MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

eRouška

POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

DATA PROTECTION IMPACT ASSESMENT (DPIA)

Projekt: eRouška 2.0

Verze 6, 4. 2. 2021

Obsah

1 Slovník pojmů a zkratek

Aplikace	Aplikace eRouška
COVID-19	Onemocnění způsobené koronavirem SARS-CoV-2
DPIA	Posouzení vlivu na ochranu osobních údajů dle Obecného nařízení na ochranu osobních údajů – článek 35
EDPB	Evropský sbor pro ochranu osobních údajů
eHN	eHealth Network
EK	Evropská komise
eRouška	Mobilní aplikace trasující vzájemné kontakty uživatelů
EU	Evropská unie
GDPR	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)
Chytrá karanténa	Chytrá karanténa je systém, který vede k včasnému zachycení, testování infekčního onemocnění COVID-19 a izolaci v karanténě co největšího počtu potenciálně nakažených osob s využitím elektronických nástrojů.
MZ ČR	Ministerstvo zdravotnictví České republiky
NDA	Dohoda o mlčenlivosti
Obecné nařízení	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)
Posouzení vlivu	Posouzení vlivu na ochranu osobních údajů dle Obecného nařízení na ochranu osobních údajů – článek 35
ÚOOÚ	Úřad pro ochranu osobních údajů
Uživatel	Osoba, která si na svém chytrém telefonu nainstalovala aplikaci eRouška
WHO	World Health Organization (Světová zdravotnická organizace)
WP 29	Working Party 29 – Pracovní skupina pro ochranu údajů podle článku 29

2 Historie změn

Datum	Verze	Popis změny
25.5.2020	1.00	Souhrnná vstupní DPIA
19.6.2020	2.00	Vypořádání komentářů a revize
20. 7. 2020	3.00	Finální DPIA k projektu eRouška 1.0
22.7.2020	4.00	Stanovisko pověřence
14. 10. 2020	5.00	Verze pro eRouška 2.0
4.2.2021	6.00	Zapracování EFGS varianta souhlasu – po obdržení stanoviska ÚOOÚ

3 Obecná východiska

Při tvorbě tohoto Posouzení vlivu bylo primárně vycházeno z Obecného nařízení, a to konkrétně z článku 35 GDPR.

Je důležité upozornit, že hodnocení epidemiologického nebo medicínského významu či užitečnosti aplikace eRouška není předmětem této analýzy. Tato analýza se zabývá dodržováním právních předpisů na ochranu osobních údajů, dopadem na subjekty údajů a dalšími souvislostmi, které ovlivňují vztah mezi správcem osobních údajů, tedy MZ ČR a uživatelem aplikace.

3.1 Správce

- **Ministerstvo zdravotnictví a jemu podřízené hygienické stanice**
- V rámci přeshraniční výměny informací spolupracuje Ministerstvo zdravotnictví se správci obdobných aplikací jednotlivých států EU (tzv. "národních aplikací") na základě Prováděcího rozhodnutí komise (EU) 2020/1023 ze dne 15. července 2020. Společně se správci národních aplikací jednotlivých zúčastněných států, resp. jejich příslušnými orgány, jejichž seznam naleznete na tomto odkaze, je Ministerstvo zdravotnictví společným správcem **Evropské federační brány (EFGS)**, jejímž prostřednictvím si národní aplikace vyměňují informace.

3.2 Zpracovatel

- **Národní agentura pro komunikační a informační technologie, s.p.** (dále jen „NAKIT“), která postupuje pod kontrolou MZ, v rámci uzavřené smlouvy (viz Registr smluv[1]) a podle pokynů MZ.
- **Google Ireland Limited** (další zpracovatel dle čl. 28 odst. 2 a 4 GDPR, dále jen „Google“). Služby Google Ireland limited jsou aktuálně (na základě veřejné zakázky) zprostředkovány prostřednictvím poddodavatele NAKIT, res. jeho dalšího poddovatele/společnosti Revolgy Business Solutions s.r.o.

3.3 Cílová skupina

- Ministerstvo zdravotnictví
- Úřad pro ochranu osobních údajů
- Laická i odborná veřejnost, experti v technické a právní oblasti
- Provozovatel, výrobce a ostatní zúčastněné entity
- EU

3.4 Délka zpracování údajů

Údaje jsou zpracovávány po dobu 14 dní. Doba uchování pseudonymizovaných údajů je omezena na dobu významnosti jejich samotného použití vzhledem k hodnocení infekčnosti uživatelů eRouška.

[1] https://smlouvy.gov.cz/smlouva/13430376.

3.5 Dokumenty vztahující se k metodice Posouzení vlivu

- ÚOOÚ – Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů[2]
- ÚOOÚ – Metodika obecného posouzení vlivu na ochranu osobních údajů[3]
- EK – Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů[4]
- WP 29 - Opinion 03/2013 on purpose limitation. Working Paper WP 203[5]
- WP 29 - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, as last revised and adopted on 4 October 2017. Working Paper WP 248[6]
- EDPB – Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak[7]
- EDPB – Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak[8]
- EDPB – Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[9]
- EU – 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)[10]

3.6 Obsah

Základní obsahové náležitosti stanoví Obecné nařízení tak, že DPIA obsahuje alespoň:

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

3.7 Cíle

Toto posouzení vlivu na ochranu osobních údajů má za cíl:

---

[2] 10.5.2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.
[3] 10.5.2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38693.
[4] 12.5.2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42048.
[5] 10.5.2020 - https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[6] 10.5.2020 – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[7] 9.5.2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42042.
[8] 9.5.2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42043.
[9] 9.5.2020 – https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.
[10] 9.5.2020 – https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

1. ověřit a zajistit dostatečnou ochranu osobních údajů a práv subjektů údajů;
2. vysvětlit funkčnost aplikace eRouška;
3. navrhnout případná konkrétní řešení vedoucí ke zlepšení.

4 Úvod

Úvodem je třeba konstatovat, že k využití moderních technologií, zejména pak chytrých telefonů s Bluetooth, přistoupila celá řada států, za účelem efektivního dohledání potenciálně nakažených osob. Jednotlivé přístupy se liší jak využitými technologiemi, tak systémem sběru a uložení dat až po respektování principů ochrany osobních údajů. Jižní Korea, Taiwan, Singapur nebo Izrael akceptovali poměrně striktní přístup, kdy preferují jednoznačně zájem společnosti, respektive státu, nad právem ochrany soukromí jednotlivce. Evropský přístup se liší zejména ohledem na práva subjektů údajů. Panevropské konsorcium pro zachování soukromí (PEPP-PT) a projekt DP-3T nastavily základ pro vývoj aplikací sledující uživatele s ohledem na ochranu soukromí**. Ke standardizaci v oblasti aplikací pomáhajících v boji proti onemocnění COVID-19 sehrál podstatnou roli i eHealth Network[11] se svým „Common EU Toolbox for Member States"**[12] a další aktivity vedoucí ke standardizaci přeshraniční interoperability[13].

Vývoj aplikace by měl respektovat jedno ze základních pravidel GDPR, tedy „protection by design". Jinými slovy již při vývoji aplikace je třeba respektovat právo na ochranu osobních údajů uživatelů. Ochrana soukromí a zpracovávaných dat je tedy nedílnou součástí celého systému eRouška, bez negativního dopadu na její celkovou funkčnost. Součástí takového přístupu je i analýza rizik spojená s užíváním aplikace, strukturou dat, jejich uložením, retenční dobou apod. Kromě těchto technických aspektů vývoje aplikace patří k zodpovědnému vývoji i provedení posouzení vlivu dopadu na ochranu osobních údajů, tedy tzv. DPIA[14] (Data Protection Impact Assesment). Základní obsahové náležitosti stanoví obecné nařízení tak, že DPIA obsahuje alespoň:

- systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;

[11] Evropská komise, eHealth Network – 22.10.2020: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[12] Evropská komise, eHealth Network – 22.10.2020.
[13] Evropská komise, eHealth Network – 22.10.2020: https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilityspecs_en.pdf.
[14] DPIA je povinen provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob.

- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
- posouzení rizik pro práva a svobody subjektů údajů; a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Od druhé poloviny roku 2020 dochází k postupné konvergenci na distribuované řešení založené na protokolu Apple/Google Důsledky z hlediska ochrany osobních údajů, a tedy z hlediska základních práv, budou mít dopad nejen na jednotlivce, ale i na společnost jako celek. Vzhledem k výše uvedeným skutečnostem je třeba připravit i DPIA k takovému projektu.

Hned v úvodu článku 35, odstavci 1 Obecného nařízení o ochraně osobních údajů se uvádí, že „Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.[15]“ V této souvislosti lze konstatovat, že dle dosavadních zjištění správce u projektu eRouška 2.0 v zásadě vykonává odpovědnost stanovenou Obecným nařízením v článku 5, odstavci 2 v souladu s požadavky na ochranu osobních údajů.

Cílem tohoto Posouzení vlivu je výhradně identifikovat rizika a ochranná opatření podle kritérií definovaných GDPR. Smyslem je analyzovat účinky na všechna základní práva a svobody fyzických osob při zvážení veškerých zpracování osobních údajů. Posouzení vlivu se nezabývá jen samotnou aplikací eRouška 2.0, ani se nezaměřuje jen na významnou část technologie, ale chápe proces zpracování jako celek, sestávající se z několika zpracovatelských činností osobních údajů, v nichž probíhají procesy nebo série procesů – částečně podporovaných technologií. Samotná aplikace není komplexním (celým) zpracováním osobních údajů. Zásadním kritériem je proto chápání rizik z pohledu subjektů údajů.

4.1 Obecné přístupy

K řešením, která se nabízí, patří jak OpenTrace, na kterém bylo založeno řešení eRoušky 1.0 nebo původní polské řešení, tak například Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT/PEPP[16]). Jedná se o otevřený protokol, který má usnadnit trasování digitálních kontaktů infikovaných účastníků. Dalším nabízejícím se řešením je Decentralized Privacy-Preserving Proximity Tracing (DP^{3}T[17]). Jedná se také o otevřený protokol, který stejně jako konkurenční protokol Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), využívá technologii Bluetooth Low Energy (BTLE[18]) ke sledování a protokolování setkání s ostatními uživateli dané aplikace. Protokoly se mezi sebou liší svým mechanismem vykazování, protože protokol PEPP-PT vyžaduje, aby klienti odesílali protokoly kontaktů na centrální server, zatímco u systému DP-3T nemá nikdy centrální server přístup k protokolům kontaktů ani neodpovídá za zpracování a

[15] 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) – 14.5.2020 – https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679.

[16] PEPP PT – 10.5.2020 – https://www.pepp-pt.org/datenschutz.

[17] DP-3T Whitepaper – 11.5.2020 - https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[18] Bluetooth Low Energy – 13.5.2020 - https://en.wikipedia.org/wiki/Bluetooth_Low_Energy.

informování klientů o uskutečněném kontaktu. Protože protokoly kontaktů u DP^{3}T nejsou nikdy přenášeny na třetí strany, má oproti přístupu PEPP-PT hlavní výhody v oblasti ochrany soukromí. Této ochrany osobních údajů je však dosaženo na úkor většího výpočetního výkonu na straně klienta při zpracování zpráv o možné infekci.

Za podstatný moment lze považovat vstup Apple/Google řešení **Exposure Notification** (EN) API, které po technologické linii prosazuje decentralizovaný přístup. Hlavním přínosem řešení Apple/Google je vyšší míra ochrany osobních údajů za cenu snížení efektivity epidemiologického šetření, dále pak korektní fungování na operační platformě iOS, resp. obecně fungování garantované výrobci mobilních OS a možnost přeshraniční interoperability. Toto jsou také důvody, pro které bylo u nové verze aplikace eRouška 2.0 zvoleno řešení Apple/Google.

Uvedené protokoly nejsou samotnými aplikacemi. V případě iOS jde o sadu funkcí operačního systému, v případě Android o sadu funkcí knihovny Google Play Services. Případné aplikace mohou využít těchto protokolů k záznamům o setkání jednotlivých Bluetooth zařízení. Jedná se tedy o systém zpracování dat, ale implementace se budou lišit v závislosti na jednotlivých aplikacích. Smyslem je nabídnout svobodu jednotlivým státům v řešení trasovací aplikace, ale zároveň zajistit fungování přeshraniční interoperability. V této souvislosti je klíčovým aspektem skutečnost, že výše uvažované protokoly nespecifikují důležité technické vlastnosti a charakteristiky, které by měly závažné důsledky pro ochranu osobních údajů. Podstatným momentem se tedy stává architektura samotné aplikace a trasovacího systému. Principiálně lze rozlišit tři základní přístupy:

a) **Centralizovaná architektura**: Anonymita uživatelů a důvěrnost dat o kontaktech je poskytována pouze s ohledem na vnější subjekty, tedy ostatní uživatele nebo externí aktéry; provozovatel a ostatní zúčastněné autority (např. epidemiologové) mohou identifikovat všechny uživatele a propojit je k zaznamenané a uskutečněné historii kontaktů.
b) **Částečně decentralizovaná architektura**: Uživatelé a data o uskutečněných kontaktech jsou skryta pouze před ostatními uživateli a třetími stranami; server však může de-anonymizovat pozitivně testované uživatele. Systém má také funkci odeslání dat, díky níž uživatelé mohou rozhodnout o sdílení své historie uskutečněných kontaktů pro účely epidemiologického výzkumu. Pokud uživatel data odešle, provozovateli a ostatním zúčastněným autoritám se zviditelní potenciálně pozitivní kontakty uživatelů. Jednalo se o aktuální řešení eRoušky 1.0.
c) **Decentralizovaná architektura:** Uživatelé si zachovávají svou anonymitu vůči ostatním uživatelům a třetím stranám, jejich data o kontaktech zůstávají ostatním entitám skryté. Provozovatel a autority mohou de-anonymizovat pozitivně testované uživatele, ale nikoli jejich historii kontaktů. Epidemiologický výzkum není možný. V zásadě chybí vazba kontakt–nakažený. Jedná se o aktualizované řešení eRoušky 2.0.

