

U S N E S E N Í

Nejvyšší správní soud rozhodl v senátu složeném z předsedy Petra Mikeše a soudců Milana Podhrázkého a Jitky Zavřelové v právní věci navrhovatele: **RK**, zast. JUDr. Denisou Sudolskou, advokátkou se sídlem Italská 1219/2, Praha 2, proti odpůrci: **Ministerstvo zdravotnictví**, se sídlem Palackého náměstí 375/4, Praha 2, v řízení o návrhu na zrušení opatření obecné povahy odpůrce ze dne 29. 12. 2021, čj. 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,

t a k t o :

- I. Soudnímu dvoru Evropské unie se předkládá následující předběžná otázka:

Dochází 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, které jsou Českou republikou používány pro vnitrostátní účely, národní aplikací „ČTečka“ k automatizovanému zpracování osobních údajů ve smyslu čl. 4 odrážky 2) 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), a je tak dána věcná působnost obecného nařízení o ochraně osobních údajů podle čl. 2 odst. 1 tohoto nařízení?

- II. Řízení se přerušuje.

O d ů v o d n ě n í :

I. Předmět řízení

[1] Odpůrce mimořádným opatřením ze dne 29. 12. 2021, čj. MZDR 14601/2021-34/MIN/KAN (dále jen „mimořádné opatření“), vydaným k ochraně obyvatelstva před dalším rozšířením onemocnění covid-19 na základě § 69 odst. 1 písm. i) a odst. 2 zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění účinném od 1. 5. 2020, a § 2 odst. 2 písm. b) až e) a písm. i) zákona č. 94/2021 Sb., o mimořádných opatřeních při epidemii onemocnění COVID-19 a o změně některých

souvisejících zákonů, ve znění účinném do 14. 1. 2022 (dále „pandemický zákon“), stanovil s účinností od 3. 1. 2022 podmínky pro vstup osob do některých vnitřních a venkovních prostor nebo pro účast na hromadných akcích nebo na jiných činnostech.

[2] Pro možnost využití některých služeb, vstup do provozoven či účast na akcích bylo jednotlivými ustanoveními mimořádného opatření mj. vyžadováno naplnění podmínek dle čl. I bodu 15 mimořádného opatření. Těmito podmínkami bylo a) absolvování RT-PCR vyšetření na přítomnost viru SARS-CoV-2 s negativním výsledkem nejdéle před 72 hodinami, jde-li o i) osobu do dovršení 18 let věku, ii) osobu, která se nemůže podrobit očkování proti onemocnění covid-19 pro kontraindikaci, nebo iii) osobu tzv. rozočkovanou; b) uplynutí nejméně 14 dní od dokončeného očkovacího schématu, a to schváleným léčivým přípravkem; nebo c) prodělání laboratorně potvrzeného onemocnění covid-19, jestliže uplynula doba izolace a od prvního pozitivního testu neuplynulo více než 180 dní (dále jen „podmínky tzv. bezinfekčnosti“).

[3] Odpůrce mj. v čl. I bodu 2 písm. c), bodu 8 písm. b), bodu 9 písm. b), bodu 10 písm. b), bodu 11 písm. c), bodu 13 písm. c) a bodu 14 písm. c) mimořádného opatření stanovil zákazníkům (divákům, účastníkům) povinnost prokázat splnění podmínek tzv. bezinfekčnosti a povinnost provozovatelům (organizátorům) splnění těchto podmínek kontrolovat prostřednictvím aplikace „čTečka“. Neprokázal-li zákazník splnění podmínek tzv. bezinfekčnosti, bylo provozovateli zakázáno poskytnout zákazníkovi službu, vpustit ho do prostor nebo na akci či mu umožnit účast na skupinové prohlídce nebo na akci.

