Spolek pro ochranu osobních údajů

Předběžné vyjádření Spolku pro ochranu osobních údajů k novele zákona č. 127/2005 Sb., navržené Ministerstvem zdravotnictví 30.11.2020

Ministerstvo zdravotnictví připravilo v prosinci 2020 komplexní novelu zákona č. 258/2000 Sb., o ochraně veřejného zdraví, reagující na nedostatečné zakotvení postavení některých státních orgánů a jejich kompetence při boji s epidemiemi (aktuálně COVID-19). Součástí tohoto návrhu (dále jen „*novela*“) je i změna zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen „*ZEK*“), jejímž cílem je zakotvit oprávnění Státní hygienické služby k získávání lokalizačních údajů osob, které prokazatelně onemocněly infekčním onemocněním.

Text navrhované úpravy ZEK zní:

„§ 89a

(1) Operátor je povinen na žádost Státní hygienické služby jí bezodkladně poskytnout pro účely epidemiologického šetření osobní údaje o místech pobytu fyzické osoby, která prokazatelně onemocněla infekčním onemocněním. Součástí požadavku Státní hygienické služby musí být identifikátor mobilní stanice, která pro účely epidemiologického šetření jednoznačně identifikuje tuto osobu. Data se poskytují za časové období nejdéle 3 týdnů zpětně od okamžiku provedení epidemiologického šetření, a to pro každé místo, kde se podle záznamů v operátorem udržované databázi provozně-lokalizačních dat vyskytovala určená mobilní stanice po dobu delší než 20 minut. Data poskytovaná pro každé toto místo jsou

a) časový interval s přesností věcně potřebnou právě a jen pro účely epidemiologického šetření,

b) data o poloze mobilní stanice vyjádřené jako GPS souřadnice náhodně určeného bodu uvnitř polygonu dominance buňky mobilní sítě pro toto místo,

c) technické parametry přesnosti měření polohy pro toto místo, a to zejména polohová rozlišovací schopnost daná technickými parametry mobilní sítě.

(2) Operátor osobní údaje předané Státní hygienické službě podle odstavce 1 neuchovává.

(3) Operátor bezodkladně zašle zprávu na mobilní stanici o tom, že předal údaje uvedené v odstavci 1, vztahující se k této mobilní stanici, Státní hygienické službě za účelem epidemiologického šetření.“.

Podle důvodové zprávy k novele byla tato změna motivována tím, že *„…Státní hygienická služba získá možnost vyžádat si od mobilního operátora lokalizační údaje mobilní stanice v případě, že uživatel mobilní stanice je osobou, která prokazatelně onemocněla infekčním onemocněním. Takové opatření by mělo rozšířit nástroje, které může Státní hygienická služba využít pro omezování šíření infekčních onemocnění.*“
Ohledně záruk spojených s tímto zásahem do základních práv důvodová zpráva uvádí:

„Pokud jde o navrženou změnu zákona o elektronických telekomunikacích, tato změna byla navržena tak, aby byla v souladu s přímo použitelným nařízením EU, a to nařízením Evropského parlamentu a

Rady (EU) č. 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"), GDPR). To samé platí i pro nově zakládané oprávnění ministerstva zřídit službu mobilní aplikace pro účely epidemiologického šetření a zpracovávat osobní údaje získané jejím prostřednictvím. S ohledem na text nového odstavce 2, který se vkládá do § 62a zákona o ochraně veřejného zdraví, je i v tomto případě zřejmé, že při jeho aplikaci se nelze odchýlit od nařízení GDPR. Stejný přístup pak platí i pro případ přenosu výkonu některých činností v rámci epidemiologického šetření na externí subjekt podle § 62a odst. 3 – veřejnoprávní smlouva, jíž k přenosu dochází, musí obsahovat ujednání o ochraně osobních údajů."

Rádi bychom tímto předběžně upozornili na některé aspekty navrhované úpravy, které podle našeho názoru předkladatel nevzal zcela do úvahy a jež mohou vést k nesouladu navrhované úpravy s ústavními předpisy a právními předpisy EU.

