Pokyny 04/2020 k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19

Přijato dne 21. dubna 2020

přijato

Historie verzí

Verze 1.1	5. května 2020	Drobné opravy
Verze 1.0	21. dubna 2020	Přijetí pokynů

Obsah

Evropský sbor pro ochranu osobních údajů (EDPB),

s ohledem na čl. 70 odst. 1 písm. e) 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 (dále jen „nařízení GDPR“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI této dohody a protokol 37 k této dohodě, ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[1],

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TYTO POKYNY:

1 ÚVOD A SOUVISLOSTI

1 Vlády a soukromé subjekty začínají v rámci reakce na pandemii COVID-19 používat řešení založená na údajích, což vyvolává řadu otázek týkajících se soukromí.

2 EDPB zdůrazňuje, že právní rámec pro ochranu údajů byl navržen tak, aby byl flexibilní, a jako takový je schopen dosáhnout účinné odezvy při omezování pandemie i při ochraně základních lidských práv a svobod.

3 EDPB je pevně přesvědčen, že pokud zvládnutí pandemie COVID-19 vyžaduje zpracování osobních údajů, je ochrana údajů nezbytná k vybudování důvěry, k vytvoření podmínek pro společenskou přijatelnost jakéhokoli řešení, a tudíž k zaručení účinnosti těchto opatření. Protože virus nezná hranice, zdá se, že nejvhodnějším řešením bude vyvinout společný evropský přístup v reakci na současnou krizi nebo alespoň zavést interoperabilní rámec.

4 EDPB se obecně domnívá, že údaje a technologie používané jako pomoc v boji s onemocněním COVID-19 by měly sloužit spíše k posílení jednotlivců než k jejich kontrole, stigmatizaci nebo utlačování. Kromě toho, údaje a technologie sice mohou být důležité nástroje, avšak jsou ze své podstaty omezené a mohou pouze zvýšit účinnost jiných opatření v oblasti veřejného zdraví. Obecnými zásadami účinnosti, nezbytnosti a proporcionality se musí řídit každé opatření přijaté členskými státy nebo orgány EU, jež zahrnuje zpracování osobních údajů v rámci boje s onemocněním COVID-19.

5 Tyto pokyny objasňují podmínky a zásady pro přiměřené používání lokalizačních údajů a nástrojů k vysledování kontaktů, a to pro dva zvláštní účely:

- využívání lokalizačních údajů na podporu reakce na pandemii modelováním šíření viru za účelem posouzení celkové účinnosti opatření omezujících volný pohyb osob,
- vysledování kontaktů, jehož cílem je uvědomit jednotlivce o skutečnosti, že se nacházeli v bezprostřední blízkosti někoho, u koho se nakonec potvrdí, že je přenašečem viru, aby se co nejdříve přerušily řetězce nákazy.

6 Účinnost pomoci aplikací pro vysledování kontaktů při zvládání pandemie závisí na mnoha faktorech (např. procentním podílu lidí, kteří by si je měli nainstalovat; definici „kontaktu“, pokud jde o blízkost a trvání). Tyto aplikace navíc musejí být součástí komplexní strategie v oblasti veřejného zdraví pro boj s pandemií, která mimo jiné zahrnuje i testování a následné manuální vysledování kontaktů, aby byly odstraněny pochybnosti. Jejich zavedení by měla doprovázet podpůrná opatření, která zajistí, aby byly informace poskytované uživatelům

1 Odkazy na „členské státy“ v celém tomto dokumentu je třeba chápat jako odkazy na „členské státy EHP“.

uvedeny do kontextu a aby varování byla užitečná pro systém veřejného zdravotnictví. Jinak by tyto aplikace nemusely plně využít svůj potenciál.

7 EDPB zdůrazňuje, že nařízení GDPR i směrnice 2002/58/ES (dále jen „směrnice“) obsahují konkrétní pravidla, která umožňují využívání anonymních nebo osobních údajů na podporu orgánů veřejné moci a dalších subjektů na vnitrostátní a unijní úrovni při sledování a omezování šíření viru SARS-CoV-2[2].

8 V tomto ohledu již EDPB zaujal stanovisko ke skutečnosti, že používání aplikací pro vysledování kontaktů by mělo být dobrovolné a nemělo by spoléhat na sledování pohybů jednotlivců, ale spíše na informace o přiblížení, jež se týkají uživatelů[3].

[2] Viz předchozí prohlášení EDPB o rozšíření onemocnění COVID-19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 VYUŽÍVÁNÍ LOKALIZAČNÍCH ÚDAJŮ

2.1 Zdroje lokalizačních údajů

9 Existují dva hlavní zdroje lokalizačních údajů, které jsou k dispozici pro modelování šíření viru a celkové účinnosti opatření omezujících volný pohyb osob:

- lokalizační údaje shromažďované poskytovateli služeb elektronických komunikací (jako jsou mobilní telekomunikační operátoři) v průběhu poskytování služeb a
- lokalizační údaje shromažďované pomocí aplikací poskytovatelů služeb informační společnosti, jejichž fungování vyžaduje používání těchto údajů (např. navigace, přepravní služby atd.).

10 EDPB připomíná, že lokalizační údaje[4] shromážděné od poskytovatelů elektronických komunikací mohou být zpracovány pouze v rámci působnosti článků 6 a 9 směrnice. To znamená, že tyto údaje mohou být předány orgánům nebo jiným třetím stranám pouze tehdy, pokud byly anonymizovány poskytovatelem, nebo v případě údajů určujících zeměpisnou polohu koncového zařízení uživatele, které nejsou provozními údaji, s předchozím souhlasem uživatelů[5].

11 Co se týče informací, včetně lokalizačních údajů, jež byly shromážděny přímo z koncového zařízení, použije se čl. 5 odst. 3 směrnice. Ukládání informací v zařízení uživatele nebo získání přístupu k již uloženým informacím je tudíž povoleno pouze tehdy, pokud i) uživatel udělil souhlas[6] nebo ii) je uložení a/nebo získání přístupu nezbytně nutné pro službu informační společnosti, kterou si uživatel výslovně vyžádal.

