Východiska právní úpravy vyjádřené v preambuli (odůvodnění) GDPR

[15] V prvním tematickém okruhu si Účastník dovoluje shrnout východiska ze kterých Evropský parlament vycházel při přijetí GDPR, kdy jednotlivé recitály představují jakési metanormy se zásadní interpretační hodnotou pro stanovení rozsahu věcné působnosti GDPR v předkládaném případě. Účastník je toho názoru, že právě preambule může být pomyslným jazýčkem na vahách, ze které bude možno dovodit, zda evropský zákonodárce GDPR koncipoval jako technicistní normu spíše užšího zaměření na systematické činnosti, či zda jejím účelem je spíše širší ochrana osobních údajů, a tím spíše silnější ochrana zvláštních kategorií osobních údajů, jako je právě údaj o zdravotním stavu a tzv. bezinfekčnosti.

[16] Účastník je toho názoru, že z analýzy jednotlivých níže citovaných recitálů preambule GDPR lze dovodit, že účelem GDPR je poskytovat ochranu osobních údajů v co možná nejširším rozsahu, a že z recitálů je možné takovýto záměr evropského zákonodárce bezpečně vyčíst.

[17] Z preambule GDPR vyplývá, že ochrana poskytovaná osobním údajům skrze GDPR je reakcí na technologie umožňující využívání osobních údajů orgánům veřejné moci a soukromým společnostem při jejích (jakékoliv) činnosti, což evropský zákonodárce považuje za **výzvu** pro oblast ochrany osobních údajů, když v 6. recitálu odůvodnění GDPR uvádí, že: „*Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu.*“

[18] Evropský zákonodárce zásadně předpokládá, že ke zpracování osobních údajů může docházet z mnoha důvodů, a samotné GDPR nepovažuje za vyčerpávající předpis poskytující ochranu právům osob při různých druzích zpracování ve specifických oblastech. Proto v recitálu 10. odůvodnění GDPR uvádí, že: „*Toto nařízení rovněž poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů („citlivé osobní údaje“). V tomto rozsahu nařízení nevylučuje, aby právo členského státu stanovilo okolnosti konkrétních situací, při nichž dochází ke zpracování, včetně přesnějšího určení podmínek, za nichž je zpracování osobních údajů zákonné.*“

[19] Pakliže Evropský zákonodárce věcnou působnost v odůvodnění *apriori* a implicitně zužuje, činí tak například v recitálu 14. preambule GDPR, kdy uvádí, že:

„Toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“;

dále pak příkladmo v recitálu 15. preambule GDPR:

„Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Záznamy nebo soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určených hledisek, by do oblasti působnosti tohoto nařízení spadat neměly.“;

nebo pravomoc zužuje explicitně, když některé činnosti z věcné působnosti zcela vyjímá, jako tak činí v recitálu 18. preambule GDPR:

„Toto nařízení se nevztahuje na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností. Činnosti osobní povahy nebo činnosti v domácnosti by mohly zahrnovat korespondenci a vedení adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi. Toto nařízení se však vztahuje na správce nebo zpracovatele, kteří pro tyto činnosti osobní povahy či činnosti v domácnosti poskytují prostředky pro zpracování osobních údajů.“

[20] Co se týče rozsahu zásad ochrany údajů, ty by se měly dle recitálu 26. preambule GDPR vztahovat na všechny informace týkající se identifikované nebo identifikovatelné fyzické osoby. Ve stejném bodu je pak aplikace zásad rozšířena i na pseudonymizované osobní údaje, které by mohly být přiřazeny fyzické osobě na základě dodatečných informací. Rovněž je uvedeno, že při rozhodování o tom, jestli je osoba identifikovatelná bude třeba přihlédnout k tomu, jaké prostředky budou při identifikaci použity. Při tomto posuzování je výslovně stanoveno, že by se mělo přihlížet k objektivním faktorům, jako jsou náklady a čas, které si identifikace žádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji.

[21] Shodně jako na vícero místech tohoto vyjádření, ale i dřívějších Vyjádřeních Účastníka adresovaných předkládajícímu soudu, je vhodné upozornit na zvláštní důraz unijního zákonodárce kladený na ochranu zpracování osobních údajů o zdravotním stavu. Tento zvláštní důraz lze dovodit z vícero ustanovení preambule, přičemž důležitou interpretační hodnotu má zejména recitál 52. preambule GDPR, který takovým údajům přisuzuje zvláštní hodnotu, která by měla být zajištěna speciálními a vhodnými zárukami. Dále se recitál o zpracování osobních údajů o zdravotním stavu vyjadřuje jako o odchylce, která může být přípustná pouze pokud je zároveň patřičně odůvodněná.

[22] Preambule na mnoha místech stanoví, že je vždy při styku, v rámci kterého dochází ke zpracování osobních údajů, na místě zajistit náležitou úroveň bezpečnosti, včetně důvěrnosti, s ohledem na stav techniky. Příkladmo je v recitálu 83. preambule GDPR uvedeno šifrování jako jeden z nástrojů, který by k bezpečnosti zcela jistě napomáhal. V tomto ohledu je možno již nyní poznamenat, že zákonodárce, který si není vědom toho,

že vytváří právní akt, v rámci jehož realizace bude docházet ke zpracování osobních údajů, logicky nebude zajišťovat náležitou úroveň bezpečnosti a důvěrnosti s ohledem na stav techniky ve smyslu GDPR. Tato skutečnost pak vede k závěru, že ani aplikace „čTečka“ nemůže dosahovat požadovaných bezpečnostních kvalit.

[23] Recitál 87. preambule GDPR dále směřuje k tomu, že je nutné, aby byla zavedena *„… veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány.“* V tomto případě lze shodně s předešlým odstavcem tohoto vyjádření dovodit, že zákonodárce, který si není vědom toho, že vytváří právní akt, v rámci jehož realizace bude docházet ke zpracování osobních údajů, nebude cítit potřebu zmíněná technická a organizační opatření inkorporovat.

[24] V obdobném duchu je možné poukázat na recitály 89. až 92. preambule GDPR, které **zdůrazňují roli dozorových orgánů** v případě rozsáhlých operací zpracování údajů, v případě, že taková zpracování mají sloužit ke zpracování značného množství osobních údajů na regionální nebo celostátní úrovni, a jež by mohly mít dopad na velký počet subjektů těchto údajů, a u nichž je pravděpodobné, že budou představovat vysoké riziko pro práva a svobody subjektů údajů. Toto platí zejména v případech, kdy s ohledem na tyto operace je pro subjekty údajů obtížnější uplatnit svá práva. Taková situace vyžaduje důkladné posouzení vlivů na ochranu osobních údajů (viz recitál č. 90), nad čímž se český zákonodárce nezamýšlel ani náznakem, kdy dozorový orgán v podobě Úřadu na ochranu osobních údajů při přípravě Mimořádného opatření nekonzultoval.

[25] Na povinnost konzultaci s dozorovým orgánem pak pamatuje recitál č. 96 preambule GDPR, přičemž Účastník je přesvědčen, že pakliže by legislativec postupoval souladně s tímto recitálem, musel by v rámci konzultací s dozorovým úřadem nutně dojít k tomu, že Mimořádné opatření upravuje zpracování osobních údajů ve smyslu GDPR, ke kterému dochází při Kontrolách, a byl by je možná býval vhodně upravil. K tomu nicméně zjevně nedošlo.

[26] Ze všech výše uvedených důvodů se Účastník domnívá, že lze učinit o GDPR následující teleologické závěry. Záměrem evropského zákonodárce bylo postihovat co možná největší škálu myslitelných situací, kdy je jakkoliv nakládáno s osobními daty, neboť tato data je třeba chránit. O nakládání zjevně tedy půjde v situacích, kdy jsou osobní data nějakým způsobem přímo či nepřímo ohrožena, nebo taková hrozba existuje alespoň latentně, z toho důvodu, že jsou data v daný okamžik zpřístupňována. V případě, že se na nějaký druh zpracování GDPR nevztahuje, evropský zákonodárce na to výslovně pamatuje, a takové věci v předpise výslovně uvádí. Evropský zákonodárce navíc dbal na to, aby předpis GDPR měl takovou kvalitu a rozsah, že bude moci být použit i za předpokladu, že v oblasti zpracování osobních údajů budou využívány nové či dostupnější technologie.

B.
Analýza Kontroly v rámci demonstrativní definice zpracování ve smyslu čl. 4 odrážky 2) GDPR a věcné působnosti GDPR

[27] V této části Účastník analyzuje problematiku věcné působnosti GDPR v obecné rovině, důkladně analyzuje pojem zpracování ve smyslu čl. 4 odrážky 2) GDPR a dále též pojem „částečně automatizované zpracování“, kterýmžto kontrola digitálního certifikátu EU COVID národní aplikací „čTečka“ dle Mimořádného opatření dle jeho názoru byla, resp. stále je. Touto analýzou dochází Účastník k názoru, že Kontrola spadá do věcné působnosti GDPR, a že v rámci Kontroly dochází k takovým operacím s osobními údaji, které v pojmových znacích odpovídají pojmu zpracování tak, jak s ním pracuje GDPR.

[28] Účastník je toho názoru, že Kontrola svojí povahou spadá do věcné působnosti GDPR, kdy se jedná o posloupný proces jednotlivých operací s osobními údaji od jejich předložení, přes vlastní načtení až po vyhodnocení jejich souladnosti s aktuálními validačními pravidly, které probíhají alespoň částečně automatizovaným způsobem, když je k nim použita aplikace „čTečka“, a to bez ohledu na to, zda intenzity zpracování dosahují již některé dílčí operace, nebo teprve až jejich souhrn.

[29] Je zjevné, že v rámci Kontroly dochází k operaci s osobními daty, kterou provádí kontrolující osoba za pomocí k tomu navrženého softwaru, který je z logiky věci automatizovaný. V rámci Kontroly se dá zjednodušeně říci, že dochází k následujícím operacím s osobními daty:

- *Předložení QR-kódu implicitně obsahujícího osobní údaje kontrolovanou osobou, tedy fyzická operace provedená kontrolovanou osobou (dále též „**Operace 1**“)*
- *Načtení QR-kódu aplikací „čTečka“, tedy fyzická operace provedená kontrolující osobou za pomocí aplikace „čTečka“ (dále též „**Operace 2**“)*
- *Převedení informací obsažených v lidsky nečitelné podobě z QR-kódu do lidsky čitelné podoby (slov), tedy operace provedená automatizovaně čistě aplikací „čTečka“ (dále též „**Operace 3**“)*
- *Vyhodnocení (validace) těchto dat za účelem povolení nebo odepření přístupu ke službě[1], tedy operace provedená automatizovaně čistě aplikací „čTečka“ (dále též „**Operace 4**“)*

[30] Rozhodnutí o nynější předběžné otázce v tomto řízení je de facto zásadním rozhodnutím pro věcnou působnost GDPR jako celku. Ve vztahu ke čl. 2 odst. 1 GDPR si Účastník dovoluje shrnout, že GDPR rozlišuje následující kategorie zpracování:

- *zpracování zcela automatizované*
- *zpracování částečně automatizované*
- *neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci*

[1] Operace 3 a 4 probíhají souběžně

- *neautomatizované zpracování osobních údajů, které mají být do evidence zařazeny.*

Zpracování zcela automatizované

[31] GDPR neobsahuje žádné vysvětlení pojmu automatizace. Zjevně ale nebude zásadnějšího sporu o to, zda může být kontrola **zpracováním zcela automatizovaným**, kdy je zřejmé, že bez přítomnosti kontrolující osoby, která používá aplikaci „čTečka" by ke zpracování nemohlo dojít vůbec. Jakkoliv postoupil vývoj v oblasti umělé inteligence daleko, jen stěží si lze představit, že by bylo možné aplikací cokoliv „zcela automatizovaně" načíst.