V rámci výše uvedených připomínek jsme se zabývali třemi základními okruhy otázek:

I. Obecným posouzením novely z pohledu předpisů na ochranu osobních údajů a šířeji základních lidských práv

II. Procesem vzniku novely z pohledu dodržení předpisů a pravidel podle GDPR a pravidel a doporučení vnitrostátních orgánů

III. Samotným textem novely.

I. Obecné posouzení novely z pohledu předpisů na ochranu osobních údajů a základních lidských práv

Zde považujeme za nutné upozornit na několik aspektů novely, které podle našeho názoru mohou způsobit nekompatibilitu novely s úpravou základních práv ať již vyjádřených v ústavních principech či v právních předpisech EU, které na ně navazují (zejména GDPR a směrnice 2002/58/ES):

1. **Zásah do základních práv**. Novela v §89a ZEK zasahuje do ústavně garantovaného práva na ochranu soukromí ve smyslu čl. 10 odst. 2 a 3, čl. 13 Listiny a čl. 8 Evropské úmluvy. Z tohoto pohledu je třeba hodnotit, zda se jedná o opatření naplňující zásadu proporcionality tak, jak byla definována zejména judikaturou Ústavního soudu, a splňující omezení stanovená GDPR a dalšími právními předpisy EU.[1] Lze očekávat, že v případě jakékoliv epidemie by byl tento institut využíván v širokém rozsahu. Takové využití s sebou ovšem nese zvýšené riziko zásahu do základních práv. Jak zdůraznil Ústavní soud: „*V každém případě však shromažďování a zadržování provozních a lokalizačních údajů znamená zvlášť závažný zásah do soukromí prakticky všech obyvatel České republiky. Princip data retention spočívá v plošném, nevýběrovém sběru významného množství dat o každé uskutečněné elektronické komunikaci, čímž je intenzivně omezeno soukromí jednotlivce, které je mu na ústavní úrovni garantováno čl. 10 odst. 2 Listiny, potažmo i čl. 10 odst. 3 Listiny ve spojení s čl. 13 Listiny. Tak závažné omezení proto jednak musí být prospěšné silnému veřejnému zájmu, a zároveň je nutno je v maximální možné míře minimalizovat, aby mezi ním a naplněním sledovaných cílů existovala spravedlivá rovnováha. Minimalizace zásahu lze dosáhnout omezením využití dat telekomunikačního provozu jen pro nejnutnější okruhy případů, stanovením přísných podmínek, za kterých jsou data jednak uchovávána, jednak zpřístupňována, a vytvořením záruk každému jednotlivci, že v*

[1] V tomto kontextu si dovolujeme odkázat i na rozhodnutí slovenského Ústavního soudu PL.ÚS 13/2020-103 ze dne 13.5.2020 a závěry v něm uvedené, byť jsme si vědomi poněkud odlišného přístupu k data retention mezi českým a slovenským ústavním soudem.

případě využití jeho údajů bude mít k dispozici účinné prostředky obrany proti případnému zneužití.“[2]

2. **Soulad s právními předpisy EU.** Ačkoliv předkladatel správně v důvodové zprávě poukázal na nařízení GDPR, zcela opomněl, že oblast elektronických komunikací je regulována taktéž směrnicí 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „směrnice ePrivacy“). Tato směrnice v čl. 9 stanoví, že zpracování tzv. lokalizačních údajů: *„…je …. pouze poté, co byly anonymizovány údaje, anebo se souhlasem uživatelů nebo účastníků v nezbytném rozsahu a po nezbytnou dobu pro poskytování služeb s přidanou hodnotou. Poskytovatel služeb musí informovat uživatele nebo účastníky před obdržením jejich souhlasu o druhu lokalizačních údajů odlišných od provozních údajů, které budou zpracovávány, o účelu a délce doby zpracování a o tom, zda budou údaje předány třetí osobě za účelem poskytování služeb s přidanou hodnotou. Uživatelé nebo účastníci musí mít možnost kdykoliv vzít zpět svůj souhlas se zpracováním lokalizačních údajů odlišných od provozních údajů.“*