12 Odchylky od práv a povinností stanovených ve směrnici jsou však možné v souladu s článkem 15, pokud představují nezbytné, vhodné a přiměřené opatření v demokratické společnosti v zájmu určitých cílů[7].

13 Pokud jde o opakované použití lokalizačních údajů shromážděných poskytovatelem služeb informační společnosti pro účely modelování (např. prostřednictvím operačního systému nebo některé již dříve nainstalované aplikace), musí být splněny dodatečné podmínky. Ostatně pokud byly údaje shromážděny v souladu s čl. 5 odst. 3 směrnice, mohou být dále zpracovány pouze s dodatečným souhlasem subjektu údajů nebo na základě práva Unie nebo členského státu, které představuje nezbytné a přiměřené opatření v demokratické společnosti za účelem zajištění cílů uvedených v čl. 23 odst. 1 nařízení GDPR[8].

2.2 Zaměření na používání anonymizovaných lokalizačních údajů

14 EDPB zdůrazňuje, že pokud jde o využívání lokalizačních údajů, mělo by se vždy upřednostnit zpracování anonymizovaných údajů před zpracováním osobních údajů.

15 Anonymizací se rozumí používání souboru technik za účelem odstranění možnosti propojit údaje s identifikovanou či identifikovatelnou fyzickou osobou při jakémkoli „přiměřeném“ úsilí. Tento „test přiměřenosti“ musí brát v úvahu jak objektivní aspekty (čas, technické prostředky), tak skutečnosti vyplývající z kontextu, které se mohou lišit případ od případu (vzácnost daného jevu s přihlédnutím například k hustotě obyvatel, povaze a objemu dat). Pokud údaje tímto testem neprojdou, znamená to, že nebyly anonymizovány, a tím pádem zůstávají v oblasti působnosti nařízení GDPR.

---

[4] Viz čl. 2 písm. c) směrnice.
[5] Viz články 6 a 9 směrnice.
[6] Pojem souhlas dle směrnice zůstává shodný s pojmem souhlas stanoveným v nařízení GDPR a musí splňovat všechny požadavky souhlasu uvedené v čl. 4 odst. 11 a článku 7 nařízení GDPR.
[7] Pro účely výkladu článku 15 směrnice viz také rozsudek Soudního dvora EU ze dne 29. ledna 2008 ve věci C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU.
[8] Viz oddíl 1.5.3 pokynů 1/2020 pro zpracování osobních údajů v souvislosti s propojenými vozidly.

16 Hodnocení důkladnosti anonymizace vychází ze tří kritérií: i) vyčlenění (izolace jednotlivce uvnitř větší skupiny na základě údajů); ii) propojitelnost (propojení dvou záznamů týkajících se stejného jednotlivce) a iii) vyvození (vydedukování neznámých informací o jednotlivci se značnou pravděpodobností).

17 Pojem anonymizace je často nesprávně chápán a zaměňován s pseudonymizací. Zatímco anonymizace umožňuje využívat údaje bez jakéhokoli omezení, pseudonymizované údaje jsou stále v rozsahu působnosti nařízení GDPR.

18 Existuje mnoho možností účinné anonymizace[9], avšak s určitou výhradou. Údaje nemohou být anonymizovány samostatně, což znamená, že pouze soubory údajů jako celek mohou nebo nemusí být anonymizovány. V tomto smyslu může být jakýkoli zásah na úrovni jednotlivého datového vzorce (prostřednictvím šifrování nebo jiných matematických transformací) považován přinejlepším za pseudonymizaci.

19 Procesy anonymizace a útoky založené na opětovné identifikaci patří mezi aktivní oblasti výzkumu. Je velmi důležité, aby každý správce uplatňující řešení založená na anonymizaci sledoval aktuální vývoj v této oblasti, zejména s ohledem na lokalizační údaje (pocházející od telekomunikačních operátorů a/nebo služeb informační společnosti), o kterých je velmi dobře známo, že se anonymizují obtížně.

20 Z rozsáhlého výzkumu skutečně vyplývá[10], že *lokalizační údaje považované za anonymizované* ve skutečnosti anonymizované být nemusí. Stopy mobility jednotlivců jsou ze své podstaty vysoce korelované a jedinečné. Proto mohou být za určitých okolností zranitelné vůči pokusům o opětovnou identifikaci.

21 Jednotlivý datový vzorec, který sleduje polohu jednotlivce po značnou dobu, nemůže být plně anonymizován. Toto posouzení může stále platit, není-li přesnost zaznamenaných zeměpisných souřadnic dostatečně snížena nebo jsou-li podrobnosti o trase odstraněny, a dokonce i je-li uchovávána pouze poloha míst, kde subjekt údajů setrvává po delší dobu. To platí i pro lokalizační údaje, které nejsou řádně agregovány.

22 K dosažení anonymizace musejí být lokalizační údaje pečlivě zpracovány, aby byl splněn test přiměřenosti. V tomto smyslu takové zpracování zahrnuje zohlednění souborů lokalizačních údajů jako celku, jakož i zpracování údajů z přiměřeně velkého souboru jednotlivců za použití dostupných spolehlivých technik anonymizace za předpokladu, že jsou řádně a účinně prováděny.

23 Vzhledem ke složitosti procesů anonymizace se také důrazně doporučuje transparentnost týkající se metodiky v oblasti anonymizace.

[9] (de Montjoye et al., 2018) „On the privacy-conscientious use of mobile phone data“.
[10] (de Montjoye et al., 2013) „Unique in the Crowd: The privacy bounds of human mobility“ a (Pyrgelis et al., 2017) „Knock Knock, Who's There? Membership Inference on Aggregate Location Data“.

3 APLIKACE PRO VYSLEDOVÁNÍ KONTAKTŮ

3.1 Obecná právní analýza

24 Systematické a rozsáhlé sledování polohy fyzických osob a/nebo kontaktů mezi nimi je závažným zásahem do jejich soukromí. Může být legitimizováno jedině na základě dobrovolného přijetí uživateli pro jednotlivé příslušné účely. To by znamenalo zejména to, že jednotlivci, kteří se rozhodnou tyto aplikace nepoužívat nebo je používat nemohou, by neměli být nijak znevýhodněni.

