MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Informace o zpracování osobních údajů v rámci aplikace eRouška 2.0

Kdo jsme

Jsme Ministerstvo zdravotnictví ČR (dále jen "ministerstvo") a provozujeme mobilní aplikaci eRouška (dále jen "aplikace"), která pomáhá ministerstvu a jemu podřízeným hygienickým stanicím při zvládání epidemie nemoci Covid-19 způsobené koronavirem SARS-CoV-2 (dále jen "koronavirus"). Tato aplikace pomocí Bluetooth technologie[1] zaznamenává setkání s ostatními telefony s nainstalovanou aplikací eRouška.
Správcem osobních údajů je ministerstvo. Na zajištění provozu aplikace eRouška se spolu s námi podílí technický dodavatel, Národní agentura pro komunikační a informační technologie, s.p. (dále jen „NAKIT") v roli zpracovatele osobních údajů, který postupuje pod naší kontrolou, v rámci uzavřené smlouvy[2] a podle našich pokynů.

Aplikace eRouška je důležitou součástí projektu Chytrá karanténa. Bližší informace o fungování celého projektu Chytrá karanténa naleznete zde

S vašimi osobními údaji pracujeme v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 (dále jen "GDPR") a v souladu se zákonem č. 110/2019 Sb., zákon o zpracování osobních údajů.

Jak to celé funguje

Včasné upozornění osob, které byly vystaveny riziku nákazy Covid-19, může významně snížit šíření této nemoci v populaci. Zajištění včasné lékařské péče u dotčené (potenciálně) nakažené osoby může významně snížit riziko zdravotních komplikací. Aby byla zajištěna včasná diagnostika osob, jež mohou být nakaženy touto nemocí, přistoupila většina států k zavedení aplikací podobných naší aplikaci eRouška.

Celý systém funguje tak, že eRouška přes technologii Bluetooth ukládá do paměti další telefony s touto aplikací v okolí. Když někdo onemocní, tak může jejím prostřednictvím

[1] přesněji Bluetooth Low Energy (dále jen „Bluetooth LE")
[2] viz Registr smluv na adrese https://smlouvy.gov.cz/smlouva/13430376

Palackého náměstí 4, 128 01 Praha 2
tel./fax: +420 224 972 457, e-mail: oia@mzcr.cz, www.mzcr.cz

snadno, pomocí notifikace, varovat ostatní před možným rizikem nákazy. Díky tomu pomáhá v boji proti koronaviru.

Proč zpracování provádíme a co nás k němu opravňuje

Účel aplikace

Mobilní aplikace eRouška pomáhá snadněji, efektivněji a rychleji upozorňovat uživatele, kteří v poslední době přišli do styku s osobami pozitivně testovanými na Covid-19 a byli přitom vystaveni vysokému riziku nákazy. Aplikaci eRouška, ani údaje z ní získané, nebudeme využívat pro jiné účely, než je provoz a další rozvoj této aplikace.

Jak jste v rámci aplikace identifikováni?

Aplikace eRouška je vyvinuta tak, aby neprováděla přímo vaši identifikaci a aby minimalizovala zpracování osobních údajů fyzických osob (dále jen „subjektů údajů“) na nejnižší možnou úroveň.

Aplikace samotná neobsahuje vaše osobní údaje. Ministerstvo zdravotnictví v tomto technickém řešení v rámci aplikace nemůže ztotožnit konkrétního uživatele aplikace, tedy ani vás.

Aplikace vám zprostředkuje informaci, že jste se v některý konkrétně určený den setkali s osobou, která byla pozitivně testována na Covid-19. Tzn., že budete za určitých okolností schopní, např. pokud jste se v daný den setkali pouze s jedinou osobou, odhadnout, kdo je tímto nakaženým. Stejné platí samozřejmě i opačně – jiný uživatel této aplikace by takto mohl ve výjimečných případech vyvodit, že tím nakaženým jste byli vy. To je ale vlastnost aplikace, kterou nelze vyloučit, protože bez toho by aplikace nefungovala řádně a nemohla by přispět k vaší větší ochraně před Covid-19. My, Ministerstvo zdravotnictví, Vás v rámci aplikace nejsme schopní ztotožnit a nejsme schopní ani zjistit, s kým jste se setkali. Celý systém je záměrně navržen tak, aby se naprosto minimalizovalo riziko zneužití údajů a aby všichni ti, kdo se na provozu aplikace podílejí, včetně společností Apple a Google, získali jen nezbytné množství údajů.

