Úradný vestník Európskej únie

C 124 I

Slovenské vydanie

Informácie a oznámenia

Ročník 63

17. apríla 2020

Obsah

SK

II

(Oznámenia)

OZNÁMENIA INŠTITÚCIÍ, ORGÁNOV, ÚRADOV A AGENTÚR EURÓPSKEJ ÚNIE

EURÓPSKA KOMISIA

OZNÁMENIE KOMISIE

Usmernenie týkajúce sa aplikácií podporujúcich boj proti pandémii COVID-19 v súvislosti s ochranou údajov

(2020/C 124 I/01)

1 KONTEXT

Pandémia COVID-19 spôsobila, že Únia a členské štáty, ako aj ich systémy zdravotnej starostlivosti, spôsob života, hospodárska stabilita a hodnoty stoja pred bezprecedentnou výzvou. Digitálne technológie a údaje zohrávajú významnú úlohu v boji proti kríze spôsobenej ochorením COVID-19. Mobilné aplikácie, ktoré sú obvykle nainštalované v smartfónoch, môžu podporiť orgány verejného zdravotníctva na vnútroštátnej úrovni a na úrovni EÚ pri monitorovaní a obmedzovaní šírenia pandémie COVID-19 a majú osobitný význam vo fáze zrušenia opatrení na obmedzenie šírenia. Môžu poskytovať priame usmernenia pre občanov a podporovať úsilie pri sledovaní kontaktov. V mnohých krajinách, tak v rámci EÚ, ako aj vo svete, vnútroštátne orgány, regionálne samosprávy alebo vývojári oznámili vytvorenie aplikácií s rôznymi funkciami zameranými na podporu boja proti vírusu.

Komisia 8. apríla 2020 prijala Odporúčanie o spoločnom súbore nástrojov Únie na využívanie technológií a údajov na boj proti kríze spôsobenej ochorením COVID-19 a jej prekonanie, najmä pokiaľ ide o mobilné aplikácie a využívanie anonymizovaných údajov o mobilite (ďalej len „odporúčanie“) ([1]). Účelom uvedeného odporúčania je okrem iného vytvoriť spoločnú európsku koncepciu („súbor nástrojov“) používania mobilných aplikácií koordinovanú na úrovni EÚ s cieľom umožniť občanom prijímať účinné opatrenia obmedzovania sociálnych kontaktov a vystríhať pred kontaktmi, brániť im a sledovať ich v snahe obmedziť šírenie ochorenia COVID-19. V odporúčaní sa stanovujú všeobecné zásady, ktorými by sa mal riadiť vývoj takéhoto súboru nástrojov, a uvádza sa v ňom, že Komisia uverejní ďalšie usmernenie vrátane usmernenia týkajúceho sa ochrany osobných údajov a dôsledkov, ktoré môže mať používanie aplikácií v tejto oblasti na súkromie.

V spoločnom európskom pláne na zrušenie opatrení na zamedzenie šírenia COVID-19 Komisia v spolupráci s predsedom Európskej rady stanovila niekoľko zásad na usmernenie postupného rušenia opatrení na zamedzenie šírenia zavedených v dôsledku vypuknutia nákazy COVID-19. Mobilné aplikácie vrátane funkcií sledovania kontaktov môžu v tejto súvislosti zohrávať dôležitú úlohu. V závislosti od vlastností aplikácií a rozsahu, v akom ich obyvateľstvo používa, môžu mať významný vplyv na diagnostiku ochorenia COVID-19, jeho liečbu a manažment v nemocničnom prostredí aj mimo neho. Obzvlášť dôležité sú vtedy, keď sa opatrenia na zamedzenie šírenia rušia a keď sa zvyšuje riziko nákazy, keďže čoraz viac ľudí je vo vzájomnom kontakte. Tieto aplikácie môžu pomôcť prerušiť reťazce nákazy rýchlejšie a efektívnejšie než všeobecné opatrenia na zamedzenie šírenia a môžu výrazne znížiť riziko šírenia vírusu. Mali by byť preto dôležitým prvkom stratégie ukončenia opatrení a mali by dopĺňať iné opatrenia, ako je napríklad zvýšenie kapacít testovania ([2]). Dôležitým predpokladom pre vývoj, akceptáciu a využívanie týchto aplikácií jednotlivcami je dôvera. Ľudia musia mať istotu, že je zabezpečené dodržiavanie základných práv a že tieto aplikácie sa budú používať len na osobitne vymedzené účely, nebudú sa používať na hromadné sledovanie a že jednotlivci budú mať naďalej kontrolu nad svojimi údajmi. Toto je

([1]) Odporúčanie C(2020) 2296 final z 8. apríla 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

základom presnosti a účinnosti týchto aplikácií pri zamedzovaní šírenia vírusu. Je preto nevyhnutné identifikovať riešenia, ktoré predstavujú čo najmenší zásah do práva na súkromie a sú v plnom súlade s požiadavkami na ochranu osobných údajov a súkromia stanovenými v právnych predpisoch EÚ. Okrem toho by sa tieto aplikácie mali deaktivovať najneskôr vtedy, keď sa vyhlási, že pandémia je pod kontrolou. Aplikácie by mali obsahovať aj najmodernejšie ochranné prvky na zaručenie informačnej bezpečnosti.

V tomto usmernení sa zohľadňuje príspevok Európskeho výboru pre ochranu údajov (EDPB) ([3]) a rokovania v rámci siete elektronického zdravotníctva. EDPB plánuje v nadchádzajúcich dňoch uverejniť usmernenia týkajúce sa geolokalizácie a iných nástrojov na sledovanie v súvislosti s pandémiou COVID-19.