[32] Zpracování zcela automatizované je zjevně takové zpracování, při kterém dochází k výpočetním operacím bez lidské iniciativy a lidské ingerence. Český národní Úřad na ochranu osobních údajů k pojmu automatizace vykládá následovně: „*Automatizaci lze vyložit tak, že jde o zpracování pomocí informačních systémů, tj. prostřednictvím softwaru, který je z logiky věci automatizovaný. Lze tedy zjednodušit, že automatizovaně znamená prostřednictvím výpočetní techniky.*"[2]

[33] Lidská činnost v rámci Kontroly byla elementárním předpokladem výkonu Kontroly, neboť se jednalo o povinnost stanovenou obecně vymezenému okruhu **osob** (provozovatelů regulovaných podniků)**,** které měly povinnost Kontrolu provádět za pomocí aplikace „čTečka" a bez jejich iniciativy a přispění by ke Kontrole ani nemohlo dojít. Za takové situace lze relativně bezpečně usoudit, že Kontrola **není zpracováním zcela automatizovaným**.

[34] Lze snad polemizovat, zda by na toto právní posouzení mělo dopad, kdyby v rámci procesu Kontroly absentovala kontrolující osoba, a kontrolující mobilní aplikace „čTečka" by byla na turniketu u vstupu do regulovaného podniku - pak by šlo uvažovat i o tom, že byla Kontrola pojmově zpracováním osobních údajů zcela automatizovaným. Vzhledem k tomu, že v praxi nicméně byla Kontrola prováděna osobami pověřenými regulovanými podniky (číšníky, hosteskami, prodavači vstupenek etc.), kteří na základě výsledku Kontroly rozhodli o poskytnutí služby či nikoliv, o zcela automatizované zpracování zřejmě nešlo. Je nicméně pravdou, že taková případná nuance by neměla dopad na to, zda Kontrola spadá do věcné působnosti GDPR, když by tomu tak bylo v obou případech – jediný rozdíl by byl v tom že by šlo o zpracování zcela automatizované bez dalšího. Zjevně by byl však nelogickým případný závěr, kdyby „turniketová" kontrola za pomocí aplikace „čTečka" zpracováním byla, a skutečně probíhající Kontrola nikoliv jen z toho důvodu, že byla do Kontroly zapojena kontrolující osoba.

[2] https://www.uoou.cz/3-nejdulezitejsi-pojmy/d-27293/p1=4744

Zpracování částečně automatizované v rámci Operace 2 a úvaha nad QR-kódem, jakožto osobním údajem sui generis

[35] V této části Účastní míní Účastník vypořádat úvahu, kterou vyjádřil předkládající soud v bodě 20 svého předkládacího usnesení, totiž, že načtení QR-kódu aplikací čTečka a jejich převedení Operacemi 2 a 3 spíše není zpracováním osobních údajů, neboť e jedná o „pouhý překlad". Předkládající soud přímo uvedl: „*Při pouhém překladu informací ze strojové podoby do podoby čitelné pro člověka a jejich zobrazení na mobilním telefonu totiž nehrozí, že dojde ke zneužití osobních údajů a k zásahu do práva na ochranu osobních údajů, neodesílá-li nikam aplikace data za účelem jejich překladu. Fakticky jde totiž o pouhou výpočetní operaci, při které není s osobními údaji jakkoliv nakládáno."* S tímto vyjádřeným názorem Účastník nemůže souhlasit.

[36] Jak již ostatně vyplývá z podnadpisu této části vyjádření, nabízí se otázka, zda je QR-kód skutečně jenom určitým způsobem zachycení sumy osobních údajů, nebo zda v případě vytvoření QR-kódu zachycujícího informace o jeho držiteli, které jsou jinak vedeny i v lidsky čitelné podobě na certifikátu, nevzniká osobní údaj zcela nový.

[37] Definice osobních údajů ve čl. 4 odst. 1 GDPR je definicí velice širokou. Osobními údaji rozumí **veškeré informace o identifikované nebo identifikovatelné fyzické osobě**, kdy identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

[38] V případě samotného QR-kódu je z jeho fungování zřejmé, že se jedná o soubor jednotlivých informací o jednotlivých osobách. QR-kód každého držitele certifikátu je tedy ze své podstaty unikátní, a odlišitelný od osoby jiné.

[39] Z této premisy vcelku jednoznačně vyplývá, že vytvořením QR-kódu pro účely digitálního certifikátu EU COVID pro konkrétní osobu, je vytvořen pro každého držitele QR-kódu zcela nový **identifikátor**, který je schopen s naprostou spolehlivostí odlišit jednotlivé držitele již z titulu svojí **unikátní** grafické podoby.

[40] Z velice podobné logiky koneckonců vychází i samotné Nařízení č. 2021/953, které zakotvuje to, že digitální certifikáty EU COVID v sobě obsahují tzv. „jedinečný identifikátor certifikátu", jakožto jedinečný identifikátor přidělený na základě společné struktury každému certifikátu vydanému. Takovýto jedinečný identifikátor je kupř. v případě certifikátu Účastníka lidsky čitelný, avšak na první pohled má pro neznalou osobu absolutně nic neříkající výpovědní hodnotu.

[41] Z recitálu č. 19 Nařízení č. 2021/953 nicméně vyplývá, že je na základě „jedinečného identifikátoru certifikátu" možná **nikoliv přímá identifikace držitele** certifikátu, nicméně

stále ještě identifikace. Zároveň recitál uvádí, že „*použití jedinečného identifikátoru certifikátu zabraňuje tomu, aby bylo třeba zpracovávat **další** osobní údaje, které by jinak byly k identifikaci jednotlivých certifikátů nezbytné.*“ – kde užívá recitál slovní spojení „**další** osobní údaje“ a tím zjevně implikuje, že už jedinečný identifikátor certifikátu je osobním údajem, na základě jehož je možné určitou osobu identifikovat. Ostatně taktéž z předposlední věty recitálu č. 19 Nařízení č. 2021/953, která zní „*Seznamy zrušených certifikátů by neměly obsahovat **žádné osobní údaje s výjimkou jedinečných identifikátorů certifikátu.“***, lze vcelku bezpečně vyčíst, že „nicneříkající“ jedinečný identifikátor certifikátu je také osobním údajem.

[42] Pakliže je osobním údajem s potenciálem identifikovat držitele certifikátu jedinečný identifikátor certifikátu, přestože nemá na první pohled významnější výpovědní hodnotu, je možné uvažovat o tom, že totožně je osobním údajem samotný QR-kód jakožto osobní údaj *sui generis*.

[43] Přestože QR-kód obsažený v digitálním certifikátu „obsahuje“ „jednoznačné“ osobní údaje, jako je jméno, příjmení či datum narození, je vhodné si uvědomit, že i grafická podoba certifikátu je způsobilá, byť nikterak snadno, zcela spolehlivě rozlišit jednotlivé držitele osobních údajů, a sama grafická podoba QR-kódu je tedy osobním údajem **identifikovatelné osoby,** tak jak s tímto pojmem pracuje věta druhá čl. 4 odst. 1 GDPR.

[44] K identifikaci osoby už tedy může dojít na základě výše pojmenované Operace 2, tedy samotným načtením QR-kódu, byť je zřejmé, že s dnešními technickými možnostmi problematický dopad do osobní sféry držitele certifikátu „prozatím“ nastává až Operacemi 3 a 4. Zpracováním by tedy bylo již samotné načtení QR-kódu jakožto osobního údaje *sui generis* v Operaci 2, bez nutnosti toho, aby celá Kontrola byla zpracováním osobních údajů teprve pro jejich zpracování v rámci Operací 3 a 4.

[45] Pakliže by byl přijat závěr, že QR-kód je osobním údajem *sui generis*, bylo by jeho načtení, resp. vyfocení aplikací čtečka zpracováním úplně totožně, jako je kupř. analogické zpracování osobního údaje načtením resp. vyfocením podoby člověka při automatické pasové kontrole na letištích, která je dostupná pro občany Evropské unie, kteří jsou zároveň držiteli biometrického pasu, při cestování v rámci Schengenského prostoru.

[46] S ohledem na skutečnost, že i GDPR v recitálu 6 připouští, že je GDPR reakcí na technologický rozvoj, nelze vyloučit, že dojde k technologickému posunu, kupř. v oblasti kyber-implantátů, který do budoucna umožní „dekódování“ QR-kódů prostým lidským zrakem. [3] Za takových okolností je vhodné zvažovat i tu eventualitu, že osobním údajem způsobilým identifikace držitele je i samotný QR-kód bez ohledu na jeho obsah, neboť ten sám o sobě je již přiřazen držiteli konkrétního digitálního certifikátu EU COVID.

Zpracování částečně automatizované - převod QR-kódu do lidsky čitelné podoby v rámci Operace 3

[47] V rámci samostatné Operace 3 dochází k překladu lidsky (pravděpodobně[4]) nečitelného QR-kódu do lidsky čitelné podoby, kdy dochází ke zobrazení dat obsažených v QR-kódu v lidsky srozumitelných slovech a číslech (jména, věcné informace a data).

[48] Předkládající soud se domnívá, že se jedná o pouhou *výpočetní operaci, při které není s osobními údaji jakkoliv nakládáno,* a z toho důvodu dovozuje, že Operace 3 sama o sobě pravděpodobně není zpracováním osobních údajů ve smyslu čl. 4 odst. 2 GDPR. S tímto vyjádřeným názorem Účastník nesouhlasí.

[49] Pojmová definice čl. 4 odst. 2 GDPR je definicí širokou a extenzivní, která zaručuje ochranu adresátům normy před tím, aby jakákoliv operace s osobními daty představovala riziko jejich úniku. Definice obsažená ve čl. 4 odst. 2 GDPR je toliko definicí demonstrativní, nicméně je zřejmý úmysl zákonodárce postihovat všechny operace při kterých může dojít k diseminaci osobních údajů osobám, které potenciálně mohou ochranu osobních údajů jednotlivce ohrozit.

[50] Z výše uvedeného důvodu proto přímo čl. 4 odst. 2 GDPR definuje, že zpracováním *je* ***jakákoliv operace nebo soubor operací****, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.*

[51] Z výše uvedených demonstrativních příkladů možností, jak zpracovávat osobní údaje v případě Operace 3, přichází v úvahu hned několik předložených. Těm jsou zejména:

- **zaznamenání;**
- **přizpůsobení;**
- **nahlédnutí;**
- **použití;**
- **jakékoliv jiné zpřístupnění.**

[52] O **zaznamenání** se může jednat s ohledem na skutečnost, že minimálně po dobu trvání Kontroly jsou osobní údaje zaznamenány, byť nikoliv trvale, do operační paměti zařízení, ve kterém je příslušná aplikace „čTečka“. Je však otázkou, zda je na místě vykládat pojem „*zaznamenání*“ i jako operaci při které dochází k pouze „dočasnému“ zaznamenání osobního údaje, a to pouze po dobu trvání Kontroly.

[4] k rozlišovací schopnosti QR-kódu bez jeho dekódování viz výše v bodě 39. tohoto vyjádření

[53] Z podstaty věci je **zaznamenáním** osobního údaje jeho zápis, nebo jiná sumarizace v časem přítomném pro další použití v čase budoucím, kdy k tomuto spíše nedochází, neboť osobní údaje mají být zaznamenány pouze pro účely kontroly v daném čase a místě. Přesto však nelze vyloučit, že po dobu trvání této operace musí být zaznamenány alespoň v operační paměti, či mezipaměti aplikace „čTečka“ a určitý záznam je tedy alespoň po určitý časový interval zaznamenáván.

[54] O něco jednoznačnější je pak nicméně situace v otázce toho, zda v rámci Kontroly mohlo dojít k **přizpůsobení** osobních údajů do podoby, ve které je zobrazuje právě aplikace „čTečka“. Pakliže přijmeme závěr, že QR-kód je záznamem osobních dat v lidsky nečitelné podobě, který je pro účely Kontroly potřeba převést do lidsky čitelné podoby (v rámci Operace 3), pak je zřejmě bezpečné učinit závěr, že právě Operace 3 je přizpůsobením osobních údajů ve smyslu čl. 4 odst. 2 GDPR.

[55] Samotný předpis význam slova přizpůsobení (resp. adaptation v anglické jazykové verzi) nikterak nevysvětluje. Dalo by se snad uvažovat, že by přizpůsobení mohlo dotýkat pozměňování osobních údajů za účelem toho, aby s nimi bylo možné unifikovaně nakládat v rámci určité databáze, nicméně pro tyto situace zjevně GDPR ve čl. 4 odst. 2 používá pojem ***pozměnit***.

