II

(Sdělení)

SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

EVROPSKÁ KOMISE

SDĚLENÍ KOMISE

Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů

(2020/C 124 I/01)

1 SOUVISLOSTI

Pandemie COVID-19 postavila Unii a členské státy, jejich systémy zdravotní péče, způsob života, hospodářskou stabilitu a hodnoty před nebývalou výzvu. Digitální technologie a data hrají v boji proti krizi COVID-19 významnou úlohu. Mobilní aplikace běžně nainstalované na chytrých telefonech mohou fungovat jako podpora pro zdravotnické orgány na vnitrostátní úrovni i na úrovni EU při monitorování a zvládání probíhající pandemie COVID-19 a jsou obzvláště důležité při uvolňování opatření k omezení šíření nákazy. Mohou občanům předávat přímé pokyny a podporovat vysledování kontaktů. Vnitrostátní či regionální orgány nebo vývojáři v řadě zemí (v EU i mimo ni) ohlásili spuštění aplikací s různými funkcemi zaměřenými na boj proti koronaviru.

Komise dne 8. dubna 2020 přijala doporučení o společné sadě nástrojů Unie pro využití technologií a dat k boji proti krizi COVID-19 a ukončování souvisejících mimořádných opatření, zejména pokud jde o mobilní aplikace a využívání anonymizovaných dat o mobilitě (dále jen „doporučení“) ([1]). Účelem uvedeného doporučení je mimo jiné vytvořit společný evropský přístup (sadu nástrojů) pro používání mobilních aplikací koordinovaný na úrovni EU s cílem posílit postavení občanů, pokud jde o přijímání opatření k omezení fyzického kontaktu, a pro varování, prevenci a vysledování kontaktů s cílem pomoci omezit šíření onemocnění COVID-19. Doporučení stanoví obecné zásady, jimiž by se měl vývoj této sady nástrojů řídit, a uvádí, že Komise zveřejní další pokyny, včetně informací o dopadech používání aplikací v této oblasti na ochranu osobních údajů a soukromí.

Ve společném evropském plánu k odstranění opatření k zamezení šíření nákazy Komise ve spolupráci s předsedou Evropské rady stanovila řadu zásad, jimiž se má řídit postupné rušení opatření k zamezení šíření COVID-19. V této souvislosti mohou hrát mobilní aplikace, včetně funkcí sloužících k vysledování kontaktů, důležitou úlohu. Podle toho, jaké mají tyto aplikace funkce a jak široce jsou občany používané, mohou mít významný dopad na diagnózu onemocnění COVID-19, jeho léčbu a zvládání v nemocničním prostředí i mimo něj. Jsou obzvláště relevantní ve fázi, kdy jsou opatření k omezení šíření viru rušena a kdy riziko nákazy roste spolu s tím, jak roste počet kontaktů mezi lidmi. Tyto aplikace mohou pomoci přerušit mechanismy nákazy rychleji a účinněji než obecná omezující opatření a mohou tak snížit riziko významného rozšíření viru. Měly by tedy být důležitým prvkem strategie pro ukončování mimořádných opatření a doplňovat jiná opatření, jako například zvýšené kapacity pro testování ([2]). Nezbytným předpokladem pro vývoj těchto aplikací, jejich akceptování a využívání občany, je důvěra. Lidé musí mít jistotu, že jejich základní práva jsou dodržována a že aplikace budou používány pouze pro specificky definované účely. Tedy že nebudou sloužit k hromadnému sledování a že jednotlivci budou mít nadále nad svými údaji kontrolu. To je základem pro přesnost a účinnost takových aplikací při

([1]) Doporučení C(2020) 2296 final ze dne 8. dubna 2020. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

omezování šíření viru. Je proto zásadní najít řešení, která co nejméně narušují soukromí a která jsou plně v souladu s požadavky na ochranu osobních údajů a soukromí stanovenými v právu Unie. Kromě toho by tyto aplikace měly být deaktivovány nejpozději ve chvíli, kdy bude pandemie prohlášena za zvládnutou. Dále by zabezpečení informací v těchto aplikacích mělo zahrnovat nejmodernější ochranné prvky.

Tyto pokyny zohledňují příspěvek Evropského sboru pro ochranu osobních údajů (EDPB) ([3]) a diskuse v rámci sítě pro elektronické zdravotnictví. Sbor EDPB plánuje v nadcházejících dnech zveřejnit pokyny týkající se geolokalizace a dalších nástrojů sloužících k vysledovávání v souvislosti s pandemií COVID-19.