Provozovatel a autority mohou	Centralizovaná architektura	Částečně decentralizovaná architektura	Decentralizovaná architektura
de-anonymizace všech uživatelů	ano	ne	ne
de-anonymizace pozitivně testovaných	ano	ano	ano

de-anonymizace dat o kontaktech	ano	částečně	ne

Tato DPIA zpracovaná pro projekt eRouška 2.0 se vzhledem k architektuře projektu týká především popisu typu decentralizované architektury, jenž je z pohledu dopadu na soukromí subjektů údajů nejvíce šetrná k procesům zpracování osobních údajů.

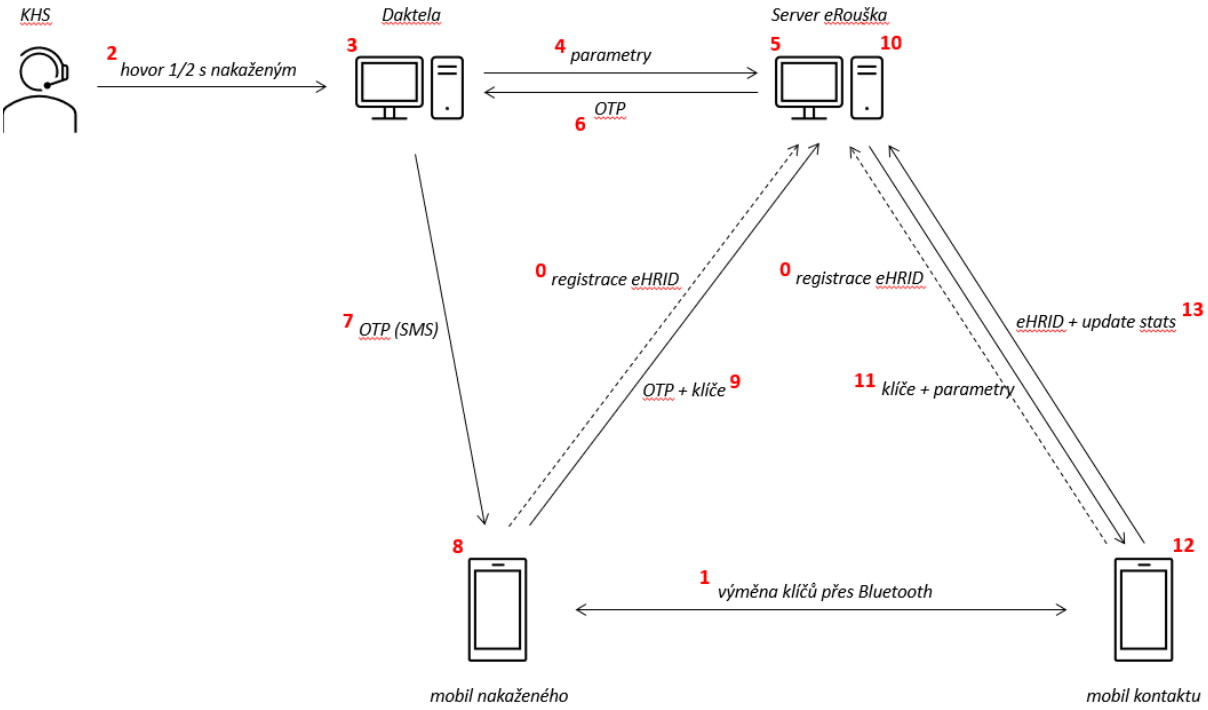
5 Popis fungování eRoušky 2.0

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 snadno, pomocí notifikace, varovat ostatní před možným rizikem nákazy.

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.

Aplikace eRouška využívá jako jediná v ČR Apple/Google Exposure Notification API (viz webové stránky společností Apple a Google) 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.

5.1 Zjednodušené schéma fungování eRoušky 2.0:



Krok	Popis
0	Při prvním spuštění aplikace vygeneruje unikátní kód instance eHRID a registruje ho na serveru eRouška. eHRID není vázán na žádné osobní údaje.
1	Mobilní aplikace generuje vlastní unikátní dočasné klíče, které si při setkání s jiným mobilem s aplikací eRouška vyměňují přes Bluetooth. Aplikace zaznamenává cizí klíče, se kterými se setká. Klíče jsou náhodné a anonymní.
2	KHS kontaktuje nakaženou osobu, provede epidemiologické šetření, v rámci kterého zaznamená v Daktele informace o datu příznaků a rizikovosti nakaženého (parametry vyhodnocování specifické pro nakaženého).
3	Pokud nakažený má eRoušku a pokud souhlasí, spustí KHS proces autorizace nakaženého k odeslání klíčů (tlačítko „eRouška“ v Daktele).
4	Daktela odešle serveru eRouška žádost o OTP (jednorázový kód) spolu s parametry vyhodnocování specifické pro nakaženého.
5	Server eRouška vygeneruje OTP, uloží si dočasný záznam s OTP a parametry (platnost 15 minut, pak smaže).

6	Server eRouška odešle OTP zpět Daktele.
7	Daktela odešle OTP na mobil nakaženého prostřednictvím SMS. Daktela OTP neukládá.
8	Nakažený stiskne tlačítko „Odeslat data“ a vyplní OTP kód (možnost předvyplnění v aplikaci z SMS).
9	Mobil nakaženého odešle na server eRouška OTP + svoje vlastní klíče
10	Server eRouška porovná OTP, doplní parametry vyhodnocování (globální i specifické pro nakaženého) a připraví klíče k distribuci ostatním mobilům. *Pozn. Tento krok ve skutečnosti zahrnuje ještě jedno nezakreslené komunikační kolečko mezi serverem eRouška a mobilem nakaženého, neboť parametry vyhodnocování musí být ve skutečnosti přiloženy ke klíčům a společně kryptograficky podepsány na mobilu.*
11	Všechny mobily si pravidelně stahují klíče a parametry vyhodnocování nových nakažených a porovnávají je s klíči zaznamenanými při setkání s jinými mobily.
12	Pokud aplikace eRouška vyhodnotí rizikový kontakt s nakaženým, vytvoří lokální notifikaci a dá uživateli instrukce, jak postupovat.
13	Aplikace eRouška aktualizuje na serveru statistiku počtu notifikací – anonymně, pouze s využitím eHRID pro ochranu proti spamu.

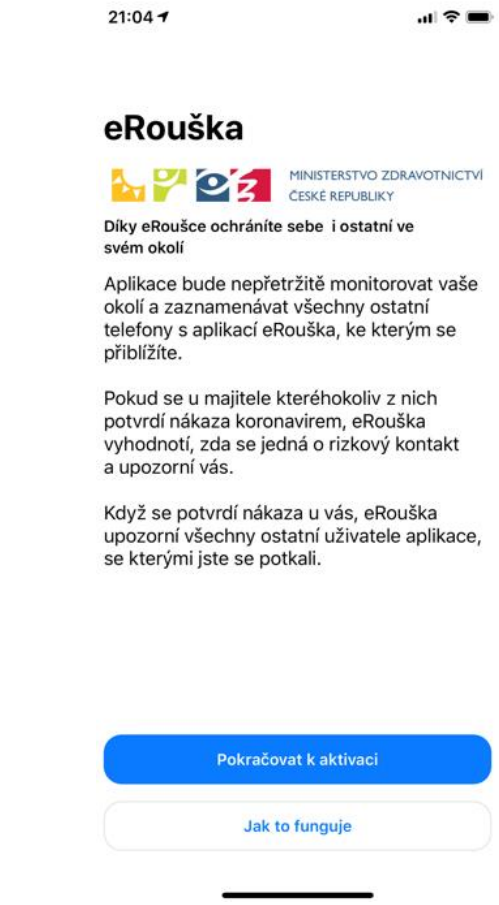
5.2 Instalace, aktivace a deaktivace aplikace eRouška

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 mobilu, ani s žádnými osobními identifikátory uživatelů, 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.

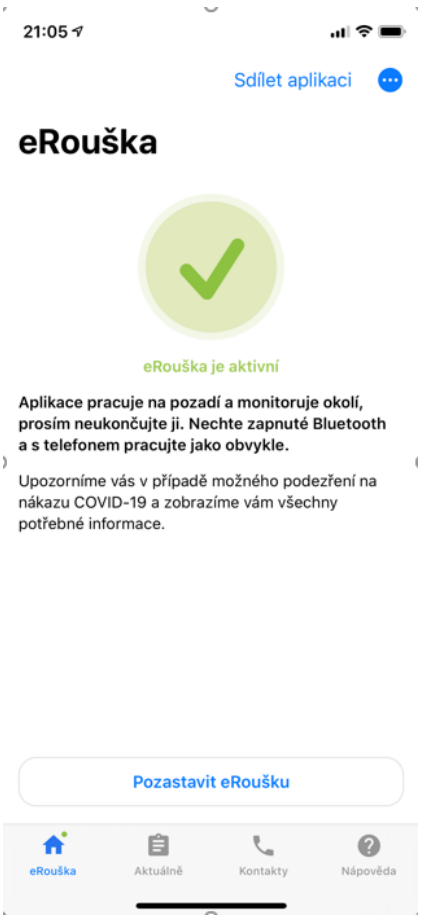


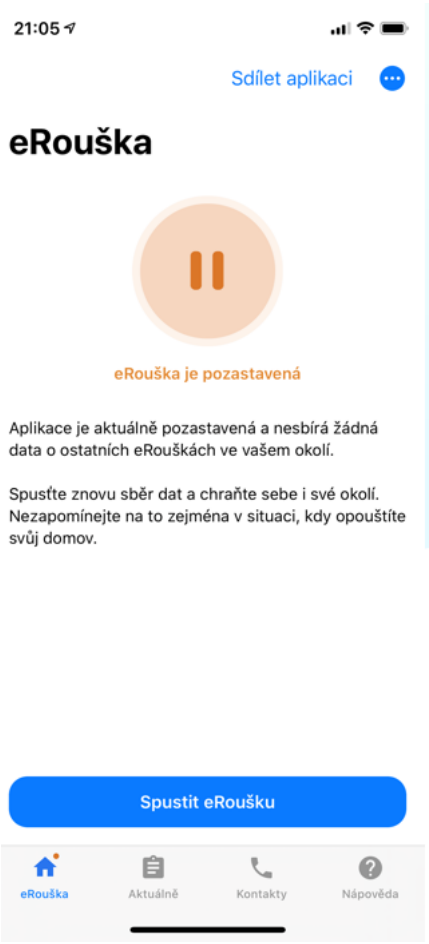
5.3 Běžný provoz aplikace eRouška

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 polohu, pouze na 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 kdo potkal. Klíče cizích aplikací navíc zůstávají uložené pouze ve v zařízení, server eRouška nemá žádné záznamy (ani pseudonymizované), která zařízení byla v kontaktu. Ke klíčům cizích aplikací uloženým v zařízení nemá uživatel aplikace přístup.

Uživatel aplikace má možnost výše uvedený provoz aplikace eRouška pozastavit. Poté, co na hlavní obrazovce aplikace stiskne 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).





5.4 Co se děje, když je subjekt údajů nakažený

Informace o tom, prokázaném onemocnění COVID-19, může poskytnout výhradně pracovník hygienické služby nebo 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 kontaktu s nakaženou osobou a těmto osobám poskytnout informace, jak v takové situaci postupovat.

Pokud osoba podstoupila vyšetření na onemocnění COVID-19 a test byl pozitivní, nastane jeden nebo oba z následujících scénářů:

- Centrální systém hygienické služby (Daktela) automaticky po obdržení výsledku z laboratoře pošle SMS s jednorázovým náhodným autorizačním kódem. Vzhledem k omezené časové platnosti jednorázového kódu jsou SMS odesílány pouze v denních hodinách.
- Bude ji kontaktovat pracovník hygienické služby a v rámci epidemiologického šetření 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 pohybuje). V závěru

epidemiologického rozhovoru se pracovník hygienické služby dotáže, zda osoba používá aplikaci eRouška, a zda jí může odeslat ověřovací kód pro předání klíčů z její aplikace.

Smyslem tohoto kroku je autorizace aplikace eRouška k odeslání klíčů ostatním uživatelům aplikace eRouška, aby mohli vyhodnotit, zda s touto osobou byli v rizikovém kontaktu. Autorizace proběhne formou odeslání jednorázového náhodného kódu, který přijde prostřednictvím SMS.