Rozsah pôsobnosti usmernenia

S cieľom zabezpečiť jednotný prístup v celej EÚ a poskytnúť členským štátom a vývojárom aplikácií usmernenie sa v tomto dokumente stanovujú vlastnosti a požiadavky, ktoré by aplikácie mali spĺňať, aby sa zabezpečil súlad s právnymi predpismi EÚ o ochrane súkromia a osobných údajov, najmä so všeobecným nariadením o ochrane údajov ([4]) a so smernicou o súkromí a elektronických komunikáciách ([5]). Toto usmernenie sa nezaoberá žiadnymi ďalšími podmienkami ani obmedzeniami, ktoré môžu byť súčasťou vnútroštátnych právnych predpisov členských štátov, pokiaľ ide o spracúvanie údajov týkajúcich sa zdravia.

Toto usmernenie nie je právne záväzné. Nie je ním dotknutá úloha Súdneho dvora EÚ, ktorý je jedinou inštitúciou, ktorá môže poskytovať záväzný výklad práva EÚ.

Toto usmernenie sa týka len dobrovoľných aplikácií podporujúcich boj proti pandémii COVID-19 (aplikácie stiahnuté, nainštalované a používané na dobrovoľnom základe jednotlivcami) s jednou alebo viacerými z týchto funkcií:

— poskytovanie presných informácií o pandémii COVID-19 jednotlivcom,

— poskytovanie dotazníkov na posudzovanie svojho zdravotného stavu a usmernení pre jednotlivcov (funkcia overovania príznakov) ([6]),

— upozorňovanie osôb, ktoré boli počas určitej doby v blízkosti nakazenej osoby, s cieľom poskytnúť im informácie o tom, či by mali podstúpiť samokaranténu a kde sa majú nechať otestovať (funkcia sledovania kontaktov a výstrahy),

— poskytovanie komunikačného fóra medzi pacientmi a lekármi v prípade samoizolácie osôb alebo v prípade, že sa poskytuje ďalšie poradenstvo pri určovaní diagnózy a liečby (častejšie používanie telemedicíny).

Podľa smernice o súkromí a elektronických komunikáciách je uloženie povinnosti používať aplikáciu, ktorá zahŕňa práva na dôvernosť komunikácií stanovené v článku 5, možné len prostredníctvom právneho predpisu, ktorý je nevyhnutný, vhodný a primeraný na ochranu určitých špecifických cieľov. Vzhľadom na vysokú mieru zásahu do práva na súkromie, ktoré z takéhoto prístupu vyplýva, a na výzvy spojené s týmto prístupom, aj pokiaľ ide o zavedenie primeraných záruk, Komisia zastáva názor, že pred použitím tejto možnosti sa vyžaduje dôkladná analýza. Z týchto dôvodov Komisia odporúča používanie dobrovoľných aplikácií.

Toto usmernenie sa nevzťahuje na aplikácie zamerané na presadzovanie karanténnych požiadaviek (vrátane aplikácií, ktoré sú povinné).

2 PRÍNOS APLIKACIÍ K BOJU PROTI ŠIRENIU OCHORENIA COVID-19

Funkcia overovania príznakov predstavuje nástroj pre orgány verejného zdravotníctva na usmerňovanie občanov, pokiaľ ide o testovanie na vírus COVID-19, informácie o samoizolácii, o tom, ako sa vyhnúť jeho prenosu na iných a kedy vyhľadať zdravotnú starostlivosť. Môže zároveň dopĺňať dohľad nad primárnou starostlivosťou a poskytnúť lepší prehľad o miere prenosu COVID-19 medzi obyvateľmi.

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

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119, 4.5.2016, s. 1.

([5]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 31.7.2002, s. 37.

([6]) Ak aplikácie poskytujú informácie týkajúce sa diagnostiky, prevencie, monitorovania, predpovedania alebo prognózy, malo by sa posúdiť ich možné zaradenie ako zdravotníckych pomôcok v súlade s regulačným rámcom pre zdravotnícke pomôcky. Pokiaľ ide o uvedený rámec, pozri smernicu Rady 93/42/EHS zo 14. júna 1993 o zdravotníckych pomôckach (Ú. v. ES L 169, 12.7.1993, s. 1) a nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach (Ú. v. EÚ L 117, 5.5.2017, s. 1).

Funkcia sledovania kontaktov a výstrahy predstavuje pre orgány verejného zdravotníctva nástroj na identifikovanie osôb, ktoré boli v kontakte s osobou infikovanou vírusom COVID-19, a na ich informovanie o vhodných ďalších krokoch, napríklad o samokaranténe, testovaní alebo na poskytnutie rady o tom, čo robiť, ak sa u nich prejavia príznaky. Táto funkcia je preto užitočná tak pre jednotlivcov, ako aj pre orgány verejného zdravotníctva. Môže zohrávať dôležitú úlohu aj pri riadení opatrení na obmedzenie pohybu v rámci deeskalačných scenárov. Ich vplyv možno umocniť uplatnením stratégie, ktorá napomáha rozšíriť testovanie osôb s miernymi príznakmi.

Obe funkcie môžu byť relevantným zdrojom údajov pre orgány verejného zdravotníctva a uľahčiť zasielanie takýchto údajov národným epidemiologickým orgánom a Európskemu centru pre prevenciu a kontrolu chorôb (ECDC). To by pomohlo získať prehľad o spôsoboch prenosu a v kombinácii s výsledkami testov odhadnúť pozitívnu prediktívnu hodnotu respiračných príznakov v danej komunite a poskytnúť informácie o úrovni cirkulácie vírusu.