[4] K povinnosti provozovatelů kontrolovat splnění podmínek tzv. bezinfekčnosti aplikací „čTečka“ odpůrce v odůvodnění mimořádného opatření uvedl, že *„[v]šude, kde se provozovatelům zařízení, poskytovatelům služeb a organizátorům akcí nařizuje kontrolovat splnění podmínek podle bodu I/15, nařizuje se činit tak prostřednictvím mobilní aplikace Ministerstva zdravotnictví „čTečka“, neboť se jedná o způsob zaručující spolehlivé ověření pravosti a platnosti prokazovaného dokladu obsahujícího QR kód, a to i vzhledem k rostoucímu množství zpráv o prokazování se nepravdivými, resp. falešnými potvrzeními.“*

[5] Navrhovatel se návrhem na zrušení opatření obecné povahy podaným u Nejvyššího správního soudu dne 20. 1. 2022 domáhal zrušení mimořádného opatření v záhlaví uvedeném rozsahu. V návrhu mj. namítal, že stanovením povinnosti prokázat splnění podmínek tzv. bezinfekčnosti došlo k nepřiměřenému zásahu do jeho osobnostních práv, zejména do práva na ochranu soukromí. Odpůrce v odůvodnění mimořádného opatření neuvedl, proč stanovil povinnost užívat aplikaci „čTečka“, a nevyjádřil se k otázce ochrany osobních údajů. Po načtení QR kódu se na zařízení provozovatele v aplikaci zobrazí osobní údaje kontrolované osoby, a to jméno, příjmení, datum narození a státní příslušnost [čl. 4 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „nařízení GDPR“)], a údaj o podstoupení očkování včetně data a typu použité očkovací látky nebo o prodělání onemocnění či o podstoupení PCR testu (čl. 4 odst. 15 nařízení GDPR). Mimořádné opatření přeneslo povinnost nakládat s osobními údaji na provozovatele a zákazníky. Nestanovilo však pravidla pro zpracování osobních údajů zvláštní kategorie. Chybí jakékoliv zamyšlení nad zásahem do práva na ochranu soukromí. Rozsah kontroly a povinnosti stanovené provozovatelům a zákazníkům jsou v rozporu se zásadami zpracování osobních údajů. Odpůrce mimořádným opatřením zatížil

pokračování

provozovatele nakládáním s citlivými osobními údaji, aniž by je seznámil s rozsahem jejich práv a povinností a aniž by učinil jakékoliv opatření k ochraně zpracovávaných osobních údajů. Není zřejmé, proč má být provozovatelům předkládán údaj o podstoupení očkování nebo o prodělání onemocnění. V mimořádném opatření není uveden legitimní účel nakládání s citlivými osobními údaji.

[6] Odpůrce ve vyjádření k návrhu uvedl, že povinnost kontrolovat splnění podmínek tzv. bezinfekčnosti nijak nezasahuje do práv navrhovatele, neboť ten se může prokázat certifikátem v elektronické i fyzické podobě. Kontrolou není porušeno nařízení GDPR. V této souvislosti odpůrce odkázal na rozsudek NSS ze dne 28. 1. 2022, čj. 8 Ao 29/2021-98, č. 4312/2022 Sb. NSS, *společenství vlastníků jednotek*, ve kterém Nejvyšší správní soud dospěl k závěru, že při pouhé vizuální kontrole certifikátů není dána věcná působnost nařízení GDPR, neboť nedochází k automatizovanému zpracování osobních údajů a v případě neautomatizovaného zpracování není vedena jejich evidence. Navrhovatel neuvedl žádnou ucelenou argumentaci, ze které by vyplývalo, jak konkrétně je napadená část mimořádného opatření v rozporu s nařízením GDPR.

[7] Navrhovatel v replice k vyjádření odpůrce uvedl, že to, že mimořádným opatřením není regulována možnost nakládání s osobními údaji provozovateli, představuje značné riziko pro právo na soukromí a na ochranu osobních údajů. Nejvyšší správní soud se v rozsudku *společenství vlastníků jednotek* nezabýval povinností prokázat tzv. bezinfekčnost certifikátem nebo jiným dokladem čitelným aplikací „čTečka“. Certifikát však představuje strukturovaný soubor citlivých údajů. Kontrola je přinejmenším částečně automatizovaným zpracováním osobních údajů ve smyslu čl. 2 odst. 1 nařízení GDPR. I kdyby se toto nařízení neuplatnilo, uplatní se zásady z něj plynoucí. Odpůrce neodůvodnil rozsah kontrolovaných údajů. K zásahu do práva na soukromí dochází spojením povinnosti kontrolovat a povinnosti prokázat splnění podmínek.