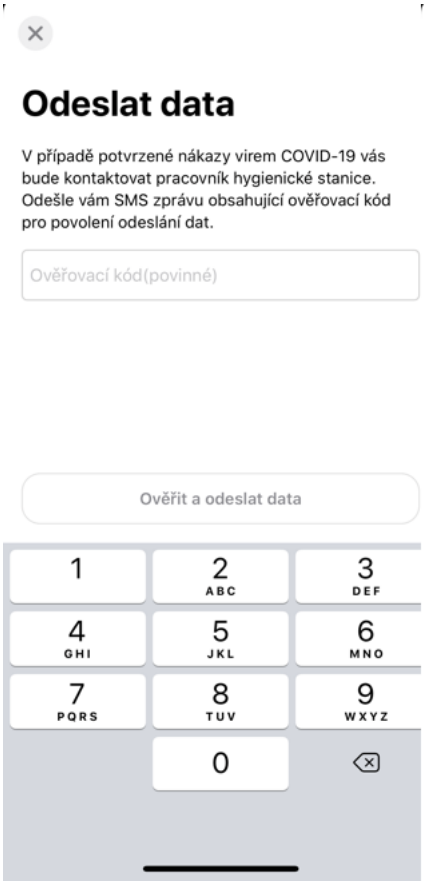
Autorizační kód je vygenerován serverem eRouška, předán informačnímu systému hygienické služby (Daktela), který zajistí jeho odeslání prostřednictvím SMS. Celý proces vytvoření a zpracování potvrzovacího kódu je navržen tak, aby server eRouška získal pouze jednorázový náhodný autorizační kód, ale žádné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

Platnost jednorázového autorizačního kódu je 12 hodin[19]. V informačním systému hygienické služby se jednorázový autorizační kód neukládá.

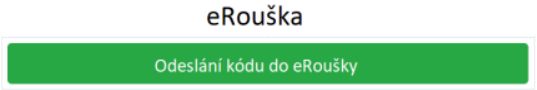
Po obdržení potvrzovacího kódu použije osoba v aplikaci eRouška funkci „Odeslat data“, která vyžaduje vložení autorizačního kódu a po jeho zadání odešle data na server eRoušky. Odeslání dat (klíčů), tj. odeslání informace, že je uživatel dané aplikace eRouška nakažený, je dobrovolné a současně je podmíněné 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.

[19] Prodlouženo z předchozího nastavení 4 hodin na základě zkušeností z reálného provozu a vyhodnocení rizik.



5.4.1 Role pracovníků hygienické stanice



Rolí pracovníků hygienické stanice je vydání autorizačního kódu nakaženým osobám. To se děje v rámci epidemiologického šetření – prvního hovoru v Daktela. Provádí se stiskem jednoduchého tlačítka v záznamu prvního hovoru s nakaženým.

Pracovník hygienické stanice se nakaženého zeptá, jestli má aplikaci eRouška a jestli je ochoten sdílet informaci o svém nakažení s ostatními uživateli eRouška a tím je varovat před rizikem nákazy. Ostatní uživatelé eRouška nepoznají identitu nakaženého a nikdo, ani hygienická služba, nebude znát seznam jeho kontaktů. Není třeba žádných speciálních souhlasů.

Pokud nakažený souhlasí, pracovník KHS stiskne tlačítko a odešle SMS s potvrzovacím kódem, který uživatel přepíše do aplikace eRouška. Jediným dalším parametrem, který Daktela odesílá spolu s potvrzovacím kódem, je datum prvních příznaků, které aplikaci eRouška umožní přesněji určit infekční období a vyhledávat kontakty pouze v tomto období.

Vydaný kód má časovou platnost 12 hodin, pokud uživatel nezadá včas, je možné odeslání kódu stiskem tlačítka opakovat.

5.4.2 Kontakty identifikované eRouškou i v rámci epidemiologckého šetření KHS

Řadu kontaktů nakaženého identifikuje jak eRouška, tak standardní epidemiologické šetření KHS. V takovém případě neplatí pro vyhledaný kontakt instrukce eRoušky, ale instrukce hygienika – tak ho informuje i eRouška. Přidanou hodnotou eRoušky je rychlost informování kontaktů a možnost dohledat i kontakty, které nakažený osobně nezná nebo si aktuálně nevzpomene (např. spolucestující v hromadné dopravě).

5.5 Vyhodnocení rizikového kontaktu

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

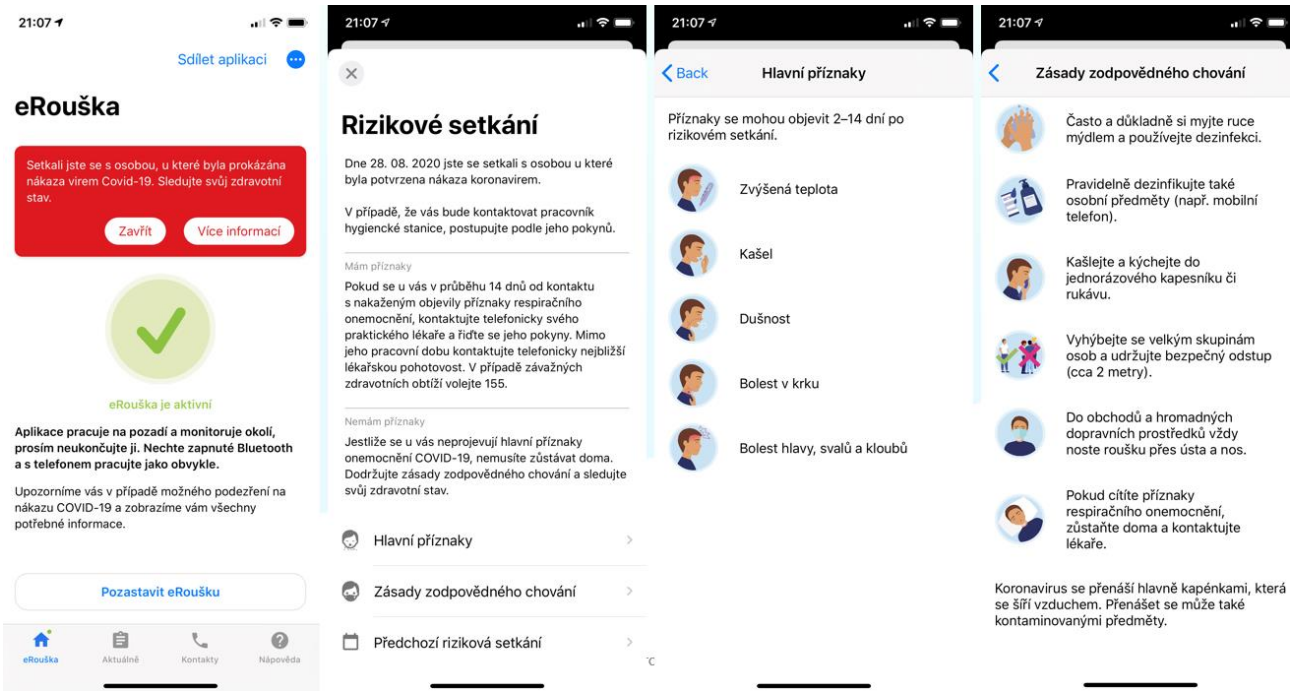
Všechny aktivní aplikace eRouška pravidelně stahují nové klíče nakažených osob a vyhodnocují, jestli odpovídají cizím klíčům zaznamenaným při setkání a jestli délka kontaktu a síla signálu odpovídají kritériím pro rizikový kontakt. V případě, že Vaše aplikace eRouška na základě takto zpracovaných dat 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[20] 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 obdrží pouze uživatel aplikace, ve které k vyhodnocení došlo, nemá ji ani server eRouška, ani nakažená osoba, se kterou jste se setkali, ani hygienická služba. **Na základě notifikace v aplikaci eRouška nebude nikdo uživatele kontaktovat, protože nikdo nezná jeho kontaktní údaje ani neví, že k vyhodnocení rizikového kontaktu došlo právě u něj.**

Aplikace eRouška odesílá na server kromě eHRID pouze pseudonymní 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, 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.

[20] Proces pseudonymizace 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.



5.6 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, Advertising ID) 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.

5.7 Kontext užití aplikace

- Dobrovolnost aplikace

Dobrovolnost užití aplikace je klíčovým prvkem celého projektu, který je založen na důvěře. V prostředí České republiky se jedná o zjevný přístup autorit a nelze hovořit o tom, že by dobrovolnost byla klamná.

- Zpracování dat zvláštní kategorie

Při zpracování dat je třeba mít neustále na paměti, že se jedná o zpracování dat, která se mohou týkat zdravotního stavu a jsou nositelem informace, která může vést k identifikaci onemocnění uživatele, tedy **dle GDPR jde o data zvláštní kategorie**. Tyto osobní údaje jsou zpracovávány s ohledem na tuto skutečnost.

- Anonymita uživatelů

Vzhledem k výše uvedeným skutečnostem je naprosto nezbytné pomocí právních, technických a organizačních opatření udržet anonymitu uživatelů v maximální možné míře. Aplikace byla vyvíjena tak, aby **neprováděla přímo identifikaci osob** a **minimalizovala zpracování osobních údajů** – princip data protection by design a data protection by default. Současně je **vývoj aplikace postavený na bázi open source serverového a aplikačního softwaru včetně všech komponent**, což je nezbytným předpokladem transparentnosti při implementaci principů ochrany osobních údajů. Princip minimalizace se neomezuje pouze na hodnocení zpracovávaných údajů z hlediska jejich technického objemu ve smyslu zpracování jednotlivých bitů, ale jde spíše o korelaci mezi zpracovávanými údaji a samotnou totožností fyzické osoby.

5.8 Apple/Google Exposure Notification API – obecný popis

Společnosti Google[21] a Apple[22] společně vytvořily systém oznámení o možném kontaktu, který pomáhá státním úřadům i globální komunitě v boji s pandemií prostřednictvím sledování kontaktů. Sledování kontaktů je technologie, kterou veřejné zdravotnické instituce používají, aby mohly kontaktovat a informovat uživatele, kteří se mohli dostat do kontaktu s osobou trpící onemocněním COVID-19. Tato technologie bude klíčovou součástí návratu k běžnému životu a úsilí o snížení rizika dalších vln pandemie. Tradiční metody sledování kontaktů jsou klíčové k zastavení šíření infekce. Toto úsilí lze podpořit technologiemi, které veřejným zdravotnickým institucím umožní rychle oznámit lidem, že mohli být v blízkosti osoby nakažené onemocněním COVID-19 (včetně osob, které možná ani neznají). Prvním krokem je technologie oznámení o možném kontaktu pro chytré telefony, které aplikacím veřejných zdravotnických institucí umožňují odesílat oznámení o tom, že jste pravděpodobně byli vystaveni onemocnění COVID-19. Aplikace ke sledování kontaktů vyvíjejí místní zdravotnické instituce, nikoliv společnosti Google a Apple.

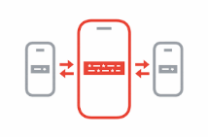
Jak to funguje?

Orgány ochrany veřejného zdraví z celého světa vyvíjejí aplikace, které prostřednictvím systému oznámení o možném kontaktu sledují kontakty uživatelů. Aplikaci pro danou oblast (pokud je k dispozici) najdou v obchodu s aplikacemi.

Když se uživatel do systému oznámení přihlásí, bude se pro jeho zařízení generovat náhodná ID. Ta se každých 10–20 minut mění, aby ho pomocí nich nebylo možné identifikovat ani lokalizovat.

[21] Google – 21.10.2020: https://www.google.com/covid19/exposurenotifications/.
[22] Apple – 21.10.2020: https://www.apple.com/cz/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

Uživatelům telefon a telefony v okolí si tato náhodná ID respektující soukromí vyměňují na pozadí přes Bluetooth. Není třeba mít aplikaci otevřenou.



Telefon pravidelně kontroluje všechna náhodná ID přidružená k pozitivním případům COVID-19 a porovnává je se svým seznamem.

Pokud najde shodu, aplikace uživateli zobrazí oznámení s pokyny od orgánu ochrany veřejného zdraví, jak chránit sebe i okolí.

Oznámení o možném kontaktu a ochrana soukromí. Společnosti Apple a Google rozumí tomu, jak je ochrana soukromí důležitá. Celý systém je detailně popsán na webových stránkách společností.[23]

Uživatel si může nastavit, zda chce dostávat oznámení o možném kontaktu. Tato technologie funguje pouze s výslovným souhlasem uživatele. Pokud změní názor, může ji kdykoli vypnout.

Systém oznámení o možném kontaktu nesleduje uživatelovu polohu. Systém oznámení o možném kontaktu nevyužívá ani nesdílí údaje o poloze zařízení. K detekci vzájemné blízkosti dvou zařízení používá Bluetooth, aniž by byla odhalena poloha zařízení.

Google, Apple ani ostatní uživatelé nezjistí uživatelovu identitu. Vyhledávání možného kontaktu probíhá přímo v zařízení. Uživatelova identita není sdílena s ostatními uživateli, Applem ani Googlem.

[23] Apple/Google, oznámení o možném kontaktu: technologie, která veřejným zdravotnickým institucím pomáhá v boji s onemocněním COVID-19 – 21.10.2020: https://www.google.com/covid19/exposurenotifications/#exposure-notifications-and-privacy .

Tento systém mohou používat pouze veřejné zdravotnické instituce. Přístup k technologii bude udělen pouze aplikacím od veřejných zdravotnických institucí. Tyto aplikace musí splňovat přísná pravidla ohledně ochrany soukromí, zabezpečení a využívání dat.

Systém je doporučován také Evropskou komisí, konkrétně pracovní skupiny eHealth Network:

„Devices should have an interoperable way to broadcast and sense proximity with other devices enabled with a contact tracing and exposure notification Bluetooth service.