Stupeň spoľahlivosti odhadov priamo súvisí s počtom a spoľahlivosťou poskytnutých údajov.

Preto môžu funkcie overovania príznakov a sledovania kontaktov v kombinácii s vhodnými testovacími stratégiami poskytovať informácie o úrovni cirkulácie vírusu a byť prínosné pri posudzovaní účinnosti zachovávania fyzického odstupu, ako aj opatrení na obmedzenie pohybu. Ako sa uvádza v odporúčaní, medzi IT riešeniami rôznych členských štátov by sa mala zabezpečiť interoperabilita s cieľom umožniť cezhraničnú spoluprácu a zabezpečiť detekciu kontaktov medzi používateľmi rôznych aplikácií (čo je obzvlášť dôležité pri cezhraničných pohyboch občanov). Ak je infikovaná osoba v kontakte s používateľom aplikácie iného členského štátu, cezhraničný prenos osobných údajov tohto používateľa k orgánom verejného zdravotníctva jeho členského štátu by mal byť možný v nevyhnutne potrebnom v rozsahu. Na tejto otázke sa bude pracovať v rámci súboru nástrojov uvedeného v odporúčaní. Interoperabilita by sa mala zabezpečiť stanovením technických požiadaviek a zlepšením komunikácie a spolupráce medzi vnútroštátnymi orgánmi verejného zdravotníctva. Model konkrétnej spolupráce ([7]) by sa mohol použiť aj ako model riadenia aplikácií na sledovanie kontaktov počas pandémie COVID-19.

3 PRVKY ZABEZPECUJUCE DOVERYHODNE A ZODPOVEDNE POUZIVANIE APLIKACII

Funkcie zahrnuté do aplikácií môžu mať rôzny vplyv na širokú škálu práv zakotvených v Charte základných práv EÚ, ako je ľudská dôstojnosť, rešpektovanie súkromného a rodinného života, ochrana osobných údajov, sloboda pohybu, nediskriminácia, sloboda podnikania a sloboda zhromažďovania a združovania. Keďže niektoré funkcie sú založené na modeli intenzívne využívajúcom údaje, obzvlášť výrazný môže byť zásah do súkromia a do práva na ochranu osobných údajov.

Cieľom nasledujúcich prvkov je poskytnúť usmernenie, ako obmedziť zásah funkcií obsiahnutých v aplikácií do práva na súkromie, aby boli v súlade s právnymi predpismi EÚ o ochrane osobných údajov a súkromia.

3.1 Vnútroštátne orgány verejného zdravotníctva (alebo subjekty vykonávajúce úlohy vo verejnom záujme v oblasti zdravia) ako prevádzkovateľ

Aby sa určila zodpovednosť za súlad s pravidlami EÚ o ochrane osobných údajov, je zásadne dôležité zistiť, kto rozhoduje o prostriedkoch a účeloch spracúvania údajov (prevádzkovateľ), a najmä: kto by mal poskytnúť informácie osobám, ktoré si stiahnu aplikáciu, o tom, čo sa stane s ich osobnými údajmi (už existujúcimi alebo tými, ktoré vygeneruje zariadenie, napríklad smartfón, na ktorom je aplikácia nainštalovaná), aké budú ich práva, kto bude zodpovedný v prípade porušenia ochrany údajov atď.

Vzhľadom na citlivosť príslušných osobných údajov a nižšie opísaný účel spracovania údajov sa Komisia domnieva, že aplikácie by mali byť navrhnuté tak, aby boli prevádzkovateľmi vnútroštátne orgány verejného zdravotníctva (alebo subjekty vykonávajúce úlohy vo verejnom záujme v oblasti zdravia) ([8]). Prevádzkovatelia sú zodpovední za súlad so všeobecným nariadením o ochrane údajov (zásada zodpovednosti). Rozsah takéhoto prístupu by mal byť obmedzený na základe zásad opísaných v oddiele 3.5.

([7]) Takáto spolupráca už prebieha v súvislosti s projektom MyHealth@EU na účely výmeny zdravotných záznamov o pacientoch a elektronických lekárskych predpisov. Pozri aj článok 5 ods. 5 a odôvodnenie 17 vykonávacieho rozhodnutia Komisie 2019/1765.

([8]) Pozri odôvodnenie 45 všeobecného nariadenia o ochrane údajov.

Zároveň to prispeje k zvýšeniu dôvery medzi obyvateľmi, a teda aj k prijatiu aplikácií (a podkladových informačných systémov pre reťazce prenosu infekcií), a zabezpečí sa tým, že budú spĺňať účel ochrany verejného zdravia. Zodpovedné vnútroštátne orgány verejného zdravotníctva by mali zosúladiť a koordinovane vykonávať príslušné politiky, požiadavky a kontroly.