Oblast působnosti pokynů

V zájmu zajištění jednotného přístupu v celé EU a poskytnutí pokynů členským státům a vývojářům aplikací stanoví tento dokument prvky a požadavky, které by aplikace měly splňovat, aby bylo zajištěno dodržování právních předpisů EU v oblasti ochrany soukromí a osobních údajů, zejména obecného nařízení o ochraně osobních údajů (GDPR) ([4]) a směrnice o soukromí v elektronických komunikacích ([5]). Tyto pokyny se nezabývají žádnými dalšími podmínkami a ani omezeními, která mohou být součástí vnitrostátních právních předpisů členských států v oblasti zpracování údajů o zdravotním stavu.

Tyto pokyny nejsou právně závazné. Není jimi dotčena úloha Soudního dvora EU jako jediného orgánu, který může poskytnout závazný výklad práva EU.

Tyto pokyny se týkají pouze dobrovolných aplikací podporujících boj proti pandemii COVID-19 (aplikace dobrovolně stažené, instalované a používané jednotlivci), které mají jednu nebo několik z těchto funkcí:

— poskytují jednotlivcům přesné informace o pandemii COVID-19,

— poskytují dotazníky pro sebehodnocení a pokyny pro jednotlivce (funkce vyhodnocování příznaků) ([6]),

— upozorňují osoby, které se po určitou dobu nacházely v blízkosti nakažené osoby, s cílem poskytnout informace, zda podstoupit domácí karanténu a kde se nechat otestovat (funkce vysledování kontaktů a varování),

— poskytují komunikační fórum mezi pacienty v samoizolaci a lékaři, nebo v případě, kdy je zajišťováno poradenství ohledně další diagnostiky a léčby (větší využívání telemedicíny).

Podle směrnice o soukromí v elektronických komunikacích je povinné používání aplikace zahrnující práva na důvěrný charakter sdělení uvedený v článku 5 možné pouze prostřednictvím právního předpisu, který je nezbytný, vhodný a přiměřený k ochraně určitých specifických cílů. Vzhledem k vysoké míře narušení soukromí, kterou tento přístup obnáší, a k souvisejícím problémům, například pokud jde o zavedení vhodných záruk, je Komise toho názoru, že před použitím této možnosti je nutná pečlivá analýza. Z těchto důvodů Komise doporučuje používání aplikací na dobrovolné bázi.

Tyto pokyny se nevztahují na aplikace zaměřené na prosazování karanténních požadavků (včetně těch povinných).

2 PRISPEVEK APLIKACI K BOJI PROTI COVID-19

Funkce vyhodnocování příznaků je nástroj, který orgánům veřejného zdraví umožňuje poskytnout občanům pokyny pro testování na COVID-19, poskytovat informace o samoizolaci, o tom, jak zabránit přenosu viru na další osoby, a kdy vyhledat zdravotní péči. Může také doplňovat dozor v primární péči a poskytovat spolehlivější informace o míře přenosu COVID-19 v populaci.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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) (Úř. věst. L 119, 4.5.2016, s. 1).

([5]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

([6]) Pokud aplikace poskytují informace týkající se diagnostiky, prevence, monitorování, predikce nebo prognózy, mělo by se posoudit možné zařazení mezi zdravotnické prostředky podle regulačního rámce pro zdravotnické prostředky. Zmíněný rámec viz směrnice Rady 93/42/EHS ze dne 14. června 1993 o zdravotnických prostředcích (Úř. věst. L 169, 12.7.1993, s. 1) a nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích (Úř. věst. L 117, 5.5.2017, s. 1).

Funkce vysledování kontaktů a varování jsou nástroje k identifikaci osob, které byly v kontaktu s osobou nakaženou onemocněním COVID-19. Tyto nástroje mají uvedené osoby informovat o dalších vhodných krocích, jako je domácí karanténa, testování nebo poskytování poradenství ohledně dalšího postupu v případě příznaků. Tato funkce je proto užitečná jak pro jednotlivce, tak pro orgány veřejného zdraví. Může rovněž hrát důležitou úlohu při řízení opatření k omezení šíření nákazy v deeskalačních scénářích. Její dopad lze zvýšit pomocí strategie podporující širší testování osob vykazujících mírné příznaky.

Obě funkce mohou být rovněž důležitým zdrojem údajů pro orgány veřejného zdraví a usnadnit předávání těchto dat vnitrostátním epidemiologickým orgánům a Evropskému středisku pro prevenci a kontrolu nemocí (ECDC). Mohou napomoci pochopení vzorců přenosu a v kombinaci s výsledky testování k odhadu pozitivní prediktivní hodnoty respiračních příznaků v dané komunitě, a poskytnout tak informace o míře cirkulace viru.

Míra spolehlivosti odhadů přímo souvisí s množstvím a spolehlivostí předávaných dat.