25 Aby byla zajištěna odpovědnost, měl by být jasně stanoven správce každé aplikace pro vysledování kontaktů. EDPB se domnívá, že správci[11] této aplikace by mohly být vnitrostátní zdravotnické orgány, přičemž je možné počítat i s dalšími správci. Pokud však zavedení aplikací pro vysledování kontaktů zahrnuje různé subjekty, jejich úlohy a povinnosti je třeba hned na začátku jasně stanovit a vysvětlit uživatelům.

26 Navíc, co se týče zásady účelového omezení, musí být účely dostatečně konkrétní, aby vylučovaly další zpracování pro účely nesouvisející s řešením zdravotní krize způsobené onemocněním COVID-19 (např. obchodní účely nebo účely vymáhání práva). Jakmile bude cíl jasně vymezen, bude nutné zajistit, aby používání osobních údajů bylo vhodné, nezbytné a přiměřené.

27 V souvislosti s aplikací pro vysledování kontaktů je třeba pečlivě zvážit zásadu minimalizace údajů a záměrnou a standardní ochranu osobních údajů:

- aplikace pro vysledování kontaktů nevyžadují sledování polohy jednotlivých uživatelů. Místo toho by měly být využívány údaje o vzájemném přiblížení,
- vzhledem k tomu, že aplikace pro vysledování kontaktů mohou fungovat bez přímé identifikace jednotlivců, měla by být zavedena vhodná opatření, která zabrání opětovné identifikaci,
- shromážděné informace by se měly nacházet v koncovém zařízení uživatele a shromažďovány by měly být pouze relevantní informace, když je to naprosto nezbytné.

28 Pokud jde o zákonnost zpracování, EDPB konstatuje, že aplikace pro vysledování kontaktů zahrnují ukládání informací a/nebo přístup k informacím již uloženým v koncovém zařízení, na něž se vztahuje čl. 5 odst. 3 směrnice. Pokud jsou tyto operace nezbytně nutné, aby poskytovatel aplikace mohl poskytovat službu výslovně vyžádanou uživatelem, ke zpracování není potřeba souhlas dotyčné osoby. U operací, které nejsou nezbytně nutné, si musí poskytovatel souhlas uživatele vyžádat.

29 Kromě toho EDPB poznamenává, že pouhá skutečnost, že se používání aplikací pro vysledování kontaktů uskutečňuje na dobrovolné bázi, neznamená, že zpracování osobních údajů bude nutně založeno na souhlasu. Pokud orgány veřejné moci poskytují službu na základě zmocnění, které jim bylo svěřeno právními předpisy a v souladu s požadavky uloženými právními předpisy, je zřejmé, že nejrelevantnějším právním základem pro zpracování je nezbytnost plnění úkolu ve veřejném zájmu, tj. čl. 6 odst. 1 písm. e) nařízení GDPR.

30 Čl. 6 odst. 3 nařízení GDPR objasňuje, že základ pro zpracování podle čl. 6 odst. 1 písm. e) musí být stanoven právem Unie nebo členského státu, které se na správce vztahuje. Účel zpracování musí být určen v uvedeném právním základu, nebo pokud jde o zpracování podle odst. 1 písm. e), musí být toto zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce[12].

[11] Viz také dokument Evropské komise nazvaný „Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů“, Brusel, 16.4.2020, C(2020) 2523 final.
[12] Viz 41. bod odůvodnění.

31 Právní základ nebo legislativní opatření poskytující zákonný základ pro používání aplikací pro vysledování kontaktů by však měly začleňovat smysluplná ochranná opatření, včetně odkazu na dobrovolnou povahu aplikace. Je třeba zahrnout jasné stanovení účelu a výslovná omezení týkající se dalšího využívání osobních údajů, jakož i jasné určení zapojeného správce / zapojených správců. Dále je třeba určit kategorie údajů a rovněž subjekty, kterým (a účely, pro něž) je možné osobní údaje zpřístupnit. Podle úrovně zásahu by měla být začleněna dodatečná ochranná opatření s ohledem na povahu, rozsah a účely zpracování. A na závěr EDPB také doporučuje zahrnout co nejdříve kritéria k určení toho, kdy bude aplikace odstraněna a který subjekt bude za toto rozhodnutí odpovědný.

32 Pokud však zpracování údajů vychází z jiného právního základu, jako je například souhlas (čl. 6 odst. 1 písm. a))[13], správce bude muset zajistit splnění přísných požadavků, aby byl tento právní základ platný.

33 Používání aplikace pro boj s pandemií COVID-19 navíc může vést ke shromažďování údajů o zdravotním stavu (například o stavu nakažené osoby). Zpracování těchto údajů je povoleno, pokud je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví při splnění podmínek čl. 9 odst. 2 písm. i) nařízení GDPR[14] nebo pro účely zdravotní péče uvedené v čl. 9 odst. 2 písm. h) nařízení GDPR[15]. V závislosti na právním základě by mohlo být založeno rovněž na výslovném souhlasu (čl. 9 odst. 2 písm. a) nařízení GDPR).

34 V souladu s prvotním účelem čl. 9 odst. 2 písm. j) nařízení GDPR rovněž umožňuje zpracování údajů o zdravotním stavu, je-li to nezbytné pro účely vědeckého výzkumu nebo statistické účely.

35 Současná zdravotní krize by neměla být využívána jako příležitost ke stanovování mandátů k nepřiměřenému uchovávání údajů. Omezení uložení by mělo zohlednit skutečné potřeby a relevantnost pro zdravotní účely (to může zahrnovat úvahy motivované z hlediska epidemiologie, jako je inkubační doba atd.) a osobní údaje by měly být uchovávány pouze po dobu trvání krize COVID-19. Poté by měly být v zásadě všechny osobní údaje vymazány nebo anonymizovány.

36 EDPB má za to, že tyto aplikace nemohou nahradit manuální vysledování kontaktů prováděné kvalifikovaným zdravotnickým personálem, který může rozhodnout, zda je pravděpodobné, že blízké kontakty budou mít za následek přenos viru, nebo nikoliv (např. při interakci s někým, kdo je chráněn vhodným vybavením – pokladní atd. – nebo ne), nýbrž toto vysledování mohou pouze podpořit. EDPB zdůrazňuje, že postupy a procesy, jež zahrnují příslušné algoritmy uplatňované aplikacemi pro vysledování kontaktů, by měly fungovat za přísného dohledu kvalifikovaných pracovníků, aby se omezil výskyt jakýchkoli falešně pozitivních a negativních výsledků. Zejména úkol spočívající v poskytování poradenství ohledně dalších kroků by neměl být založen pouze na automatizovaném zpracování.