3.2 **Údaje pod kontrolou jednotlivca**

Aby mohli ľudia aplikáciám dôverovať, musí sa preukázať, že kontrolu nad svojimi osobnými údajmi budú mať aj naďalej jednotlivci. Komisia sa preto domnieva, že by sa mali splniť najmä tieto podmienky:

— inštalácia aplikácie na ich zariadeniach by mala byť dobrovoľná a bez akýchkoľvek negatívnych dôsledkov pre toho, kto sa rozhodne, že si aplikáciu nestiahne alebo ju nebude používať;

— rôzne funkcie aplikácií (napr. poskytovania informácií, overovania príznakov, sledovania kontaktov a varovania) by nemali byť zoskupené, aby jednotlivec mohol poskytnúť súhlas s každou funkciou zvlášť. To by nemalo používateľom brániť, aby rôzne funkcie aplikácií kombinovali, ak to poskytovateľ ponúka ako možnosť;

— ak sa používajú údaje o blízkosti [údaje získané výmenou signálov v nízkoenergetickom systéme Bluetooth (BLE) medzi zariadeniami v rámci epidemiologicky relevantnej vzdialenosti a v priebehu epidemiologicky relevantného času], mali by sa uchovávať v zariadení danej osoby. Ak sa tieto údaje majú poskytnúť orgánom verejného zdravotníctva, malo by sa tak stať, až keď sa potvrdí, že dotknutá osoba je infikovaná vírusom COVID-19, a pod podmienkou, že sa tak táto osoba rozhodne;

— orgány verejného zdravotníctva by mali poskytnúť jednotlivcom všetky potrebné informácie týkajúce sa spracúvania ich osobných údajov (v súlade s článkami 12 a 13 všeobecného nariadenia o ochrane údajov a článkom 5 smernice o súkromí a elektronických komunikáciách);

— jednotlivec by mal mať možnosť uplatniť svoje práva, ktoré mu prislúchajú podľa všeobecného nariadenia o ochrane údajov (najmä právo na prístup, opravu a vymazanie). Akékoľvek obmedzenie práv podľa všeobecného nariadenia o ochrane údajov a smernice o súkromí a elektronických komunikáciách by malo byť v súlade s týmito aktmi a malo by byť nevyhnutné, primerané a stanovené v právnych predpisoch;

— aplikácie by sa mali deaktivovať najneskôr vtedy, keď sa vyhlási, že pandémia je pod kontrolou; deaktivácia by nemala závisieť od toho, či užívateľ aplikácie odinštaluje.

3.3 **Právny základ pre spracúvanie**

Inštalácia aplikácií a ukladanie informácií na zariadení používateľa

Ako sa uvádza vyššie, podľa smernice o súkromí a elektronických komunikáciách (článok 5) je ukladanie informácií na zariadení používateľa alebo získavanie prístupu k informáciám, ktoré sú už uložené, povolené len vtedy, ak i) používateľ dal súhlas alebo ii) uloženie a/alebo sprístupnenie je nevyhnutne potrebné pre službu informačnej spoločnosti (napr. aplikáciu), ktorú používateľ výslovne vyžiadal (t. j. nainštaloval a aktivoval).

Ukladanie informácií na zariadení jednotlivca a získavanie prístupu k informáciám, ktoré sú už uložené na tomto zariadení, je zvyčajne potrebné na to, aby fungovali aplikácie. Funkcia sledovania kontaktov a výstrahy si okrem toho vyžaduje aj uloženie niektorých ďalších informácií na zariadení používateľa (ako sú napríklad efemérne, pravidelne sa meniace prezývky, teda používateľské mená používateľov tejto funkcie v blízkosti). Táto funkcia si navyše môže vyžadovať, aby (nakazený alebo pravdepodobne nakazený) používateľ nahrával údaje o blízkosti. Takéto nahrávanie nie je potrebné na fungovanie aplikácie ako takej. Požiadavky možnosti ii) uvedené v predchádzajúcom odseku preto nie sú splnené. Súhlas [možnosť i) uvedená vyššie] sa teda považuje za najvhodnejší dôvod pre príslušné činnosti. Tento súhlas by mal byť „slobodne daný“, „konkrétny“, „výslovný“ a „informovaný“ v zmysle všeobecného nariadenia o ochrane údajov. Mal by byť vyjadrený prostredníctvom jednoznačného potvrdzujúceho úkonu jednotlivca; nepatria sem tiché formy súhlasu (napr. mlčanie; nečinnosť) ([9]).

([9]) Pozri usmernenia Európskeho výboru pre ochranu údajov o súhlase: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Právny základ pre spracúvanie vnútroštátnymi orgánmi verejného zdravotníctva – právne predpisy Únie alebo členského štátu

Vnútroštátne orgány verejného zdravotníctva zvyčajne spracúvajú osobné údaje vtedy, keď existuje zákonná povinnosť stanovená v právnych predpisoch EÚ alebo členského štátu, ktorými sa upravuje takéto spracúvanie a ktoré spĺňajú podmienky článku 6 ods. 1 písm. c) a článku 9 ods. 2 písm. i) všeobecného nariadenia o ochrane údajov, alebo ak je takéto spracúvanie potrebné na splnenie úlohy vykonávanej v záujme presadzovania verejného záujmu, ktorý je uznaný právnymi predpismi EÚ alebo členského štátu ([10]).

V každom vnútroštátnom právnom predpise sa musia stanoviť osobitné a vhodné opatrenia na ochranu práv a slobôd dotknutých osôb. Vo všeobecnosti platí, že čím silnejší je vplyv na slobody jednotlivcov, tým by sa mali v príslušnom právnom predpise stanoviť prísnejšie zodpovedajúce záruky.

Právne predpisy EÚ a členských štátov, ktoré existovali pred vypuknutím ochorenia COVID-19, a predpisy, ktoré členské štáty prijímajú osobitne na boj proti šíreniu epidémie, sa v zásade môžu použiť ako právny základ pre spracúvanie údajov jednotlivcov, ak stanovujú opatrenia umožňujúce monitorovanie epidémie a ak daný právny predpis spĺňa ďalšie požiadavky stanovené v článku 6 ods. 3 všeobecného nariadenia o ochrane údajov.