Following the Bluetooth Specification[24] by Apple and Google, this means to:

1. *Broadcast and scan for the Exposure Notification Service (for detecting devices proximity), in the 16-bit service UUID section preceding the Service Data section.*
2. *Include a Service Data section containing two subsections:*
   - *A 16 byte Rolling Proximity Identifier: a privacy-preserving identifier derived from the Temporary Exposure Key and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 minutes to prevent wireless tracking of the device[25]“*

6 Server eRouška

Server eRouška je provozován v prostředí Google Cloud Platform, provozovaném společností **Google Ireland Limited,** Gordon House, Barrow Street, Dublin 4, Ireland. Server eRouška je založen na dvou hlavních serverových platformách:

- **Google Firebase** – framework pro vývoj a správu mobilních aplikací na platformách Android a iOS. Poskytuje funkce jako aktivace instance, remote config, zasílání push notifikací apod. Nezpracovává osobní údaje, pouze eHRID identifikátor instancí aplikace. Google Firebase je cloud služba nativní v prostředí Google Cloud Platform.
- **Google Exposure Notification Reference Server**. Jedná se o open source referenční implementaci serveru pro EN API aplikace Zdrojový kód referenčního serveru je k dispozici na GitHubu a lze jej nasadit na ne Google Cloud Platform nebo i na vlastní infrastruktuře nebo jiném poskytovateli cloudu. podporujícím technologii Kubernetes.

Server je zodpovědný za následující funkce:

- Přijímání klíčů nakažených uživatelů z mobilních zařízení.
- Uložení klíčů nakažených do databáze.

[24] Version 1.2, April 2020 https://covid19-static.cdnapple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotificationBluetoothSpecificationv1.2.pdf.
[25] Evropská komise, eHealth Network – 22.10.2020: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

- Pravidelně generuje přírůstkové soubory, které budou staženy mobilními zařízeními, aby bylo možné provést algoritmus shody klíčů na mobilním zařízení.
- Digitální podepisování přírůstkových souborů pomocí soukromého klíče. Odpovídající veřejný klíč je registrován u společností Apple a Google a je jejich prostřednictvím předáván implementaci EN API v mobilních zařízení.
- Pravidelně mazání starých klíčů nakažených po 14 dnech

Google Exposure Notification Reference Server má dvě hlavní komponenty:

- Exposure Notifications Verification Server (Ověřovací server oznámení o nákaze)
- Exposure Notification Reference Key Server (Referenční klíč pro oznámení o nákaze)

6.1 Exposure Notifications Verification Server

Účelem Verification serveru ve schématu eRouška 2.0 je zpracování a ověření jednorázových autorizačních kódů, včetně integrace Daktela, a poskytnutí přístupových údajů pro Key Server.

Obecné vlastnosti referenčního serveru

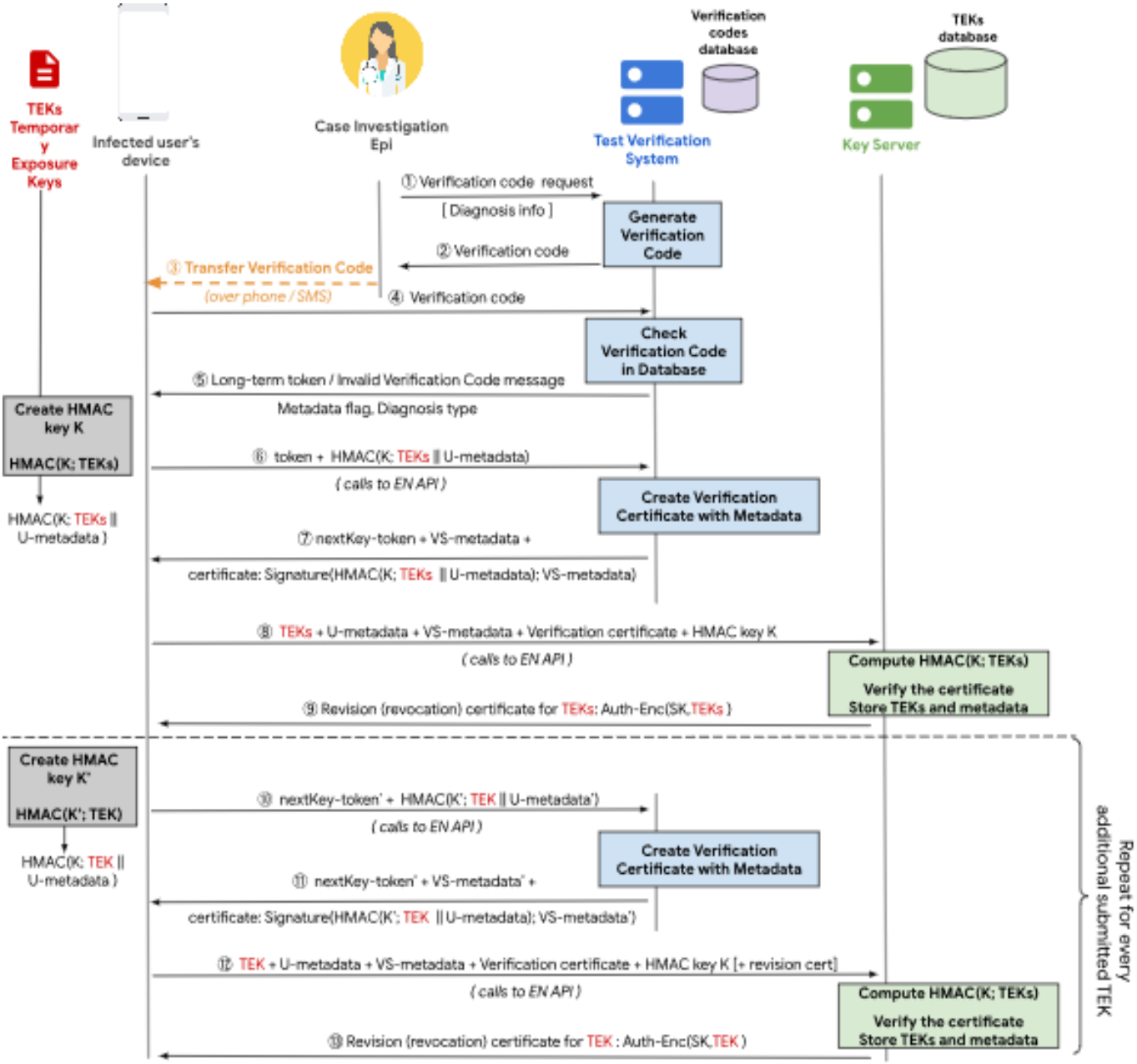
1. Ověřuje a autorizuje lidi pomocí platformy identity[26] (v eRouška 2.0 využíváno v módu ověřování jednorázových autorizačních kódů)
2. Poskytuje webové rozhraní pro epidemiology (tzv. epi) pro zadání testovacích parametrů (např. stav + datum testu) pro vydání ověřovacího kódu (v eRouška 2.0 využíváno pouze pro testovací a administrační účely, pro produkční provoz tuto funkci plní integrace s Daktela).
   - Krátké ověřovací kódy jsou obvykle 6-10 číselných číslic a lze je číst po telefonu pacientovi, posílat SMS a manuálně opisovat. Obvykle kratší platnost (využíváno eRouška 2.0, platnost aktuálně 12 hodin).
   - Delší ověřovací kódy lze zasílat přímo pacientovi prostřednictvím SMS formou tzv. deep-links. Tyto kódy obvykle mají delší platnost, 24 hodin a více (nevyužíváno eRouška 2.0, zejména z praktických důvodů podpory deep-links na některých starších verzích mobilních OS).
3. Poskytuje rozhraní API JSON-over-HTTP pro výměnu ověřovacího kódu pro ověřovací token. Toto rozhraní API se nazývá zařízení pacienta (nevyužíváno eRouška 2.0).
   - Ověřovací tokeny jsou podepsané JWT s konfigurovatelnou dobou platnosti.
4. Poskytuje rozhraní API JSON-over-HTTP pro výměnu ověřovacího tokenu za ověřovací certifikát. Toto volání rozhraní API také vyžaduje HMAC data+metatata dočasného klíče expozice (TEK). Tato hodnota HMAC[27] je podepsána ověřovacím serverem, který bude později přijat serverem oznámení o expozici. Stejná data TEK použitá ke generování HMAC zde musí být předána serveru oznámení o expozici, jinak bude požadavek odmítnut (využíváno eRouška 2.0 pro získání přístupových údajů pro Exposure Notification Key Server)

[26] Identity Platform – 21.10.2020: https://cloud.google.com/identity-platform.
[27] HMAC – 21.10.2020: https://en.wikipedia.org/wiki/HMAC.

- Viz dokumentace pro výpočet HMAC[28]
- Ověřovací certifikát je také JWT

Více se lze o následujících funkcionalitách dozvědět na stránkách GitHub[29]:

Diagram architektury



[28] HMAC Calculation – 21.10.2020: https://developers.google.com/android/exposure-notifications/verification-system#hmac-calc.
[29] GitHub – 21.10.2020: https://github.com/google/exposure-notifications-verification-server.

Podrobnosti o architektuře:

- Tato aplikace se skládá z následujících služeb, které jsou navrženy tak, aby byly nezávisle bez serveru a škálovány:
  - cmd/server – Webové uživatelské rozhraní pro vytváření ověřovacích kódů
  - cmd/apiserver – Server pro aplikace pro mobilní zařízení k ověření
  - cmd/adminapi - (volitelně) Server pro připojení stávajících PHA aplikací k ověřovacímu systému.
  - cmd/Cleanup – Server pro čištění starých dat. Vyžaduje se, aby bylo možné recyklovat a znovu použít ověřovací kódy po delší časové období.
- Databáze PostgreSQL pro sdílený stav. Jiné databáze mohou fungovat, ale v tuto chvíli se zaměřujeme pouze na podporu Postgresu.
- Redis pro ukládání do mezipaměti a distribuované omezení rychlosti.
- Platforma identity pro přihlášení.

Integrace Daktela

Informační systém hygienické služby Daktela, jehož hlavní funkcí je podpora manuálního (telefonického) trasování kontaktů nakažených osob, získává pomocí webové služby pro každého nakaženého jednorázový autorizační kód z Verification serveru. Verification server touto cestou nezíská žádné osobní údaje ani žádnou vazbu na identifikaci osoby. Server Daktela, který není součástí eRouška 2.0, krátkodobě pracuje s vazbou mezi jednorázovým autorizačním kódem a identitou nakažené osoby, odesílá nakažené osobě SMS s autorizačním kódem, autorizační kód dlouhodobě neukládá.

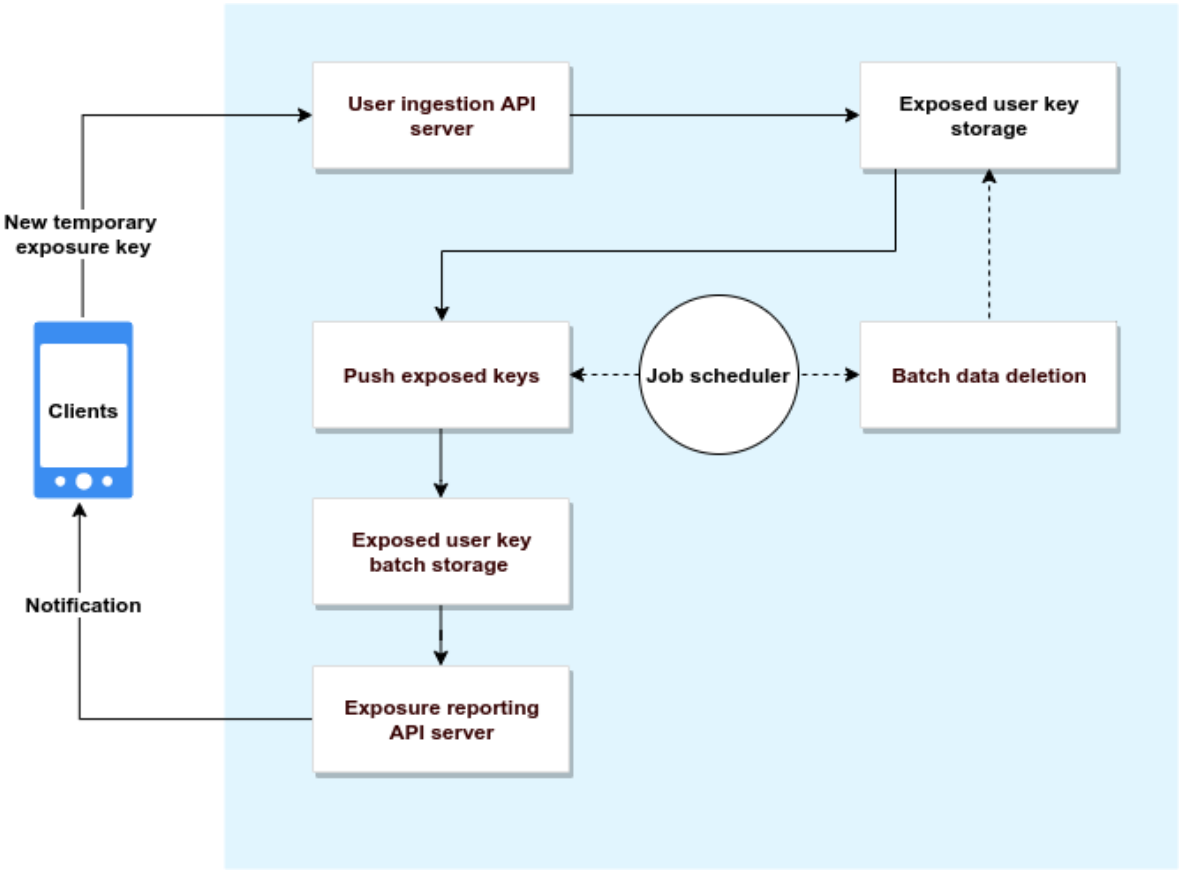
Platnost jednorázového autorizačního kódu je 12 hodin. Platnost byla prodloužena z předchozího nastavení 4 h na základě zkušeností z reálného provozu a vyhodnocení rizik – statistiky počtu klíčů nakažených neindikují podezření na zneužívání klíčů, nebyly zaznamenány žádná hlášení ani podezření na zneužívání. Prodloužení nastavení naopak řeší časté uživatelské problémy s pozdním zadáváním klíčů.