II. Použitelné právo Evropské unie a vnitrostátní právní úprava

[8] Podle čl. 2 odst. 1 nařízení GDPR platí, že *toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.*

[9] Podle čl. 4 odrážky 1) nařízení GDPR se pro účely tohoto nařízení rozumí „osobními údaji“ *veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); 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 proků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*

[10] Podle čl. 4 odrážky 2) nařízení GDPR se pro účely tohoto nařízení rozumí „zpracováním“ *jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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.*

[11] Podle čl. 4 odrážky 15 nařízení GDPR se pro účely tohoto nařízení rozumí „údaji o zdravotním stavu“ *osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.*

[12] Podle čl. 9 odst. 1 nařízení GDPR platí, že se zakazuje *zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.*

[13] Podle čl. 1 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 jen „nařízení o digitálních certifikátech“) platí, že *toto nařízení stanoví rámec pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, testu a zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění výkonu práva jejich držitelů na volný pohyb během pandemie COVID-19. Toto nařízení přispěje rovněž k usnadnění postupného zrušení omezení volného pohybu, jež byla zavedena členskými státy v souladu s právem Unie za účelem koordinovaného omezení šíření SARS-CoV-2. Toto nařízení stanoví právní základ pro zpracování osobních údajů nezbytných k vydávání těchto certifikátů a ke zpracování informací nezbytných k ověření a potvrzení pravosti a platnosti těchto certifikátů v plném souladu s nařízením (EU) 2016/679.*

[14] Podle čl. 10 odst. 1 až 3 nařízení o digitálních certifikátech platí, že *1. Na zpracování osobních údajů při provádění tohoto nařízení se použije nařízení (EU) 2016/679. 2. Pro účely tohoto nařízení se osobní údaje obsažené v certifikátech vydaných podle tohoto nařízení zpracovávají pouze pro účely přístupu k informacím uvedeným v certifikátu a jejich ověření, aby se usnadnil výkon práva na volný pohyb v Unii během pandemie COVID-19. Po uplynutí doby použitelnosti tohoto nařízení nesmí být prováděno žádné další zpracování osobních údajů. 3. 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.*

[15] Podle § 2 odst. 1 pandemického zákona platilo, že *ministerstvo zdravotnictví (dále jen „ministerstvo“), krajská hygienická stanice nebo Hygienická stanice hlavního města Prahy (dále jen „krajská hygienická stanice“) může za účelem likvidace epidemie COVID-19 nebo nebezpečí jejího opětovného vzniku nařídit mimořádné opatření, kterým přikáže určitou činnost přispívající k naplnění uvedeného účelu, nebo zakáže nebo omezí určité činnosti nebo služby, jejichž výkonem by mohlo být šířeno onemocnění COVID-19, anebo stanoví podmínky provádění takových činností nebo poskytování takových služeb. Ministerstvo může nařídit mimořádné opatření podle věty první s celostátní působností nebo s působností na území několika krajů. Krajská hygienická stanice může mimořádné opatření nařídit na území svého správního obvodu.*

III. Rozbor předkládané předběžné otázky

pokračování

[16] Předmětem sporu v projednávané věci je mj. otázka, zda odpůrce v mimořádném opatření stanovil pravidla ochrany osobních údajů v souvislosti s kontrolou certifikátů o očkování, prodělaném onemocnění nebo provedeném testu provozovateli prostřednictvím aplikace „čTečka“. Navrhovatel totiž namítá, že se odpůrce touto otázkou v odůvodnění mimořádného opatření nezabýval, že v mimořádném opatření nejsou stanovena pravidla pro zpracování osobních údajů zvláštní kategorie, že v něm chybí zamyšlení se nad zásahem do práva na ochranu soukromí, že odpůrce neseznámil provozovatele s jejich právy a povinnostmi stran zvláštní kategorie osobních údajů, že neučinil žádné opatření k ochraně zpracovávaných osobních údajů a že z mimořádného opatření současně nevyplývá žádný účel nakládání s osobními údaji zvláštní kategorie.

[17] Pro posouzení této otázky Nejvyšším správním soudem je nezbytné předně vyjasnit, zda při kontrole podmínek tzv. bezinfekčnosti pomocí aplikace „čTečka“ dochází k automatizovanému zpracování osobních údajů ve smyslu čl. 4 odrážky 2) nařízení GDPR, a zda je tedy dána věcná působnost nařízení GDPR podle čl. 2 odst. 1 tohoto nařízení.