Vzhľadom na povahu dotknutých osobných údajov (najmä údajov týkajúcich sa zdravia ako osobitnej kategórie osobných údajov), ako aj okolnosti súčasnej pandémie COVID-19, by odvolávanie sa na konkrétny právny predpis ako na právny základ prispelo k právnej istote, pretože by i) podrobne predpisovalo spracovanie špecifických údajov týkajúcich sa zdravia a jasne určilo účely spracovania; ii) jasne určilo, kto je prevádzkovateľom, t. j. subjektom, ktorý spracúva údaje, a kto okrem prevádzkovateľa môže mať prístup k takýmto údajom; iii) vylúčilo možnosť spracovať takéto údaje na iné účely ako tie, ktoré sú uvedené v právnych predpisoch, a iv) poskytlo osobitné záruky. Aby nedošlo k narušeniu verejnej prospešnosti a akceptácie aplikácií, vnútroštátny zákonodarca by mal venovať osobitnú pozornosť tomu, aby zvolené riešenie bolo čo najinkluzívnejšie vo vzťahu k občanom.

Spracúvanie údajov orgánmi verejného zdravotníctva na základe právnych predpisov nemení nič na tom, že jednotlivci majú naďalej možnosť rozhodnúť sa medzi nainštalovaním a nenainštalovaním aplikácie, ako aj súhlasiť či nesúhlasiť so zdieľaním svojich údajov s orgánmi verejného zdravotníctva. Odinštalovanie aplikácie by nemalo mať teda pre používateľa žiadne nepriaznivé dôsledky.

Aplikácie na sledovanie kontaktov a výstražné aplikácie umožňujú varovanie jednotlivcov. V prípade, že funkciu výstrahy obsahuje priamo aplikácia, Komisia upozorňuje na zákaz podrobiť jednotlivcov rozhodnutiu založenému výlučne na automatizovanom spracovaní údajov, z ktorého vyplývajú právne účinky alebo ktoré ovplyvňuje danú osobu podobne významným spôsobom (článok 22 všeobecného nariadenia o ochrane údajov).

3.4 **Minimalizácia údajov**

Údaje získané prostredníctvom zariadení a už predtým uložené na týchto zariadeniach sú chránené takto:

— „Osobné údaje“, t. j. akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (článok 4 ods. 1 všeobecného nariadenia o ochrane údajov), sú chránené podľa všeobecného nariadenia o ochrane údajov. V súvislosti s údajmi týkajúcimi sa zdravia sa poskytuje dodatočná ochrana (článok 9 všeobecného nariadenia o ochrane údajov).

— „Lokalizačné údaje“, t. j. údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, s uvedením zemepisnej polohy koncového zariadenia používateľa, sú chránené podľa smernice o súkromí a elektronických komunikáciách (článok 5 ods. 1 a články 6 a 9) ([11]).

— Všetky informácie uložené v koncovom zariadení používateľa a sprístupnené z neho sú chránené podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

Iné ako osobné údaje (napríklad nezvratne anonymizované údaje) nie sú podľa všeobecného nariadenia o ochrane údajov chránené.

Komisia pripomína, že zásada minimalizácie údajov vyžaduje, aby sa spracovávali len osobné údaje, ktoré sú vhodné, relevantné a obmedzené na to, čo je nevyhnutné v súvislosti s daným účelom ([12]). Posúdenie potreby spracovania osobných údajov a relevantnosti takýchto osobných údajov by sa malo vykonať s ohľadom na sledovaný(-é) účel (-y).

Komisia napríklad poznamenáva, že ak je účelom funkcie overovanie príznakov alebo telemedicína, tieto účely si nevyžadujú prístup k zoznamu kontaktov osoby, ktorá je vlastníkom zariadenia.

([10]) Článok 6 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov.

([11]) V kódexe elektronických komunikácií sa stanovuje, že služby, ktoré sú funkčne rovnocenné s elektronickými komunikačnými službami, sú tiež zahrnuté.

([12]) Zásada minimalizácie údajov.

Generovanie a spracúvanie menšieho množstva údajov obmedzuje bezpečnostné riziká. Preto dodržiavanie opatrení na minimalizáciu údajov predstavuje aj bezpečnostné záruky.

— Funkcia poskytovania informácií:

Aplikácia, ktorá má len túto funkciu, nebude musieť spracúvať žiadne údaje týkajúce sa zdravia jednotlivcov. Len im poskytne informácie. S cieľom splniť tento účel sa žiadne informácie uložené v koncovom zariadení a sprístupnené z neho nedajú spracovať iným spôsobom, než aký je potrebný na poskytnutie informácií.

— Funkcia overovania príznakov a funkcia telemedicíny:

Ak aplikácia zahŕňa jednu z týchto funkcií alebo obe funkcie, bude spracúvať osobné údaje týkajúce sa zdravia. Zoznam údajov, ktoré možno spracovať, by sa preto mal vymedziť v príslušných právnych predpisoch, ktoré sa uplatňujú na orgány verejného zdravotníctva.

Okrem toho môžu orgány verejného zdravotníctva potrebovať telefónne čísla osôb, ktoré použili funkciu overovania príznakov a nahrali výsledky. Informácie uložené v koncovom zariadení a sprístupnené z neho sa môžu spracúvať len vtedy, ak je to potrebné na to, aby aplikácia plnila svoj účel, a na umožnenie jej fungovania.