[56] Definičním znakem přizpůsobení tedy je zřejmě jakákoliv operace s osobním údajem, která nemá za následek změnu jeho podstaty (obsahu / vypovídající hodnoty), ale má za následek to, že osobní údaj změní svoji formu, kupř. z formy nikoliv elektronické do formy elektronické.

[57] K takové situaci zjevně došlo v rámci Operace 3, kdy mohla být papírová forma certifikátu na základě QR-kódu obratem převedena do formy elektronické, která se zobrazila v aplikaci „čTečka“. Změna formy certifikátu z papírové formy, do digitální formy „záznamu“ o certifikátu v aplikaci „čTečka“ dle názoru Účastníka pojmově odpovídá zpracování osobního údaje přizpůsobením.

[58] Zároveň i v případě, kdy dojde k načtení certifikátu, který je již v digitální podobě (kupř. je ve formátu .pdf zobrazen na mobilním telefonu kontrolované osobě) dochází k přizpůsobení údajů do formátu, který používá aplikace „čTečka“, třebaže jsou v obou případech v digitální a nikoliv papírové podobě, a třebaže nejsou nijak pozměněny.

[59] Pakliže by Operace 3 byla pouhým převodem a nikoliv zpracováním spočívajícím v **přizpůsobení**, pak by bylo otázkou co už jiného lze podřadit pod pojem přizpůsobení. Bylo by pak nelogicky nutné uzavřít, že pojem přizpůsobení je ve čl. 4 odst. 2 GDPR používán bezúčelně, neboť jiný příklad zpracování osobního údaje přizpůsobením lze dle Účastníka nalézt jen těžko.

[60] Obdobné právní posouzení a právní argumentace dopadají též na pojem **nahlédnutí** užitý ve čl. 4 odst. 2 GDPR. Stejně jako v případě zaznamenání a přizpůsobení ani pojem nahlédnutí nikterak GDPR nevysvětluje.

[61] Účastník nemá pochyb o tom, že v případě Kontroly dochází v pravém slova smyslu k nahlédnutí do jeho osobních údajů, kdy kontrolující osoba skutečně nahlíží do jeho osobních údajů uvedených v certifikátu, a to za pomocí alespoň částečně automatizovaného zpracování.

[62] Ke zpracování nahlédnutím může jistě docházet kupř. při nahlédnutí do již existující databáze (evidence) osobních údajů. Účastník je nicméně toho názoru, že je lhostejno „kam" je nahlíženo, neboť bez ohledu na to, zda je nahlíženo jednorázově do existující evidence, nebo jednorázově do digitálního certifikátu EU COVID, neboť v obou případech je dopad na osobní údaj jednotlivce totožný.

[63] Nahlížením je dle Účastníka třeba rozumět situaci, kdy je umožněno určité osobě seznámit se s osobním údajem, a v takovém případě jde o zpracování. V rámci kontroly je kontrolující osobě umožněno nahlížet alespoň částečně automatizovaným způsobem na konkrétní osobní údaje kontrolované osoby, a tímto je naplněna premisa zpracování nahlížením ve smyslu čl. 4 odst. 2 GDPR.

[64] Nad slunce jasné je, že v rámci Kontroly dochází k **použití osobních údajů**, z definice čl. 4 odst. 2 GDPR. Údaje, bez ohledu v na to v jaké konkrétní Operaci, nebo v jejich souhrnu, jsou použity za účelem kontroly splnění předpokladu bezinfekčnosti. Použitím osobních údajů je třeba rozumět jejich využití k určitému účelu, naplnění jejich potenciálu nebo obecně užití osobního údaje jako nástroje se schopností rozlišit osobu naplňující určitá kritéria od osoby taková kritéria nenaplňující.

[65] V případě, že by byl přijat závěr, že se v případě Kontroly nejedná o zpracování osobních údajů jejich použitím, implikoval by takový závěr, že celý proces Kontroly byl bezúčelným, neboť bez **použití** osobních údajů by Kontrola postrádala smysl. Podstatou Kontroly je totiž použití osobních údajů za účelem vyhodnocení toho, zda bude konkrétní osobě umožněno využít regulované služby, či nikoliv.

[66] Kdyby v tomto duchu nebyly osobní údaje kontrolované osoby použity ve smyslu GDPR, zjevně neexistuje právní pojem, který by postihoval to, jak s nimi bylo v rámci Kontroly nakládáno. **V rámci Kontroly totiž osobní údaje rozhodovaly o tom, zda bude kontrolované osobě umožněn výkon práva, či nikoliv.** Úvahu, že o zpracování nešlo je třeba striktně odmítnout, tím spíše za situace, kdy Česká republika podzákonným předpisem vyžadovala, aby použitím osobních údajů pro účely Kontroly byla omezována (!sic) základní lidská práva.

[67] Z výše uvedeného důvodu se Účastník domnívá, že v rámci Kontroly dochází bez pochyby ke zpracování osobních údajů jejich použitím.

[68] Konečně shodný osud jako výše uvedené druhy zpracování sdílí i zpracování **jakýmkoliv jiným zpřístupněním**. Lze snad spekulovat, zda evropský zákonodárce nemínil touto formulací postihovat případy diseminace a zveřejnění osobních údajů, nicméně bez konkrétního vodítka není možné zcela spolehlivě vyloučit, že předložení certifikátu k jeho kontrole je právě jakýmkoliv jiným zpřístupněním.

[69] **Závěrem této části** si dovoluje Účastník opakovaně připomenout, že definice ve čl. 4 odst. 2 GDPR je definicí demonstrativní, a jak ukazuje výše nastíněná analýza byť jen pěti z demonstrativních modů zpracování osobních údajů, je definicí velice širokou.

[70] Spolehlivý závěr, který lze dle výše uvedeného výkladu přijmout je ten, že ani kdyby pojmově Operace 1-4 neodpovídaly jednotlivým modům zpracování ve smyslu čl. 4 odst. 2 GDPR, hned návětí článku hovoří o tom, že zpracováním je **jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji**, a v podstatných znacích se shodují alespoň s některými analyzovanými mody zpracování.

Zpracování částečně automatizované a (de)pseudonymizace v rámci Operace 3

[71] Následně se jeví účelným posoudit, zda může být Kontrola **zpracováním částečně automatizovaným**. Je zjevné, že jde o operaci s osobními daty, kterou provádí kontrolující osoba za pomocí k tomu navrženého softwaru, který je z logiky věci automatizovaný. Z výše uvedených operací je zjevné, že k Operacím 2, 3 a Operaci 4 je potřeba aplikace „čTečka“, která v souladu s výkladem automatizace Úřadu na ochranu osobních údajů (viz výše), pomocí výpočetní techniky s těmito údaji nakládá.

[72] V rámci Operace 3 dochází k operaci se samotným QR kódem. Co se týče samotného QR kódu, anglická encyklopedie Britannica k němu nabízí následující definici: „*QR Code, in full Quick Response Code, a type of bar code that consists of a printed square pattern of small black and white squares that encode data which can be scanned into a computer system… QR Codes are usually* ***read with laser scanners or cameras on mobile telephones, which then use special software to decode the pattern.“***[5]

[73] Jinými slovy QR-kód je způsobem zaznamenání určitého objemu dat, který je převeden do kompaktní, lidsky nečitelné podoby, a je tedy tzv. zakódován, resp. zašifrován. K tomu aby byl převeden do lidsky čitelné podoby je potřeba jej za pomocí konkrétního softwarového řešení **dekódovat**, resp. dešifrovat.

[74] V okamžiku, kdy aplikace „čTečka“ převádí údaje z lidsky nečitelné podoby do podoby lidsky čitelné, dochází k dekódování / dešifrování osobních údajů, bez kterého by kontrolující osoba Kontrolu vůbec nemohla provést. Předkládající soud ve svém Usnesení 8 Ao 7/2022 -71 ze dme 12. října 2022 (dále též „**Usnesení**“) vyjádřil k Operaci 3 v bodě

[5] https://www.britannica.com/technology/QR-Code

20. Usnesení následující názor: „*Při pouhém překladu informací ze strojové podoby do podoby čitelné pro člověka a jejich zobrazení na mobilním telefonu totiž nehrozí, že dojde ke zneužití osobních údajů a k zásahu do práva na ochranu osobních údajů, neodesílá-li nikam aplikace data za účelem jejich překladu. Fakticky jde totiž o pouhou výpočetní operaci, při které není s osobními údaji jakkoliv nakládáno.*“

[75] Ve výše citovaném bodě 20. Usnesení tedy předkládající soud uvádí, že dochází k „pouhému překladu“ a ten pojmově nemůže být zpracování, neboť není operací s osobními daty. Účastník tento názor nesdílí. Bez použití aplikace „čTečka“ by totiž ze samotného QR-kódu nebylo kontrolující osobě zřejmé vůbec nic. Osobní údaje obsažené v QR-kódu je totiž zjevně potřeba **dešifrovat** a tedy s nimi nakládat.

[76] Takto zúžený názor by fakticky mohl mít následující nelogické implikace. V případech, kdy dochází k přenosu chráněných dat v kódované, kupř. anonymizované nebo pseudonymizované podobě, jako třeba v případech, kdy státní instituce poskytují občanům informace na základě práva na svobodný přístup k informacím, by takovýto výklad v praxi znamenal, že nedochází ke zpracování (a ohrožení) osobních údajů v situaci, kdy by se někdo takto chráněná data pokusil (a to třeba i nezákonně) **dešifrovat**. S takovým názorem se nelze ztotožnit.

[77] Dá se dokonce uvažovat o tom, že zašifrováním osobních údajů a údajů o zdravotním stavu do podoby QR-kódu dochází k tzv. „pseudonymizaci“ ve smyslu čl. 4 odst. 5 GDPR, neboť je zjevné, že bez použití aplikace „čTečka“ a údajích v jejím softwaru nemůže dojít k jejich přiřazení ke konkrétnímu subjektu. Definice pseudonymizace přitom hovoří o tom, že se pseudonymizací rozumí: „***zpracování*** *osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.*“

[78] Je zřejmé, že informace a „překladový kód“ jakožto dodatečná informace potřebná k identifikaci osoby na základě jejího QR-kódu je uchováván odděleně, elementární technická opatření jsou taktéž zavedena, a nelze tedy vyloučit, že kódováním osobních údajů do QR-kódů na základě 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 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 tedy dochází k tzv. pseudonymizaci ve smyslu čl. 4 odst. 5 GDPR.

[79] Pakliže by takový závěr byl přijat, a již převod osobních údajů do QR-kódu by byl pseudonymizací a tedy „zpracováním“ ve smyslu GDPR, byl by logický závěr, že zpětným převodem musí shodně docházet taktéž ke „zpracování“. De facto se totiž jedná o de-pseudonymizaci. Je však otázkou, zda je účelné pojem pseudonymizace takto rozšiřovat i na případ „změny formy“ dat, a činit výklad takto širokým.

[80] V případě, že by došlo k přijetí závěru, že se v případě kontroly v rámci Operace 2 a Operace 3 jedná o rozšifrování osobního údaje, který byl pseudonymizován do podoby QR-kódu, který je na první pohled anonymní, a přiřadit k určité osobě je možné jej až za použití dat obsažených v aplikaci „čTečka“, je zjevné, že dochází ke zpracování osobních údajů teprve v rámci Operace 3, neboť osobní údaj z QR-kódu je „vydobyt“ až teprve v rámci jeho převedení do lidsky čitelné podoby. Toto se pak uplatní pouze za předpokladu kdy nadepsaný soud odmítne úvahu o tom, že QR-kód je sám osobním údajem s rozlišovací schopností.

[81] Snad jen na okraj si dovoluje Účastník vypořádat ještě další citaci z bodu 20. Usnesení předkládacího soudu, ve kterém se uvádí, že: „*Pokud by již v tomto případě šlo o nakládání s osobními údaji, pak by nakládání s osobními údaji představovala jakákoliv operace provedená elektronickým zařízením, která načte jakýkoliv kód a zobrazí ho na elektronickém zařízení, byť s ním dále nepracuje. Mohlo by tak jít například i o načtení QR kódu z vizitek, který ulehčí uložení si údajů z vizitky do mobilního telefonu.“* Účastník nemá pochyb o tom, že i takový proces by zpracováním byl, nicméně se neztotožňuje s tím, že by toto mělo mít dalekosáhlé implikace pro „obyčejný život“, a že by takový výklad měl nepřiměřeně rozšířit působnost GDPR.