[18] Nejvyšší správní soud proto vyzval odpůrce k tomu, aby soudu sdělil a popsal, jakým způsobem aplikace „čTečka“ funguje. Odpůrce k výzvě uvedl, že aplikace „čTečka“ slouží ke kontrole a ověření platnosti digitálních certifikátů vydávaných podle nařízení o digitálních certifikátech. 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. Tento proces může probíhat i off-line. Při instalaci aplikace na mobilní telefon je uživateli zobrazen text, ve kterém se uvádí, že „[a]plikace čTečka je provozována v souladu s právem EU a ČR a usnadňuje volný pohyb osob a přístup ke službám a akcím během pandemie COVID-19. Aplikace zpracovává osobní údaje držitelů Digitálních COVID certifikátů z členských států EU za účelem jejich kontroly osobami oprávněnými na základě nařízení EU, mimořádných opatření MZ ČR nebo na dobrovolné bázi. Aplikace neuchovává ani nikam neodesílá osobní ani zdravotní údaje kontrolovaných osob. Detailní informace o zpracování osobních údajů najdete v podmínkách používání.“¹

[19] Nejvyšší správní soud nemá pochybnosti o tom, že údaje obsažené v certifikátech, tj. jméno, příjmení, datum narození a údaj o očkování, prodělaném onemocnění či negativním testu, představují osobní údaje ve smyslu čl. 4 odrážky 1) GDPR. V tomto ohledu lze odkázat na čl. 5 až 7 nařízení o digitálních certifikátech, ve kterých je stanoveno, jaké kategorie osobních údajů jednotlivé certifikáty obsahují. Nejvyšší správní

¹ <https://ockodoc.mzcr.cz/napoveda/ctecka/cz/podminky-pouzivani/>

soud má nicméně pochybnosti o tom, zda jsou tyto osobní údaje při kontrole certifikátů aplikací „čTečka“ zpracovávány ve smyslu čl. 4 odrážky 2) nařízení GDPR.

[20] Podle čl. 3 odst. 2 nařízení o digitálních certifikátech musí certifikát vydávaný členským státem obsahovat interoperabilní čárový kód umožňující ověření jeho pravosti, platnosti a integrity. Česká republika v souladu s prováděcím rozhodnutím Komise (EU) 2021/1073 ze dne 28. června 2021, kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro digitální certifikát EU COVID stanoveného nařízením Evropského parlamentu a Rady (EU) 2021/953, vydává certifikáty s QR kódem, který obsahuje strojově čitelné informace o certifikátu a jeho držiteli. QR kód tak v sobě zahrnuje výše uvedené osobní údaje, které jsou prostřednictvím aplikace „čTečka“ z QR kódu zobrazeny na mobilním telefonu. Přeložení dat ze strojové podoby do čitelné podoby pro člověka se proto děje pomocí automatizovaného postupu, tj. aplikací. Již naskenování QR kódu aplikací „čTečka“ a převedení v něm obsažených informací do podoby čitelné pro člověka tak může naplňovat definici zpracování osobních údajů ve smyslu čl. 4 odrážky 2) nařízení GDPR. Jde totiž o operaci s osobními údaji, při které dochází k jejich přizpůsobení do podoby čitelné pro člověka a zpřístupnění na mobilním telefonu. Nabízí se však otázka, zda je namíste vykládat pojem zpracování takto široce. 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, nedešlá-li nikam aplikace data za účelem jejich překladu. Fakticky jde totiž o pouhou výpočetní operaci, při které není s osobními údaji jakkoliv nakládáno. 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. Jiným příkladem by bylo přečtení údajů na osobních dokladech zpracovaných ve strojově čitelné zóně (v ČR například na občanských průkazech nebo cestovních pasech) nebo vízech [viz k tomu pro EU Společnou a konzulární instrukci k vízům pro diplomatické mise a konzulární úřady (2005/C 326/01)].

[21] Nejde-li při pouhém naskenování QR kódu z certifikátu aplikací „čTečka“ o zpracování osobních údajů, nabízí se otázka, zda ke zpracování osobních údajů nedochází v okamžiku, kdy kontrolující osoba v rámci kontroly podmínek tzv. bezinfekčnosti nahlédne do osobních údajů zobrazených na mobilním telefonu. Nejvyšší správní soud v této souvislosti nemá pochybnosti o tom, že pouhé vizuální nahlédnutí kontrolující osobou na certifikát, ať v tištěné nebo elektronické podobě, nespadá do věcné působnosti nařízení GDPR podle čl. 2 odst. 1 tohoto nařízení. Nedochozí totiž k automatizovanému zpracování osobních údajů a v případě neautomatizovaného zpracování není splněna podmínka vedení evidence takto zjištěných osobních údajů (viz bod 24 rozsudku *společensství vlastníků jednotek*). Nejvyšší správní soud si však není jist, zda k automatizovanému zpracování osobních údajů nedochází následně tím, že kontrolující osoba do nich nahlédne skrze aplikaci „čTečka“ po naskenování QR kódu. Bez této aplikace by totiž kontrolující osoba nebyla schopna informace obsažené v QR kódu dekodovat a přečíst, respektive do nich nahlédnout. Nejvyšší správní soud však podotýká, že z hlediska kontrolující osoby není žádný rozdíl mezi tím, zda v rámci kontroly podmínek tzv. bezinfekčnosti nahlédne do tištěného nebo elektronického certifikátu či zda