37 Aby byla zajištěna jejich spravedlnost, odpovědnost a obecněji i jejich soulad s právními předpisy, musí být algoritmy kontrolovatelné a měly by být pravidelně přezkoumávány nezávislými odborníky. Zdrojový kód aplikace by měl být veřejně dostupný pro nejširší možnou kontrolu.

38 Vždy se budou do určité míry objevovat falešně pozitivní výsledky. Vzhledem k tomu, že zjištění rizika nákazy pravděpodobně může mít značný dopad na jednotlivce, jako je například setrvání v samoizolaci, dokud nebude test negativní, je nutná možnost opravy údajů a/nebo výsledků následné analýzy. To by se samozřejmě mělo týkat pouze scénářů a realizací, v rámci kterých

[13] Správci (zejména orgány veřejné moci) musí věnovat zvláštní pozornost skutečnosti, že souhlas by neměl být považován za svobodný, pokud jednotlivec nemá skutečnou možnost souhlas odmítnout nebo odvolat, aniž by byl poškozen.

[14] Zpracování musí být založeno na právu Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství.

[15] Viz čl. 9 odst. 2 písm. h) nařízení GDPR.

jsou údaje zpracovávány a/nebo uchovávány způsobem, při němž je tato oprava technicky proveditelná a kdy je pravděpodobné, že dojde k nepříznivým účinkům uvedeným výše.

39 EDPB se taktéž domnívá, že před zavedením takového nástroje musí být provedeno posouzení vlivu na ochranu osobních údajů, jelikož dané zpracování se považuje za pravděpodobně vysoce rizikové (údaje o zdravotním stavu, předpokládané rozsáhlé přijetí, systematické sledování, použití nového technologického řešení)[16]. EDPB důrazně doporučuje, aby byla posouzení vlivu na ochranu osobních údajů zveřejňována.

3.2 Doporučení a požadavky na fungování

40 V souladu se zásadou minimalizace údajů by, mimo jiná opatření záměrné a standardní ochrany osobních údajů[17], měly být zpracované údaje omezeny na nezbytné minimum. Aplikace by neměla shromažďovat nesouvisející nebo nepotřebné informace, mezi něž může patřit osobní stav, komunikační identifikátory, položky v adresáři zařízení, zprávy, záznamy hovorů, lokalizační údaje, identifikátory zařízení atd.

41 Údaje vysílané pomocí aplikací musí zahrnovat pouze některé jedinečné a pseudonymní identifikátory, které byly aplikací vygenerovány a jsou pro ni specifické. Tyto identifikátory musí být pravidelně obnovovány, s četností slučitelnou s účelem zastavení šíření viru a dostatečnou pro omezení rizika identifikace a fyzického sledování jednotlivců.

42 Implementace pro vysledování kontaktů se mohou zakládat na centralizovaném nebo decentralizovaném přístupu[18]. Obě možnosti by měly být považovány za použitelné, pokud jsou zavedena náležitá bezpečnostní opatření, přičemž s každou se pojí řada výhod i nevýhod. Koncepční fáze vývoje aplikací by tudíž měla vždy zahrnovat důkladné posouzení obou koncepcí při pečlivém zvážení příslušných účinků na ochranu údajů / soukromí a možných dopadů na práva jednotlivců.

43 Každý server zapojený do systému pro vysledování kontaktů smí shromažďovat pouze historii kontaktů nebo pseudonymní identifikátory uživatele, u nějž byla diagnostikována nákaza v důsledku řádného posouzení provedeného zdravotnickými orgány a dobrovolného jednání uživatele. Popřípadě musí server uchovávat seznam pseudonymních identifikátorů nakažených uživatelů nebo jejich historie kontaktů pouze po dobu potřebnou k informování potenciálně nakažených uživatelů o jejich expozici a neměl by se pokoušet potenciálně nakažené uživatele identifikovat.

44 Zavádění metodiky pro globální vysledování kontaktů, včetně aplikací i manuálního sledování, může v některých případech vyžadovat zpracování dalších informací. V této souvislosti by tyto další informace měly zůstat v koncovém zařízení uživatele a měly by být zpracovány pouze v nezbytně nutných případech a s předchozím a zvláštním souhlasem uživatele.

45 Musí být uplatňovány nejmodernější šifrovací techniky, které ochrání údaje uložené na serverech a v aplikacích a výměny mezi aplikacemi a vzdáleným serverem. Rovněž musí být provedena vzájemná autentizace mezi aplikací a serverem.

46 Nahlašování uživatelů v aplikaci jako nakažených virem SARS-CoV-2 musí podléhat řádnému ověření, například prostřednictvím kódu na jedno použití vázaného na pseudonymní totožnost nakažené osoby a propojeného s testovací stanicí nebo zdravotnickým pracovníkem. Pokud nemůže být potvrzení získáno bezpečným způsobem, nemělo by dojít k žádnému zpracování údajů, které předpokládá platnost stavu uživatele.

---

[16] Viz pracovní skupina zřízená podle článku 29 – Pokyny (přijaté EDPB) pro posouzení vlivu na ochranu osobních údajů a stanovení, zda je „pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679.

[17] Viz Pokyny EDPB 4/2019 týkající se článku 25 Záměrná a standardní ochrana osobních údajů.

[18] Obecně je decentralizované řešení více v souladu se zásadou minimalizace.

47 Správce musí ve spolupráci s orgány veřejné moci jasně a explicitně informovat o odkazu ke stažení oficiální vnitrostátní aplikace pro vysledování kontaktů, aby zmírnil riziko, že jednotlivci budou využívat aplikace třetích stran.