Z pohledu principů GDPR k identifikaci konkrétní osoby může dojít pouze nepřímo a ve velmi omezených případech – např. pomocí tzv. výběru vyčleněním z pohledu správce[3]

[3] recitál 26 GDPR

nebo formou zpětné reidentifikace subjektů údajů ze strany adresáta notifikace[4]; tyto situace mohou nastat pouze v případě kombinace pseudonymizovaných údajů v aplikaci eRouška, vzájemné kombinace znalostí o procesu sdílení informací a kontextu z pohledu uživatele aplikace[5].

Právní základ zpracování

Osobní údaje zpracováváme na základě čl. 6 odst. 1 písm. e) a čl. 9 odst. 2 písm. i) GDPR jako nezbytné pro splnění úkolu prováděného ve veřejném zájmu, kterým je pověřen správce v oblasti veřejného zdraví, při ochraně před vážnými přeshraničními zdravotními hrozbami. Postupujeme při tom jako ústřední orgán státní správy, a stejně jako krajské hygienické stanice plníme své úkoly dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví a dle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách).

Samotná aplikace je však vždy instalována s vaším svolením, tzn. jen vy rozhodujete, zda aplikace bude do vašeho telefonu či jiného zařízení instalována, nebo ne. Odinstalací aplikace zajistíte, že se nadále nebudete na fungování tohoto systému účastnit.

K instalaci aplikace by vás neměl nikdo nutit, ani váš zaměstnavatel ani např. vlastníci prostor, do nichž vstupujete.

Samozřejmě stále platí, že čím více osob si aplikaci nainstaluje, tím účinnější bude ochrana, kterou poskytuje.

S jakými údaji pracujeme a co s nimi děláme

Aplikace eRouška využívá Apple/Google Exposure Notification API[6] a dodržuje všechna pravidla publikovaná společnostmi Apple a Google pro použití tohoto API. Dále jsou uvedeny informace o rozsahu zpracovávaných údajů v jednotlivých fázích užívání aplikace eRouška.

---

[4] jde o teoretickou možnost reidentifikace subjektů údajů s využitím přiměřených prostředků pro identifikaci, zejména informací o tom s kým se v inkriminované době setkal

[5] správce by měl vždy uvažovat náklady a čas potřebný k takovéto identifikaci, dále dostupnou technologii v době zpracování a pravděpodobný technologický vývoj

[6] viz https://developer.apple.com/exposure-notification; https://www.google.com/covid19/exposurenotifications

Instalace, aktivace a deaktivace aplikace eRouška

Instalace aplikace probíhá standardním způsobem z Apple Store nebo Google Play.

Při prvním spuštění po instalaci dojde k aktivaci aplikace. Při aktivaci je každé aplikaci přidělen a na serveru eRouška zaevidován náhodný unikátní identifikátor (instance aplikace) eHRID, který slouží k administrativním účelům správy nainstalovaných aplikací – např. k počítání aktivních aplikací a ochraně proti spamu při sbírání statistik o provozu. eHRID je pseudonymní identifikátor, který slouží pouze těmto účelům a není na straně serveru eRouška propojen s žádnými dalšími identifikátory vašeho mobilu, ani s žádnými osobními identifikátory, a v případě předávání klíčů nakaženého (viz dále) ani s těmito klíči.

Pro běžný provoz (viz níže) aplikace vyžaduje souhlas se zapnutím Bluetooth a souhlas se zapnutím Oznámení o možném kontaktu (Exposure Notification API). Jde o funkce operačního systému telefonu, bez jejichž aktivace není možné aplikaci eRouška používat.