— Funkcia sledovania kontaktov a výstrahy:

K nákaze COVID-19 vo väčšine prípadov dochádza prostredníctvom kvapôčok, ktoré sa prenášajú len na obmedzenú vzdialenosť. Kľúčovým faktorom prerušenia reťazca nákazy je čo najrýchlejšie identifikovať osoby, ktoré sa nachádzali v blízkosti infikovanej osoby. Rozhodujúca blízkosť je funkciou vzdialenosti a trvania kontaktu, pričom ju treba stanoviť z epidemiologického hľadiska. Prerušenie reťazca nákazy má mimoriadny význam z hľadiska predídenia opätovnému výskytu infekcií počas fázy ukončovania opatrení.

Na tento účel by mohli byť potrebné údaje o tom, v akej blízkosti sa dotknuté osoby nachádzali. Zdá sa, že komunikácia medzi zariadeniami prostredníctvom nízkoenergetického systému Bluetooth (BLE) je pri meraní blízkosti a úzkych kontaktov presnejšia, a preto vhodnejšia, než používanie geolokalizačných údajov (GNSS/GPS alebo údajov o lokalizácii mobilného telefónu). Nízkoenergetický systém Bluetooth neumožňuje sledovanie (na rozdiel od geolokalizačných údajov). Komisia preto odporúča, aby sa na určenie blízkosti používali údaje o komunikácii z tohto systému (alebo údaje generované rovnocennou technológiou).

Lokalizačné údaje nie sú na účely funkcií sledovania kontaktov potrebné, keďže ich cieľom nie je sledovať pohyb jednotlivcov ani presadzovať predpisy. Navyše, spracúvanie lokalizačných údajov v súvislosti so sledovaním kontaktov by bolo, vzhľadom na zásadu minimalizácie údajov, ťažké odôvodniť a mohlo by viesť k problémom v oblasti bezpečnosti a ochrany súkromia. Komisia preto odporúča, aby sa v tejto súvislosti nepoužívali lokalizačné údaje.

Bez ohľadu na to, aké technické prostriedky sa použijú na určenie blízkosti, nezdá sa potrebné uchovávať presný čas kontaktu alebo miesto, kde k nemu došlo (ak je k dispozícii). Užitočné by však mohlo byť uchovávať deň kontaktu, aby bolo možné zistiť, či ku kontaktu došlo, keď sa u danej osoby objavili príznaky (alebo 48 hodín predtým ([13])), a doplniť následnú správu o informácie, ako dlho by mala trvať samokaranténa.

Údaje o blízkosti by sa mali generovať a spracúvať len v prípade, že skutočne hrozí riziko infekcie (na základe toho, aký úzky bol kontakt a koľko trval).

Treba poznamenať, že nevyhnutnosť a primeranosť zberu údajov bude teda závisieť od faktorov, ako je miera dostupnosti testovacích zariadení, najmä keď už boli nariadené opatrenia ako izolácia. Osoby, ktoré boli v úzkom kontakte s infikovanou osobou, možno výstrahu sprostredkovať dvojakým spôsobom:

Pri prvom prístupe sa výstraha prostredníctvom aplikácie automaticky zašle osobám, ktoré boli s infikovanou osobou v úzkom kontakte, keď používateľ notifikuje aplikácii – so súhlasom orgánu verejného zdravotníctva alebo s jeho potvrdením, napríklad prostredníctvom QR alebo TAN kódu –, že výsledok jeho testu boli pozitívny (decentralizované spracúvanie). Bolo by vhodné, aby obsah výstražnej správy stanovil orgán verejného zdravotníctva. Pri druhom prístupe sa na back-end serveri prevádzkovanom orgánom verejného zdravotníctva uchovávajú náhodne generované dočasné identifikátory (riešenie s back-end serverom). Používatelia sa nedajú na základe týchto údajov priamo identifikovať. Používatelia, ktorí boli v úzkom kontakte s používateľom s pozitívnym výsledkom testu, dostanú na základe identifikátorov výstrahu do svojho zariadenia. Ak budú chcieť orgány verejného zdravotníctva kontaktovať používateľov, ktorí boli v úzkom kontakte s infikovanou osobou, aj prostredníctvom telefónu alebo SMS, budú si musieť vyžiadať súhlas používateľov s poskytnutím telefónnych čísiel.

([13]) Infikovaná osoba je nákazlivá 48 hodín pred nástupom symptómov.

3.5 **Obmedzenie zverejňovania údajov a prístupu k nim**

— Funkcia poskytovania informácií:

Orgánom verejného zdravotníctva nemožno poskytovať žiadne informácie, ktoré sa uchovávajú v koncových zariadeniach a ku ktorým sa pristupuje z koncových zariadení, s výnimkou informácií potrebných na zabezpečenie funkcie poskytovania informácií. Keďže táto funkcia slúži len ako prostriedok na komunikáciu, orgány verejného zdravotníctva nezískajú prístup k žiadnym iným údajom.

— Funkcia overovania príznakov a funkcia telemedicíny:

Funkcia overovania príznakov môže byť pre členské štáty užitočná v tom, že občanom pomôže zistiť, či by sa mali dať otestovať, poskytne informácie o izolácii a tiež o tom, ako a kedy sa obrátiť na zariadenia zdravotnej starostlivosti, najmä pre rizikové skupiny. Táto funkcia môže zároveň dopĺňať sledovanie v rámci primárnej zdravotnej starostlivosti a pomôcť zistiť mieru premorenia populácie nákazou COVID-19. Preto možno rozhodnúť, že zodpovedné orgány verejného zdravotníctva a vnútroštátne epidemiologické orgány by mali mať prístup k informáciám poskytnutým pacientom. ECDC by na účely epidemiologického dohľadu mohlo od vnútroštátnych orgánov dostávať agregované údaje.