4 ZÁVĚR

48 Svět čelí významné zdravotní krizi, která vyžaduje rázná řešení, jež budou mít dopad i nad rámec této mimořádné situace. Automatizované zpracování údajů a digitální technologie mohou být klíčovými složkami v boji proti onemocnění COVID-19. Je však třeba si dávat pozor na „dominový efekt“. Je naší povinností zajistit, aby každé opatření přijaté za těchto mimořádných okolností bylo nezbytné a časově omezené, aby mělo minimální rozsah a aby podléhalo pravidelným a skutečným přezkumům, jakož i vědeckému hodnocení.

49 EDPB zdůrazňuje, že člověk by neměl být nucen vybírat si mezi účinnou odezvou na stávající krizi a ochranou našich základních práv: můžeme dosáhnout obojího, a zásady ochrany údajů navíc mohou sehrát velmi důležitou úlohu v boji proti viru. Evropské právní předpisy o ochraně údajů umožňují odpovědné používání osobních údajů pro účely řízení v oblasti zdraví, a současně také zajišťují, aby v tomto procesu nebyly ohroženy práva a svobody jednotlivců.

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)

PŘÍLOHA – APLIKACE PRO VYSLEDOVÁNÍ KONTAKTŮ PŘÍRUČKA PRO ANALÝZU

0. Prohlášení o vyloučení odpovědnosti

Následující pokyny nejsou normativní ani vyčerpávající a jediným účelem této příručky je poskytnout obecné pokyny pro vývojáře a implementátory aplikací pro vysledování kontaktů. Mohou být použita i jiná řešení než ta, která jsou zde uvedena, a mohou být legitimní, pokud jsou v souladu s příslušným právním rámcem (tj. s nařízením GDPR a směrnicí).

Také je třeba poznamenat, že tato příručka má obecný charakter. Proto nelze doporučení a povinnosti obsažené v tomto dokumentu vnímat jako vyčerpávající. Jakékoli posouzení musí být prováděno na základě jednotlivých případů a konkrétní aplikace mohou vyžadovat další opatření, která v této příručce nejsou zahrnuta.

1. Shrnutí

Zúčastněné strany v mnoha členských státech zvažují používání aplikací pro *vysledování kontaktů*, aby pomohly obyvatelům zjistit, zda byli v kontaktu s osobou nakaženou virem SARS-CoV-2.

Podmínky, za kterých by tyto aplikace účinně přispěly ke zvládnutí pandemie, dosud nebyly stanoveny. A tyto podmínky by bylo třeba stanovit ještě před zavedením dané aplikace. Přesto je vhodné stanovit pokyny, které budou od začátku přinášet příslušné informace vývojovým týmům, aby mohla být ochrana osobních údajů zaručena od rané fáze návrhu.

Je třeba poznamenat, že tato příručka má obecný charakter. Proto nelze doporučení a povinnosti obsažené v tomto dokumentu vnímat jako vyčerpávající. Jakékoli posouzení musí být prováděno na základě jednotlivých případů a konkrétní aplikace mohou vyžadovat další opatření, která v této příručce nejsou zahrnuta. Účelem této příručky je poskytnout obecné pokyny pro vývojáře a implementátory aplikací pro vysledování kontaktů.

Některá kritéria mohou překročit přísné požadavky vyplývající z rámce pro ochranu údajů. Jejich cílem je zajistit co nejvyšší úroveň transparentnosti za účelem podpory společenského přijetí těchto aplikací pro vysledování kontaktů.

Za tímto účelem by vydavatelé aplikací pro vysledování kontaktů měli zohlednit tato kritéria:

- Používání této aplikace musí být zcela dobrovolné. Nesmí podmiňovat přístup k jakýmkoli právům zaručeným podle práva. Jednotlivci musí mít neustále plnou kontrolu nad svými údaji a měli by mít možnost se o využívání této aplikace svobodně se rozhodnout.
- Je pravděpodobné, že aplikace pro vysledování kontaktů budou mít za následek vysoké riziko pro práva a svobody fyzických osob a bude třeba, aby bylo před jejich zavedením provedeno posouzení vlivu na ochranu osobních údajů.
- Informace o vzájemném přiblížení mezi uživateli aplikace lze získat i bez jejich lokalizace. Tento druh aplikace nevyžaduje – a neměl by tedy zahrnovat – používání lokalizačních údajů.
- Pokud je u uživatele diagnostikována nákaza virem SARS-CoV-2, měly by být informovány pouze ty osoby, s nimiž byl tento uživatel v blízkém kontaktu během epidemiologicky relevantní doby uchovávání údajů pro vysledování kontaktů.

- Provoz tohoto typu aplikace by mohl v závislosti na zvolené architektuře vyžadovat použití centralizovaného serveru. V tomto případě a v souladu se zásadami minimalizace údajů a záměrné ochrany osobních údajů by měly být údaje zpracovávané centralizovaným serverem omezeny na nezbytné minimum:
    - Pokud je uživatel diagnostikován jako nakažený, mohou být informace týkající se jeho předchozích blízkých kontaktů nebo identifikátorů vysílaných prostřednictvím aplikace uživatele shromážděny pouze s jeho souhlasem. Je třeba zavést ověřovací metodu, která umožní potvrdit, že je osoba skutečně nakažená, aniž by byl uživatel identifikován. Technicky toho lze dosáhnout tak, že kontakty budou upozorněny až po zásahu zdravotníka, například za použití zvláštního jednorázového kódu.
    - Informace uložené v centrálním serveru by neměly umožnit, aby správce mohl identifikovat uživatele, u nichž byla diagnostikována nákaza nebo kteří byli s těmito uživateli v kontaktu, ani by neměly umožnit vyvození vzorců kontaktů, které nejsou k určení relevantních kontaktů zapotřebí.
- Provoz tohoto typu aplikace vyžaduje vysílání údajů, které jsou čteny zařízeními jiných uživatelů, a poslech těchto vysílání:
    - Stačí výměna pseudonymních identifikátorů mezi mobilními zařízeními uživatelů (počítače, tablety, propojené hodinky atd.), kupříkladu jejich vysíláním (např. prostřednictvím technologie Bluetooth Low Energy).
    - Identifikátory musí být vytvářeny pomocí nejmodernějších šifrovacích postupů.
    - Identifikátory musí být pravidelně obnovovány, aby se snížilo riziko fyzického sledování a útoků spočívajících v propojení údajů.
- Je třeba zajistit, aby tento typ aplikace zaručoval bezpečné technické postupy. Zejména platí následující:
    - Aplikace by neměla uživatelům sdělovat informace, které jim umožní odvodit totožnost nebo diagnózu jiných osob. Centrální server nesmí uživatele identifikovat ani o nich vyvozovat informace.