pokračování

nejprve naskenuje aplikací QR kód a poté se podívá na informace z něj vyplývající. V každém z těchto případů totiž uvidí shodné osobní údaje, které jsou obsaženy v certifikátu. Nadto při použití aplikace „čTečka“ uvidí nejprve základní identifikační údaje držitele certifikátu (jméno, příjmení a datum narození) a stav platný/neplatný. Kompletní sadu informací obsaženou v certifikátu uvidí až po kliknutí na tlačítko (viz bod [18] výše). Byť je tedy k dekodování QR kódu použit určitý automatizovaný nástroj, z hlediska kontrolující osoby jde i nadále o pouhé vizuální nahlédnutí do osobních údajů kontrolované osoby.

[22] Podle názoru NSS nelze za zpracování osobních údajů považovat pouhé nahlédnutí do osobních údajů, které osoba získá aplikací z QR kódu, jestliže tyto údaje nejsou dále nijak zpracovávány (např. uloženy či kamkoliv dále odesílány). Jde-li totiž pouze o výsledek výpočetní operace, při které jsou strojová data přeložena do podoby čitelné pro člověka, aniž by byla jakkoliv dále využita, tak není dán rozdíl mezi tím, zda osoba nahlédne na certifikát čitelný pro člověka (vytištěný na papíře s příslušnými údaji), nebo zda k jeho překladu do podoby čitelné pro člověka použije aplikaci, ve které následně uvidí tytéž údaje. Nicméně vzhledem k tomu, že k výkladu těchto otázek Soudní dvůr doposud nevyjadřoval, nemůže NSS vyloučit, že Soudní dvůr zaujme odlišný výklad již k této fázi operace s osobními údaji.

[23] Zpracování osobních údajů by dále mohlo představovat ověření platnosti certifikátu aplikací „čTečka“. Při kontrole platnosti certifikátu totiž dochází fakticky k použití osobních údajů stran zdravotního stavu kontrolované osoby obsažených v certifikátu. Aby mohla aplikace vyhodnotit, zda je certifikát platný či nikoliv, musí nutně porovnat údaje o zdravotním stavu dané osoby, tj. např. datum očkování, počet dávek, typ vakcíny, s validačními pravidly platnými v dané době. Osobní údaje zvláštní kategorie obsažené v certifikátu jsou tak aplikací používány pro to, aby kontrolující osoba zjistila, zda kontrolovaná osoba splňuje podmínky tzv. bezinfekčnosti stanovené mimořádným opatřením. V případě pouhé vizuální kontroly musel tuto operaci provést kontrolující. Například tedy podle data prodělání nemoci vyhodnotil, zda certifikát stále umožňoval využít regulovanou službu. Tento úkon aplikace „čTečka“ ulehčila, neboť podle validačních pravidel sama vyhodnotila, zda daný certifikát (například právě o prodělané nemoci) umožňuje službu využít. Za tímto účelem aplikace pravidelně stahovala aktuálně účinná validační pravidla. Aplikace tak při změně pravidel byla automaticky schopna vyhodnotit, zda předkladatel certifikátu po změně pravidel splňuje podmínky tzv. bezinfekčnosti. I to by mohlo představovat (byť nepřímě) zpracování osobních údajů. Při ověřování platnosti certifikátu však osobní údaje stran zdravotního stavu aplikace nezasílala nikam dále, aby byly např. porovnány s národní databází o očkování či prodělaném onemocnění covid-19. Osobní údaje o zdravotním stavu tak nejsou použity k jinému účelu, než k jejich porovnání s validačními pravidly. Tato pravidla se však uplatňovala i tehdy, kdy byly certifikáty kontrolovány pouze vizuálně, avšak nikoliv automaticky jako v případě aplikace „čTečka“. Tato pravidla navíc nebyla vázána na konkrétní osobu, ale jenom na údaje o tzv. bezinfekčnosti. V rámci validace tedy bylo jedno, které konkrétní osoby se údaj týká, protože podstatné bylo jen to, že v jejím certifikátu je obsaženo aktuálně platné pravidlo.