   Směrnice ePrivacy z tohoto zákazu sice umožňuje v čl. 15 odst. 1 výjimky, nicméně tyto výjimky je nutné vykládat restriktivně. Navíc z pohledu možnosti jejich aplikace na ochranu veřejného zdraví není text čl. 15 zcela jednoznačný: *„Členské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, vhodné a přiměřené opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/46/ES. Za tímto účelem mohou členské státy mimo jiné přijmout legislativní opatření umožňující uchovávání údajů po omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o Evropské unii.“* Zde upozorňujeme na to, že výslovně není předpokládána výjimka z důvodu ochrany veřejného zdraví. Zda by tato výjimka mohla být dovozována z důvodu veřejné bezpečnosti, považujeme za sporné.[3] O to více by mělo být dbáno při zakotvení zásahu do těchto základních práv do národního právního řádu na dodržení základních principů ochrany osobních údajů, zejména minimalizace doby zpracování, zásady nezbytnosti a přiměřenosti. Význam řádné aplikace směrnice ePrivacy zdůrazňuje taktéž EDPB ve svých „*Pokynech 04/2020 k používání lokalizačních údajů a nástrojů k trasování kontaktů v souvislosti s propuknutím onemocnění COVID-19*“

3. **Absence dostatečné veřejné kontroly**. Novela podle našich informací svěřuje výlučnou pravomoc k rozhodování o žádosti Státní hygienické službě. (nejspíše pak i včetně vlastního rozhodování, u jakých typů infekčních nemocí takovýto invazivní prostředek využije). V tomto smyslu se tak jedná o povinnost předávání údajů mobilními operátory zcela mimo doposud obecně akceptovaných specifických situací. Ve srovnání s jinými zásahy do telekomunikačního tajemství tak není v daném případě přítomen prvek předchozí veřejné (zejména soudní) kontroly, jako je např. v případě vyžádání provozních a lokalizačních údajů pro účely trestního řízení dle trestního řádu[4] (dle dikce trestního řádu „údaje o telekomunikačním provozu“), či

[2] nález Pl. ÚS 45/17; k tomu srov např. také rozsudek SDEU ve věci C-623/17, zejména body 70 až 80 jeho odůvodnění
[3] Viz např. čl. 52 Smlouvy o fungování EU, který rozlišuje „veřejnou bezpečnost“ a „ochranu zdraví“.
[4] Viz § 88a zákona č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

v případě odposlechů[5] – i pro tak závažný účel, jakým je bezesporu trestní řízení, je oprávněn nařídit vydání provozních a lokalizačních údajů, resp. nařídit odposlech, výhradně předseda senátu a v přípravném řízení soudce. Právě na uvedeném příkladu vyžádání provozních a lokalizačních údajů dle trestního řádu lze přitom ilustrovat, že – právě s ohledem na míru a intenzitu zásahu do základních práv a svobod, který zpracování provozních a lokalizačních údajů představuje – ani trestní řád neumožňuje získání těchto dat pro jakékoli trestní řízení a omezuje je pouze na trestní řízení vedená pro trestné činy pro tento účel vymezené v trestním řádu. Toto omezení se přitom postupně vyvíjelo pod vlivem a v reakci na posuzování problematiky provozních a lokalizačních údajů Ústavním soudem ČR.[6]

Kontrola však nespočívá pouze v ingerenci soudu ve stadiu nařízení vydání provozních a lokalizačních údajů. Trestní řád v § 88a odst. 2 ukládá povinnost informovat po pravomocném skončení věci o nařízeném zjišťování provozních a lokalizačních údajů osobu uživatele, jehož provozní a lokalizační údaje byly takto vyžádány. Na tuto úpravu pak navazuje Řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu, které je dle § 314 a následujících trestního řádu oprávněna iniciovat u Nejvyššího soudu dotčená osoba.