[82] Zásadním rozdílem je však to, že v případě načítání QR kódu z vizitky, který ulehčí ukládání údajů do mobilního telefonu, není dána působnost GDPR ze zcela jiného důvodu, a to konkrétně z toho důvodu, že čl. 2 odst. 2 písmene c) výslovně uvádí, že nařízení GDPR se **nevztahuje na zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností**.

[83] V tomto duchu lze odkázat i na Rozsudek čtvrtého soudu Evropského soudního dvora ve věci C-212/13, ECLI:EU:C:2014:2428, ze dne 11. prosince 2014, František Ryneš proti Úřadu pro ochranu osobních údajů, který byl na to konto iniciován předběžnou otázkou stejného soudu jako v nynějším případě, ze kterého lze vyčíst, že evidence vizitek na základě QR-kódů by byla zřejmě taktéž zpracováním údajů prováděná v průběhu výlučně osobních či domácích činností.

[84] Z výše uvedeného rozsudku lze ostatně vyčíst opětovně to, že pakliže měl evropský zákonodárce při přípravě GDPR zájem na tom, aby něco do věcné působnosti GDPR nespadalo, tak tak uvedl ve čl. 2 GDPR, v rámci čtyř velice úzce vymezených výjimek, které mají být na to konto vykládány striktně.[6]

[85] Zcela konkrétně lze odkázat na čl. 28 výše uvedeného Rozsudku ve věci C-212/13 ze dne 11. prosince 2014, ve kterém nadepsaný soud doslova uvádí: „*V této souvislosti je třeba poukázat na to, že podle ustálené judikatury platí, že ochrana základního práva*

[6] K tomu srov. čl. 27 – 29 Rozsudku čtvrtého soudu Evropského soudního dvora ve věci C-212/13 ze dne 11. prosince 2014, František Ryneš proti Úřadu pro ochranu osobních údajů

na soukromí, zaručeného článkem 7 Listiny základních práv Evropské unie, vyžaduje, aby výjimky z ochrany osobních údajů a její omezení byly činěny v mezích toho, co je naprosto nezbytné". Účastník tedy hodnotí úvahu předkládajícího soudu o tom, že by ukládání QR-kódů z vizitek snad nemělo být zpracováním jako zcela nepřípadnou.

Zpracování automatizované při vyhodnocení platnosti certifikátu v rámci Operace 4

[86] Bez ohledu na výše uvedenou polemiku na téma toho v rámci které z Operací 1 až 3 již mohlo dojít ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR (kdy se Účastník domnívá, že tomu tak může být již v případě Operací 2 a 3), zcela bez pochyb se jeví, že ke zpracování osobních údajů dochází v rámci Operace 4.

[87] V rámci Operace 4 (která probíhá současně s Operací 3) totiž dochází k tomu, že osobní údaje jsou bez dalšího zpracovány tak, že jsou porovnány s aktuálními validačními pravidly. K tomu dochází za použití určitého algoritmu na základě zdrojového kódu aplikace „čTečka", kdy jsou osobní údaje kontrolované osoby za pomocí logických příkazů konfrontovány s aktuální regulací (tedy kupř. kolik dní od potvrzeného RT-PCR testu na přítomnost onemocnění covid-19 u konkrétní kontrolované osoby uplynulo, nebo kolik dní uplynulo od aplikace druhé dávky té které vakcíny proti onemocnění covid-19).

[88] Výsledkem logických operací s QR-kódem je pak kromě jeho zobrazení taktéž **vyhodnocení osobních údajů**, za účelem posouzení toho, zda daná osoba splňuje, nebo nesplňuje aktuální validační kritéria, kterými je podmíněn vstup do regulovaného podniku.

[89] Výsledkem Kontroly je pak kromě samotného zobrazení / zpřístupnění osobních údajů kontrolující osobě právě jejich vlastní posouzení, přičemž výsledkem tohoto posouzení je závěr o splnění nebo nesplnění aktuálních validačních kritérií, kdy tyto výsledky jsou představovány buďto „zelenou fajfkou" nebo „červeným křížkem".

[90] Lze zároveň říci, že tato Operace 4, spočívající v „udělení" pozitivního nebo negativního hodnocení kontrolované osobě, je operací, kterou provádí aplikace „čTečka" již sama o sobě, a dá se tedy uvažovat o tom, že sama Operace 4 izolovaně představuje zpracování zcela automatizované. Je nicméně zřejmé, že Operace 4 je operací, která má do osobní sféry kontrolované osoby zdaleka nejzásadnější dopad.

[91] V dikci GDPR by jenom tato samotná operace představovala zpracování osobních údajů, a to už z toho důvodu, že se jedná o operaci s osobními údaji, v rámci které jsou osobní údaje:

- alespoň po určitou dobu **zaznamenány** v aplikaci kontrolující osoby;
- pro účely kontroly jsou osobní údaje **přizpůsobeny** či **uspořádány** pro účely zobrazení v grafickém uživatelském rozhraní[7] aplikace čtečka;

[7] https://www.britannica.com/summary/graphical-user-interface

- jsou předloženy k **nahlédnutí;**
- jsou tedy i jinak zpřístupněny;
- a zejména pak jsou **použity k rozhodnutí o poskytnutí či neposkytnutí služby.**

[92] Právě v Operaci 4 dochází k tomu, že je s osobními údaji pracováno tak, že dochází k rozlišení toho, zda konkrétní osoba splňuje, či nesplňuje stanovená validační pravidla v daném místě a čase. Tyto údaje jsou tedy z dikce GDPR **použity**, k učinění závěru o poskytnutí či neposkytnutí služby. Účastník nemá pochyb, že Operace 4 sama o sobě činí z procesu Kontroly zpracování ve smyslu čl. 4 odst. 1 GDPR.

[93] Předkládající soud v tomto duchu vyjádřil myšlenku, že přestože jsou osobní údaje použity, nejedná se vlastním slova smyslu o zpracování, neboť postup Operace 4 pouze nahrazuje posouzení, které mohla kontrolující osoba provést i bez použití aplikace, a proto se jeví nepřípadným považovat toto za zpracování. S tímto bagatelizujícím názorem se nemůže Účastník ztotožnit.

[94] Tato argumentace je totiž asi tak případná, jako kdybychom připustili, že zachycení podoby osoby jejím vyfocením mobilním telefonem není zpracováním ve smyslu GDPR, protože vyfocení osoby je možné nahradit zachycením její podoby štětcem a temperou, k čemuž mobilní telefon není potřeba. Taková úvaha je zcela lichá.

C.
Analýza čl. 10 Nařízení 2021/953 ze dne 14. června 2021

[95] Pakliže by i po výše předložených argumentech trvala pochybnost o tom, zda je Kontrola digitálního certifikátu EU COVID zpracováním osobních údajů ve smyslu čl. 4 odst. 2 GDPR, dovoluje si Účastník předložit rubrikovanému soudu taktéž jednoduchý systematický výklad ustanovení čl. 10 Nařízení 2021/953, kterým byly digitální certifikáty EU COVID zavedeny.

[96] Článek 10 Nařízení 2021/953 v odst. 1 stanoví, že na zpracování osobních údajů se použije nařízení GDPR.

[97] Porovnáme-li dále článek 10 Nařízení 2021/953, konkrétně odst. 2, dozvíme se, že se **osobní údaje obsažené v certifikátech vydaných podle tohoto nařízení zpracovávají pouze pro účely přístupu k informacím v certifikátu a jejich ověření.**

[98] Již ze článku 10 odst. 2 Nařízení 2021/953 věty první, je tedy možné vyčíst, že zpřístupnění a ověření informací ověřených v certifikátu **je zpracováním** – v rámci Kontroly pak nedochází k ničemu jinému, než ke zpřístupnění v Operaci 3 a k jejich ověření v rámci Operace 4. **Jinými slovy, i evropský zákonodárce při přijetí Nařízení 2021/953 předpokládal, že validace certifikátů prováděná způsobem shodným jako při Kontrole, je zpracováním osobních údajů ve smyslu čl. 4 odst. 2 GDPR.**

[99] Kdyby však ani spojení článku 10 odst. 1 a 2 Nařízení 2021/953 nestačilo, odstavec 3 poskytuje Účastníku naprostou jistotu. Ten přímo stanoví, že: „***Osobní údaje*** *uvedené v certifikátech podle čl. 3 odst. 1* ***zpracovávají*** *příslušné orgány členského státu určení či tranzitu nebo* ***provozovatelé služeb přeshraniční přepravy cestujících, kteří jsou podle vnitrostátního práva povinni provádět během pandemie COVID-19 určitá opatření*** *v oblasti veřejného zdraví, pouze k tomu,* ***aby ověřili a potvrdili*** *očkování, výsledek testu nebo zotavení držitele.* ***Proto se osobní údaje omezí na to, co je nezbytně nutné. Osobní údaje zpřístupněné podle tohoto odstavce se neuchovávají.“***

[100] Ze čl. 10 odst. 3 Nařízení 2021/953 lze tedy vyčíst následující spolehlivé závěry:

- **Osobní údaje uvedené v certifikátech jsou zpracovávány v případě, že jsou certifikáty ověřovány za účelem potvrzení očkování, výsledku testu nebo zotavení držitele;**
- **O zpracování se jedná bez ohledu na to, že je rozsah omezený na nezbytně nutné údaje;**
- **O zpracování se jedná bez ohledu na to, že se údaje zpřístupněné v rámci takového zpracování neuchovávají.**

[101] Kontrola prováděná v rámci České republiky nebyla ničím jiným než obdobou kontroly prováděné provozovateli služeb přeshraniční přepravy – shodně se jednalo o osoby povinné

během pandemie COVID-19 provádět určitá opatření, byť v České republice se zcela nedostatečným (pod)zákonným podkladem. V případě kontrol prováděných provozovateli přeshraniční přepravy se jednalo o zpracování osobních údajů pouze k tomu aby bylo ověřeno a potvrzeno splnění „protiepidemických podmínek“, aniž by došlo k jakémukoliv uchovávání osobních údajů. Přesto však evropský zákonodárce v rámci Nařízení 2021/953 ani náznakem nepochybuje o tom, že i taková operace je zpracováním osobních údajů ve smyslu čl. 4 odst. 2 GDPR.

[102] Lze tedy uzavřít, že jakákoliv pochybnost o tom, zda Kontrola spadá do věcné působnosti GDPR je rozptýlena, **neboť kontrola certifikátů provozovateli služeb přeshraniční přepravy prováděná podle Nařízení 2021/953, která je pojmově shodná s Kontrolou prováděnou v České republice do věcné působnosti GDPR spadá** již proto, že to stanoví právě Nařízení 2021/953.

[103] Jakýkoliv jiný výklad by v praxi znamenal, že zatímco kontroly prováděné provozovateli některých služeb do působnosti GDPR spadají, tak kontroly prováděné provozovateli služeb vymezených v Mimořádném opatření nespadají. Pro takový závěr jednoduše neexistuje ospravedlnění.

D.
Užitelná prejudikatura evropských soudů a Soudního dvora ve věci zpracování ve smyslu čl. 4 odrážky 2) GDPR

[104] Konečně si dovoluje Účastník poukázat na některá z významných rozhodnutí rubrikovaného soudu, která mohou bez ohledu na vše výše uvedené poskytnout významná judikaturní vodítka i v nyní projednávané věci.

[105] Určité výkladové tendence lze nalézt v Rozsudku Soudního dvora (velkého senátu) ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238 (dále jen „**Rozsudek Digital Rights Ireland**"), ve kterém se rubrikovaný soud zabýval zásahem do práva na soukromí zaručeného Listinou základních práv ve čl. 8, který spočíval toliko v uchovávání osobních údajů o osobách na základě povinnosti provozovatelů služeb telefonické komunikace pro účely předcházení, odhalování a vyšetřování trestných činů.