Při odinstalování aplikace je zrušena vazba mezi zařízením a identifikátorem eHRID přiděleném při aktivaci. Pokud je aplikace na zařízení, ze kterého byla odinstalována, opět aktivována, je jí přidělen nový identifikátor eHRID. Veškeré typy možných údajů jsou tedy uloženy jen uvnitř tohoto zařízení, resp. aplikace eRouška.

Běžný provoz aplikace eRouška

Aplikace eRouška generuje v rámci svého běžného provozu každých 10-20 minut náhodná ID (tzv. klíče), která si ukládá a následně vyměňuje prostřednictvím Bluetooth LE technologie s dalšími aktivními aplikacemi eRouška v dosahu Bluetooth signálu (řádově ve vzdálenosti jednotek metrů). Aplikace eRouška nezná a nezaznamenává vaši polohu, pouze na vašem mobilu zaznamenává klíče ostatních aplikací eRouška, které „potkala“ spolu s informací o čase, době trvání kontaktu a síle Bluetooth signálu. Klíče ostatních aplikací, se kterými se eRouška setkala, eviduje po dobu 14 dnů, poté jsou tyto klíče smazány.

Klíče ostatních aplikací eRouška, zaznamenané při setkání, jsou náhodné a mění se v čase, a proto nelze z aplikace zpětně konkrétně zjistit, koho jste potkal(a). Klíče cizích aplikací navíc zůstávají uložené pouze ve vašem zařízení, server eRouška nemá žádné záznamy (ani anonymizované), která zařízení byla v kontaktu. Ke klíčům cizích aplikací uloženým na vašem zařízení nemáte jako uživatel aplikace přístup ani vy.

Jako uživatel aplikace máte možnost výše uvedený provoz aplikace eRouška pozastavit. Poté, co na hlavní obrazovce aplikace stisknete tlačítko „Pozastavit eRoušku“, aplikace

přestane vysílat svoje klíče a přestane zaznamenávat a ukládat klíče ostatních aplikací. Téhož efektu uživatel aplikace dosáhne, pokud v nastavení svého telefonu vypne Bluetooth nebo Oznámení o možném kontaktu (Exposure Notification API).

Co se děje, když jsem nakažený

Informace o tom, že jste onemocněli nemocí Covid-19, vám může poskytnout výhradně pracovník hygienické služby nebo váš ošetřující lékař na základě laboratorních výsledků provedeného testu. **Aplikace eRouška neslouží ke zjištění nákazy, ani není určena k informování o pozitivním výsledku laboratorních testů.** Cílem aplikace je pouze identifikovat osoby, které byly v rizikovém kontatku s nakaženou osobou a těmto osobám poskytnout informace, jak v takové situaci postupovat.

Pokud jste podstoupili vyšetření na onemocnění Covid-19 a váš test byl pozitivní, bude vás kontaktovat pracovník hygienické služby a v rámci epidemiologického šetření s vámi zjistí upřesňující údaje pro vyhodnocení rizikových setkání, jako je infekční období (na základě termínu objevení příznaků) a rizikovost (na základě intenzity příznaků a prostředí, ve kterém se pohybujete). V závěru epidemiologického rozhovoru se vás pracovník hygienické služby dotáže, zda používáte aplikaci eRouška, a zda vám může odeslat ověřovací kód pro předání klíčů z vaší aplikace. Smyslem tohoto kroku je autorizace vaší aplikace eRouška k odeslání klíčů ostatním uživatelům aplikace eRouška, aby mohli vyhodnotit, zda s vámi byli v rizikovém kontaktu. Autorizace proběhne formou odeslání jednorázového náhodného kódu, který vám přijde prostřednictvím SMS.

Autorizační kód je vygenerován serverem eRouška, předán informačnímu systému hygienické služby, který zajistí jeho odeslání prostřednictvím SMS. Celý proces vytvoření a zpracování potvrzovacího kódu je navržen tak, aby server eRouška získal pouze jednorázový náhodný autorizační kód, ale žádné identifikátory, které by mohly identifikovat nakaženého. Server eRouška tedy nezná identitu nakaženého.

Platnost jednorázového autorizačního kódu je 15 minut. V informačním systému hygienické služby se jednorázový autorizační kód neukládá.