Ačkoliv se podle navrhovaného znění § 89a odst. 3 ZEK subjekt údajů dozví o tom, že byly jeho lokalizační údaje předány, bude se jednat (už s ohledem na použitou technologii SMS) o zcela kusou informaci, která méně zkušeným uživatelům nemusí dostatečně ozřejmit, k jakému předání došlo a z jakého důvodu. Navíc by se v případě SMS zjevně nejednalo o materiál srovnatelný se shora popisovanou informací poskytovanou dle trestního řádu dotčené osobě po pravomocném skončení věci – zásad do základních práv je přitom zcela srovnatelný a je tedy důvodné požadovat možnost dotčené osoby iniciovat obdobný soudní přezkum takového zásahu. Nadto se pro mobilní operátory může jednat o nové zpracování osobních údajů specifické povahy, resp. speciálních osobních údajů s prvkem zdravotního stavu.

Kromě předběžné i dodatečné soudní kontroly, která je aplikována v případě vydání provozních a lokalizačních údajů ze strany operátorů pro účely trestního řízení, je třeba poukázat i na další nepřímé kontrolní mechanismy aplikované v těchto případech. Jedná se o povinné vedení evidence dle §97 odst. 10 ZEK, kdy z návrhu §89a ZEK není zřejmé, nakolik by měly být do této evidence zahrnuty i žádosti Státní hygienické služby.

Významný prvek veřejné kontroly nad využitím provozních a lokalizačních údajů představuje také Stálá komise Poslanecké sněmovny Parlamentu ČR pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací, resp. Stálá komise pro kontrolu činnosti Bezpečnostní informační služby a Stálá komise pro kontrolu činnosti Vojenského zpravodajství. Jejich existence je dokladem závažnosti zásahu do základních práv, který zpracování provozních a lokalizačních údajů v praxi představuje.

4. **Absence detailnější úpravy nakládání se získanými údaji ze strany Státní hygienické služby.** Zde je třeba zejména upozornit na povinnosti podle čl. 6 odst. 3 GDPR:

   „3. Základ pro zpracování podle odst. 1 písm. c) a e) musí být stanoven:

[5] K možnosti srovnání využití lokalizačních údajů s odposlechy a jeho limitům srov. např. nález Ústavního soudu ze dne 14. května 2019 sp. zn. Pl. ÚS 45/17 ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, a vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

[6] Viz nálezy Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22.3.2011 a Pl. ÚS 24/11 ze dne 20.12.2011.

a) právem Unie nebo

b) právem členského státu, které se na správce vztahuje.

Účel zpracování musí vycházet z tohoto právního základu, nebo pokud jde o zpracování uvedené v odst. 1 písm. e), musí být toto zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Tento právní základ může obsahovat konkrétní ustanovení pro přizpůsobení uplatňování pravidel tohoto nařízení, včetně obecných podmínek, kterými se řídí zákonnost zpracování správcem, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupů zpracování, jakož i dalších opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace, při nichž dochází ke zpracování, než stanoví kapitola IX. Právo Unie nebo členského státu musí splňovat cíl veřejného zájmu a musí být přiměřené sledovanému legitimnímu cíli."

Zejména podrobnější úprava retenční doby, účelu nakládání s těmito údaji a jejich zabezpečení by jistě oslabila riziko zneužití takových údajů, či přímo zásahu do základních práv osob touto úpravou. Zde je možné opětovně odkázat na výše zmíněný pokyn EDPB č. 04/2020.

Tato podrobnější úprava by podle našeho názoru mohla přitom být svěřena i podzákonnému předpisu (např. vyhláška ministerstva).

Současně je též dle našeho hodnocení zcela nezbytné, aby na straně orgánu, který by zpracovával natolik senzitivní údaje, jakými jsou nepochybně provozní a lokalizační údaje, zvláště pak ve spojení s údaji o zdravotním stavu konkrétních osob, byly vytvořeny dostatečné mechanismy a přijata odpovídající technická a organizační opatření, která zajistí bezpečné zpracování předmětných údajů. Tato opatření musejí být úměrná rizikům, která představuje případný neoprávněný přístup k provozním a lokalizačním údajům (případně též v naznačené kombinaci s údaji o zdravotním stavu), či zneužití těchto údajů.