Prohlášení o vyloučení odpovědnosti: výše uvedené zásady souvisejí jen a pouze s uváděným účelem aplikací pro *vysledování kontaktů*, jejichž jediným cílem je automaticky informovat osoby potenciálně vystavené viru (aniž by byly identifikovány). Provozovatelé této aplikace a její infrastruktury mohou být kontrolováni příslušným dozorovým úřadem. Dodržování všech nebo části těchto pokynů nemusí nutně postačovat k zajištění plného souladu s rámcem pro ochranu údajů.

2. Definice

Kontakt	V případě aplikace pro vysledování kontaktů se kontaktem rozumí uživatel, který se účastnil interakce s uživatelem, u něhož se potvrdilo, že je přenašečem viru, přičemž délka a vzdálenost této interakce představují riziko významné expozice vůči virové nákaze. Parametry pro délku expozice a vzdálenost mezi lidmi musí odhadnout zdravotnické orgány a lze je nastavit v aplikaci.

Lokalizační údaje	Tento pojem se vztahuje na všechny údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací (podle definice uvedené ve směrnici), jakož i na údaje z potenciálních jiných zdrojů, které se týkají: • zeměpisné šířky, zeměpisné délky či nadmořské výšky koncového zařízení, • směru cesty uživatele nebo • času, kdy byly informace o poloze zaznamenány.
Interakce	V souvislosti s aplikací pro vysledování kontaktů je interakce definována jako výměna informací mezi dvěma zařízeními, která se nacházejí ve vzájemné bezprostřední blízkosti (v prostoru a čase), v dosahu používané komunikační technologie (např. Bluetooth). Tato definice nezahrnuje polohu obou uživatelů, kteří se interakce účastní.
Přenašeč viru	V tomto dokumentu považujeme za přenašeče viru uživatele, kteří byli na virus pozitivně testováni a kteří obdrželi oficiální diagnózu od lékaře nebo zdravotnického zařízení.
Vysledování kontaktů	U lidí, kteří byli v blízkém kontaktu (podle kritérií stanovených epidemiology) s jedincem nakaženým virem, existuje značné riziko, že byli rovněž nakaženi a že následně nakazí další osoby. Vysledování kontaktů je metodika pro tlumení nákaz, která vytváří seznam všech lidí, kteří se nacházeli v bezprostřední blízkosti přenašeče viru, aby bylo možné zkontrolovat, zda jim hrozí nákaza, a přijmout ve vztahu k nim vhodná hygienická opatření.

3. Obecné informace

GEN-1	Aplikace musí být doplňujícím nástrojem k tradičním technikám pro vysledování kontaktů (jako jsou zejména rozhovory s nakaženými osobami), tzn. že musí být součástí širšího programu v oblasti veřejného zdraví. Může být používána pouze do doby, kdy budou techniky manuálního vysledování kontaktů schopny samy zvládnout objem nových případů nákazy.
GEN-2	Nejpozději v okamžiku, kdy příslušné orgány veřejné moci rozhodnou o „návratu k normálu“, musí být zaveden postup k zastavení shromažďování identifikátorů (globální deaktivace aplikace, pokyny k odinstalování aplikace, automatické odinstalování atd.) a k aktivaci vymazání všech shromážděných údajů ze všech databází (mobilních aplikací a serverů).
GEN-3	Zdrojový kód aplikace a jejího backendu musí být otevřený a technické specifikace je třeba zveřejnit, aby mohla kterákoli z dotčených stran tento kód

	kontrolovat a v příslušných případech přispívat k jeho zlepšení, k opravě možných chyb a k zajištění transparentnosti při zpracování osobních údajů.
GEN-4	Fáze zavedení aplikace musí umožňovat postupné osvědčení její účinnosti z hlediska veřejného zdraví. Za tímto účelem je třeba předem definovat hodnotící protokol, který stanoví ukazatele umožňující měření účinnosti aplikace.

4. Účely

PUR-1	Aplikace musí sloužit pouze účelu vysledování kontaktů, aby lidé potenciálně vystavení viru SARS-CoV-2 mohli být upozorněni a aby o ně bylo postaráno. Nesmí být používána za jiným účelem.
PUR-2	Aplikace se nesmí odchýlit od svého primárního použití za účelem sledování souladu s karanténními opatřeními či opatřeními omezujícími volný pohyb osob a/nebo s omezením fyzického kontaktu.
PUR-3	Aplikace nesmí být používána k vyvozování závěrů o poloze uživatelů na základě jejich interakce a/nebo pomocí jakýchkoli jiných prostředků.

5. Funkční aspekty

FUNC-1	Aplikace musí poskytovat funkce, které uživatelům umožní, aby byli informováni v případě potenciálního vystavení viru, přičemž tyto informace musí být založeny na přiblížení k nakaženému uživateli v rozmezí X dní před pozitivním screeningovým testem (kde je hodnota X stanovena zdravotnickými orgány).
FUNC-2	Aplikace by měla poskytovat doporučení uživatelům, u nichž bylo určeno, že mohli být vystaveni viru. Měla by předávat pokyny týkající se opatření, jimiž by se tito uživatelé měli řídit, a tyto pokyny by měly uživateli umožňovat žádat o rady. V těchto případech by byl povinný lidský zásah.
FUNC-3	Algoritmus, který měří riziko nákazy na základě faktorů vzdálenosti a času, a určuje tak, kdy je třeba kontakt zaznamenat na seznam pro vysledování kontaktů, musí být bezpečně laditelný, aby mohl zohlednit nejnovější poznatky o šíření viru.
FUNC-4	**Uživatelé musí být informováni v případě, že byli vystaveni viru**, nebo musí pravidelně dostávat informace o tom, zda byli nebo nebyli vystaveni viru, v průběhu inkubační doby viru.
FUNC-5	Aplikace by měla být interoperabilní s dalšími aplikacemi, jež byly vyvinuty v různých členských státech, aby mohli být uživatelé cestující mezi jednotlivými členskými státy efektivně informováni.