[106] Účastník si je vědom, že Rozsudek Digital Rights Ireland, chronologicky předchází účinnost předpisu GDPR, nicméně i tak je z něj možno vyčíst některé tendence v otázce ochrany osobních údajů, byť tyto přímo neposkytují rozklíčování otázky o rozsahu věcné působnosti GDPR.

[107] Zejména lze z Rozsudku Digital Rights Ireland odkázat na odstavce 54 – 55, ve kterých se uvádí, že: „*…právní úprava tak musí stanovit jasná a přesná pravidla pro rozsah a použití dotčeného opatření, která stanoví minimální požadavky, tak aby osoby, jejichž údaje byly uchovány, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití a proti veškerému neoprávněnému přistupování k údajům a jejich protiprávnímu využívání*"[8], a dále pak, že „***Potřeba takových záruk je o to významnější v případě, kdy…jsou osobní údaje zpracovávány automaticky a existuje značné riziko neoprávněného přistupování k těmto údajům.***"[9]

[108] Vztáhneme-li výše uvedené závěry Rozsudku Digital Rights Ireland na nynější případ, lze dovodit, že jakýkoliv zásah do ochrany soukromí by měl být jasně a přesně regulován, přičemž rozsah takové regulace je přímo odvislý od druhu osobních údajů a způsobu jejích zpracování. **V nynějším případě docházelo ke zpracování osobních údajů zvláštní kategorie, přesto však regulace k jejich ochraně nebyla ani jasná, ani přesná, protože taková regulace prostě neexistovala.**

[8] Rozsudku ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238; odst. 54
[9] tamtéž, odst. 55

[109] Ve shodném duchu lze odkázat taktéž na Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317 (dále jen „**Rozsudek Google**"), ve kterém se rubrikovaný soud zabýval výkladem pojmu zpracování ve vztahu k internetovým vyhledávačů, které podle tohoto má být vykládáno ve prospěch co možná nejširší ochrany adresátů.

[110] Z Rozsudku Google lze mimo jiné vyčíst, že uspořádávání a seskupování informací v rámci vyhledávače je zpracováním osobních údajů, třebaže v některých případech jen zjednodušuje uživatelům přístup k takovým údajům, které existují nezávisle na daném vyhledávači. [10]

[111] Konkrétně pak z odstavce 42 Rozsudku Google vyplývá, že operace s osobními údaji, která spočívá v jejich **byť jen dočasném ukládání**, je zpracováním osobních údajů. tak jak jej dříve definovala dnes již neúčinná Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Přestože je tato směrnice neúčinná, je Rozsudek Google dle názoru Účastníka aplikovatelný i na nynější případ a to zejména proto, že definice zpracování obsažená ve čl. 2 písm. b) dotčené směrnice se od GDPR nijak neliší.

[112] Dále je možno odkázat též na odstavce 53 a 54 Rozsudku Google, ve kterém rubrikovaný soud uvedl, že „*Kromě toho s ohledem na předmět směrnice 95/46 zajistit účinnou a úplnou ochranu základních práv a svobod fyzických osob, zejména práva na soukromí, ve vztahu ke zpracování osobních údajů,* ***nelze posledně uvedený pojem vykládat restriktivně***"[11], a dále pak, že: „*V tomto kontextu je třeba uvést, že zejména z bodů 18 až 20 odůvodnění a z článku 4 směrnice 95/46 vyplývá, že* ***unijní zákonodárce zamýšlel stanovením obzvláště široké územní působnosti zabránit tomu, aby jakákoli osoba mohla být vyloučena z jím zaručené ochrany a aby docházelo k obcházení této ochrany****."*

[113] Pakliže převedeme závěry citované z Rozsudku Google na nyní projednávanou věc, docházíme k následujícím aplikovatelným závěrům:

- pro posouzení zda v rámci Kontroly docházelo ke zpracování není důležité, zda byla založena na pouze dočasném ukládání;
- pojem zpracování, obdobně jako pojem provozovna je v souladu s příslušnými recitály třeba vykládat extenzivně, a nikoliv restriktivně a to s ohledem nutnost zajistit účinnou a úplnou ochranu základního práva na soukromí;
- ze čl. 4 odst. 2 GDPR a příslušných recitálů 5 až 7 preambule GDPR lze shodně dovodit, že unijní zákonodárce zamýšlel (obdobně jako u územní působnosti směrnice 95/46) stanovením obzvláště široké věcné působnosti zabránit tomu, aby

[10] k tomu viz Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014, Google Spain a Google, C-131/12, EU:C:2014:317, odst. 37
[11] vykládaným pojmem byl v daném případě pojem „provozovna" ve smyslu čl. 4 odst. 1 písm. a) směrnice 95/46

určité procesy byly vyloučeny z jím zaručené ochrany **a aby docházelo k obcházení této ochrany.**

[114] Dále je pak možno odkázat na Rozsudek Tribunálu (osmého rozšířeného senátu) ze dne 7. dubna 2022, ve spojených věcech T-710/21, T-722/21 a T-723/21, Robert Roos a další proti Evropskému parlamentu (dále též „**Rozsudek Roos**"), ve kterém se zabýval Tribunál zákonností aplikací fungujících na totožném principu jako aplikace „čTečka", kdy implicitně došel k závěru, že na kontroly prováděné aplikacemi CovidScan a CovidCheck.lu dopadá věcná působnost GDPR (resp. tam věcná působnost Nařízení č. 2018/1725, které nicméně zpracování definuje stejně jako GDPR).

[115] Rozsudku Roos se ostatně věnuje i předkládající soud, když na něj sám poukazuje v bodech 27. a 28 svého předkládacího Usnesení. Správně z něj vyplývá, že Tribunál SDEU neměl nejmenších pochybností o tom, že v případě kontroly scanováním QR-kódu (obsahujícího osobní údaje) dochází ke zpracování osobních údajů, stejně jako v nynějším případě Účastník.

[116] Z Rozsudku Roos si Účastník dovoluje odkázat pozornost rubrikovaného soudu zejména na odst. 178 ve kterém se podává, že: „*V každém případě, i kdyby se předpokládalo, že bezpečnostní pracovníci Parlamentu mohou zjistit dobu platnosti certifikátů a vyvodit z ní, že dotyčná osoba byla očkována, nebo že se zotavila či podstoupila test s negativním výsledkem,* ***nemusí to nutně způsobit závažné dopady, na něž poukazují žalobci****."* a na odst. 179, ve kterém je uvedeno, že: „*Jak totiž uvádí Parlament,* ***jeho pracovníci jsou školeni k tomu, aby při zpracování údajů dodržovali důvěrnost, a obdrželi pokyny v tom smyslu, aby osobní údaje, k nimž mají přístup, nesdíleli s jinými osobami než s těmi, které se podílejí na kontrole přístupu do budov****."*

[117] Opět vztaženo na nynější případ, v případě České aplikace „čTečka" byly kontroly prováděny osobami, které neprošly školením vůbec žádným, autor Mimořádného opatření je na jejich povinnosti při nakládání s osobními údaji nijak neupozornil, a naopak dlouhodobě zastával názor, že o zpracování osobních údajů se v případě Kontroly nejedná. Na rozdíl od aplikací CovidScan a CovidCheck.lu je tedy v případě aplikace „čTečka" zcela potlačena ochrana osobních údajů, a to zejména laxním přístupem ze strany českého zákonodárce.

[118] Dále si dovolí Účastník z Rozsudku Roos odkázat na odst. 180, ve kterém se uvádí, že: „*Z informací, které Parlament sdělil na jednání a které žalobci nezpochybnili, navíc vyplývá, že* ***není technicky proveditelné, aby byl prostřednictvím některé z aplikací používaných bezpečnostními pracovníky Parlamentu pořízen během kontroly covid certifikátu snímek obrazovky****. Je tedy nutné mít za to, že dokonce i nepravděpodobná situace, v níž by došlo během procesu čtení QR kódu uvedeného na covid certifikátu k přenosu informací týkajících se doby platnosti certifikátů, s sebou nese jen* ***velmi nízké, či dokonce nulové riziko, že by bezpečnostní pracovníci mohli zaznamenat informace zobrazené na čtecím zařízení aplikace, kterou používají, a že by tyto informace mohli***

***rozšířit mimo okruh osob, jež jsou k tomuto účelu zmocněny**.“* V projednávaném případě aplikace „čTečka“ se dá ve vztahu k odstavci 180. Rozsudku Roos uvést následující:

- v případě aplikace „čTečka“ není vyloučeno pořízení snímku obrazovky (tzv. printscreenu – pouze se zobrazí upozornění ve znění „*Provádíte záznam obrazovky. Upozorňujeme, že zneužití osobních údajů se trestá podle příslušného zákona“*[12]*;*
- i kdyby bylo vyloučeno pořízení snímku obrazovky tzv. printscreenem, nic nebrání tomu zachytit údaje na kontrolujícím zařízení jiným způsobem (třeba prostě vyfocením jiným mobilním telefonem), kdy jsou údaje již mimo dispozici kontrolované osoby;
- okruh osob, které byly v České republice povinovány k provádění Kontroly nebylo absolutně nijak vymezen (pouze druhově, kdy se jednalo o provozovatele regulovaných podniků, a na rozdíl od situace v Rozsudku Roos bylo riziko rozšíření osobních údajů nikoliv nulové, ale naopak naprosto nepřiměřené danému účelu. Lze říci, že v případě kontrol aplikací CovidScan a CovidCheck.lu bylo nezákonné šíření osobních údajů podmíněno tím, že by osoba, která si byla vědoma svých povinností, tyto povinnosti vědomě porušila;
- V případě České republiky si provozovatelé regulovaných podniků nebyli vědomi (a s ohledem na komunikaci ze strany České republiky ani vědomi být nemohli), že zpracovávají osobní údaje, a není tedy vyloučeno, že si je zcela bezelstně ukládali za účelem vytvoření seznamu svých klientů, nebo i k jiným, třeba i závažnějším účelům;
- Rizika disperze osobních údajů v případě kontroly aplikací CovidScan a CovidCheck.lu si byl Tribunál v Rozsudku Roos očividně vědom, pouze ji neshledal v případě těchto konkrétní aplikací, protože ty byly využívány odpovědnými a pověřenými osobami, které si byly svých práv a povinností vědomy – na rozdíl od osob užívajících aplikaci „čTečka“.

[119] Konečně si dovoluje Účastník poukázat na Rozsudek Soudního dvora (čtvrtého senátu) ze dne 11. prosince 2014, František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13, Ryneš, ECLI:EU:C:2014:2428, (dále jen „**Rozsudek Ryneš**“) kterým se okrajově zabývá již v úvodu toho vyjádření.

[120] Hlavní aplikovatelný závěr vyplývající z Rozsudku Ryneš je ten, formulovaný v odst. 27 až 29, totiž že věcná působnost dotčené Směrnice 95/46 je třeba vykládat toliko striktně s ohledem na ochranu základního práva na soukromí zaručeného článkem 7 Listiny základních práv Evropské unie.

[12] Účastník se domnívá, že tato hláška byla přidána do aplikace teprve po účinnosti Mimořádného opatření, byť takovou informací nedisponuje

[121] V tomto duchu si dovoluje Účastník obecně shrnout, že z textace GDPR je zřejmá tendence unijního zákonodárce postihovat co možná nejvíce operací s osobními údaji s výjimkou těch o kterých výslovně stanoví, že se na ně nařízení GDPR nevztahuje.

[122] Z textace GDPR je zřejmé, že obsahuje toliko dvě redukční klauzule, a to čl. 2 odst. 1 GDPR a čl. 2 odst. 2 GDPR. První odstavec implicitně zužuje věcnou působnost o neautomatizované zpracování osobních údajů, které nejsou obsaženy v evidenci a ani do ní nemají být zařazeny. Druhý odstavec pak zužuje věcnou působnost o zpracování prováděné ve čtyřech taxativně vymezených případech, do kterých nicméně Kontrola nespadá.