5. **Zohlednění práv třetích osob**. Ačkoliv se novela § 89a ZEK věnuje právům osob, jejichž údaje budou ze strany telekomunikačních operátorů předávány, ponechává zcela stranou otázku, k jakému trasování budou tyto údaje využity a jak budou zajištěna práva osob, jež budou prostřednictvím takovýchto poměrně invazivních prostředků (např. v kombinaci s jinak získanými údaji či příslušnými identifikátory fyzických osob) vytrasovány.
   Toto si lze taktéž dát do souvislosti se současnými námitkami mobilních operátorů, že takovéto uložení (pro ně) další povinnosti bez toho, aniž by bylo provedeno detailní vyhodnocení (ne)účinnosti (včetně provedení analýzy DPIA, viz také dále) již současných nasazených nástrojů a opatření, a současně bez přechozího projednání s nimi, je velmi obtížné obhájit prosazení takto invazivního prostředku s jednoznačným zásahem do svobod fyzických osob, jejichž údaje budou takto přenášeny bez obdržení bližší informace o způsobu a účelech zpracování těchto údajů.
6. **Nejasně nastavené podmínky předávání**. V prvé řadě je možné za problematické body považovat absenci jednoznačného (bližšího) vymezení podmínek předání. Druhým, neméně problematickým, bodem je samotná otázka rozsahu, struktury a formy požadovaných údajů (včetně dané lhůty), kdy z pohledu disponibility mobilních operátorů požadovanými údaji v požadované struktuře nejsou v předmětné důvodové zprávě přesně rozvedeny jednotlivé prvky „provozně-lokalizačních" údajů v kontextu jednotlivých bodů, přičemž tak není vůbec řešeno, zdali samotní mobilní operátoři disponují takovýmito typy údajů v požadované

struktuře, a to jak údaji čistě technického rázu, tak údaji o držitelích, resp. držitelích a uživatelích. Z faktického hlediska je tak jen konstatována takováto nově uložená povinnost, která vychází z předpokladu, že operátoři uchovávají i po uskutečnění přenosu zpráv prostřednictvím sítě elektronických komunikací všechny potřebné údaje pro vyřízení žádosti. Tak tomu ovšem může být pouze při dodržení přísných podmínek stanovených směrnicí 2002/58/ES (viz bod 2 výše), respektive při splnění některé z výjimek dle § 90 odst. 3 až 6 ZEK nebo díky plošnému uchování provozních a lokalizační údajů podle § 97 odst. 3 ZEK.[7] V důsledku toho je třeba na založení nové povinnosti operátorů k předání údajů Státní hygienické službě pohlížet jako na zpracování osobních údajů pro jiný účel, než pro který byly osobní údaje shromážděny. Takové zpracování musí být dle čl. 6 odst. 4 GDPR založeno na právu Evropské unie či členského státu a tento další účel zpracování musí představovat v demokratické společnosti nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1 GDPR. Tento důležitý aspekt by měl být pochopitelně také součástí analýzy DPIA, viz dále.

II. Připomínky k procesu vzniku novely z pohledu dodržení předpisů a pravidel podle GDPR a pravidel a doporučení vnitrostátních orgánů

Článek 35 GDPR upravuje tzv. posouzení vlivu na ochranu osobních údajů. Toto posouzení je třeba provést, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

Podle našeho názoru v případě zpracování předpokládaného novelou je tento požadavek naplněn.

Podle čl. 37 odst. 7 GDPR posouzení vlivu na ochranu osobních údajů musí obsahovat alespoň:

„a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;
b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
c) posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1; a
d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.“

Čl. 35 odst. 10 sice umožňuje vyloučit pravidla pro provedení posouzení vlivu, ovšem pouze za splnění těchto předpokladů: *„Pokud má zpracování podle čl. 6 odst. 1 písm. c) nebo e) právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, odstavce 1 až 7 se nepoužijí, ledaže by členské státy považovaly provedení tohoto posouzení před činnostmi zpracování za nezbytné.“*[8]

V návaznosti na tuto úpravu Úřad pro ochranu osobních údajů uveřejnil na svých webových stránkách metodické materiály týkající se **povinnosti provedení posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů**. Obecný návod je určen legislativním útvarům ministerstev a jiných ústředních správních úřadů jako pomůcka, jak splnit tuto povinnost.