Po obdržení potvrzovacího kódu použijte v aplikaci eRouška funkci „Odeslat data“, která vyžaduje vložení autorizačního kódu a po jeho zadání odešle data na server eRoušky. Odeslání vašich dat (klíčů), tj. odeslání informace, že je uživatel dané aplikace eRouška nakažený, je z vaší strany dobrovolné a současně je podmíněné autorizací ze strany hygienické služby, tak aby nebylo možné tuto informaci zaslat omylem a také nebylo možné aplikaci eRouška zneužít.

Při odeslání klíčů posílá aplikace eRouška pouze vlastní klíče, tj. klíče, které při setkání s jinými aplikacemi „vysílala“. Proto jsou odeslané klíče nazývány klíči nakažené osoby. Nedochází k odeslání klíčů ostatních aplikací, se kterými se vaše aplikace setkala.

Vyhodnocení rizikového kontaktu

Server eRouška vystavuje všechny přijaté klíče nakažených osob pro stažení. Klíče jsou na serveru eRoušky uchovávány 14 dní, poté jsou smazány.

Všechny aktivní aplikace eRouška pravidelně stahují nové klíče nakažených osob a vyhodnocují, jestli odpovídají cizím klíčům zaznamenaným při setkání a jestli délka kontaktu a síla signálu odpovídají kritériím pro rizikový kontakt. V případě, že Vaše aplikace eRouška na základě takto zpracovaných dat vyhodnotí, že došlo k rizikovému kontaktu, vygeneruje lokální notifikaci (např. zobrazí na vašem telefonu informační okno, podle nastavení notifikací ve vašem telefonu), upozorní vás na rizikový kontakt a zobrazí vám pokyny, jak postupovat. Vše probíhá v rámci instalace aplikace uložené ve vašem telefonu tzn., že nikdo jiný se o tomto kroku nedozví.

Notifikace obsahuje pouze pozitivní informaci, že jste byli pravděpodobně vystaveni rizikovému kontaktu s nakaženou osobou a den kontaktu (další podrobnosti ani přesnější informace o čase, či místu kontaktu s nakaženým aplikace eRouška nemá a nelze je zjistit). Aplikace eRouška nemá informaci, kdo je nakažená osoba, dokonce ani nedokáže identifikovat její anonymní[7] klíče nakažené osoby, neboť ty jsou v Exposure Notification API zpracovávány v dávkách a není jasné, který konkrétní klíč z dávky byl vyhodnocen jako rizikový kontakt.

Informaci o rizikovém kontaktu obdržíte pouze vy jako uživatel aplikace, ve které k vyhodnocení došlo, nemá ji ani server eRouška, ani nakažená osoba, se kterou jste se setkali, ani hygienická služba. **Upozrňujeme: Na základě notifikace v aplikaci eRouška vás nebude nikdo kontaktovat, protože nikdo nezná vaše kontaktní údaje ani neví, že k vyhodnocení rizikového kontaktu došlo právě u vás.**

Aplikace eRouška odesílá na server kromě eHRID pouze anonymní statistickou/agregovanou informaci, že došlo k notifikaci rizikového kontaktu. Tato informace není vázána na žádný identifikátor uživatele ani jeho mobilu a slouží pouze ke kalkulaci statistických informací o účinnosti systému eRouška kolik bylo vygenerováno notifikací,

[7] proces anonymizace údajů nevylučuje použití konvenčních pseudonymizačních technik, pokud jsou zavedeny kontrolní mechanismy na straně správce, které zabraňují jakkoliv získat či poskytovat identifikovatelné údaje o fyzických osobách třetím stranám či jiným subjektům údajů

jaký je poměr počtu notifikací k počtu nakažených osob apod. K potvrzení autenticity zprávy využívá aplikace přidělený eHRID, ten následné stvrzuje, že zpráva přichází z aktivní aplikace eRouška, ale nemůže sloužit k vaší identifikaci.