Proto mohou funkce vyhodnocování příznaků i funkce vysledování kontaktů, v kombinaci s vhodnými strategiemi testování, poskytnout informace o míře cirkulace viru a pomoci vyhodnotit dopad opatření zaměřených na omezování fyzického kontaktu a izolaci. Jak je uvedeno v doporučení, v zájmu přeshraniční spolupráce a zajištění detekce kontaktu mezi uživateli různých aplikací (což je obzvláště důležité při přeshraničním pohybu občanů) by měla být zajištěna interoperabilita mezi IT řešeními různých členských států. Je-li nakažená osoba v kontaktu s uživatelem aplikace jiného členského státu, mělo by být přeshraniční předávání osobních údajů tohoto uživatele zdravotnickým orgánům jeho členského státu v nezbytně nutném rozsahu možné. Tato otázka se bude řešit v rámci souboru nástrojů oznámeného v doporučení. Interoperabilita by měla být zajištěna jak pomocí technických požadavků, tak i lepší komunikace a spolupráce mezi vnitrostátními zdravotnickými orgány. Jako model řízení pro aplikace sloužící k vysledování kontaktů během pandemie COVID-19 lze rovněž použít model zvláštní spolupráce ([7]).

3 PRVKY PRO DUVERYHODNE A ODPOVEDNE POUZIVANI APLIKACI

Funkce obsažené v uvedených aplikacích mohou mít různý dopad na širokou škálu práv zakotvených v Listině základních práv EU, jako je lidská důstojnost, respektování soukromého a rodinného života, ochrana osobních údajů, svoboda pohybu, nediskriminace, svoboda podnikání a svoboda shromažďování a sdružování. Zasahování do soukromí a práva na ochranu osobních údajů může být obzvláště významné vzhledem k tomu, že některé funkce jsou založeny na datově náročném modelu.

Cílem níže uvedených prvků je poskytnout pokyny, jak omezit narušování soukromí ze strany funkcí aplikací s cílem zajistit soulad s právními předpisy EU v oblasti ochrany osobních údajů a soukromí.

3.1 Vnitrostátní zdravotnické orgány (nebo subjekty plnící úkoly ve veřejném zájmu v oblasti zdraví) jako správce údajů

Určení toho, kdo rozhoduje o prostředcích a účelech a zpracování údajů (správce údajů), má zásadní význam pro stanovení toho, kdo je odpovědný za dodržování pravidel EU pro ochranu osobních údajů, a zejména toho: kdo by měl poskytovat informace osobám, které si aplikaci stáhnou, o tom, co se stane s jejich osobními údaji (které již existují nebo které budou vygenerovány prostřednictvím zařízení, jako je chytrý telefon, v němž se aplikace nainstaluje), jaká budou jejich práva, kdo bude odpovědný v případě porušení zabezpečení údajů atd.

Vzhledem k citlivosti dotčených osobních údajů a účelu zpracování údajů popsanému níže má Komise za to, že aplikace by měly být navrženy tak, aby správci byly vnitrostátní zdravotnické orgány (nebo subjekty plnící úkoly ve veřejném zájmu v oblasti zdraví) ([8]). Správci odpovídají za dodržování nařízení GDPR (zásada odpovědnosti). Rozsah takového přístupu by měl být omezen na základě zásad popsaných v oddíle 3.5 níže.

([7]) Tato spolupráce již funguje v rámci projektu MyHealth@EU, pokud jde o výměnu pacientských souhrnů a elektronické předpisy. Viz rovněž čl. 5 odst. 5 a 17. bod odůvodnění prováděcího rozhodnutí Komise 2019/1765.

([8]) Viz 45. bod odůvodnění nařízení GDPR.

To rovněž přispěje k větší důvěře mezi populací, a tím k akceptaci těchto aplikací (a souvisejících informačních systémů zachycujících mechanismus přenosu nákazy) a zajistí, aby plnily zamýšlený účel ochrany veřejného zdraví. Příslušné politiky, požadavky a kontroly by měly být sladěny a koordinovaně realizovány odpovědnými vnitrostátními zdravotnickými orgány.

3.2 **Zajištění toho, aby měly osoby své údaje stále pod kontrolou**

Určujícím faktorem pro to, aby osoby aplikacím důvěřovaly, je ukázat jim, že mají své osobní údaje stále pod kontrolou. Aby to bylo zajištěno, má Komise za to, že by měly být splněny zejména tyto podmínky:

— instalace aplikace na jejich zařízení by měla být dobrovolná a bez jakýchkoli negativních důsledků pro osoby, které se rozhodnou aplikaci nestáhnout/nepoužívat,

— různé funkce aplikace (např. funkce informační, vyhodnocování příznaků, vysledování kontaktů a varování) by neměly být spojeny, aby osoba mohla poskytnout souhlas pro každou funkci zvlášť. To by nemělo uživateli bránit v tom, aby různé funkce aplikace kombinoval, nabízí-li to poskytovatel jako možnost,