6.2 Exposure Notification Key Server

Role Key Serveru je přijímání klíčů nakažených od mobilních zařízení a jejich poskytování ostatním mobilním zařízením

Dokumentace serveru je na GitHub.[30]

Architektura:



Komponenty serveru jsou odpovědné za následující funkce:

- Přijímání klíčů nakažených z mobilních zařízení, ověřování autorizace k odeslání klíčů těchto klíčů prostřednictvím Verification serveru
- Pravidelně generovat přírůstkové soubory ke stažení klientskými zařízeními pro provádění algoritmu shody klíčů, který je spuštěn na mobilním zařízení. Přírůstkové soubory **musí být digitálně podepsány soukromým klíčem**. Odpovídající veřejný klíč je registrován u společností Apple a Google a je jejich prostřednictvím předáván implementaci EN API v mobilních zařízení.
- Databáze pro uložení publikovaných klíčů nakažených.
- Pravidelné mazání starých klíčů nakažených po 14 dnech.

6.3 Google Firebase

Google Firebase je aplikace, která pomáhá vývojovým týmům mobilních a webových aplikací zjednodušit procesy. Díky ní lze vytvářet aplikace rychle, bez správy infrastruktury. Firebase poskytuje funkce jako analytika, databáze, zasílání zpráv a hlášení o selhání, aby se vývojáři mohli rychle pohybovat a soustředit se na své uživatele. Firebase je postaven na infrastruktuře Google a automaticky se přizpůsobuje i těm největším aplikacím. Jedna platforma s produkty, které spolu lépe fungují. Produkty Firebase fungují skvěle jednotlivě,

ale sdílejí data a přehledy, takže společně fungují ještě lépe. Infrastruktura a procesy jsou podrobně a kvalitně popsány na stránkách společnosti Google vždy v aktuální verzi.[31]

7 Mezinárodní spolupráce – EFGS

7.1 Úvod

Síť pro elektronické zdravotnictví (eHealth Network, dále jen „eHN“) byla zřízena na základě směrnice 2011/24/EU o uplatňování práv pacientů v přeshraniční zdravotní péči a propojuje vnitrostátní orgány odpovědné za elektronické zdravotnictví.

V souvislosti s pandemií COVID-19 a nalezením vhodných digitálních řešení, které by mohly být v boji s pandemií využity bylo ustanoveno několik dočasných pracovních podskupin. Některé z nich již naplnily účel, pro nějž byly ustanoveny, a již nezasedají (např. epidemiologická podskupina, pracovní podskupina pro zajištění interoperability mezi decentralizovanými modely, pracovní podskupina pro právní aspekty aj.). Níže uvádíme přehled aktuálních platforem:

7.1.1 e-HN

V souvislosti s pandemií COVID-19 byla svolána mimořádná jednání sítě eHN s cílem zajistit lepší využití digitálních technologií v boji s pandemií COVID-19. Od června 2020 zasedá síť eHN pravidelně každý týden.

Témata, která jsou na této platformě projednávána souvisí z velké části s využitím mobilních aplikací pro trasování či zajištěním její interoperability. Síť eHN však diskutuje i zapojení AI, využití telemedicíny, využití finančních prostředků pro podporu digitálních řešení, klinické systémy (CPMS, CMSS) aj.

7.1.2 e-HN technical subgroup

V souvislosti s řešením technických problému mobilních aplikací a nalezení technického řešení pro zajištění interoperability, jímž se nakonec stal server Federation Gateway, byla ustanovena technická pracovní podskupina, která jedná pravidelně každý týden.

Technická podskupina slouží jako platforma pro řešení technických problémů, jímž jednotlivé členské státy čelí (zejm. stažení/nahrávání klíčů, problém s technologiemi – např. BTLE aj.). Komise v jejím rámci poskytuje informace o technickém serveru Federation Gateway, řeší záležitosti a problémy s operačními systémy iOS a Android, a členské státy v jejím rámci reportují o mobilních aplikací (zejm. počet uživatelů, efektivita v rámci epidemiologického šetření aj.).

7.1.3 e-HN interoperability subgroup: joint controllers

V souvislosti s přijetím prováděcího rozhodnutí Komise souvisejícího s přeshraniční výměnou dat mezi mobilními aplikacemi určenými pro trasování v rámci boje s COVID-19, byla ustanovena pracovní skupina společných správců, tzv. Joint controllers. Zmíněné prováděcí rozhodnutí Komise ve svých přílohách uvádí, že

[31] Firebase - 22.10.2020: https://firebase.google.com/docs.

členské státy plní roli společných správců dat, přičemž Komise zastává funkci zpracovatele. První jednání této podskupiny se uskutečnilo dne 22. července 2020.

V rámci této platformy poskytují členské státy přehled o mobilních aplikacích, které vyvíjí/využívají se zaměřením na ochranu dat (tedy poskytují informace o tom, zda je vyžadován souhlas uživatele, kdo je zpracovatelem dat na národní úrovni, kdo plní roli správce dat aj.).

7.1.4 e-HN piloting group

V souvislosti s pilotním testováním serveru Federation Gateway plánuje Komise zahájit jednání tzv. pilotní skupiny. Jednání by se měla konat každý týden a měla by sloužit jako platforma, v jejímž rámci bude Komise informovat o harmonogramu a výsledcích pilotního testování. Avizovaný záměr vzniku této pracovní podskupiny Komise definitivně potvrdí.

7.2 European Federation Gateway Service (EFGS)

ČR se zapojila do pilotní skupiny pro testování serveru Federation Gateway, který je technickým řešením interoperability mobilních aplikací pro trasování v EU. Evropská komise na jednání sítě eHealth Network, informovala, že kromě splnění technických požadavků je rovněž nutné projít oficiální procedurou pro udělení povolení a statutu „go live“. ČR je v tomto ohledu povinna, stejně jako všechny zainteresované členské státy, zaslat Evropské komisi žádost, na jejímž základě proběhne audit, resp. posouzení vlivu na ochranu osobních údajů (DPIA). Poté bude ČR oficiálně využívat server Federation Gateway a mobilní aplikace eRouška 2.0 bude přeshraničně interoperabilní.

V souvislosti s interoperabilitou mobilních aplikací byla ustanovena komunikační skupina, v jejímž rámci bylo diskutováno téma společné mediální komunikace členských států, jejichž mobilní aplikace budou fungovat interoperabilně, vůči veřejnosti a médiím. Německo apelovalo na společný přístup členských států a zapojení příslušných ministrů do mediální kampaně na podporu využití mobilních aplikací (ministr zdravotnictví ČR projevil předběžný souhlas se zapojením se do mediální kampaně EU). Komise bude o dalším postupu v této záležitosti informovat na nadcházejících jednáních, nejdříve musí vše zkoordinovat v rámci své vnitřní struktury.

7.3 Popis funkcionality mezinárodní spolupráce a EFGS

V rámci mezinárodní výměny informací spolupracujeme se správci obdobných aplikací jednotlivých států EU (tzv. "národních aplikací"). Výměna informací s národními aplikacemi jiných států je rozšířením konceptu eRouška 2.0, prostřednictvím Evropské federační brány (EFGS) umožňuje odesílat klíče nakažených a vzájemně varovat i uživatele různých národních aplikací. Uživatelé eRoušky mohou tedy být varováni o setkání s nakaženými cizinci (uživateli ostatních národních aplikací), které potkali v cizině nebo v České republice. Zároveň umožňuje nakaženým uživatelům eRoušky varovat uživatele ostatních národních aplikací. Poskytuje tedy možnost vzájemného varování uživatelů spolupracujících národních aplikací jak v případě uživatele eRoušky cestujícího do zahraničí, tak v případě uživatelů národních aplikací jiných států cestujících do ČR.

Mezinárodní spolupráce je rozšířením konceptu fungování eRoušky. Stejně, jako se pseudonymní klíče nakaženého vystavují pro všechny uživatele eRoušky k vyhodnocení, posílá je server eRoušky prostřednictvím

Evropské federační brány (EFGS) ostatním národním aplikacím, aby je mohly vystavit svým uživatelům. Prostřednictvím EFGS je předáván stejný rozsah dat o nakažených jako prostřednictvím serveru eRouška – klíče nakaženého a datum prvních příznaků (pokud je známé) - doplněné o identifikátory země původu (Country of Origin) a cílových zemí (Coutry of Interest).

EFGS umožňuje uživatelům národních aplikací v nastavení aplikace přesně určovat sadu zemí, ze kterých konkrétní uživatel dostává informace o nakažených a do kterých odesílá svoje údaje. eRouška implementuje zjednodušený model, nazvaný "EU Traveler", ve kterém si uživatel eRoušky volí pouze "Spolupráce s EU" ANO/NE. Parametr "Spolupráce s EU" uživatel eRoušky nastavuje jednak pro stahování informací z ostatních národních aplikací, a to na speciální stránce, která je dostupná z domácí stránky a zároveň je zobrazena při aktualizaci eRoušky na verzi podporující EU spolupráci. Pro odesílání vlastních klíčů nakaženého uživatel eRoušky nastavuje parametr "Spolupráce s EU" ještě na dodatečné stránce při odesílání dat ("Anonymním upozornění ostatních").

Mezinárodní spolupráce národních aplikací funguje pouze pro národní aplikace využívající protokol Apple/Google Exposure Notification API a zapojené do spolupráce prostřednictvím EFGS. Jejich seznam a další související dokumenty lze najít na stránkách Evropské komise[32]. V souladu s podmínkami použití Exposure Notification API může být v každém státě pouze jedna národní aplikace. EFGS je provozována EU a má svou vlastní GDPR dokumentaci (Informace o zpracování osobních údajů EFGS v příloze tohoto dokumentu).

Ve všech scénářích dochází k výměně náhodných klíčů při setkávání uživatelů různých národních aplikací automaticky, na základě faktu, že jejich telefony používají stejný protokol Exposure Notification API. Rozdíly jsou v tom, jestli a jak si jejich aplikace následně vymění klíče nakažených osob a mají možnost vyhodnotit rizikovost setkání.

Scénáře použití mezinárodní spolupráce z pohledu uživatele eRoušky:

1) Byl jsem nebo jsem v zahraničí a zajímá mě, jestli jsem tam nepotkal nakaženého

Uživatel eRoušky, který je nebo byl v zahraničí, si zapne volbu "Spolupráce s EU" na speciální stránce, která je dostupná z domácí stránky. Jeho eRouška začne kromě souboru s klíči nakažených uživatelů eRouška stahovat i soubory klíčů nakažených uživatelů ostatních národních aplikací v EU, které server eRouška pravidelně získává prostřednictvím EFGS, a vyhodnocovat potenciální setkání s nimi.

2) Byl jsem nebo jsem v zahraničí, jsem nakažený, chtěl bych varovat i zahraniční uživatele aplikací

Uživatel, který je nebo byl v zahraničí, si při odeslání dat ("Anonymní upozornění ostatních") zapne volbu "Spolupráce s EU" na dodatečné stránce v rámci procesu odeslání dat. Tím dává souhlas k odeslání jeho klíčů prostřednictvím EFGS na servery národních aplikací ostatních států EU, které jeho klíče zpřístupní uživatelům svých národních aplikací.

3) Potkávám v Čechách zahraniční turisty a zajímá mě, jestli nebyli nakažení

Jde o symetrický případ k 2) z pohledu uživatele národní aplikace jiného státu EU.

Zahraniční turista s národní aplikací svého státu EU, u kterého je potvrzená nákaza, zvolí (způsobem specifickým pro jeho národní aplikaci) odesílání klíčů do všech států EU nebo specificky do České republiky.

[32] Viz https://ec.europa.eu/health/ehealth/key_documents_en.

Jeho národní aplikace odešle prostřednictvím EFGS jeho klíče i do serveru eRouška, který je zařadí do souboru "českých" nakažených. Soubor si automaticky stahují všechny eRoušky v ČR, nezávisle na nastavení volby "Spolupráce s EU", a vyhodnocují rizikovost setkání.

4) Zahraniční turista je nebo byl v Čechách a zajímá se, jestli tady nepotkal nakaženého

Jde o symetrický případ k 1) z pohledu uživatele národní aplikace jiného státu EU.

Zahraniční turista s národní aplikací svého státu EU, u kterého je potvrzená nákaza, zvolí (způsobem specifickým pro jeho národní aplikaci) stahování souborů nakažených z celé EU nebo specificky z České republiky. Server jeho národní aplikace pravidelně získává soubor klíčů nakažených z ČR a nabízí ho všem uživatelům národní aplikace k vyhodnocení.