Další zpracování

Abychom zajistili funkčnost aplikace, budeme pracovat i s **údaji o jejím fungování** (např. záznamy o pádech aplikace a používání aplikace) na vašem telefonu a budeme k tomu používat standardní nástroje (Firebase Crashlytics a Google Analytics) od společnosti Google. Telemetrická data odesílaná aplikací do těchto služeb neobsahují identifikátory vaší osoby nebo vašeho telefonu (jako je například tel. číslo, IMEI, AdvertisingID) a zpracováváme je za účelem vyhledávání a odstraňování kritických chyb, evidenci aktualizací aplikace a statistického zmapování používání aplikace uživateli. Aplikace nezná vaše osobní údaje, a tato telemetrická data tak nelze žádným způsobem navázat na vaši osobu. S takto získanými telemetrickými údaji pracujeme maximálně po dobu 180 dní.

Kde s Vašimi údaji pracujeme

S Vašimi osobními údaji budeme pracovat jen na území EU a v důvěryhodných třetích zemích, kde jsou umístěny servery společnosti Google, která jako subzpracovatel poskytuje prostřednictvím zpracovatele část serverových služeb pro fungování aplikace. Předání do zahraničí se řídí podle standardních smluvních doložek, což jsou nástroje, které podle GDPR zajišťují dostatečnou ochranu vašich práv. Vaše údaje budou tedy zpracovávány u ověřených a dostatečně důvěryhodných zpracovatelů a subzpracovatelů.

Kdo má k Vašim údajům přístup

Údaje uvedené v tomto dokumentu jsou primárně uložené ve vašem telefonu a přístup k nim máte pouze vy. Ministestvo zdravotnictví a ostatní uživatelé aplikace eRouška mají přístup pouze k anonymním klíčům nakažených osob, které jsou odesíláním prostřednictvím serveru eRouška všem ostatním užiatelům. Ministerstvo zdravonictví má dále přístup k identifikátorům instalovaných aplikací eRouška eHRID, využívaným pro statistické účely a v případě technických problémů k anonymním crash logům vaší aplikace pro účely odstraňování kritických chyb.

Vaše práva

Právní předpisy na ochranu osobních údajů, zejména GDPR, vám zaručují různá práva v oblasti ochrany osobních údajů: V rozsahu, v jakém vám to garantují předpisy na ochranu osobních údajů a kontextu daného zpracování osobních údajů můžete od ministerstva jakožto od správce požadovat výmaz dle čl. 17 GDPR (a to vždy, pokud jsou pro to splněny zákonné podmínky). Výmaz je možné technicky uskutečnit pomocí odinstalace aplikace eRouška ze svého telefonu. Vaše náhodná ID (tzv. klíče) jsou automaticky smazána po 14 dnech, tak jak je již uvedeno v úvodu.

Pro uplatnění jakéhokoliv z těchto práv prosím kontaktujte pověřence pro ochranu osobních údajů:

Ministerstvo zdravotnictví ČR
Pověřenec pro ochranu osobních údajů
Palackého nám. 4
128 01 Praha 2

IČO: 00024341

tel.: +420 224 972 457
e-mail: oia@mzcr.cz
web: www.mzcr.cz

Pokud byste se domnívali, že zpracování Vašich osobních údajů porušuje právní předpisy, můžete podat stížnost u národního dozorového úřadu, kterým je Úřad pro ochranu osobních údajů (www.uoou.cz).

Rizika s používáním aplikace spojená

Aplikace eRouška je navržena tak, aby naprosto minimalizovala okruh zpracovávaných údajů a riziko jejich zneužití. Za tím účelem je v ní zapracována celá žada ochranných prvků, počínaje tím, že my, Ministerstvo zdravotnictví, nejsme nijak schopni konkrétně ztotožnit uživatele aplikace.

Nicméně použití technologie Bluetooth – která je ovšem pro fungování aplikace nezbytná – s sebou nese určitá rizika a související podmínky provozování, které jsou popsány zde.

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Jak využíváme cookies

Informace o využívání cookies na webu erouska.cz naleznete na stránce Informace o cookies.

Palackého náměstí 4, 128 01 Praha 1
tel./fax: +420 224 972 457, e-mail: oia@mzcr.cz, www.mzcr.cz