— pokud jsou využívána data o vzájemném přiblížení (data vygenerovaná výměnou signálů „Bluetooth Low Energy“ (BLE) mezi zařízeními v rámci epidemiologicky relevantní vzdálenosti a během epidemiologicky relevantní doby), měla by být ukládána v zařízení dané osoby. Jestliže tato data mají být sdílena se zdravotnickými orgány, měla by být sdílena až poté, co bude potvrzeno, že je dotčená osoba onemocněním COVID-19 nakažena, a za podmínky, že se tak rozhodne učinit,

— zdravotnické orgány by měly osobám poskytnout veškeré nezbytné informace týkající se zpracování jejich osobních údajů (v souladu s články 12 a 13 nařízení GDPR a článkem 5 směrnice o soukromí v elektronických komunikacích),

— osoba by měla mít možnost uplatňovat svá práva podle nařízení GDPR (zejména právo na přístup, opravu, výmaz). Případné omezení práv podle nařízení GDPR a směrnice o soukromí v elektronických komunikacích by mělo být v souladu s těmito akty a mělo by být nezbytné, přiměřené a stanovené v právních předpisech,

— aplikace by měly být deaktivovány nejpozději tehdy, až bude prohlášeno, že pandemie je pod kontrolou; deaktivace by neměla být závislá na odinstalování uživatelem.

3.3 **Právní základ pro zpracování údajů**

Instalace aplikací a ukládání informací v zařízení uživatele

Jak se uvádí výše, podle směrnice o soukromí v elektronických komunikacích (článku 5) je ukládání informací v zařízení uživatele nebo získávání přístupu k již uloženým informacím povoleno pouze tehdy, pokud i) uživatel poskytl souhlas, nebo ii) uložení a/nebo přístup jsou nezbytně nutné pro službu informační společnosti (např. aplikaci) výslovně vyžádanou (tj. nainstalovanou a aktivovanou) uživatelem.

Ukládání informací v zařízení osoby a získávání přístupu k informacím, které již jsou na tomto zařízení uloženy, je pro fungování aplikací obvykle nezbytné. Kromě toho funkce vysledování kontaktů a varování vyžaduje, aby byly v zařízení uživatele uloženy některé další informace (například krátkodobé, pravidelně se měnící alias ID uživatelů této funkce v blízkém okolí). Dále může tato funkce vyžadovat, aby (nakažený nebo pravděpodobně nakažený) uživatel odesílal data o vzájemném přiblížení. Takové odesílání dat není pro fungování aplikace jako takové nezbytné. Požadavky možnosti ii) zmíněné v předchozím odstavci nejsou splněny. Proto tedy pro relevantní aktivity zůstává nejvhodnějším základem souhlas (možnost i) výše). Tento souhlas by měl být „svobodný“, „konkrétní“, „výslovný“ a „informovaný“ ve smyslu nařízení GDPR. Měl by být vyjádřen jasným potvrzením ze strany dané osoby; to vylučuje tiché formy souhlasu (např. mlčení, neaktivitu) ([9]).

([9]) Viz pokyny Evropského sboru pro ochranu osobních údajů týkající se souhlasu: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Právní základ pro zpracování vnitrostátními zdravotnickými orgány – právo Unie nebo členských států

Vnitrostátní zdravotnické orgány obvykle zpracovávají osobní údaje, jestliže existuje právní povinnost stanovená v právu EU nebo členského státu, které takové zpracování stanoví a splňuje podmínky čl. 6 odst. 1 písm. c) a čl. 9 odst. 2 písm. i) nařízení GDPR, nebo jestliže je takové zpracování nezbytné pro splnění úkolu prováděného na podporu veřejného zájmu uznaného právem EU nebo členského státu ([10]).

Jakékoli vnitrostátní právo musí stanovit zvláštní a vhodná opatření na ochranu práv a svobod subjektů údajů. Obecně platí, že čím silnější je dopad na svobody osob, tím silnější odpovídající záruky by měly být v příslušném právu stanoveny.

V zásadě mohou být jako právní základ pro zpracovávání údajů osob použity právní předpisy EU a členských států, které již existovaly před rozšířením onemocnění COVID-19, a právní předpisy, jež členské státy přijímají konkrétně za účelem boje proti šíření epidemií, pokud jsou v těchto předpisech stanovena opatření umožňující monitorování epidemií a pokud splňují další požadavky stanovené v čl. 6 odst. 3 nařízení GDPR.

Vzhledem k povaze dotčených osobních údajů (zejména údajů o zdravotním stavu jako zvláštních kategorií osobních údajů), jakož i k okolnostem současné pandemie COVID-19 by použití práva jako právního základu přispělo k právní jistotě, neboť by se takto i) podrobně stanovilo zpracování konkrétních údajů o zdravotním stavu a jasně by se specifikovaly účely zpracování; ii) jasně určilo, kdo je správce, tj. subjekt zpracovávající údaje, a kdo vedle správce může mít k těmto údajům přístup; iii) vyloučila možnost zpracovávat tyto údaje pro jiné účely, než které jsou uvedeny v právních předpisech, a iv) stanovily zvláštní záruky. Aby se neoslabila veřejná užitečnost a akceptace těchto aplikací, měl by vnitrostátní normotvůrce věnovat zvláštní pozornost tomu, aby zvolené řešení bylo ve vztahu k občanům co možná nejinkluzivnější.