8 Bezpečnost dat

Zajištění důvěrnosti, dostupnosti a integrity dat je zaručena celou řadou rozsáhlých organizačních a technických opatření využívající nejnovějších technologií a ověřených postupů. Společnost Google[33] a další provozovatelé[34] jsou držitelem mnoha bezpečnostních certifikátů. Systémy jsou kvalitně a rozsáhle vždy v aktuální podobě popsány na jednotlivých webových stránkách. Více se bezpečnosti bude věnovat analýza rizik.

Subjekt údajů jako takový není schopen ovlivnit bezpečnost zpracování. To má za následek, že je odpovědností správce navrhnout zpracování bezpečným způsobem poskytujícím přiměřená ochranná opatření, tak aby nemohlo dojít k poškození jeho práv.

Při samotném zpracování údajů dochází k zaznamenání (logování) údajů jen pro nezbytné provozní potřeby IT administrátorů a veškeré ukládané údaje či metadata jsou vždy kompletně odstraněna, jakmile již nejsou potřebné k samotnému zpracování.

Integrita a přesnost zpracovávaných údajů v rámci aplikace eRouška může být ověřována pomocí provádění ručních penetračních testů a testů odolnosti, minimálně v rámci vydávání nových verzí aplikace.

9 Popis účelů a popis operací zpracování osobních údajů

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, nejsou využívány pro jiné účely, než je provoz a další rozvoj této aplikace.

[33] Google Secret Manager, Store API keys, passwords, certificates, and other sensitive data – 21.10.2020: https://cloud.google.com/secret-manager.

[34] Key Vault Safeguard cryptographic keys and other secrets used by cloud apps and services – 21.10.2020: https://azure.microsoft.com/en-us/services/key-vault/.

Aplikace eRouška je vyvinuta tak, aby neprováděla přímo identifikaci subjektu údajů a aby minimalizovala zpracování osobních údajů na nejnižší možnou úroveň.

Aplikace samotná neobsahuje osobní údaje. Ministerstvo zdravotnictví ani hygienické stanice v tomto technickém řešení v rámci aplikace nemůže ztotožnit konkrétního uživatele aplikace.

Aplikace zprostředkuje informaci, že se někdo v konkrétní den setkal s osobou, která byla pozitivně testována na COVID-19. Tzn., že bude subjekt údajů za určitých okolností schopen, např. pokud se v daný den setkal 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 byl konkrétní subjekt údajů. To je ale vlastnost aplikace, kterou nelze vyloučit, protože bez toho by aplikace nefungovala řádně a nemohla by přispět k větší ochraně před COVID-19. Ministerstvo zdravotnictví a hygienické stanice nejsou v rámci aplikace schopní ztotožnit konkrétní subjekt údajů a nejsou také schopni ani zjistit, s kým se subjekt údajů setkal. **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 (recitál 26 GDPR) nebo formou zpětné reidentifikace subjektů údajů ze strany adresáta notifikace (jde o teoretickou možnost reidentifikace subjektů údajů s využitím přiměřených prostředků pro identifikaci, zejména informací o tom s kým se v inkriminované době setkal); 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 (správce by měl vždy uvažovat náklady a čas potřebný k takovéto identifikaci, dále dostupnou technologii v době zpracování a pravděpodobný technologický vývoj).

Z rozhodnutí společných správců osobních údajů v EFGS (joint controllers group) jsou klíče nakažených získané z EFGS obecně považovány za pseudonymizované[35] osobní údaje. Z tohoto důvodu jsou obtížněji uplatnitelná práva subjektů údajů, včetně odvolání samotného souhlasu.

10 Právní titul zpracování osobních údajů

Osobní údaje jsou zpracovávány 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 hygienické stanice plníme své úkoly dle zákona **č. 258/2000 Sb., o ochraně**

[35] Tzn., že zpracování údajů v rámci EFGS je nastaveno takovýmto způsobem, aby jednak nedošlo k propojení pseudonymů na fyzické osoby a nemohlo dojít k žádným zpětným de-anonymizacím. Konstrukce samotného zpracování zdůrazňuje následně minimalizaci dat z hlediska korelace mezi shromažďovanými daty a samotnou identitou fyzických osob, ohledně těchto dat.

veřejného zdraví a dle § 33 odst. 5 **zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování** (zákon o zdravotních službách)[36].

Samotná aplikace je však vždy instalována se svolením subjektu údajů, tzn. jen on rozhodujete, zda aplikace bude do jeho telefonu či jiného zařízení instalována, nebo ne. Odinstalací aplikace je zajištěno, že se nadále nebude na fungování tohoto systému účastnit.

K instalaci aplikace nesmí být nikdo nucen, ani zaměstnavatelem ani např. vlastníky prostor, do nichž je vstupováno.

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

Mezinárodní spolupráce v rámci EU je založena na Prováděcím rozhodnutí komise (EU) 2020/1023 ze dne 15. července 2020[37] a v případě odesílání klíčů nakaženého do EFGS i **na základě souhlasu uživatele podle čl. 6 odst. 1 písm. a) a podle čl. 9 odst. 2 písm. a) GDPR.** Odeslání klíčů nakaženého uživatelům ostatních národních aplikací prostřednictvím EFGS je založeno na samostatném souhlasu potvrzeném uživatelem v momentě odesílání klíčů. Po odeslání klíčů nakaženého již není možné souhlas odvolat, protože již bylo zahájeno jednorázové zpracování dat s tímto souhlasem související. Souhlas je ovšem jednorázový, tzn. v případě opakovaného pozitivního testu bude uživatel požádán o nový souhlas s předáním klíčů, čímž je opakovaně zajištěna dobrovolnost v rámci udělování souhlasu.

Oprávněnost právního titulu byla také konzultována s Úřadem pro ochranu osobních údajů, který v závěru svého dopisu MZ doporučil zakotvení povinnosti v *„novele zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, případně v jiném zákoně*“. Jelikož však doposud nedošlo k předmětné novelizaci zákonné legislativy, je nezbytné pro oprávnění k využívání přeshraniční interoperability nadále získávat primárně souhlas od uživatelů aplikace.

Právo subjektů údajů odvolat souhlas pro aplikaci interoperability je omezeno, jelikož dochází k předávání pseudonymizovaných ID mezi ostatními členskými státy EU v rámci efektivního fungování interoperability, což znesnadňuje následně omezit či dokonce zastavit zpracování těchto pseudonymizovaných ID.

Uživatel svým souhlasem opravňuje správce ke sdílení údajů se všemi aktuálně zapojenými členskými státy EU do interoperability, zároveň se však tento udílený souhlas vztahuje i na budoucí zpracování ostatními členskými státy EU, které však ještě v současnosti nejsou součástí interoperabilního rámce, či se na jeho aplikaci v rámci jejich domácí aplikace připravují.

Jelikož je volba souhlasu pro využití interoperability volitelnou funkcionalitou eRoušky, na zpracování údajů jako celku nemá tato funkcionalita vliv. Možnost sdílení údajů s ostatními členskými státy EU je tedy svobodně udílenou volnou každého uživatele eRoušky.

[36] „Právo na informace o zdravotním stavu pacienta, a to pouze v nezbytném rozsahu, mají rovněž osoby, které s pacientem přišly do styku a tyto informace jsou rozhodné pro ochranu jejich zdraví.“

[37] Viz https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32020D1023&from=CS.

11 Kategorie osobních údajů

Níže jsou popsány kategorie použitých osobních údajů, příjemci těchto údajů a případně přenos do třetí země nebo mezinárodní organizace.

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.

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. Údaje o klíčích ostatních eRoušek, čase, době trvání kontaktu a síle Bluetooth signálu jsou uloženy v operačním systému mobilu, nejsou dostupné aplikaci eRouška ani uživateli.

Nakažený uživatel odesílá na server eRouška vlastní klíče, tj. klíče, které při setkání s jinými aplikacemi jeho aplikace „vysílala“. Proto jsou odeslané klíče nazývány **klíči nakažené osoby**. Nedochází k odeslání klíčů ostatních aplikací, se kterými se vaše aplikace setkala. V případě souhlasu uživatele jsou klíče nakažené osoby také odesílány prostřednictvím EFGS dalším spolupracujícím národním aplikacím.

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, vytvoří lokální upozornění (např. zobrazí na vašem telefonu informační okno, podle nastavení notifikací ve vašem telefonu), která vás **upozorní na rizikový kontakt** a zobrazí vám pokyny, jak postupovat. Uživatel se nedozví s kým, v jaký čas (pouze datum) a kde ke kontaktu došlo, pouze informaci o rizikovém kontaktu a datum. Vše probíhá v rámci instalace aplikace uložené ve vašem telefonu tzn., že nikdo jiný se o tomto kroku nedozví.

12 Kontext zpracování

Zpracování osobních údajů pomocí aplikace eRouška souvisí s celosvětovou pandemií koronaviru COVID-19 a smrtelným nebezpečím, které části populace při nakažení hrozí. Je zjevné, že Česká republika díky včasným celoplošným opatřením efektivně zabránila šíření této choroby, ale za cenu velkých ekonomických a sociálních obětí. Smyslem využití moderních technologií je snaha vrátit běžný život do standardních kolejí s minimálními omezeními pro většinu populace. K tomuto návratu má přispět i využití aplikace eRouška.

12.1 Historický kontext

Níže uvedená posloupnost není kompletním výčtem rozhodnutí a opatření, ale pouze přehledem zásadních kroků, které souvisely s opatřeními bránícími šíření nákazy COVID-19. Tento historický kontext poukazuje na míru plošných opatření a omezení celé populace, která s tím souvisí.

Konec ledna – První výskyt infekcí v Evropě na konci ledna 2020 - nejprve v Itálii, následně Francii 24. ledna, o čtyři dny později v Německu.

26. ledna 2020 – byla za účasti odborníků společně řešena otázka bezpečnosti občanů ČR a přijatá opatření.

30. ledna 2020 – WHO vyhlásila tzv. globální stav nouze.

3. února 2020 – podepsal ministr zdravotnictví ochranné opatření, kterým se od neděle 9. února 2020 až do odvolání zakazují všechny přímé lety z Číny na všechna mezinárodní letiště v České republice, protože podle dostupných informací původ nákazy koronavirem byl identifikován v čínském Wu-Chanu.

26. února 2020 – vydalo Ministerstvo zdravotnictví vzhledem k aktuální epidemiologické situaci doporučení cestovatelům, kteří pobývali v období od poloviny ledna 2020 v severoitalských regionech, aby v následujících 14 dnech po opuštění regionu sledovali svůj zdravotní stav se zaměřením se na příznaky počínajícího respiračního onemocnění (především horečka nad 38 st. C, dýchací obtíže).

1. března 2020 – oznámil ministr zdravotnictví potvrzení prvních třech případů nákazou COVID-19 v České republice. Všichni tři pacienti, dva Češi a jedna studentka americké národnosti.

4. března 2020 – zasedala Bezpečností rada státu a Ministerstvo zdravotnictví následně přijalo mimořádné opatření, kterým všem pořadatelům hromadných akcí na území ČR s předpokládanou účastí nad 5000 osob denně nařizuje oznámit takové akce místně příslušné krajské hygienické stanici.

10. března 2020 opět zasedala Bezpečnostní rada státu. Bylo rozhodnuto o přijetí dalších dvou mimořádných opatření v souvislosti s onemocněním COVID-19. Zakázány byly všechny hromadné akce, kde je najednou více než 100 osob a také byla zakázaná osobní účast na výuce na základních, středních, vysokých i vyšších odborných školách.

12. března 2020 – vláda ČR vyhlásila kvůli koronaviru nouzový stav na celém území ČR. Nouzový stav začal platit od 14:00 dne 12. března 2020. Důvodem vyhlášení bylo ohrožení zdraví obyvatel. Nouzový stav je státní krizové opatření vyhlašované v případě závažných situací, které ve značném rozsahu ohrožují životy, zdraví či majetek anebo vnitřní pořádek a bezpečnost.

14. března 2020 – vláda přijala krizové opatření s cílem zamezit šíření nákazy koronaviru v ČR. Od soboty 14. března 2020 od 6:00 hodin do 24. března 2020 do 6:00 hodin se uzavřely veškeré obchody s výjimkou prodejen potravin, hygienického a drogistického zboží, lékáren a výdejen zdravotnických prostředků, paliv a pohonných hmot a dalších. Ve stejném období začal také platit zákaz přítomnosti veřejnosti v provozovnách stravovacích služeb s výjimkou provozoven, které neslouží pro veřejnost.

16. března 2020 – je zakázán volný pohyb osob na území České republiky s výjimkou cest do zaměstnání, do zdravotnických zařízení, za rodinou a dalších nezbytných cest, dále zákaz vstupu do České republiky pro všechny cizince bez trvalého či přechodného pobytu v délce nad 90 dní a občanům České republiky a cizincům s trvalým či přechodným pobytem v délce nad 90 dní se zakazuje vycestovat z České republiky.

19. března 2020 –se dle usnesení vlády zakazuje všem osobám pohyb a pobyt na všech místech mimo bydliště bez ochranných prostředků dýchacích cest.

24. března 2020 – je možné pobývat na veřejně dostupných místech nejvýše v počtu dvou osob, s výjimkou členů domácnosti, výkonu povolání, podnikatelské nebo jiné obdobné činnosti či účasti na pohřbu. Při kontaktu s ostatními osobami je nutné zachovávat odstup nejméně 2 metry, pokud je to možné.

14. dubna 2020 – vyhlásila vláda plán postupného uvolňování opatření v souvislosti s výskytem epidemie COVID-19 na území ČR[38].