7 Ohledně limitů plošného uchování provozních údajů lze odkázat kromě výše uvedeného nálezu Ústavního soudu ze dne 14. května 2019 ve věci sp. zn. Pl. ÚS 45/17 nejnověji také na rozsudek (velkého senátu) Soudního dvora Evropské Unie ze dne 6. října 2020 ve věci C-623/17 a spojených věcech

8 Na tuto úpravu pak navazuje § 10 zákona č. 110/2019 Sb.

Zveřejněný materiál je veden zejména snahou o nápravu dlouhodobě nedostatečného dodržování povinnosti státu: „Kvalitní a podrobné posouzení vlivu na ochranu osobních údajů provedené v rámci návrhu právních předpisů je totiž od okamžiku účinnosti nového zákona jediným a nezbytným návodem pro instruování správců a zpracovatelů, vodítkem pro poznání, jaké hrozby na osobní údaje působí, jaké jsou dopady do soukromí a jaká technická a organizační opatření mají při zpracováních uložených zákonem tyto subjekty přijmout".

Posouzení vlivu na ochranu osobních údajů u vládních návrhů právních předpisů a jejich novel je navrhovatel povinen vypracovat také na základě článku 4 odst. 1 písm. g), článku 9 odst. 2 písm. h), článku 14 odst. 1 písm. g) a článku 16 odst. 4 legislativních pravidel vlády jako „*zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů*". Posouzení vlivu na ochranu osobních údajů je součást obecné části důvodové zprávy nebo odůvodnění.

V případě novely podle našeho názoru nebyl bohužel dostatečně naplněn téměř žádný z bodů metodického návodu Úřadu pro ochranu osobních údajů, zejména nezbytné body 6 až 12.

Kapitola E. novely „Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů" obecné části důvodové výše uvedené posouzení v dostatečném rozsahu neobsahuje.

V zásadě jediné „zhodnocení" vlivu v kapitole E zní „*Právní úprava byla navržena tak, aby byla v souladu s přímo použitelným nařízení EU – nařízením GDPR. To samé platí i pro nově zakládané oprávnění Ministerstva zdravotnictví zřídit službu mobilní aplikace pro účely epidemiologického šetření a zpracovávat osobní údaje získané jejím prostřednictvím i pro přenos výkonu některých činností souvisejících s epidemiologickým šetřením.*" Takové posouzení je ovšem zcela nedostatečné a nenaplňuje jak kritéria stanovená evropským zákonodárcem, tak požadavky stanovené ze strany ÚOOÚ. Uvedený odstavec nelze považovat za plnohodnotné posouzení vlivu na ochranu osobních údajů (DPIA). Přitom právě detailní DPIA by tak masivní zásah do práv a svobod občanů[9] mělo předcházet. Samozřejmostí by měla být minimálně odborná (když ne veřejná) diskuse a posouzení dalšími dotčenými subjekty (když ne samotnými občany). Ani současná složitá epidemiologická situace nemůže ospravedlnit tak významný zásah státu do demokratického fungování společnosti.

GDPR v recitálu č. 96 navíc doplňuje povinné zpracování DPIA následně: „*V průběhu příprav legislativního nebo regulačního opatření, jímž bude stanoveno zpracování osobních údajů, by měl být rovněž konzultován dozorový úřad, aby byl zajištěn soulad zamýšleného zpracování s tímto nařízením, a zejména zmírněno související riziko pro subjekt údajů.*". Tomu odpovídá text čl. 36 odst. 4 GDPR – Dle dostupných informací k tomuto kroku doposud nebylo přistoupeno.