Zpracovávání údajů zdravotnickými orgány na základě právních předpisů nemění nic na skutečnosti, že osoby se stále mohou svobodně rozhodnout, zda si aplikaci nainstalují, nebo ne a zda budou své údaje se zdravotnickými orgány sdílet. Pro uživatele by tak neměly plynout žádné negativní důsledky z toho, když si aplikaci odinstalují.

Aplikace pro vysledování kontaktů a varování zajišťují varování osob. Pokud je toto varování poskytováno přímo prostřednictvím aplikace, upozorňuje Komise na to, že je zakázáno, aby osoby byly předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, které má pro ně právní účinky nebo se jich obdobným způsobem významně dotýká (článek 22 nařízení GDPR).

3.4 **Minimalizace údajů**

Údaje produkované prostřednictvím zařízení a v těchto zařízeních již dříve uložené jsou chráněny takto:

— Jako „osobní údaje“, tj. veškeré informace o identifikované nebo identifikovatelné fyzické osobě (čl. 4 odst. 1 nařízení GDPR), jsou chráněny podle nařízení GDPR. Údaje o zdravotním stavu požívají další ochrany (článek 9 nařízení GDPR).

— Jako „lokalizační údaje“, tj. údaje zpracovávané v rámci sítě elektronických komunikací nebo službou elektronické komunikace, udávající zeměpisnou polohu koncového zařízení uživatele, jsou chráněny podle směrnice o soukromí v elektronických komunikacích (čl. 5 odst. 1 a články 6 a 9) ([11]).

— Veškeré informace, které jsou uložené v koncovém zařízení uživatele a ke kterým je z tohoto zařízení získáván přístup, jsou chráněny podle čl. 5 odst. 3 směrnice o soukromí v elektronických komunikacích.

Neosobní údaje (jako například nevratně anonymizované údaje) nejsou chráněny podle nařízení GDPR.

Komise připomíná, že zásada minimalizace údajů požaduje, že zpracovávány smí být pouze osobní údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu ([12]). Posouzení nezbytnosti zpracovávat osobní údaje a relevantnosti těchto osobních údajů by mělo být provedeno s ohledem na sledovaný účel / sledované účely.

Komise podotýká, že například pokud je účelem dané funkce vyhodnocování příznaků nebo telemedicína, nevyžadují takové účely přístup k seznamu kontaktů osoby, která zařízení vlastní.

([10]) Ustanovení čl. 6 odst. 1 písm. e) nařízení GDPR.

([11]) Kodex pro elektronické komunikace stanoví, že sem patří i služby, které jsou funkčně rovnocenné službám elektronických komunikací.

([12]) Zásada minimalizace údajů.

Generování a zpracovávání méně údajů omezuje bezpečnostní rizika. Proto soulad s opatřeními minimalizace údajů dává rovněž bezpečnostní záruky.

— Informační funkce:

Aplikace, která má pouze tuto funkci, nebude potřebovat zpracovávat žádné údaje o zdravotním stavu osob. Bude jim pouze poskytovat informace. K plnění tohoto účelu nesmí být zpracovávány žádné jiné informace, které jsou uložené v koncovém zařízení a ke kterým je z tohoto zařízení získáván přístup, než které jsou pro poskytování informací nezbytné.

— Funkce vyhodnocování příznaků a telemedicíny:

Pokud aplikace obsahuje jednu nebo obě z těchto funkcí, bude zpracovávat osobní údaje o zdravotním stavu. Proto by v souvisejících právních předpisech platných pro zdravotnické orgány měl být uveden seznam údajů, které smí být zpracovány.

Zdravotnické orgány mohou navíc potřebovat telefonní čísla osob, které vyhodnocování příznaků využily a výsledky odeslaly. Informace, které jsou uložené v koncovém zařízení a ke kterým je z tohoto zařízení získáván přístup, smí být zpracovávány pouze do té míry, nakolik je to nezbytné k tomu, aby aplikace plnila svůj účel a mohla fungovat.

— Funkce vysledování kontaktů a varování:

K většině případů COVID-19 dochází prostřednictvím kapének, které se přenášejí pouze na omezenou vzdálenost. Klíčovým faktorem pro přerušení mechanismu nákazy je co nejrychlejší identifikace případných osob, které se vyskytly v blízkém okolí nakažené osoby. Určování vzájemného přiblížení je funkcí vzdálenosti a trvání kontaktu a mělo by být prováděno z epidemiologického hlediska. Přerušení mechanismu nákazy je relevantní zejména pro to, aby se zabránilo opakovanému výskytu nákaz ve fázi ukončování mimořádných opatření souvisejících s krizí.