30. září 2020 – vyhlásila vláda ČR vyhlásila kvůli koronaviru nouzový stav na celém území ČR. Nouzový stav začal platit od 00:00 dne 05. října 2020 po dobu 30 dnů. Důvodem vyhlášení bylo zhoršená epidemiologická situace a ohrožení zdraví obyvatel. Nouzový stav byla nadále prodlužován až do roku 2021.

V době psaní tohoto Posouzení vlivu platil nouzový stav a platí mnohá omezení, která mají zásadní ekonomický a sociální dopad na většinu populace.

12.2 Technologický kontext

O technologicky podporovaných zpracovatelských činnostech se v současné době diskutuje. Nasazení aplikace v kontextu s Chytrou karanténou by mělo zejména umožnit:

1) sledovat šíření pandemie, aby bylo možné předvídat její další šíření,
2) zastavit pandemii a alespoň její šíření mít pod kontrolou,
3) informovat potenciálně infikované osoby o jejich možné infekci.

Přecházet tak od obecných opatření plošné povahy, jako jsou obecné zákazy, k mitigaci rizik a opatření specifických pro jednotlivé cílové skupiny, aby se minimalizoval dopad opatření na ekonomiku státu.

V řadě zemí, včetně Čínské lidové republiky, Jižní Koreje, Singapuru, Izraele a Rakouska, byla zavedena celá řada technologicky podporovaných zpracovatelských činností v souvislosti s ochranou před onemocněním COVID-19.

Čínská vláda ve spolupráci se společností Alipay od poloviny února 2020 nařízením zavázala své občany k instalaci a používání aplikace v jejich chytrém telefonu, která sleduje jejich pohyb za účelem vymáhání karanténních opatření a identifikace osob se kterými dotyčný občan přišel do styku. Aplikace přenáší data o pohybu na server(y), kde jsou identifikovány (možné) kontakty s infikovanými osobami. Majitelé chytrých telefonů jsou pak informováni barevnými kódy o tom, jak by se měli chovat – od relativní svobody pohybu po nucenou izolaci po dobu několika týdnů. Aplikace zobrazuje stav uživatele vztahující se ke koronavirové infekci a musí být na požádání policie či dalších kontrolních místech zobrazena na telefonu. K identifikaci místa pohybu a stavu v okolí slouží i QR kódy nalepené na vstupech do jednotlivých domů či MHD. Aktuálně se používá se ve více než 200 čínských městech[39].

[38] MZ ČR – 14.5.2020 – https://koronavirus.mzcr.cz/vyvoj-udalosti-v-case/.

[39] China's coronavirus detection app is reportedly sharing citizen data with police – 13.5.2020 – https://thenextweb.com/china/2020/03/03/chinas-covid-19-app-reportedly-color-codes-people-and-shares-data-with-cops/.

Singapurská vládní technologická agentura zahájila 20. března distribuci aplikace pro chytré telefony „TraceTogether“[40], jejímž cílem je podpora trasování infikovaných kontaktů pro Ministerstvo zdravotnictví. Pomocí aplikace jsou uživatelé identifikováni na centrálním serveru, poté je do aplikace odesláno centrálně přiřazené pseoudonymizační ID, které je následně prostřednictvím Bluetooth vyměňováno a sdíleno s ostatními zařízeními v dosahu. Tato data o provedených kontaktech jsou také odesílána na server. V případě infikované osoby jsou kontakty identifikovány a příslušné osoby informovány o případné nutnosti vstoupit do karantény. Tato karanténa je vynucena sledováním infikovaných osob pomocí údajů o poloze GPS jejich chytrých telefonů. Nakažené osoby musí prokázat, že jsou skutečně ve svém domě, a na požádání poskytnout fotografie za svého okolí nebo bytu.

Jižní Korea používá údaje z telefonních přístrojů a kreditních karet infikovaných osob ke sledování jejich pohybu za účelem identifikace osob se kterými uživatel přišel do kontaktu[41]. Osoby, u nichž bylo zjištěno, že se nacházejí v blízkosti infikovaných osob, jsou následně telefonicky kontaktovány s informacemi o svém pohybu a dalšími instrukcemi. Sledování pohybu probíhá také u osob v karanténě, ti jsou navíc několikrát za den telefonicky kontaktováni a je ověřováno místo jejich pohybu například pomocí GPS telefonu, na který je jim voláno. Kromě toho jsou údaje o pohybu infikovaných osob anonymně zveřejňovány, ale mnoho nemocných již bylo zpětně identifikováno a vyskytly se případy sociální stigmatizace a vyloučení. Jedná se o aplikace Corona 100m[42].

Izraelská vláda 18. března 2020 schválila obejít izraelský parlament Kneset nařízením, které umožňuje domácí zpravodajské službě Shin Bet a policii sledovat mobilní telefony potvrzených a podezřelých pacientů COVID-19. Všechna data z mobilních telefonů, která se roky tajně shromažďují, pravděpodobně pro účely boje proti terorismu, se nyní používají k boji proti pandemii[43]. Tato preventivní opatření jsou navržena tak, aby vynucovala komplexní karanténní opatření, a to jak proti těm, jejichž infekce jsou již potvrzeny nebo pravděpodobně infikováni, tak proti všem, s nimiž infikované osoby přišly do styku během posledních 14 dnů. Jsou analyzovány nejen údaje o poloze a pohybu, ale také údaje o finančních transakcích[44]. Jedná se o projekt nazvaný „Hamagen“ – štít.

Coronavirus Australia[45] je aplikace vydaná australskou vládou, jejímž cílem je umožnit uživatelům přístup k informacím o pandemii COVID-19 v Austrálii. Tato aplikace byla vyvinuta společností Delv Pty Ltd pro Ministerstvo zdravotnictví a vydána dne 29. března 2020. Od vydání byla aplikace stažena více než milionkrát a na prvním místě v kategorii „Zdraví a fitness“ v Apple App Store. Vzhledem ke krátkému období vývoje v délce dvou týdnů aplikace původně sloužila především jako souhrn odkazů na oficiální vládní webové stránky. Krátce po vydání aktualizace byl přidán dobrovolný formulář „isolation registration“, který shromažďoval

[40] TraceTogether, safer together – 13.5.2020 – https://www.tracetogether.gov.sg/.
[41] South Korea is relying on technology to contain COVID-19, including measures that would break privacy laws in the US – 14.5.2020 – https://www.businessinsider.com/coronavirus-south-korea-tech-contact-tracing-testing-fight-covid-19-2020-5.
[42] South Korea to stepup online coronavirus tracking – 14.5.2020 – https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109.
[43] To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data – 14.5.2020 – https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.
[44] Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data– 12.5.2020 – https://www.haaretz.com/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383.
[45] Federal Government launches Coronavirus Australia app and WhatsApp feature – 14.5.2020 – https://www.abc.net.au/news/2020-03-29/federal-government-launches-coronavirus-australia-app/12100680.

osobní údaje místa, jména, věku, čísla mobilního telefonu, data zahájení izolace a různé další podrobnosti o uživatelích, kteří se sami dobrovolně izolovali. 14. dubna 2020 byla na základě singapurské aplikace TraceTogether a protokolu BlueTrace vydána samostatná aplikace pro sledování kontaktů, COVIDSafe[46]. COVIDSafe[47] je aplikace pro sledování kontaktů pomocí mobilních zařízení, kterou vydala australská vláda, aby pomohla bojovat proti probíhající pandemii COVID-19. Aplikace rozšiřuje tradiční trasování kontaktů tím, že automaticky sleduje setkání mezi uživateli a později umožňuje orgánům zdravotní péče, státu nebo krajům varovat uživatele, že se dostali do kontaktu s infikovaným pacientem do vzdálenosti menší než 1,5 metru po dobu nejméně 15 minut. Tato funkce není součástí dříve publikované aplikace Coronavirus Australia.

V případě USA se jedná především o inciativu společností Google a Apple – COVID-19 Apple[48] / Google[49] App. Projekt sledování kontaktů Google / Apple na ochranu osobních údajů je protokol pro digitální sledování kontaktů vytvořený pro pandemii COVID-19. Byl vyvinut společností Google a Apple pro jejich příslušné mobilní platformy, tedy Android a iOS. Poprvé byl odhalen 10. dubna 2020. Jedná se o decentralizovaný protokol založený na založený na kombinaci technologie Bluetooth Low Energy a kryptografie chránící soukromí. Podle společnosti Google byl přístup firem založen na protokolu DP-3T vytvořeném také pro pandemii COVID-19. Kromě tohoto projektu, který není aplikací sám o sobě, je v rámci USA vyvíjena například aplikace společnosti Microsoft CovidSafe[50], dále pak aplikace How We Feel, Private Kit: Safe Paths, Covid Watch, CoEpi a NOVID.

Apple a partner společnosti Google vyvíjejí technologii sledování kontaktů COVID-19, která je velmi podobná DP-3T. Je také decentralizovaná a na server je v případě pozitivní diagnostiky infekce přeneseno pouze vlastní dočasné ID. Společnosti plánují ve dvou fázích nejprve vytvořit API a poté komplexní, na bázi Bluetooth založenou platformu pro sledování kontaktů, zabudovanou do svých vlastních operačních systémů. Tato API umožní nahrát uživatelovo vlastní dočasné ID, které v případě infekce může být vloženo i orgánem zdravotní péče, na server nebo srovnáním ID stažených ze serveru s identifikacemi kontaktů, se kterými se dotyčný uživatel setkal a byl vystaven riziku expozice. V tomto řešení pak není možné extrahovat dočasné ID ze samotné aplikace.

Indie vydala nejen svou celostátní aplikace, ale také jednotlivé indické státy nabídly uživatelům své aplikace. Jedná se o Aarogya Setu, COVA Punjab, COVID-19 Feedback, COVID-19 Quarantine Monitor, Corona Kavach, GoK Direct, Mahakavach, Quarantine Watch, Test Yourself Goa, Test Yourself Puducherry. Jedná se o různé aplikace s rozdílnou úrovní zabezpečení, funkcí i účelem.

Kromě mobilních aplikací monitorujících kontakty s obdobnými mobilními zařízeními se začínají objevovat i řešení na úrovni hardware. Příkladem takového řešení je „Contact Tracing“ společnosti Mappedin[51]. Systém funguje tak, že na základě konkrétních parametrů identifikuje pracovníky první linie, kteří přišli do kontaktu s jiným zaměstnancem. Identifikuje situace, kdy dvě zařízení přijdou do kontaktu bližšího než 5 metrů po

[46] The Government’s COVID-19 tracking app is called CovidSafe and is launching today! – 13.5.2020 – https://techau.com.au/the-governments-covid-19-tracking-app-is-called-covidsafe-and-is-launching-today/.
[47] COVIDSafe – 12.5.2020 – https://play.google.com/store/apps/details?id=au.gov.health.covidsafe&hl=en_US.
[48] Apple and Google partner on COVID-19 contact tracing technology – 12.5.2020 – https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.
[49] Apple and Google partner on COVID-19 contact tracing technology – 13.5.2020 – https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/.
[50] CovidSafe – 13.5.2020 – https://covidsafe.cs.washington.edu/.
[51] Contact Tracing – 15.5.2020 – https://info.mappedin.com/contact-tracing.

dobu více jak 5 minut. Systém nabízí přehlednou vizualizaci takových setkání v čase i místě, včetně detailní mapy takových setkání.

Evropa

K evropským technologickým projektům související s onemocněním COVID-19 patří tzv. Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) and Decentralized Privacy-Preserving Proximity Tracing (DP-3T) – protokoly chránící soukromí osob sdílejících data, dále aplikace „Corona Data Donation“[52] Institutu Roberta Kocha (RKI) určená zejména pro „wearables“[53], tedy například chytré hodinky nebo návrh Linuse Neumanna na aplikaci pro sledování kontaktů. 15. dubna 2020 Evropská komise zveřejnila ve spolupráci s členskými státy a Evropským sborem pro ochranu osobních údajů (EDPB) koncept, jak koordinovaným způsobem přistoupit k trasovacím aplikacím a uvolnit tak plošná opatření bránící šíření koronaviru.

Cílem celoevropského projektu na zachování soukromí (PEPP-PT), který má být zřízen jako nezisková organizace ve Švýcarsku, je navrhnout technické mechanismy a normy, které plně ochrání soukromí a zároveň využijí možností digitálních technologií. Smyslem je maximalizace reakční rychlosti národních států v reálném čase na aktuální pandemickou situaci. Projekt slibuje prosazování ochrany osobních údajů, včetně pseudonymizace dat, v souladu s GDPR a požadavky na kybernetickou bezpečnost. Chytré telefony, na kterých je aplikace spuštěna, odesílají dočasně platné „anonymní“ ID identifikátory, které jsou přijímány a ukládány jinými mobilními zařízeními. Historii kontaktů nemůže nikdo získat, včetně uživatelů samotných. Starší záznamy by byly automaticky smazány, jakmile se stanou epidemiologicky irelevantními. Pokud dojde ke zjištění, že uživatel aplikace je infikován, bude následně kontaktován, aby povolil (odeslal) oznámení o svých kontaktech. Projekt slibuje, že na server budou přenášena pouze „anonymní“ ID z historie kontaktů. Aplikace si pravidelně stahuje aktualizace ze serveru, včetně ID kontaktů infikovaných uživatelů, což uživatelům umožňuje zjistit, zda byli v kontaktu s infikovanými osobami. Každá aplikace vyvinutá podle této normy musí být certifikována konsorciem PEPP-PT[54].