[123] Tendence zákonodárce (jak bylo uvedeno i dříve při rozboru preambule) je zjevně taková, že skrze GDPR mají být postihovány všechny varianty zpracování osobních údajů, s výjimkou těch u kterých to výslovně GDPR vyloučí. K tomu je však nutné podotknout též to, že redukční klauzule ve článku 2 odst. 2 GDPR je třeba vykládat tak, že i v těchto situacích se jedná o zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR, ale z věcné působnosti jsou tato zpracování uměle vyňata. Jejich vynětí z věcné působnosti však neznamená, že se o zpracování osobních údajů nejedná.

[124] Vztáhneme-li výše uvedené závěry z Rozsudku Ryneš na nynější případ, nelze z žádného recitálů preambule, jakož ani z vlastního těla předpisu GDPR vyčíst, že by se na zpracování osobních údajů v rámci Kontroly nařízení GDPR nemělo vztahovat.

[125] Lze tedy uzavřít, že všechna předložená judikaturní vodítka poukazují na to, že:

- pojem zpracování má být vykládán co možná nejvíce v souladu s požadavkem ochrany soukromí a osobních údajů;
- v pochybnostech se operace s osobními údaji za zpracování osobních údajů spíše považují;
- v případě, že některá z operací s osobními údaji zpracováním osobních údajů není, dozví se to adresát normy bez výkladových obtíží;

a je tedy vcelku bezpečně možné učinit závěr, že Kontrola je zpracováním osobních údajů, protože doslova žádné analyzované vodítko nenaznačuje opak.

E.
Relevantní stanoviska orgánů ochrany osobních údajů ve vztahu k digitálním certifikátům EU-COVID

[126] Účastník míní shodně poukázat na již existující indikativní stanoviska existující v oblasti digitálních certifikátů EU COVID, zejména pak na ta stanoviska, která se zabývají jejich zásahy do oblasti ochrany soukromí. Shodně pak poslouží též dostupné autoritativní a metodické pokyny, které Účastník předkládá v této části níže.

Společné stanovisko Evropského sboru pro ochranu osobních údajů a evropského inspektora ochrany údajů č. 4/2021

[127] Účastník si v prvé řadě dovoluje pozornost nadepsaného soudu odkázat na ***Společné stanovisko Evropského sboru pro ochranu osobních údajů a evropského inspektora ochrany údajů č. 4/2021 k návrhu nařízení Evropského parlamentu a Rady o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů oočkování, testování a uzdravení za účelem usnadnění volného pohybu během pandemie COVID-19 (digitální zelený certifikát)*** ze dne 31. března 2021 [13] (dále jen „Společné stanovisko“), ve kterém dotčené orgány již v roce 2021 predikovaly nebezpečí, která Ministerstvo České republiky aplikací „čTečka“ skutečně vytvořila.

[128] V bodě č. 24 Společného stanoviska se konkrétně uvádí následující:

- *„pokud by se členské státy i přesto snažily zavádět digitální zelený certifikát na základě práva členského státu pro jakékoli další možné využití kromě zamýšleného účelu usnadnění volného pohybu mezi členskými státy EU, mohlo by to vést k nezamýšleným důsledkům a rizikům pro základní práva občanů EU“*
- *„Rozšíření použití digitálního zeleného certifikátu na další situace, aby se zmírnila stávající omezení, již bylo skutečně navrženo, a členské státy by mohly plánovat jeho zavedení jako faktického požadavku, např. pro vstup do obchodů, restaurací, klubů, bohoslužebných míst nebo tělocvičen nebo jej používat v jiných souvislostech, týkajících se např. zaměstnání.“*
- *„Z tohoto důvodu* ***Evropský sbor pro ochranu osobních údajů a Evropský inspektor ochrany údajů zdůrazňují, že jakékoli případné další využití rámce, digitálního zeleného certifikátu a osobních údajů s ním souvisejících na úrovni členských států musí respektovat*** *články 7 a 8 Listiny* ***a musí být v souladu s GDPR, včetně čl. 6 odst. 4 GDPR.*** *“*

[129] Skoro až nadbytečným se jeví jakkoliv komentovat, že Společné stanovisko velice přesně predikovalo, že se objeví Ministerstvo zdravotnictví České republiky, které na ochranu

[13] dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=53780

osobních údajů **zcela rezignuje,** a bude využívat rámec digitální certifikátu EU COVID, jako by snad certifikát osobní údaje ani neobsahoval.

[130] Se Společným stanoviskem se nemůže Účastník než ztotožnit, protože je zjevné, že upozorňuje, že zavedení digitálního certifikátu EU COVID pro účely Kontroly musí být v souladu s GDPR, neboť zjevně nepochybuje o tom, že by docházelo ke zpracování ve smyslu GDPR.

[131] Že se tyto výhrady týkají i Kontroly provedené nascanováním QR-kódu lze pak vyčíst i z toho, že ve čl. 39 Společného stanoviska zpochybňuje, že v QR-kódu musí být obsaženy všechny navrhované kategorie osobních údajů, a to s ohledem na požadavek minimalizace osobních údajů. Doslovně se v bodě 39. Společného stanoviska uvádí, že: „*Evropský sbor pro ochranu osobních údajů a Evropský inspektor ochrany údajů se navíc domnívají, že by mělo být podrobněji objasněno, zda všechny kategorie osobních údajů stanovené v příloze I musí být zahrnuty také v kódu rychlé odpovědi (dále jen „QR kódu“) digitálních i papírových certifikátů.“*

[132] Lze se spolehlivě domnívat, že kdyby Evropský sbor pro ochranu osobních údajů a Evropský inspektor ochrany údajů měl pochybnosti o tom, že při nascanovaní QR-kódu dochází ke zpracování osobních údajů, zřejmě by asi neuvažoval o tom, že takové nascanovaní je jako zpracování osobních údajů nutno minimalizovat.

Zvláštní zpráva senátu III Účetního dvora „Nástroje usnadňující cestování v rámci EU během pandemie COVID-19 Iniciativy byly relevantní, ale jejich dopad sahal od úspěchu až po omezené využití“

[133] Dále je možné poukázat na Zvláštní zprávu senátu III Účetního dvora „***Nástroje usnadňující cestování v rámci EU během pandemie COVID-19 Iniciativy byly relevantní, ale jejich dopad sahal od úspěchu až po omezené využití*“** ze dne 22. listopadu 2022[14], z jejíhož bodu 42. se podává, že členské státy jako společní správci údajů ve smyslu GDPR: „*sdílejí odpovědnost za rozhodování o tom, jak a za jakým účelem se osobní údaje zpracovávají, a za zavedení vhodných kontrol.* ***Každý z nich musí vypracovat posouzení dopadu na ochranu údajů s cílem určit a zmírnit rizika vyplývající z používání těchto aplikací ke zpracování osobních údajů****.“*

[134] Je zjevné, že Účetní dvůr si na rozdíl od Ministerstva zdravotnictví České republiky uvědomoval rizika vztahující se k aplikacím, a zdůraznil, že užívání aplikací by mělo být opřeno o posouzení dopadů, které kupř. v České republice má podobu studie RIA (hodnocení dopadů regulace). Vzhledem k tomu, že v České republice byla povinnost užívat aplikaci „čTečka“ stanovena Mimořádným opatřením, který jako podzákonným předpisem, který obsahuje toliko odůvodnění, je zřejmé, že k účinnému posouzení dopadů aplikace „čTečka“ ani nemohlo dojít.

[14] dostupné z: https://www.eca.europa.eu/Lists/ECADocuments/SR23_01/SR_Free_Movement_II_CS.pdf

COVID-19 - Digital verification of certificates upon entry of Commission sites in Brussels and Luxembourg

[135] Dále si dovoluje Účastník odkázat na stanovisko „COVID-19 - Digital verification of certificates upon entry of Commission sites in Brussels and Luxembourg, privacy statement ze dne 17.1.2022[15], ref. č. DPR-EC-11557.2.

[136] Výše uvedený dokument stanovisko upravoval a informoval o zpracování při obdobné kontrole jako v případě kontroly aplikací „čTečka“ za pomocí aplikací CovidScan a CovidCheck.lu kdy se mělo bez dalšího jednat o zpracování ve smyslu Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, jak bylo ostatně diskutováno výše v souvislosti s Rozsudkem Roos.

[137] Z dotčeného dokumentu *COVID-19 - Digital verification of certificates upon entry of Commission sites in Brussels and Luxembourg* lze učinit následující závěry:

- Z tohoto stanoviska je zřejmé, že Evropská komise neměla sebemenších pochyb, že při kontrolách při vstupu do budov orgánů EU dochází ke zpracování ve smyslu čl. 2 odrážky b) nařízení č. 45/2001, který zní: „*zpracováním osobních údajů" (dále jen "zpracování") rozumí jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo zničení“.*
- Nařízení č. 45/2001 je de facto GDPR pro unijní orgány, kdy svoji věcnou působnost vymezuje totožně jako GDPR ve čl. 3 odst. 2 („*Toto nařízení se vztahuje na zcela nebo* ***částečně automatizované zpracování osobních údajů****, jakož i na neautomatizované zpracování osobních údajů, které jsou obsaženy v registru nebo do něj mají být zařazeny.“)*
- Tento dokument doslovně uvádí, proč nestačí manuální kontrola covid pasů, a proč přistupuje ke kontrole na bázi scanování QR-kódů, které považuje za zpracování, když doslovně uvádí: „*Manual verification of COVID-19 certificates alone involves a significant risk of fraud, which poses a risk to Commission staff members' health. It is necessary to ensure that the COVID-19 certificates have not been forged and that they belong to the persons presenting them.* ***Verifying the validity and authenticity of the COVID-19 certificates can only be achieved effectively by using a scanning solution for validation of the QR codes displayed on COVID-19 certificates, <u>while processing the minimum amount of personal</u>***

[15] dostupné z: https://ec.europa.eu/dpo-register/detail/DPR-EC-11557

***data and without recording the results of the check, nor the content of the certificates**.“*

[138] Konec konců sám za sebe hovoří nadpis třetí části tohoto dokumentu, který je nazván „**On what legal ground(s) do we process your personal data?**“, jednoznačně implikující, že ke zpracování osobních dat při použití aplikací CovidScan a CovidCheck.lu bez pochyby dochází.

[139] Mezi aplikacemi CovidScan, CovidCheck.lu a aplikací „čTečka“ neexistuje žádný významný technologický rozdíl, a není tedy důvod docházet k odlišnému závěru, totiž že ke zpracování nedochází. Opačný výklad by nedůvodně chránil nezodpovědný přístup Ministerstva zdravotnictví ČR k ochraně osobních údajů, a to za situace, kdy Evropská komise tuto zodpovědnost bezpečně unesla, a na rozdíl od České republiky ji nikterak nezpochybňovala.

EDPS Opinion on the Commission Draft Descision regarding Additional Specific Health and Safety Rules for the Commision site of Ispra

[140] Konečně si dovoluje Účastník odkázat na další Stanovisko Evropského inspektora ochrany údajů *EDPS Opinion on the Commission Draft Descision regarding Additional Specific Health and Safety Rules for the Commision site of Ispra* ze dne 11. února 2022 (dále jen „**Stanovisko ISPRA**“), ve kterém je mimo jiné řešena otázka kontroly srovnatelné s Kontrolou aplikací „čTečka“, v tomto případě za pomocí italské aplikace „VerificaC19“.

[141] Účastník je toho názoru, že opětovně mezi způsobem fungování aplikací „čTečka“ a „VerificaC19“ neexistuje zásadního rozdílu, kdy oba pracují na principu nascanovaní QR-kódu z digitálního certifikátu EU COVID a jeho převedení do lidsky čitelné podoby.

[142] V tomto duchu se dá potom víceméně stručně odkázat na bod 3.15 Stanoviska ISPRA, ve kterém se doslovně uvádí, že: „*The processing operation as described above, i.e.* ***digital verification of certificates involving the scanning of a QR code, constitutes processing as defined by Article 2 (5) of the Regulation***[16] *and, therefore, falls within the scope of the Regulation. The EDPS considers that the* ***processing in question interferes with the individuals' fundamental rights of privacy and data protection*****.**“

[143] Výše uvedenou citaci bodu 3.15 Stanoviska ISPRA lze dle Účastníka bez dalšího vztáhnout kromě aplikace „VerificaC19“ taktéž na aplikaci „čTečka“, a to v plném rozsahu, kdy obě aplikace nascanováním QR-kódu v souladu se závazně vysloveným názorem Evropského inspektora ochrany údajů představují zpracování osobních údajů (bez ohledu na to, zda ve smyslu Nařízení 2018/1725, nebo nařízení GDPR).