K tomu by mohla být data o vzájemném přiblížení nezbytná. Pro měření vzájemného přiblížení a úzkého kontaktu se komunikace mezi zařízeními prostřednictvím „Bluetooth Low Energy“ (BLE) jeví jako přesnější, a tudíž vhodnější než využívání geolokačních údajů (GNSS/GPS nebo lokalizace pomocí sítě GSM). Technologie BLE vylučuje možnost sledování (na rozdíl od geolokačních údajů). Komise proto doporučuje používat k určování vzájemného přiblížení komunikační údaje z technologie BLE (nebo údaje generované rovnocennou technologií).

Lokalizační údaje nejsou pro účely funkcí určených k vysledování kontaktů nezbytné, protože jejich cílem není sledovat pohyby osob nebo prosazovat předpisy. Zpracovávání lokalizačních údajů v souvislosti s vysledováváním kontaktů by navíc bylo obtížně odůvodnitelné s ohledem na zásadu minimalizace údajů a mohlo by vyvolávat problémy ohledně bezpečnosti a ochrany soukromí. Z tohoto důvodu Komise doporučuje lokalizační údaje v této souvislosti nevyužívat.

Bez ohledu na technické prostředky použité k určení vzájemného přiblížení se nejeví jako nezbytné ukládat přesný čas kontaktu nebo místo (je-li k dispozici). Mohlo by však být užitečné ukládat den kontaktu, aby bylo možné zjistit, jestli ke kontaktu došlo, když se u osoby objevily příznaky (nebo 48 hodin před tím ([13])), a směřovat tak následnou zprávu s doporučením například ohledně toho, jak dlouho zůstat v domácí karanténě.

Data o vzájemném přiblížení by měla být generována a zpracovávána pouze v případě, že existuje reálné riziko nákazy (v závislosti na blízkosti a době trvání kontaktu).

Je potřeba mít na paměti, že nutnost a proporcionalita sběru dat bude proto záviset na faktorech, jako je míra disponibility testovacích zařízení, zejména v případech, kdy již bylo nařízena opatření, jako je omezení volného pohybu. Varování osob, které byly v úzkém kontaktu s nakaženou osobou, lze provést dvěma způsoby:

V prvním případě je blízkým kontaktům přes aplikaci automaticky zasláno upozornění, když uživatel informuje aplikaci – se schválením nebo potvrzením ze strany zdravotnického orgánu, například prostřednictvím kódu QR nebo TAN – že byl testován pozitivně (decentralizované zpracování). Obsah této upozorňovací zprávy by měl pokud možno stanovit zdravotnický orgán. V druhém případě jsou na backendovém serveru, který patří zdravotnickému orgánu, ukládány nahodilé dočasné identifikátory (řešení s backendovým serverem). Uživatelé nemohou být prostřednictvím těchto dat přímo identifikováni. Uživatelům, kteří byli s pozitivně testovaným uživatelem v úzkém kontaktu, přijde na jejich zařízení prostřednictvím těchto identifikátorů upozornění. Pokud zdravotnické orgány chtějí kontaktovat uživatele, kteří byli s nakaženou osobou v úzkém kontaktu, také prostřednictvím telefonu nebo SMS, potřebují k tomu souhlas těchto uživatelů s poskytnutím jejich telefonních čísel.

([13]) Nakažená osoba je nakažlivá 48 hodin před nástupem příznaků.

3.5 **Omezení poskytnutí/zpřístupnění údajů**

— Informační funkce:

Se zdravotnickými orgány nelze sdílet žádné jiné informace, které jsou uložené v koncovém zařízení a ke kterým je z tohoto zařízení získáván přístup, než informace nezbytné pro informační funkci. Protože tato funkce představuje pouze komunikační prostředek, zdravotnické orgány přístup k žádným dalším datům nezískají.

— Funkce vyhodnocování příznaků a telemedicíny:

Funkce vyhodnocování příznaků může být pro členské státy užitečná v tom, že bude sloužit jako vodítko pro občany, zda by se měli nechat otestovat, poskytne informace o izolaci a o tom, kdy a jak získat přístup ke zdravotní péči, zejména pro rizikové skupiny. Tato funkce může rovněž doplňovat dozor v primární péči a pomoci odhadnout míru nákazy COVID-19 v populaci. Proto může být rozhodnuto, že příslušné zdravotnické orgány a vnitrostátní epidemiologické orgány by měly k informacím poskytnutým pacientem získat přístup. ECDC by mohlo od vnitrostátních orgánů obdržet pro účely epidemiologického dozoru souhrnné údaje.