6. Údaje

DATA-1	Aplikace musí být schopna vysílat a přijímat údaje prostřednictvím technologií pro komunikaci na krátkou vzdálenost, jako je Bluetooth Low Energy, aby mohlo být prováděno vysledování kontaktů.
DATA-2	Tyto vysílané údaje musí zahrnovat kryptograficky silné pseudonáhodné identifikátory, které byly aplikací vygenerovány a jsou pro ni specifické.
DATA-3	Riziko kolize mezi pseudonáhodnými identifikátory by mělo být dostatečně nízké.
DATA-4	Pseudonáhodné identifikátory musí být pravidelně obnovovány, s četností dostatečnou pro omezení rizika opětovné identifikace, fyzického sledování nebo propojení jednotlivců ze strany kohokoli, včetně provozovatelů centrálního serveru, dalších uživatelů aplikace nebo třetích stran vedených zlými úmysly. Tyto identifikátory musí být vygenerovány aplikací uživatele, případně na základě inicializační hodnoty (*seed*) poskytnuté centrálním serverem.
DATA-5	V souladu se zásadou minimalizace údajů nesmí aplikace shromažďovat jiné údaje než ty, které jsou nezbytně nutné pro účely vysledování kontaktů.
DATA-6	Aplikace nesmí pro účely vysledování kontaktů shromažďovat lokalizační údaje. Lokalizační údaje mohou být zpracovávány pouze za jediným účelem, a to aby aplikaci umožnily interagovat s podobnými aplikacemi v jiných zemích, a jejich přesnost by měla být omezena na to, co je nezbytně nutné pro tento výhradní účel.
DATA-7	Aplikace by neměla shromažďovat údaje o zdravotním stavu kromě těch, které jsou nezbytně nutné pro účely aplikace, nebo jen na nepovinné bázi a výhradně za účelem pomoci při rozhodovacím procesu týkajícím se informování uživatele.
DATA-8	Uživatelé musí být informováni o všech osobních údajích, které budou shromažďovány. Tyto údaje by měly být shromažďovány pouze se svolením uživatele.

7. Technické vlastnosti

TECH-1	Aplikace by měla využívat dostupné technologie, jako je technologie pro komunikaci na krátkou vzdálenost (např. Bluetooth Low Energy), aby detekovala uživatele v blízkosti zařízení, na němž je aplikace spuštěna.
TECH-2	Aplikace by měla uchovávat historii kontaktů uživatele v zařízení po předem stanovené omezené časové období.
TECH-3	Aplikace se může opírat o centrální server za účelem provádění některých ze svých funkcí.

TECH-4	Aplikace musí být založena na architektuře, která se v co nejvyšší možné míře opírá o zařízení uživatelů.
TECH-5	Z podnětu uživatelů, u nichž byla hlášena nákaza virem, a po potvrzení jejich stavu náležitě certifikovaným zdravotníkem by jejich historie kontaktů nebo jejich vlastní identifikátory měly být předány na centrální server.

8. Bezpečnost

SEC-1	Nějaký mechanismus musí ověřit stav uživatelů, kteří se v aplikaci nahlásí jako pozitivní na virus SARS-CoV-2, například poskytnutím kódu na jedno použití propojeného s testovací stanicí nebo zdravotnickým pracovníkem. Pokud nelze potvrzení získat bezpečným způsobem, údaje nesmí být zpracovány.
SEC-2	Údaje odesílané na centrální server musí být předávány zabezpečeným kanálem. Používání oznamovacích služeb poskytovaných poskytovateli platforem operačních systémů by mělo být pečlivě posouzeno a nemělo by vést ke sdělování jakýchkoli údajů třetím stranám.
SEC-3	Požadavky nesmí být zranitelné vůči manipulaci ze strany uživatele vedeného zlými úmysly.
SEC-4	Je třeba uplatnit nejmodernější šifrovací techniky za účelem zabezpečení výměn mezi aplikací a serverem a mezi jednotlivými aplikacemi a obecně za účelem ochrany informací uložených v aplikacích a na serveru. Mezi techniky, které mohou být použity, patří například tyto: symetrické a asymetrické šifrování, hašovací funkce, *private membership test* (test přítomnosti prvku v množině bez jeho vyzrazení), *private set intersection* (určení průniku množin bez jejich vyzrazení), Bloomovy filtry, *private information retrieval* (zjištění informace bez vyzrazení, o jakou informaci šlo), homomorfní šifrování atd.
SEC-5	Centrální server nesmí uchovávat identifikátory síťového připojení (např. IP adresy) jakýchkoli uživatelů včetně těch, kteří byli pozitivně diagnostikováni a kteří předali svou historii kontaktů nebo své vlastní identifikátory.
SEC-6	Aby se zabránilo možnosti vydávat se za jiné uživatele nebo vytvářet nepravé identity uživatelů, server musí ověřit pravost aplikace.
SEC-7	Aplikace musí ověřit pravost centrálního serveru.
SEC-8	Funkce serveru by měly být chráněny před útoky přehráním.
SEC-9	Informace předávané centrálním serverem musí být podepsány, aby bylo možné ověřit jejich původ a integritu.
SEC-10	Přístup k veškerým údajům, které jsou uloženy v centrálním serveru a nejsou veřejně dostupné, musí být omezen pouze na oprávněné osoby.
SEC-11	Správce oprávnění daného zařízení na úrovni operačního systému smí žádat pouze o oprávnění nezbytná pro přístup ke komunikačním modulům a v případech potřeby pro jejich použití, pro ukládání údajů v koncovém zařízení a pro výměnu informací s centrálním serverem.

9. Ochrana osobních údajů a soukromí fyzických osob

Upozornění: následující pokyny se týkají aplikace, jejímž jediným účelem je vysledování kontaktů.