III. Připomínky k textu novely

Konkrétní poznámky pro připomínky k návrhu novely. Návrh ustanovení § 89a obsahuje několik sporných míst, v některých částech nejsou podle našeho názoru zcela dodržena legislativní pravidla vlády, zejm. čl. 2 odst. 1, odst. 2 písm. a) až d), a čl. 9 odst. 2 (většina bodů). Jak bylo zmíněno výše, v řadě případů by konkretizace mohla být ponechána na podzákonném předpisu.

Konkrétně k některým částem navrhovaného ustanovení:

<u>Odst. 1</u>

[9] V případě žádosti Státní hygienické služby, která z principu bude obsahovat osobní údaj (telefonní číslo, na základě, kterého je přímo identifikovatelná fyzická osoba) doplněný o informaci, že tato fyzická osoba onemocněla infekčním onemocněním, tedy operátor bude zpracovávat osobní údaje zvláštní kategorie. Tato změna jistě zasáhne do procesů zpracování osobních údajů, které doposud nezpracovával.

„Operátor je povinen na žádost Státní hygienické služby jí bezodkladně poskytnout pro účely epidemiologického šetření osobní údaje o místech pobytu fyzické osoby…“

- Operátor nedisponuje údajem „*o místech pobytu fyzické osoby“*. Uchovává konkrétně provozní a lokalizační údaje (zjednodušeně – údaje zpracovávané pro potřeby přenosu zprávy a údaje, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací), dále pak informace z databáze účastníků.

„…která prokazatelně onemocněla infekčním onemocněním…“

- Chybí bližší vymezení toho, kdy bude považována za naplněnou podmínka „*prokazatelného onemocnění“*.
- Chybí kontrolní mechanizmus, a zároveň i autorita, která by splnění této jediné podmínky nezávisle potvrdila a také kontrolovala.

„Součástí požadavku Státní hygienické služby…“

- Náležitosti požadavku nejsou nikde stanoveny ani odkazovány. Zároveň doporučujeme vyjasnit, v jakém režimu bude požadavek státní hygienické služby předáván, tzn. zda se bude jednat o rozhodnutí ve správním řízení či nikoliv.

„…kde se podle záznamů v operátorem udržované databázi provozně-lokalizačních dat vyskytovala určená mobilní stanice…“

- použitá terminologie neodpovídá příslušným termínům použitých v ZEK
- velmi problematické může být pojetí samotného pojmu identifikátoru mobilní stanice, za jakou se běžně považuje IMEI telefonu („stanice“), přičemž však v tomto ohledu je nejspíše za takovýto unikátní identifikátor považováno osobní telefonní číslo (resp. SIM karta) uživatele/účastníka takovéto mobilní stanice. Problematickým bodem je však v tomto kontextu i obecné nerozlišování (v rámci poskytování dat Státní hygienické službě) mezi poskytovatelem služby elektronických komunikací (MVNO) vedle samotného síťového operátora (MNO), u kterého právě nemusí být možné vždy za splnění všech podmínek uvedených v rámci poskytovaných dat takovémuto požadavku vůbec funkčně a technicky vyhovět.

„Data poskytovaná pro každé toto místo jsou
a) časový interval s přesností věcně potřebnou právě a jen pro účely epidemiologického šetření,
b) data o poloze mobilní stanice vyjádřené jako GPS souřadnice náhodně určeného bodu uvnitř polygonu dominance buňky mobilní sítě pro toto místo,
c) technické parametry přesnosti měření polohy pro toto místo, a to zejména polohová rozlišovací schopnost daná technickými parametry mobilní sítě. …“

- Doporučujeme vyjasnit, jaké náklady by si tímto stanovením požadované zpracování poskytnutých údajů v praxi vyžádalo.