Pokud bude rozhodnuto, že bude možný i kontakt přes úředníky zdravotnických orgánů, a nikoliv pouze přes samotnou aplikaci, bude nutné poskytnout telefonní čísla uživatelů aplikace také vnitrostátním zdravotnickým orgánům.

— Funkce vysledování kontaktů a varování:

— Údaje o nakažené osobě

Aplikace vytvářejí pseudonahodilé krátkodobé a pravidelně se měnící identifikátory telefonů, které jsou v kontaktu s uživatelem. Jednou možností je, aby identifikátory byly ukládány v zařízení uživatele (tzv. decentralizované zpracování). Jinou možností by bylo, že by tyto nahodilé identifikátory byly ukládány na serveru, k němuž by měly přístup zdravotnické orgány (tzv. řešení s backendovým serverem). Toto decentralizované řešení je více v souladu se zásadou minimalizace. Zdravotnické orgány by měly mít přístup pouze k datům o vzájemném přiblížení ze zařízení nakažené osoby, aby mohly kontaktovat osoby, u nichž existuje riziko, že se nakazily.

Tato data budou mít zdravotnické orgány k dispozici až poté, co jim je nakažená osoba (po testování) proaktivně poskytne.

Nakažená osoba by o totožnosti osob, s nimiž byla v potenciálně epidemiologicky relevantním kontaktu a které budou upozorněny, neměla být informována.

— Údaje o osobách, které byly v (epidemiologickém) kontaktu s nakaženou osobou

Totožnost nakažené osoby by osobám, s nimiž byla v epidemiologickém kontaktu, neměla být sdělena. Bude dostačující jim sdělit, že byly během posledních 16 dnů v epidemiologickém kontaktu s nakaženou osobou. Jak bylo uvedeno výše, údaje o čase a místě takových kontaktů by neměly být ukládány. Proto není nutné ani možné tyto údaje sdělovat.

Za účelem vysledování epidemiologických kontaktů uživatele aplikace, u něhož se potvrdí nákaza, by měly být vnitrostátní zdravotnické orgány informovány pouze o identifikátoru osoby, s níž byla nakažená osoba v epidemiologickém kontaktu od 48 hodin před nástupem příznaků do 14 dnů po jejich nástupu, a to na základě blízkosti a doby trvání kontaktu.

ECDC by mohlo od vnitrostátních orgánů obdržet pro účely epidemiologického dozoru souhrnné údaje o vysledování kontaktů podle ukazatelů vymezených ve spolupráci s členskými státy,

3.6 **Stanovení přesných účelů zpracování**

Účel zpracování by měl mít právní základ (právo Unie nebo členského státu). Účel by měl být konkrétní, aby nebylo pochyb o tom, jaký druh osobních údajů je pro dosažení sledovaného cíle nezbytný, a explicitní. .

Přesný účel(y) bude záviset na funkcích aplikace. Pro každou funkci aplikace může existovat několik účelů. Aby měly osoby nad svými údaji plnou kontrolu, doporučuje Komise nespojovat různé funkce. V každém případě by osoby měly mít možnost vybrat si mezi různými funkcemi, z nichž každá bude sledovat jiný účel.

Komise doporučuje nepoužívat údaje shromážděné za výše uvedených podmínek pro jiné účely než pro boj proti COVID-19. Pokud by byly nezbytné účely jako vědecký výzkum a statistika, měly by být zahrnuty do původního seznamu účelů a měly by být uživatelům jasně sděleny.

— Informační funkce:

Účelem této funkce je poskytovat informace relevantní z hlediska zdravotnických orgánů v kontextu krize.

— Funkce vyhodnocování příznaků a telemedicíny:

Funkce vyhodnocování příznaků může poskytnout orientační údaj o tom, jaké množství osob hlásících příznaky slučitelné s COVID-19 je skutečně nakaženo (např. prostřednictvím stěrů a otestování všech nebo náhodně vybraného počtu osob s těmito příznaky, pokud je na to kapacita). Tato identifikace účelu by měla jasně stanovit, že osobní údaje o zdravotním stavu budou zpracovávány s cílem i) poskytnout dané osobě možnost posoudit na základě souboru položených otázek, zda se u ní objevily příznaky COVID-19, nebo ii) získat po nástupu příznaků COVID-19 lékařskou radu.

— Funkce vysledování kontaktů a varování:

Pouhé uvedení účelu „prevence dalších nákaz COVID-19“ není dostatečně konkrétní. V tomto případě Komise doporučuje účel(y) dále upřesnit, například takto: „uchování kontaktů osob, které používají aplikaci a které mohly být vystaveny nákaze COVID-19 s cílem varovat osoby, které mohly být potenciálně nakaženy“.