[16] pojmem „Regulation“ je míněno v tomto případě opět Nařízení 2018/1725, Účastník tedy odkazuje v tomto ohledu na argumentaci uvedenou u aplikací CovidScan a CovidCheck.lu v bodě 137

F.
Srovnání verifikačních aplikací používaných v členských státech EU a jejich přístupu k GDPR-compliance

[144] V neposlední řadě se dá uvažovat o tom, zda je absence GDPR-compliance problémem pouze v případě české aplikace „čTečka“, nebo zda jsou v tomto duchu problematické i jiné verifikační aplikace používány k ověření platnosti digitálních certifikátů EU COVID, které byly v průběhu roku 2022 používány v jiných členských státech Evropské unie, a jedna užívaná ve Velké Británii.

[145] Výše byly zmíněny již aplikace:

- aplikace Verifica19 používaná v Itálii
- aplikace CovidScan používaná v Belgii
- aplikace CovidCheck.lu používaná v Lucembursku

kdy nad rámec těchto míní Účastník analyzovat ještě aplikace

- aplikace GreenPass používaná v Rakousku
- aplikace NHS Covid Pass Verifier

[146] Všechny analyzované aplikace mají společné to, že ve všech případech dochází k nascanovaní QR-kódu, a to v rámci operace, která je obdobná s Operací 2, tak jak byla popsána v případě „čTečka“ výše.

[147] V případě aplikace **Verifica19**, která je používána v Itálii, se přímo v aplikaci dá prokliknout na stránku *Note Legali Verifica C19*[17]*,* kdy tento dokument obsahuje sdělení italského Ministerstva zdravotnictví, přičemž v druhém odstavci, se adresát dočítá, že: *„L'App in oggetto è direttamente derivata dalla versione europea e in applicazione del principio di minimizzazione dei dati di cui all'art. 5 del Regolamento 2016/679 (EU) riduce al minimo il numero di dati visualizzabili dall'operatore nel pieno rispetto della normativa privacy.“*

[148] Je zřejmé, že italský zákonodárce si byl vědom toho, že aplikace nascanovaní QR-kódu zpracovává osobní údaje, a tedy sám sebe limitoval v duchu zásady minimalizace osobních údajů ve smyslu čl. 5 GDPR.

[149] Projev minimalizace údajů je zřejmý v okamžiku, kdy dochází k načtení QR-kódu za pomocí funkce „*SCANSIONA IL QR CODE“,* dojde pouze k vyhodnocení toho, zda je certifikát platný, či nikoliv a ke zobrazení jména kontrolované osoby a jejího data narození. V české aplikaci „čTečka“ bylo nad rámec tohoto možné vyčíst též informace o zdravotním stavu, jak už bylo ostatně uvedeno výše.

[17] https://www.dgc.gov.it/web/pn.html

[150] Zároveň lze z *Note Legali Verifica C19* dovodit, že ani tato aplikace, stejně jako „čTečka“ neuchovává osobní údaje, přesto je však zpracovává ve smyslu GDPR.

[151] Je možné vcelku bezpečně uzavřít, že italský zákonodárce, na rozdíl od toho českého, si byl vědom toho, že Kontrolou a obdobnými procesy dochází ke zpracování osobních údajů. Aplikaci tomu italský zákonodárce přizpůsobil, aby osobní data subjektů údajů chránil.

[152] Co se týče aplikací **CovidScan** a **CovidCheck.lu**, dovoluje si Účastník pro zjednodušení odkázat na body 135 – 139 tohoto vyjádření, ve kterých je důkladně rozebrán dokument, který kompletně upravoval GDPR-compliance ve věci použití těchto dvou aplikací.

[153] V případě aplikace **GreenPass,** kterou zpracoval Rakouský Červený Kříž, nedochází při využití funkce „Check Pass“ k zobrazení vůbec žádných osobních údajů o kontrolované osobě, a pouze k vyhodnocení jejich validity podle aktuálních kritérií.

[154] Analogicky k aplikaci „čTečka“ lze tedy říci, že v procesu kontroly je vynechána celá Operace 3, a zůstávají pouze Operace 1, 2 a 4, v důsledku čehož kontrolující osoba nemá skrze aplikaci GreenPass přístup k vůbec žádným osobním údajům o kontrolované.

[155] Toto potvrzují autoři aplikace GreenPass i na svých stránkách v sekci „Privacy“, kde ke scanování QR-kódů uvádí, že: „*You can use the app and this website without any personal data being stored or processed online. The collected data is only stored and processed locally and offline on your device and will be deleted when you uninstall the app.“*[18], ze kterých vyplývá, že se autoři aplikace domnívají, že aplikace GreenPass nijak údaje nezpracovává.

[156] Účastník je nicméně v duchu výše uvedené argumentace toho názoru, že i při absenci zobrazení analogického k „Operaci 3“ dochází ke zpracování osobních údajů již proto, že QR je bez dalšího sám o sobě osobním údajem *sui generis*, a ke zpracování tedy dochází již právě načtením QR-kódu.

[157] Je tedy otázkou, zda nezobrazením údajů stále nedochází ke zpracování osobních údajů, kdy se Účastník domnívá, že i bez zobrazení osobních údajů na obrazovce dochází k jejich zpracování, a to zejména kvůli tomu, že jsou osobní údaje o zdravotním stavu využity v rámci analogického vyhodnocení jako v Operaci 4.

[158] Konečně si dovoluje Účastník poukázat na aplikaci **NHS COVID Pass Verifier**, která byla užívána ve Velké Británii. Velká Británie, přestože již není vázána GDPR, je vázána jeho obdobou v podobě UK General Data Protection Regulation která byla uvedena v účinnost

[18] https://greenpassapp.eu/privacy

zákonem Data Protection Act 2018. Definice zpracování („processing“) je nicméně de facto totožná v Data Protection Act 2018 jakož i v GDPR.

[159] Aplikace NHS COVID Pass Verifier při využití funkce „Check a barcode“ nezobrazí, kupř. v případě neplatného certifikátu absolutně žádný osobní údaj.

[160] Přesto nicméně v dokumentu NHS COVID Pass Verifier app Privacy Notice (PN) ze dne 12. dubna 2022 [19] uvádí v otázce zpracování vládní agentura National Health Service následující: „***An organisation can opt to check a COVID Pass visually (which does not process data and UK GDPR does not apply), or to use the NHS COVID Pass Verifier app which processes a citizen's data.*** *The venue or travel operator will become a data controller under UK GDPR. Demographic and health information from a person's COVID-19 events are exchanged between the citizens COVID Pass screen and the camera of the Verifier app to the operator's screen processing non-human readable data. The processing is fleeting and the Verifier app does not retain, store, share or further process any personal or health information in the scanning process.“*

[161] Hned první větou National Health Service potvrzuje, že jakákoliv aplikace která načítá QR-kód obsahující osobní údaje, byť jen nahrazuje relativně snadný rozhodovací proces, zpracovává osobní údaje.

[162] Opětovně i National Health Service zastává názor, že na posouzení toho, zda dochází ke zpracování, či nikoliv nemá absolutně žádný vliv to, zda jsou soubory ukládány, či po jak dlouhou dobu, jak naznačoval výše též Účastník.

[163] **V souhrnu se dá říci, že všechny analyzované aplikace užívané ke kontrolám digitálního certifikátu EU COVID zpracovávaly údaje buďto v daleko menším rozsahu v souladu s požadavkem minimalizace, anebo si byly důsledně vědomy toho, že při nascanovaní QR-kódu dochází ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR. Tomuto pak byly jednotlivé aplikace uzpůsobeny.**

[164] **Jedinou Účastníkovi známou výjimku z tohoto pravidla tvoří aplikace „čTečka“, o které Ministerstvo zdravotnictví České republiky na svých stránkách tvrdí následující:**

- *„Aplikace čTečka nezpracovává osobní údaje uživatele aplikace čTečka, pouze osobní údaje kontrolovaných osob z Digitálních COVID certifikátů.*

  Právo na odvolání souhlasu, Právo na přístup, Právo na opravu, Právo na výmaz, Právo na omezení zpracování jsou tedy v tomto kontextu irelevantní.“[20]

[19] dostupný z: https://transform.england.nhs.uk/covid-19-response/nhs-covid-pass-verifier-app/covid-19-certification-nhs-covid-pass-verifier-privacy-notice/
[20] https://ockodoc.mzcr.cz/napoveda/ctecka/cz/podminky-pouzivani/

[165] Skutečnost, že tvůrce „čTečky“ označil zásadní práva subjektů osobních údajů za **irelevantní**, už pouze dokresluje jakým způsobem český zákonodárce k otázce ochrany osobních údajů v projednávaném případě přistoupil.

[166] V kontextu celé projednávané věci je pak zřejmé, že laxní přístup českého zákonodárce poněkud vystupuje z obecného unijního přístupu k ochraně osobních údajů, jehož cílem je chránit soukromí a osobní údaje občanů Evropské unie. Účastník neshledává žádný důvod pro to, proč by takovému postupu měla být ze strany nadepsaného soudu implicitně poskytována ochrana, v případě, že by nadepsaný soud snad došel k názoru, že v případě aplikace „čTečka“ nedocházelo při nascanovaní QR-kódu ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR.

G.
Analýza potenciálních dopadů rozhodnutí Soudního dvora o předběžné otázce na rozsah ochrany osobních údajů

[167] V této části si dovoluje Účastník předložit soudu úvahu nad implikacemi, jaké by mohlo mít rozhodnutí nadepsaného soudu o této předběžné otázce, a to ať už v podobě kladného stanoviska (tedy, že aplikace „čTečka“ osobní údaje zpracovává) nebo záporného stanoviska (tedy, že aplikace „čTečka“ osobní údaje nezpracovává).

[168] Určitou úvahu tohoto typu předvedl i Nejvyšší správní soud ČR ve svém předkládacím usnesení, kdy v bodě 20. uvedl, že by kladné rozhodnutí o předběžné otázce de facto znamenalo, že by zpracováním osobních údajů bylo kupř. načtení QR-kódu z vizitek, nebo načtení strojově čitelných osobních dokladů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2019/1157 ze dne 20. června 2019 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu (dále jen „**Nařízení 2019/1157**“).

[169] K těmto úvahám si dovoluje podotknout Účastník následující. V obou případech se samozřejmě o zpracování osobních údajů jedná, neboť bez ohledu na to, zda načítací zařízení samo o sobě s osobními údaji dále pracuje či nikoliv, osobní údaje jsou převedeny do určité podoby, zobrazují se na jiném zařízení, a jsou mimo dispozici subjektu údajů.

[170] Rozdíl je však v tom, zda takové zpracování spadá pod věcnou působnost GDPR, nebo zda je ochrana osobních údajů zaručena jinak.

[171] V případě načítání QR-kódů z vizitek se nicméně jedná typicky o zpracování osobních údajů v rámci osobní činnosti ve smyslu čl. 2 odst. 2 písm. c) GDPR, a není tedy případným domnívat se, že kladná odpověď na otázku, zda aplikace „čTečka“ zpracovávala osobní údaje by měla znamenat obavy pro adresáty GDPR, že budou zpracovateli, když si uloží vizitku do osobního adresáře v telefonu.

[172] V případě načítání strojově čitelných průkazů totožnosti na základě Nařízení 2019/1157 je opět rozdíl ten, že jejich načítání je vyhrazeno pouze řádně zmocněným osobám, a v rámci celého nařízení je kladen vysoký důraz na zabezpečení údajů v nich obsažených (a to i biometrických). Zároveň, ač to nelze vyloučit, je zjevné, že ze strojově čitelné oblasti občanského průkazu (nebo víza, nebo cestovního pasu) bez použití k tomu určené aplikace k jejímu překladu opět není možno nic vyčíst. V souladu s výše uvedenou argumentací by nicméně i strojově čitelná zóna konkrétního dokladu byla zřejmě osobním údajem, a její rozkódování automatizovaným způsobem je bez pochyby zpracováním osobních údajů.