PRIV-1	Výměny údajů musí respektovat soukromí uživatelů (a zejména dodržovat zásadu minimalizace údajů).
PRIV-2	Aplikace nesmí umožnit, aby byli uživatelé přímo identifikováni, když aplikaci používají.
PRIV-3	Aplikace nesmí umožnit sledování pohybu uživatelů.
PRIV-4	Používání aplikace by nemělo uživatelům umožnit, aby se dozvěděli něco o jiných uživatelích (a zejména to, zda jsou přenašeči viru či nikoliv).
PRIV-5	Důvěra v centrální server musí být omezená. Řízení centrálního serveru se musí držet jasně stanovených pravidel správy a musí zahrnovat všechna nezbytná opatření pro zajištění jeho bezpečnosti. Lokalizace centrálního serveru by měla umožnit účinný dohled ze strany příslušného dozorového úřadu.
PRIV-6	Musí být provedeno posouzení vlivu na ochranu osobních údajů a mělo by být zveřejněno.
PRIV-7	Aplikace by měla uživateli odhalit pouze to, zda byl vystaven viru, a – pokud možno bez odhalení informací o jiných uživatelích – počet případů a data expozice.
PRIV-8	Informace poskytnuté aplikací nesmí umožnit uživatelům, aby identifikovali uživatele, kteří jsou přenašeči viru, ani jejich pohyb.
PRIV-9	Informace poskytnuté aplikací nesmí umožnit zdravotnickým orgánům, aby identifikovaly potenciálně vystavené uživatele bez jejich souhlasu.
PRIV-10	Požadavky, které aplikace odešle na centrální server, nesmí odhalit žádné informace o přenašeči viru.
PRIV-11	Požadavky, které aplikace odešle na centrální server, nesmí odhalit žádné nepotřebné informace o uživateli, možná s výjimkou (a pouze pokud je to nezbytné) jeho pseudonymních identifikátorů a jeho seznamu kontaktů.
PRIV-12	Nesmí být možné útoky spočívající v propojení údajů.
PRIV-13	Uživatelé musí být schopni uplatňovat svá práva prostřednictvím aplikace.
PRIV-14	Odstranění aplikace musí vést k vymazání všech lokálně shromážděných údajů.
PRIV-15	Aplikace by měla shromažďovat pouze údaje přenášené prostřednictvím dané aplikace nebo interoperabilních rovnocenných aplikací. Neshromažďují se žádné údaje související s jinými aplikacemi a/nebo zařízeními pro komunikaci na krátkou vzdálenost.
PRIV-16	Aby se zabránilo opětovné identifikaci ze strany centrálního serveru, je třeba zavést proxy servery. Účelem těchto *nekoluzivních serverů* je smíchat identifikátory několika uživatelů (identifikátory přenašečů viru i identifikátory odeslané žadateli) předtím, než budou sdíleny s centrálním serverem, aby se centrální server nemohl identifikátory (jako například IP adresy) uživatelů dozvědět.

PRIV-17	Aplikace a server vyžadují pečlivý vývoj a konfiguraci, aby neshromažďovaly nepotřebné údaje (např. záznamy ze serverů by neměly obsahovat žádné identifikátory apod.) a aby se zabránilo používání jakékoli sady SDK třetí strany, která shromažďuje údaje pro jiné účely.

Je-li uživatel prohlášen za nakaženého, většina aplikací pro vysledování kontaktů, o kterých se v současné době diskutuje, se řídí v podstatě dvěma přístupy: buď mohou odeslat na server historii blízkých kontaktů, kterou obdržely prostřednictvím skenování, nebo mohou odeslat seznam svých vlastních vyslaných identifikátorů. Následující zásady jsou uvedeny na základě těchto dvou přístupů. Ačkoli jsou zde tyto přístupy probírány, neznamená to, že by jiné přístupy nebyly možné nebo dokonce vhodnější – například přístupy, které uplatňují určitou formu šifrování E2E nebo používají jiné technologie zvyšující bezpečnost nebo ochranu soukromí.

9.1. Zásady, které se uplatňují pouze tehdy, **pokud aplikace odesílá na server seznam kontaktů:**

CON-1	Centrální server musí shromažďovat historii kontaktů uživatelů nahlášených jako pozitivní na virus SARS-CoV-2 v důsledku jejich dobrovolného jednání.
CON-2	Centrální server nesmí uchovávat ani rozesílat seznam pseudonymních identifikátorů uživatelů, kteří jsou přenašeči viru.
CON-3	Historie kontaktů uložená na centrálním serveru musí být vymazána, jakmile jsou uživatelé upozorněni na to, že se přiblížili k osobě, která byla pozitivně diagnostikována.
CON-4	S výjimkou případů, kdy uživatel se zjištěnými pozitivními výsledky sdílí svou historii kontaktů s centrálním serverem nebo kdy uživatel odešle na server požadavek, aby zjistil své potenciální vystavení viru, nesmí žádné údaje opustit zařízení uživatele.
CON-5	Jakýkoli identifikátor zahrnutý v místní historii musí být vymazán po X dnech od jeho získání (hodnota X je stanovena zdravotnickými orgány).
CON-6	Historie kontaktů předložené různými uživateli by neměly být dále zpracovány, např. vzájemně korelovány za účelem vytvoření globálních map zaměřených na blízkost osob.
CON-7	Údaje v záznamech ze serverů musí být minimalizovány a musí být v souladu s požadavky na ochranu údajů.

9.2. Zásady, které se uplatňují pouze tehdy, pokud aplikace odesílá na server seznam svých vlastních identifikátorů:

ID-1	Centrální server musí shromažďovat identifikátory vysílané aplikací uživatelů nahlášených jako pozitivní na virus SARS-CoV-2 v důsledku jejich dobrovolného jednání.
ID-2	Centrální server nesmí uchovávat ani rozesílat historii kontaktů uživatelů, kteří jsou přenašeči viru.

ID-3	Identifikátory uložené v centrálním serveru musí být vymazány, jakmile byly rozeslány do ostatních aplikací.
ID-4	S výjimkou případů, kdy uživatel se zjištěnými pozitivními výsledky sdílí své identifikátory s centrálním serverem nebo kdy uživatel odešle na server požadavek, aby zjistil své potenciální vystavení viru, nesmí žádné údaje opustit zařízení uživatele.
ID-5	Údaje v záznamech ze serverů musí být minimalizovány a musí být v souladu s požadavky na ochranu údajů.