[24] Nedochozí-li ke zpracování osobních údajů ani ve výše uvedeném případě, je namístě se zabývat tím, zda zpracování nepředstavuje kombinace procesů, které při

kontrole certifikátů aplikací „čTečka“ probíhají. Tj. převedení osobních údajů z QR kódu do lidsky čitelné podoby a jejich promítnutí na mobilní telefon, nahlédnutí do nich kontrolující osobou a vyhodnocení platnosti certifikátu aplikací porovnáním osobních údajů o zdravotním stavu s validačními pravidly. Přestože jednotlivě tyto procesy nemusí dosahovat intenzity rozhodné pro naplnění definice zpracování ve smyslu čl. 4 odrážky 2) nařízení GDPR, lze si představit, že ve svém souhrnu již mohou představovat soubor operací s osobními údaji, který je prováděn pomocí automatizovaných postupů, při kterém jsou osobní údaje kontrolovány osoby obsažené v certifikátu zpracovávány za účelem kontroly podmínek tzv. bezinfekčnosti. Nejvyšší správní soud se přiklání spíše k tomu, že v souhrnu o zpracování osobních údajů jde. Oproti vizuální kontrole certifikátu kontrolující osobou jsou totiž osobní údaje při kontrole pomocí aplikace „čTečka“ použity pro automatizované vyhodnocení splnění podmínek tzv. bezinfekčnosti. Za tímto účelem aplikace převádí osobní údaje obsažené v QR kódu do lidsky čitelné podoby, porovnává je s účinnými validačními pravidly a následně je zobrazuje na mobilním telefonu tak, aby do nich mohla kontrolující osoba nahlédnout.

[25] Tento závěr podporuje i to, že nařízení o digitálních certifikátech v čl. 10 odst. 1 až 3 pro účely výkonu práva na volný pohyb v EU výslovně stanovuje, že se na zpracování osobních údajů použije nařízení GDPR, přičemž uvádí, že osobní údaje obsažené v certifikátech zpracovávají příslušné orgány členského státu určení či tranzitu nebo provozovatelé služeb přeshraniční přepravy cestujících pouze k tomu, aby ověřili a potvrdili očkovaní, výsledek testu nebo zotavení držitele. Byť Česká republika používá certifikáty vydávané podle nařízení o digitálních certifikátech ve vztahu k mimořádnému opatření pro vnitrostátní účely (kontrola podmínek tzv. bezinfekčnosti), je namístě, aby nakládání s osobními údaji v certifikátech mělo jednotný právní režim jako v případě přeshraniční přepravy. Jak se totiž uvádí v bodě 48 recitálu nařízení o digitálních certifikátech, *členské státy mohou osobní údaje pro jiné účely zpracovávat, pokud je právní základ pro zpracování těchto údajů pro jiné účely, včetně souvisejících lhůt pro jejich uchování, stanoven ve vnitrostátním právu, které musí být v souladu s právními předpisy Unie na ochranu údajů a se zásadami účinnosti, nezbytnosti a proporcionality a které by mělo obsahovat ustanovení, jež jasně stanoví oblast a rozsah zpracování, konkrétní účel, kategorie subjektů, které mohou certifikát ověřit, a příslušné záruky pro předcházení diskriminaci a zneužívání, s přihlédnutím k rizikům pro práva a svobody subjektů údajů.*

[26] Soudní dvůr se ve své judikatuře dosud nezabýval tím, zda při ověřování platnosti certifikátů vydávaných členskými státy podle nařízení o digitálních certifikátech, které jsou používány pro vnitrostátní účely, skrze národní aplikace dochází ke zpracování osobních údajů ve smyslu čl. 4 odrážky 2) nařízení GDPR, a zda je tedy dána věcná působnost nařízení GDPR podle čl. 2 odst. 1 tohoto nařízení.