[173] V obecné rovině tedy není na místě se obávat, že by kladné rozhodnutí nedůvodně rozšířilo oblasti zpracování osobních údajů, kdy je zřejmé, že již nyní ke zpracování osobních údajů načítáním QR-kódů dochází. Zároveň lze poukázat na to, že ani v dnešní době se jistě QR-

kódy obsahující osobní údaje nezpracovávají bezúčelně, a právě účel pro který jsou zpracovávány typicky zajišťuje jejich náležitou ochranu i ve smyslu GDPR – byť třeba nemusí být zřejmé ve které části načtení QR-kódu poprvé dochází ke zpracování osobních údajů ve smyslu GDPR.

[174] Zároveň je nepřípadná interpretace, že by kladné stanovisko mělo komplikovat používání QR-kódů v obecné rovině. **Problematickými jsou samozřejmě pouze ty QR-kódy, do kterých jsou zakódovány osobní údaje.**

[175] Naopak může být postaveno na jisto, že ochrana osobních údajů je jednou ze zcela zásadních priorit Evropské unie a GDPR, kterou v době automatizace není možné obcházet, nebo ignorovat způsobem, jakým to předvedlo Ministerstvo zdravotnictví České republiky.

[176] Problematickým by naopak byl opačný závěr, že ke zpracování osobních údajů v rámci načítání QR-kódu aplikací „čTečka“ nedochází.

[177] Nařízení GDPR totiž kromě otázek zákonného zpracování v obecné rovině představuje a zdůrazňuje zároveň i úpravu práv těch osob, jejichž data byla zpracována nezákonně. Zakotvuje též odpovědnost zpracovatelů a správců osobních údajů za to, když zpracování probíhá nezákonně.

[178] V případě, že by nadepsaný soud došel k závěru, že aplikace „čTečka“ osobní údaje nezpracovává, implikoval by tím zároveň to, že takovým (ne)zpracováním nemůže dojít k ohrožení osobních údajů a že nemůže být způsobena újma subjektům údajů, jejichž údaje byly (ne)zpracovány nezákonně.

[179] V praxi by pak všem subjektům údajů, kterým byla způsobena Kontrolou, nebo obdobnými kontrolami nějaká újma v oblasti ochrany osobních údajů, třeba tím, že se (ne)zpracované osobní údaje dostaly k nepovolaným osobám, byla upřena právní ochrana, kterou GDPR poskytuje.

[180] Jinými slovy, bychom došli k závěru, že Kontrolou újma ani být způsobena nemohla, a je tak kompletně vyloučeno právo na náhradu újmy a odpovědnost za ní, která je zakotvena ve článku 82 GDPR, který stanoví, že: „*Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy“.*

[181] Shodně by pak byla vyloučena odpovědnost kohokoliv za případný správní delikt spočívající v porušení některých ustanovení GDPR. Pro takto široké omezení práv subjektů údajů dle názoru Účastníka neexistuje žádná opora, a to ani v samotném předpisu, ani v žádné prejudikatuře nadepsaného soudu.

[182] Prejudikatura nadepsaného soudu totiž jednoznačně potvrzuje, že jakýkoliv výklad GDPR má být činěn ve světle základních práv chráněných Listinou základních práv Evropské unie. Shodně se zde uplatní právní zásada právní zásada *in dubio pro libertate,* resp. obecné zásady výkladu veřejnoprávní normy ve prospěch adresáta, která přikazuje přijetí výkladu, který šetří práva a svobody jednotlivce. V nynějším případě by toto výkladové pravidlo mohlo nabýt podoby **„v pochybnostech ve prospěch ochrany osobních údajů“**.

[183] V tomto duchu lze odkázat na to, že vrchní soudní instance jednotlivých členských zemí jsou ustáleny v aplikaci zásady *in dubio pro libertate*, kdy kupř. předkládající soud tuto zásadu dovodil z ústavního pořádku České republiky, kdy si dovoluje Účastník odkázat na Odlišné stanovisko soudců J. Baxy, B. Chrastilové, V. Novotného, M. Součkové, M. Tomkové a M. Turkové ke stanovisku Nejvyššího správního soudu ze dne 29. 4. 2004, č. j. Sst 2/2003-225: „*Z ústavního pořádku České republiky lze rovněž dovodit zásadu in dubio pro libertate přikazující dát přednost interpretaci šetřící práva a svobody jednotlivce, jestliže vyvstanou pochybnosti, zda přijmout výklad svědčící autonomii jedince na straně jedné, nebo výklad svědčící veřejné moci na straně druhé.“*

[184] Stejné interpretační hledisko, tedy výklad ve prospěch smyslu a účelu chráněného práva na ochranu soukromí a ochranu osobních údajů dle článků 7 a 8 Listiny základních práv Evropské unie, lze bez dalšího vyčíst též ze článku 52 Listiny základních práv Evropské unie, a není tedy důvod, aby se výkladové pravidlo ve prospěch adresátů normy (a ve prospěch ochrany osobních údajů) uplatnilo i v nynějším řízení.

[185] Lze tedy shrnout, že kladné rozhodnutí by představovalo pevné hodnotové přesvědčení nadepsaného soudu o potřebě chránit osobní údaje občanů Evropské unie, které by v praxi nikterak významně nemělo komplikovat běžný občanský styk, byť se to mohou někteří domnívat. Záporné stanovisko by v praxi znemožnilo výkon a ochranu práv, na jejichž ochraně evropsk= společenství vždy stálo, a odepřelo by bezprecedentně širokému okruhu subjektů údajů právo na právní ochranu jejich soukromí, které jim má garantovat nařízení GDPR.

IV.
Závěr

[186] Účastník se v tomto svém vyjádření komplexním způsobem věnoval problematice zpracování osobních údajů, ke kterému dle jeho názoru nepochybně docházelo při kontrolách digitálních certifikátů EU COVID.

[187] Pro zodpovězení položené předběžné otázky považoval Účastník za zásadní zejména posouzení toho, jakým způsobem Kontrola probíhá, a jak je nakládáno s osobními údaji, které jsou předmětem Kontroly.

[188] Z vyjádření je zřejmé, že Kontrola prováděná aplikací „čTečka“ není jen jakýmsi dočasným zobrazením nezneužitelných údajů, ale bez dodržení právního rámce GDPR je naopak nástrojem, který bez pochyby značně ohrozil osobní údaje milionů českých a evropských občanů.

[189] Účastník provedl rozklad Kontroly na jednotlivé kroky, které v tomto podání nazývá Operacemi 1-4, a dovodil, že ve třech krocích Kontroly, a to v Operacích 2-4 dochází ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR, zpracováním je pak i Kontrola jako celek.

[190] V daném vyjádření reflektuje, že technologicky pokročilá doba představuje výzvu pro ochranu osobních údajů, kterou není radno podcenit. Při rychlosti technologického vývoje je zřejmé, že pojem „osobní údaj“ je daleko širší, než jen souhrn tradičních identifikátorů jako je jméno a příjmení. Osobním údajem ve smyslu čl. 4 odst. 1 GDPR je dle Účastníka i samotný QR-kód jakožto osobní údaj *sui generis*, který nadto osobní údaje ještě obsahuje. **Z toho důvodu již Operace 2 představuje zpracování osobních údajů.**

[191] Účastník se zamyslel nad tím, jaká je podstata QR-kódu obsaženého v digitálním certifikátu EU COVID, a k čemu vlastně dochází při dekódování osobních údajů obsažených v samotném QR-kódu v rámci Operace 3. Účastník dovodil, že se jedná o, s nadsázkou řečeno, rozluštění šifry (kódu), kdy dochází ve smyslu čl. 4 odst. 2 GDPR nejméně k následujícím operacím s osobními údaji, a to k

- dočasnému zaznamenání osobních údajů do mezipaměti aplikace;
- uspořádání a přizpůsobení osobních údajů do formátu aplikace;
- nahlédnutí do osobních údajů kontrolující osobou;
- ke zpřístupnění osobních údajů a v konečném důsledku též ke změně jejich formy.

Z toho důvodu je Účastník toho názoru, že Operace 3 představuje zpracování osobních údajů, kdy naplňuje pojmové znaky demonstrativní definice zpracování ve smyslu čl. 4 odst. 2 GDPR.

[192] Nikoliv nepřípadnou je též úvaha Účastníka nad tím, zda lze na QR-kód nahlížet jako na pseudonymizovaný údaj ve smyslu článku 4 odst. 5 GDPR a na zdrojový kód aplikace „čTečka“ jako na dodatečné informace ve smyslu téhož článku. O pseudonymizaci GDPR ve čl. 4 odst. 5 GDPR výslovně stanoví, že je zpracování osobních údajů, tak z logiky věci je zpracováním osobních údajů též „de-pseudonymizace“. V případě, že by šlo Operaci 3 prováděnou aplikací „čTečka“ interpretovat právě jako de-pseudonymizovaný osobní údaj, pak **je zřejmé, že Operace 3 představuje zpracování i z tohoto důvodu.**

[193] V pochybách je konečně zřejmé, že zpracování představuje Kontrola za použití aplikace „čTečka“ z důvodu toho, že v Operaci 4 osobní údaje vyhodnocuje a činí na jejich základě rozhodnutí o vpuštění či nevpuštění osoby do regulovaného podniku, a tedy na základě Operace 4 dochází k umožnění nebo omezení výkonu práva kontrolované osoby. Ve smyslu čl. 4 odst. 2 GDPR tedy **nepochybně dochází k použití osobních údajů, a Operace 4 samotná je zpracování osobních údajů.**

[194] **Vzhledem ke skutečnosti, že jednotlivé Operace 2-4 mohou nebo dokonce s jistotou představují zpracování ve smyslu čl. 4 odst. 2 GDPR, je zřejmé, že v průběhu celé Kontroly nepochybně dochází ke zpracování osobních údajů.**

[195] Účel předpisu GDPR, tak jak ho v tomto vyjádření interpretuje Účastník, je poskytnutí široké ochrany subjektům osobních údajů v rámci jakýchkoliv operací s nimi, které představují riziko pro zneužití osobních údajů, a pro právo na soukromí.

[196] Účastník si váží hodnoty ochrany osobních údajů, které mu poskytuje GDPR, kdy je zřejmé, že při dodržení podmínek tohoto předpisu by mohl být při provádění Kontroly v relativním klidu, že jsou alespoň jeho osobní údaje v bezpečí – bez ohledu na to, jaký má na účel a smysl Kontroly názor.

[197] Český zákonodárce se při přípravě „čTečky“ a při uložení povinnosti „čTečku“ používat předpisem GDPR nicméně necítil vázán. Práva, která z GDPR plynou, české Ministerstvo zdravotnictví označilo za irelevantní[21]. Zákonodárce, který se necítí vázán právním předpisem, a nadto to otevřeně deklaruje, z logiky věci nemůže ani uvažovat o tom, že je potřeba práva a povinnosti z takového předpisu uvádět v život.

[198] Čtenáři tohoto vyjádření zjevně nemohlo uniknout, že Účastník na žádném z míst nereflektuje to, zda a jestli bylo používání aplikace „čTečka“ činěno v souvislosti s krizovou situací zapříčiněnou pandemií onemocnění Covid-19, pro které byla aplikace zaváděna.

[199] Účastník na tomto místě akcentuje, že právě období krize je nejtěžší zkouškou pro lidská práva. V takových dobách totiž zákonodárci mohou mít pocit, že je vhodné či možná některá práva krátkodobě omezit, nebo je prostě po nějakou dobu ignorovat s tím,

[21] https://ockodoc.mzcr.cz/napoveda/ctecka/cz/podminky-pouzivani/

že po pominutí krize nabydou omezená práva svojí původní podoby. Poučení z krizí předchozích je však takové, že na ochraně základních lidských práv je třeba trvat bezvýhradně a vždy, byť by jejich omezení bylo vedeno těmi nejčistšími úmysly.

[200] Z tohoto, i ze všech výše uvedených důvodů Účastník tímto předkládá své stanovisko, kdy je přesvědčen, že **při Kontrole digitálního certifikátu EU COVID českou národní aplikací „čTečka“ dochází ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR.**

S pozdravem

JUDr. Denisa Sudolská,
i.s
[redacted]