3.7 **Stanovení přísných omezení pro ukládání dat**

Zásada omezení uložení vyžaduje, aby osobní údaje nebyly uchovávány déle, než je nezbytné. Lhůty by měly vycházet ze zdravotnického hlediska (v závislosti na účelu aplikace: z inkubační doby atd.) a z realistického trvání administrativní kroků, které může být nutné uskutečnit.

— Informační funkce:

Pokud jsou při instalaci této funkce sbírána data, měla by být okamžitě vymazána. Pro uchovávání těchto dat není důvod.

— Funkce vyhodnocování příznaků a telemedicíny:

Tato data by měly zdravotnické orgány vymazat nejpozději po jednom měsíci (inkubační doba plus rezerva) nebo poté, co byl dané osobě proveden test s negativním výsledkem. Pro účely podávání zpráv v rámci dozoru a pro účely výzkumu mohou zdravotnické orgány uchovávat data po delší dobu, pokud jsou v anonymizované podobě.

— Funkce vysledování kontaktů a varování:

Data o vzájemném přiblížení by měla být vymazána, jakmile již nejsou pro účely upozornění osob potřebná. Tedy nejpozději po jednom měsíci (inkubační doba plus rezerva) nebo poté, co byl dané osobě proveden test s negativním výsledkem. Pro účely podávání zpráv v rámci dozoru a pro účely výzkumu mohou zdravotnické orgány uchovávat data o vzájemném přiblížení po delší dobu, pokud jsou v anonymizované podobě.

Data by měla být ukládána v zařízení uživatele; na server přístupný zdravotnickým orgánům by měla být – v případě, že byla tato možnost zvolena – nahrávána pouze data, která sdělili uživatelé a která jsou nezbytná pro splnění daného účelu (tj. na server se nahrají pouze data o „úzkých kontaktech“ osoby, která měla pozitivní výsledek testu na COVID-19).

3.8 **Zajištění bezpečnosti dat**

Komise doporučuje, aby byla data na koncovém zařízení jednotlivce ukládána v šifrované podobě za použití nejmodernějších šifrovacích technik. Jsou-li data ukládána na centrálním serveru, měly by být o přístupu, včetně administrativního přístupu, vedeny záznamy.

Data o vzájemném přiblížení by měla být na koncovém zařízení jednotlivce generována a ukládána pouze v šifrované a pseudonymizované podobě. Aby se zamezilo sledování třetími stranami, měla by být aktivace Bluetooth možná bez nutnosti aktivovat jiné lokalizační služby.

Při sběru dat o vzájemném přiblížení prostřednictvím BLE je vhodnější vytvářet a ukládat dočasná ID uživatele, která se pravidelně mění, a neukládat ID samotného zařízení. Toto opatření poskytuje dodatečnou ochranu proti odposlechu a sledování hackery, a ztěžuje tedy identifikaci jednotlivců.

Komise doporučuje, aby byl zdrojový kód aplikace zveřejněn a byl k dispozici pro účely přezkoumání.

K zabezpečení zpracovávaných dat je možné přijmout další opatření, zejména automatické vymazání nebo anonymizaci dat po uplynutí určité doby. Stupeň zabezpečení by měl obecně odpovídat množství a citlivosti zpracovávaných osobních údajů.

Veškeré přenosy z osobního zařízení směrem k vnitrostátním zdravotnickým orgánům by měly být šifrovány.

Stanoví-li vnitrostátní právní předpisy, že shromážděné osobní údaje mohou být zpracovávány také pro účely vědeckého výzkumu, měla by být v zásadě používána pseudonymizace.

3.9 **Zajištění přesnosti dat**

Zajištění přesnosti zpracovávaných osobních údajů není pouze nezbytným předpokladem efektivnosti aplikace, ale je také požadavkem podle právních předpisů na ochranu osobních údajů.

V této souvislosti je nezbytné zajistit přesnost informací o tom, zda došlo ke kontaktu s nakaženou osobou (epidemiologická vzdálenost a doba trvání), aby se minimalizovalo riziko falešně pozitivních výsledků. To by mělo platit pro scénáře, kdy jsou dva uživatelé aplikace v kontaktu na ulici, ve veřejné dopravě nebo v budově. Je nepravděpodobné, že by použití lokalizačních údajů založených na mobilních telefonních sítích bylo pro tyto účely dostatečně přesné.

Lze proto doporučit, aby byly využity technologie umožňující přesnější vyhodnocení kontaktu (např. Bluetooth).

3.10 **Zapojení úřadů pro ochranu údajů**

Úřady pro ochranu údajů by měly být v souvislosti s vývojem aplikace plně zapojeny a konzultovány a na její nasazení by měly dohlížet. Vzhledem k tomu, že zpracování údajů v souvislosti s aplikací bude představovat rozsáhlé zpracování zvláštních kategorií údajů (údajů o zdravotním stavu), poukazuje Komise na článek 35 nařízení GDPR, v němž je stanoveno posouzení vlivu na ochranu osobních údajů.