[27] Toliko Tribunál v rozsudku ze dne 27. 4. 2022, *Roos a další proti Parlamentu*, ve spojených věcech T-710/21, T-722/21 a T-723/21, EU:T:2022:262, implicitně posoudil kontrolu certifikátů pověřenými pracovníky Evropského parlamentu prostřednictvím národních aplikací „CovidScanBe“ a „Covidcheck.lu“ za zpracování osobních údajů ve smyslu čl. 3 odrážky 3) nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (dále jen „nařízení č. 2018/1725“). Aniž by

pokračování

se Tribunál výslovně zabýval tím, zda o zpracování osobních údajů jde, posoudil žalobní námítky s ohledem na právní úpravu ochrany osobních údajů obsaženou v nařízení č. 2018/1725. Zjevně proto neměl pochybnosti o tom, že se o zpracování osobních údajů jedná. Tribunál ve zmíněném rozsudku vyšel z dokumentu Evropského inspektora ochrany údajů „*Pokyny týkající se návratu na pracoviště a testování imunity nebo infekce onemocnění covid evropskými orgány*“² ve kterém Evropský inspektor ochrany údajů dospěl k závěru, že digitální ověření certifikátů, které zahrnuje skenování QR kódu, představuje zpracování osobních údajů ve smyslu čl. 3 odrážky 3) nařízení č. 2018/1725.

[28] Definice zpracování osobních údajů obsažená v čl. 3 odrážky 3) nařízení č. 2018/1725 je identická s definicí zpracování podle čl. 4 odrážky 2) nařízení GDPR. Současně aplikace „CovidScanBe“ a „Covidcheck.lu“ fungují na obdobném principu jako aplikace „čTečka“ (viz bod 176 rozsudku *Roos a další proti Parlamentu*). I z toho lze proto usuzovat na to, že při kontrole podmínek tzv. bezinfekčnosti aplikací „čTečka“ dochází ke zpracování osobních údajů ve smyslu čl. 4 odrážky 2) nařízení GDPR.

[29] Tato otázka nicméně nebyla v judikatuře Soudního dvora doposud řešena, přičemž z jeho rozhodovací činnosti nelze dovodit, jak široce má být pojem zpracování osobních údajů podle čl. 4 odrážky 2) nařízení GDPR vykládán. Nejvyšší správní soud má zároveň významné pochybnosti o výkladu autonomního pojmu unijního práva, neboť jak bylo rozebráno shora, jednotlivé operace podle jeho názoru spíše nakládání s osobními údaji nepředstavují, a je otázkou, zda jejich spojení skutečně představuje natolik novou kvalitu, že již o nakládání s osobními údaji ve smyslu GDPR může jít.

[30] Nejvyšší správní soud má dále za to, že tato předběžná otázka je navíc obecně významná pro vymezení rozsahu věcné působnosti nařízení GDPR a definice zpracování osobních údajů Soudním dvorem. Bez bližších judikатурních vodítek je totiž těžké posoudit, jaké technické operace s osobními údaji do rozsahu pojmu zpracování osobních údajů ještě spadají a jaké již nikoliv.

[31] V případě předkládané otázky proto nejsou naplněny podmínky pro nepředložení předběžné otázky Soudnímu dvoru stanovené rozsudkem ze dne 6. 10. 1982, *Srl Cilfit – v likvidaci – a další proti Ministerstvu zdravotnictví a Lanificio di Gavardo SpA proti Ministerstvu zdravotnictví*, C-283/81, EU:C:1982:335.

IV. Závěr

[32] Nejvyšší správní soud proto pokládá Soudnímu dvoru Evropské unie předběžnou otázku vymezenou v bodě I. tohoto usnesení.

[33] V návaznosti na položení předběžné otázky Nejvyšší správní soud dle § 48 odst. 1 písm. b) s. ř. s. přerušil řízení. Poté, co Soudní dvůr o předložené otázce rozhodne, bude v řízení Nejvyšší správní soud pokračovat (§ 48 odst. 6 s. ř. s.).

P o u č e n í : Proti tomuto usnesení **n e j s o u** opravné prostředky přípustné.

² EDPS. *Return to the Workplace and EUIs' screening of COVID immunity or infection status* [online]. edps.europa.eu. 9. 8. 2021. [Return to the Workplace and EUIs' screening of COVID immunity or infection status](https://edps.europa.eu/return-to-the-workplace-and-euis-screening-of-covid-immunity-or-infection-status) | European Data Protection Supervisor (europa.eu)

V Brně 12. října 2022

Petr Mikeš
předseda senátu