V prípade, že sa popri výlučnom kontakte cez aplikáciu umožní aj kontakt zo strany pracovníkov orgánov verejného zdravotníctva, bude potrebné sprístupniť vnútroštátnym orgánom verejného zdravotníctva aj telefónne čísla používateľov aplikácie.

— Funkcia sledovania kontaktov a výstrahy:

— Údaje o infikovanej osobe

Aplikácie generujú pseudonáhodne efemérne a periodicky sa meniace identifikátory telefónov, ktoré sú v kontakte s používateľom. Jedna možnosť je uchovávať tieto identifikátory v zariadení používateľa (tzv. decentralizované spracovávanie). Ďalšou možnosťou uchovávať tieto náhodné identifikátory na serveri, ku ktorému majú orgány verejného zdravotníctva prístup (tzv. centralizované uchovávanie). Decentralizované riešenie je väčšmi v súlade so zásadou minimalizácie. Orgány verejného zdravotníctva by mali mať prístup len k údajom o zariadeniach, ktoré sa nachádzali v blízkosti, zo zariadenia infikovanej osoby, aby mohli kontaktovať osoby, ktorým hrozí riziko infekcie.

Tieto údaje získajú až potom, keď im ich infikovaná osoba (po otestovaní) proaktívne poskytne.

Infikovaná osoba by nemala byť informovaná o totožnosti osôb, s ktorými bola v potenciálne epidemiologicky relevantnom kontakte a ktoré dostanú výstrahu.

— Údaje osôb, ktoré boli v (epidemiologickom) kontakte s infikovanou osobou

Osoby, s ktorými bola infikovaná osoba v epidemiologickom kontakte, by nemali byť informované o jej totožnosti. Postačí, ak sa im oznámi, že v posledných 16 dňoch boli v epidemiologickom kontakte s infikovanou osobou. Ako sme už uviedli, údaje o čase a mieste takéhoto kontaktu by sa nemali uchovávať. Preto nie je potrebné ani možné tieto údaje komunikovať.

Na účely sledovania epidemiologických kontaktov používateľa elektronickej aplikácie, u ktorého sa infekcia potvrdila, by sa vnútroštátnym orgánom verejného zdravotníctva mal poskytnúť len identifikátor osoby, s ktorou bola infikovaná osoba na základe informácií o blízkosti a trvaní kontaktu v epidemiologickom kontakte v rozmedzí od 48 hodín pred nástupom príznakov až do 14 dní po ich nástupe.

ECDC by mohlo od vnútroštátnych orgánov dostávať agregované údaje o sledovaní kontaktov na účely epidemiologického dohľadu zameraného na ukazovatele, ktoré budú vymedzené v spolupráci s členskými štátmi.

3.6 **Stanovenie presných účelov spracovania**

Účel spracovania by mal byť daný právnym základom (podľa právnych predpisov Únie alebo členského štátu). Účel by mal byť špecifický, aby nevznikali pochybnosti o tom, aký druh osobných údajov sa musí spracovávať, aby sa dosiahol požadovaný cieľ, a formálne vyjadrený. .

Presný účel, resp. účely budú závisieť od funkcií aplikácie. Jednotlivé funkcie aplikácie môžu mať viacero účelov. Komisia odporúča nezoskupovať viaceré funkcie, aby jednotlivci mali možnosť plnej kontroly nad svojimi údajmi. Jednotlivec by mal mať v každom prípade možnosť vybrať si spomedzi rôznych funkcií, z ktorých každá sleduje samostatný účel.

Komisia neodporúča využívať údaje zhromaždené za uvedených podmienok na iné účely ako na boj proti pandémii COVID-19. Ak by vznikla potreba ich využitia napríklad na účely vedeckého výskumu a štatistiky, tieto účely by mali byť zahrnuté do pôvodného zoznamu účelov a používateľom jasne oznámené.

— Funkcia poskytovania informácií:

Účelom tejto funkcie je poskytovať informácie, ktoré sú relevantné z hľadiska orgánov verejného zdravotníctva v súvislosti s krízou.

— Funkcia overovania príznakov a funkcia telemedicíny:

Funkcia overovania príznakov môže poskytnúť informáciu o tom, aký podiel jednotlivcov vykazujúcich symptómy zodpovedajúce nákaze COVID-19 je skutočne infikovaných (napr. odberom steru a otestovaním všetkých osôb alebo náhodného počtu osôb s takýmito príznakmi, ak na to existuje kapacita). Na základe takto určeného účelu by malo byť jasné, že osobné údaje o zdravotnom stave sa budú spracovávať s cieľom i) poskytnúť jednotlivcovi možnosť samoposúdenia na základe súboru otázok, či sa u neho objavili symptómy COVID-19, alebo ii) zabezpečiť lekársku konzultáciu v prípade, že sa objavili symptómy COVID-19.

— Funkcia sledovania kontaktov a výstrahy:

Samotné uvedenie cieľa „prevencia ďalších infekcií COVID-19“ nie je dosť špecifické. V tomto prípade Komisia odporúča bližšie špecifikovať tento účel (účely) na základe tejto koncepcie: „archivovanie kontaktov osôb, ktoré používajú aplikáciu a ktoré mohli byť vystavené nákaze COVID-19, s cieľom varovať osoby, ktoré mohli byť potenciálne infikované“.

3.7 **Stanovenie prísnych limitov uchovávania údajov**

Podľa zásady minimalizácie uchovávania sa vyžaduje, že osobné údaje sa nesmú uchovávať dlhšie, ako je potrebné. Lehoty by sa mali stanoviť podľa relevantnosti z lekárskeho hľadiska (v závislosti od účelu aplikácie: inkubačný čas a pod.), ako aj podľa realistického trvania administratívnych krokov, ktoré možno bude treba podniknúť.