Odst. 2:

„Operátor osobní údaje předané Státní hygienické službě podle odstavce 1 neuchovává…„

- Chápeme motivaci k doplnění tohoto návrhu, nicméně je třeba zvážit tuto úpravu i z pohledu možné kontroly zákonnosti předání (když následně bude dotčenými informacemi plně disponovat pouze veřejná správa a nebude možné provézt zpětnou kontrolu týkající se možného zneužití takových údajů ze strany Státní hygienické správy) a případného zájmu operátorů na doložení toho, že splnili povinnost stanovenou novelou. Domníváme se proto, že toto ustanovení by mělo být předmětem další diskuze.
- Požadavek na samotné neuchovávání takovýchto předaných osobních údajů je přitom možné vykládat různým způsobem, přičemž s ohledem na ostatní ustanovení ZEK předpokládáme, že je tím ve skutečnosti myšlen výmaz předané informace o místě pobytu Státní hygienické službě

o konkrétním potvrzeném (infekčním) uživateli/účastníkovi služby elektronických komunikací, nikoliv však přímo výmaz takovýchto vybraných lokalizačních údajů o konkrétním uživateli/účastníkovi z databáze účastníků služeb elektronických komunikací (což mu ostatně ani ZEK takto přímo neukládá), kde jsou nastaveny přísné retenční lhůty.

Odst. 3:

„Operátor bezodkladně zašle zprávu na mobilní stanici o tom, že předal údaje uvedené v odstavci 1…“

- Jak bylo již uvedeno výše, zejména u neinformovaných uživatelů nemusí samotné zaslání SMS dostačovat k plné a účinné informovanosti o zpracování a pochopení míry rizika z něho plynoucí.

S předchozími body souvisí i problém s absencí stanovení sankcí za nedodržení stanovených povinností ze strany veřejné správy.

Nezanedbatelnou stránkou je otázka financování, která není v návrhu vůbec řešena. Lze se tedy domnívat, že **byla podceněna finanční analýza dopadů**.

Zhodnocení dopadů

Materiál nesplňuje ani další nesplňuje požadavky na normotvorbu dané Legislativními pravidly vlády. V důvodové zprávě, konkrétně v kapitole **C. Předpokládaný hospodářský a finanční dopad navrhované právní úpravy** není výše uvedený finanční dopad (v odhadovaném řádu jednotek až desítek milionů ročně) vůbec zohledněn.

Prolomení ústavou zaručených práv a svobod je v případě poskytování provozních a lokalizačních údajů doposud umožněno pouze v mimořádných případech a vždy za přísných podmínek a s příslušným povolením předsedy senátu a v přípravném řízení soudce; příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn. Těmito oprávněnými orgány jsou (stručně) orgány činné v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem, Policie České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zpravodajské služby a Česká národní banka, a to za velmi přísných podmínek.

Výše uvedený materiál obsahuje předběžné připomínky k návrhu novely. Její podrobné zhodnocení si vyžádá další podrobnější odbornou diskuzi všech zainteresovaných stran. Kromě výše uvedeného považujeme přitom za nutné, aby navrhovatel aplikoval na tento materiál standardní test proporcionality, který v případech obdobných zásahů do základních práv aplikují ústavní soudy, vč. Ústavního soudu ČR a přijal rozhodnutí dle výsledku tohoto testu.

S ohledem na výše uvedené jsme přesvědčeni, že je zcela nezbytné výrazně dopracovat východiska a odůvodnění navrhované novely tak, aby zohlednila veškeré relevantní ústavní předpisy a předpisy EU a aby zabezpečila vysoký stupeň ochrany práv dotčených fyzických osob, jak naznačeno ve výše rozvedených bodech. Závěry takto dopracovaných východisek a odůvodnění pak dle našeho předběžného hodnocení patrně povedou k opuštění ideového záměru zpracování provozních a lokalizačních údajů pro diskutovaný účel, resp. k podstatnému přepracování návrhu novely, pro zohlednění výše uvedených bodů.

V Praze, dne 4.12.2020

Zpracovali: JUDr. Vladan Rámiš, Ph.D., Mgr. Jaroslav Hora, Mgr. Vojtěch Rusz, JUDr. Miroslav Uřičař, Mgr. Dominik Vítek, Mgr. Martin Cach

Spolek pro ochranu osobních údajů