— Funkcia poskytovania informácií:

Ak sa počas inštalovania tejto funkcie zhromažďujú nejaké údaje, mali by sa okamžite vymazať. Uchovávanie takýchto údajov nie je nijako opodstatnené.

— Funkcia overovania príznakov a funkcia telemedicíny:

Takéto údaje by orgány verejného zdravotníctva mali vymazať maximálne po jednom mesiaci (inkubačný čas plus bezpečnostná rezerva) alebo po otestovaní osoby s negatívnym výsledkom. Orgány verejného zdravotníctva môžu archivovať údaje aj na dlhšie obdobia na účely správ o dohľade a na účely výskumu za predpokladu, že údaje sú v anonymizovanej podobe.

— Funkcia sledovania kontaktov a výstrahy:

Údaje o blízkosti by sa mali odstrániť ihneď po tom, ako prestanú byť potrebné na účely upozorňovania jednotlivcov. Malo by sa to stať maximálne po jednom mesiaci (inkubačný čas plus bezpečnostná rezerva) alebo po otestovaní osoby s negatívnym výsledkom. Orgány verejného zdravotníctva môžu archivovať údaje o blízkosti aj na dlhšie obdobia na účely správ o dohľade a na účely výskumu za predpokladu, že údaje sú v anonymizovanej podobe.

Tieto údaje by sa mali uchovávať v zariadení používateľa a na server prístupný pre orgány verejného zdravotníctva by sa mali nahrávať len údaje, ktoré používateľ oznámil a ktoré sú potrebné na splnenie účelu, ak sa zvolí takáto možnosť (t. j. nahrávať na server len údaje o „blízkych kontaktoch“ osoby, ktorá bola pozitívne testovaná na infekciu COVID-19).

3.8 **Zaistenie bezpečnosti údajov**

Komisia odporúča, aby sa údaje uchovávali v koncovom zariadení jednotlivca v šifrovanej podobe s použitím najmodernejších kryptografických techník. V prípade uchovávania údajov na centrálnom serveri by sa mal prístup – vrátane administratívneho prístupu – protokolovať.

Údaje o blízkosti by sa mali generovať a ukladať do koncového zariadenia jednotlivca len v šifrovanom a pseudonymizovanom formáte. S cieľom znemožniť sledovanie tretími stranami by malo byť možné aktivovať technológiu Bluetooth bez toho, aby sa museli aktivovať iné lokalizačné služby.

Počas zhromažďovania údajov o blízkosti prostredníctvom technológie BLE sa preferuje možnosť vytvárať a ukladať dočasné používateľské identifikačné čísla, ktoré sa budú pravidelne meniť, a nie ukladať skutočné identifikačné číslo zariadenia. Toto opatrenie poskytuje dodatočnú ochranu proti odpočúvaniu a sledovaniu hackermi, takže sťažuje identifikáciu jednotlivca.

Komisia odporúča zverejniť zdrojový kód aplikácie a sprístupniť ho na preskúmanie.

Možno uvažovať aj o ďalších opatreniach na zabezpečenie spracúvaných údajov, najmä automatickým vymazaním alebo anonymizáciou údajov po určitom čase. Stupeň bezpečnosti by mal vo všeobecnosti zodpovedať množstvu a citlivosti spracúvaných osobných údajov.

Všetky prenosy údajov z osobného zariadenia vnútroštátnym orgánom verejného zdravotníctva by mali byť šifrované.

Ak sa vo vnútroštátnych právnych predpisoch stanovuje, že zhromaždené osobné údaje sa môžu spracúvať aj na účely vedeckého výskumu, v zásade by sa mala použiť pseudonymizácia.

3.9 **Zaistenie presnosti údajov**

Zaistenie presnosti spracúvaných osobných údajov je nielen predpokladom účinnosti aplikácie, ale je aj požiadavkou podľa právnych predpisov o ochrane osobných údajov.

V tejto súvislosti je nevyhnutné zabezpečiť presnosť informácií o tom, či došlo ku kontaktu s infikovanou osobou (epidemiologická vzdialenosť a trvanie), aby sa minimalizovalo riziko falošne pozitívnych informácií. Mali by sa riešiť scenáre, keď sú dvaja používatelia aplikácie v kontakte na ulici, vo verejnej doprave alebo v budove. Je málo pravdepodobné, že používanie lokalizačných údajov z mobilných telefónnych sietí je dostatočne presné na tento účel.

Z tohto dôvodu sa odporúča opierať sa o technológie umožňujúce presnejšie posúdenie kontaktu (napríklad Bluetooth).

3.10 **Zapojenie orgánov pre ochranu osobných údajov**

Orgány pre ochranu osobných údajov by mali byť plne zapojené do vývoja aplikácie a konzultované v tejto súvislosti, pričom by mali dohliadať aj na jej zavádzanie. Keďže spracúvanie údajov v kontexte aplikácie sa bude považovať za spracúvanie osobitných kategórií údajov (údaje týkajúce sa zdravia) vo veľkom rozsahu, Komisia upozorňuje na článok 35 všeobecného nariadenia o ochrane údajov o posúdení vplyvu na ochranu údajov.

ISSN 1977-1037 (elektronické vydanie)
ISSN 1725-5236 (papierové vydanie)

Úrad pre vydávanie publikácií Európskej únie
2985 Luxemburg
LUXEMBURSKO

SK