Projekt Decentralizovaného sledování při zachování soukromí (DP-3T) má v úmyslu technicky implementovat PEPP-PT v decentralizované podobě. Tento systém také vyžaduje centrální server, který ukládá pouze nezbytná data, a proto nemusí být důvěryhodný, protože „neuchovává žádná tajemství“. V první řadě se vývojáři snaží zaručit utajení dat a deklarují „utajení dat“ jako ústřední výchozí bod. Za tímto účelem je dle protokolu „DP-3T Project 2020b“ uloženo co nejvíce citlivých dat přímo na zařízeních jednotlivých uživatelů. Skóre rizika nákazy se vypočítává na základě lokálně dostupných údajů a také údajů infikovaných osob, tj. Jejich (matematicky propojených) ID, které jsou serverem pravidelně aktualizovány. Toto skóre by mělo odrážet pravděpodobnost infekce. Kromě toho aplikace založené na tomto protokolu umožňuje přenos „anonymních“ údajů o všech kontaktních událostech, které uživatelé měli se všemi osobami, o nichž je známo, že jsou infikovány, pro účely epidemiologického výzkumu[55].

Aplikace „Corona Data Donation“ Institutu Roberta Kocha (RKI) je prezentována jako nabídka „na podporu veřejných orgánů při zvládání nejvážnější sociální krize za posledních 100 let“ a podle institutu je „používána

[52] CORONA DATA DONATION – 12.5.2020 – https://www.wearable-technologies.com/tag/corona-data-donation/.
[53] Mezi wearables patří chytré hodinky, fitness náramky, sport testery, lokátory apod.
[54] EPP-PT-Projekt: Forscher fordern besseren Datenschutz bei Corona-Warn-Apps – 10.5.2020 – https://www.heise.de/newsticker/meldung/PEPP-PT-Projekt-Forscher-fordern-besseren-Datenschutz-bei-Corona-Warn-Apps-4705948.html.
[55] Decentralized Privacy-Preserving Proximity Tracing – 12.5.2020 – https://github.com/DP-3T/documents.

výhradně pro vědecké účely“[56]. Neslouží ani infikovaným, ani neinfikovaným, ale pouze RKI. Účelem je umožnit RKI automaticky sledovat osoby, které vykazují příznaky typické pro infekci virem COVID-19, až po úroveň poštovního směrovacího čísla, a vizuálně zobrazit šíření infekce na webové stránce RKI jako denně aktualizovanou mapu. Použití aplikace vyžaduje vytvoření pseudonymu uživatele. Další sběr dat je částečně prováděn manuálním vstupem, částečně senzory, jako jsou „wearables“ nebo fitness náramky nošené na těle a propojené s aplikací. Podmnožina senzorických dat je anonymizována, například formou rozsahu váhy člověka.

Linus Neumann vytvořil návrh aplikace pro získání kontaktních dat infikovaných osob s odkazem na hackathon „WirvsVirus“[57]. Jediným účelem této aplikace je umožnit osobě, u které byla diagnostikována infekce, informovat své kontakty z posledních 14 dnů. Neumann uvádí, že všechna data by měla být uchovávána výhradně „decentralizovaně“ a „anonymně“. Za tímto účelem jsou pseudonymní identifikátory generovány lokálně na chytrém telefonu v krátkých intervalech, které jsou vysílány ze smartphonu přes Bluetooth Low Energy Beacon, které následně mohou být přijímány jinými smartphony a pokud je vzdálenost mezi nimi dostatečně malá, dojde k jejich uložení. V případě infekce telefon odešle své vlastní anonymní ID na centrální server, který jej zpřístupní pro vyhledání dalšími chytrými telefony a ty pak mohou lokálně zjistit, zda došlo ke kontaktu s infikovanými osobami.

Rakouský Červený kříž spustil aplikaci „Stopp Corona[58]“ dne 25. března 2020. Na základě jedinečných uživatelských ID umožňuje tato aplikace výměnu dat mezi chytrými telefony, které jsou v blízkosti. Po vzájemné identifikaci přístrojů jsou ukládána kontaktní data. V případě infekce by uživatelé měli pomocí aplikace kontaktovat Červený kříž, který opět prostřednictvím aplikace oznámí kontaktovaným osobám, že se během posledních třech dnů dostaly do kontaktu s infekcí. Toto oznámení spouští sběr dalších údajů, včetně čísla mobilního telefonu infikované osoby. Rakouský Červený kříž se podle GDPR výslovně chová jako správce údajů. Aplikace je vyvíjena a provozována společností Accenture, služby jsou hostovány v cloudu Azure Cloud společnosti Microsoft a pro oznámení se používá služba Firebase Cloud Messaging společnosti Google[59].

V průběhu druhé poloviny roku 2021 řada dalších zemí EU spustila nové aplikace nebo nové verze aplikací založených na Apple/Google Exposure Notification API.

Aktuální seznam těchto aplikací, spolupracujících v rámci EFGS, je uveden na stránkách Evropské komise (viz https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf).

13 Analýza jednotlivých zpracovatelských činností

V této části jsou zpracovatelské činnosti postupně členěny na jednotlivé operace podle čl. 4 odst. 2 Obecného nařízení, které musí být spravedlivé a správce jej musí mít pod kontrolou.

[56] Tracking down the virus – 12.5.2020 – https://www.deutschland.de/en/topic/business/corona-apps-using-technology-to-stop-the-virus.
[57] #WirVsVirus – 10.5.2020 – https://wirvsvirushackathon.org/..
[58] Stopp Corona – 12.5.2020 – https://participate.roteskreuz.at/stopp-corona/.
[59] Google Play – 12.5.2020 – https://play.google.com/store/apps/details?id=at.roteskreuz.stopcorona&hl=en_US.

Pro každou zpracovatelskou činnost jsou zvažovány následující tři úrovně analýzy:

1) proces,
2) role,
3) služby IT.

Ve druhém kroku jsou na všech úrovních, konkrétně popsány:

- osobní údaje v nich zpracované a případně technické, organizační a personální role,
- zapojené technické systémy, služby a související provozní procesy – existující komunikační vztahy a rozhraní, která byla použita.

13.1 Zpracovatelská činnost „Zpracování na straně aplikace“

Tabulka 1

ID	Proces	Role/IT služba	Data
0	Instalace a nastavení uživatele aplikace	uživatel/aplikace	přihlašovací údaje a další uživatelská data Apple/Google Store
1	Aktivace a získání eHRID	uživatel/aplikace	eHRID
2	Běžný provoz – výměna klíčů	EN API/mobil	vlastní klíče, cizí klíče, informace o setkání (nedostupné uživateli)
3	Nakažený – autorizační SMS	Daktela (externí), SMS	SMS s autorizačním kódem
4	Nakažený – odeslání vlastních klíčů	uživatel/aplikace	vlastní klíče nakaženého
5	Stahování klíčů nakažených	aplikace	klíče nakažených v CZ, resp. EFGS
6	Vyhodnocení rizikového kontaktu	EN API	klíče nakažených v CZ, resp. EFGS, informace o setkání (nedostupné uživateli)
7	Rizikový kontakt – upozornění	uživatel/aplikace	informace o rizikovém kontaktu

13.2 Zpracovatelská činnost „Zpracování na straně serveru“

Tabulka 2

Číslo	Proces	IT služba	Data
8	Aktivace instance aplikace	Firebase	eHRID
9	Vydání jednorázového autorizačního kódu Daktele (externí)	Verification Server	autorizační kód
10	Ověření jednorázového kódu	Verification server	autorizační kód
11	Přijetí klíčů nakažených od eRoušky	Key Server	klíče nakažených
12	Přijetí klíčů nakažených od EFGS	Key Server	klíče nakažených
13	Vystavení klíčů nakažených pro eRoušku	Key Server	klíče nakažených
14	Vystavení klíčů nakažených pro EFGS	Key Server	klíče nakažených

13.3 Vztahy a rozhraní

Tabulka 3

Číslo	Proces	Role/IT služba1	Role/IT služba 2	Rozhraní
0	Instalace a nastavení uživatele aplikace	uživatel/aplikace	Apple/Google Store (externí)	TLS/internet
1	Aktivace a získání eHRID	uživatel/aplikace	Firebase	TLS/internet
2	Běžný provoz – výměna klíčů	EN API/mobil	EN API/mobil	Bluetooth LE
3	Vydání jednorázového autorizačního kódu	Daktela (externí)	Verification Server	TLS/internet
4	Nakažený – autorizační SMS	Daktela (externí)	uživatel/mobil	SMS
5	Ověření jednorázového kódu	uživatel/mobil	Verification server	TLS/internet
6	Nakažený – odeslání vlastních klíčů	uživatel/aplikace	Key Server	TLS/internet
7	Přijetí klíčů nakažených od EFGS	Key Server	EFGS (externí)	TLS/internet
8	Vystavení klíčů nakažených pro eRoušku	Key Server	aplikace	TLS/internet
9	Vystavení klíčů nakažených pro EFGS	Key Server	EFGS (externí)	TLS/internet
10	Stahování klíčů nakažených	aplikace	Key Server	TLS/internet
11	Rizikový kontakt – anonymní statistická notifikace	aplikace	Firebase	TLS/internet

13.4 Opatření k omezení účelu

Zásadní opatření k zajištění omezení činnosti zpracování osobních údajů obecně spočívají v **použití anonymizovaných, resp. pseudonymizovaných údajů**, v nichž jsou informace týkající se identifikované nebo identifikovatelné fyzické osoby v co největší míře odstraněny nebo odděleny od datových souborů, vztahů a dílčích procesů této zpracovatelské činnosti od ostatních zpracovatelských činností.

Aplikace samotná neobsahuje osobní údaje. Ministerstvo zdravotnictví v tomto technickém řešení v rámci aplikace nemůže ztotožnit konkrétního uživatele aplikace.

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[60] nebo formou zpětné reidentifikace subjektů údajů ze strany adresáta notifikace[61]; 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[62].

Klíče nakažených přijaté z EFGS jsou podle dohody společných správců EFGS považovány za pseudonymní, servery eRouška ani aplikace eRouška proto nemají přístup k případnému mapování na osobní informace uživatelů ostatních národních aplikací, čímž mohou být značně omezeny práva subjektů údajů pro jejich uplatnění napříč evropskými státy zapojenými do interoperability.

13.5 Další plánovaná ochranná opatření

Všechny zpracovatelské činnosti musí splňovat požadavky Obecného nařízení, jak je vyžadováno v čl. 5 Obecného nařízení. S ohledem na vytváření aplikace je třeba dbát zejména požadavků čl. 25 Obecného nařízení ve smyslu záměrné a standardní ochrany osobních údajů a čl. 32 Obecného nařízení týkající se zabezpečení zpracování.

V této souvislosti se bude dále pracovat s následujícími pojmy:

Důvěrnost	Confidentiality	Důvěrnost lze chápat jako zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni. Důvěrnost je zajištěna schopností ujistit se, že je vynucena nezbytná úroveň míry utajení v každém okamžiku, kdy dochází ke zpracování dat a je zajištěna prevence jejich neautorizovaného vyzrazení.
Dostupnost	Availability	Dostupnost je nejčastěji definována jako zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
Integrita	Integrity	Integrita je definována jako zajištění správnosti a úplnosti informací. Integrita je udržena, když je zajištěno, že data jsou přesná, se zaručeným obsahem a jsou provedena opatření proti jejich neautorizované změně.
Intervenabilita	Intervenability	Možnost koncových uživatelů (subjektů údajů) disponovat kontrolou nad tím, jak jsou jejich osobní údaje zpracovávány informačními systémy. Tento cíl ochrany soukromí se nazývá intervenovatelnost (Intervenabilita).
Transparentnost	Transparency	Transparentnost je povinnost týkající se těchto hlavních oblastí: informování subjektů údajů ohledně spravedlivého zpracování, jak správci komunikují se subjekty údajů v

[60] Recitál 26 GDPR.
[61] Jde o teoretickou možnost reidentifikace subjektů údajů s využitím přiměřených prostředků pro identifikaci, zejména informací o tom, s kým se v inkriminované době setkal.
[62] Správce by měl vždy uvažovat náklady a čas potřebný k takovéto identifikaci, dále dostupnou technologii v době zpracování a pravděpodobný technologický vývoj.

		souvislosti s jejich právy podle Obecného nařízení, jak správci napomáhají subjektům údajů při výkonu jejich práv.
Nespojitelnost	Unlinkability	Nespojitelnost dvou nebo více osobních údajů (Neprovázanost). Nelze dostatečně rozlišit, zda jsou daná data provázána a mají něco společného. V zásadě možnost nespojit některé údaje s konkrétní fyzickou osobou.

13.5.1 Zpracování na straně aplikace

Tato zpracovatelská činnost je technicky podporována používáním chytrého telefonu a nainstalované aplikace eRouška. Pro chytré telefony nejsou stanovena žádná další technická nebo organizační opatření pro provozní zabezpečení kromě obecných doporučení pro používání těchto přístrojů.

Důvěrnost	Historie kontaktů je chráněna OS a nedostupná aplikaci a uživateli. Dále jde o anonymizovaná/pseudonymizovaná data - viz kapitola 13.4.
Dostupnost	Aplikace nemusí být odemčena nebo jinak aktivována osobně, aby byla umožněna komunikace[63].
Integrita	Obsah datové struktury obsahující pseudonymizované klíče je technicky zabezpečena proti náhodné či úmyslné škodlivé změně a zároveň je kontrolováno, že se zde nenacházejí žádné jinak definované hodnoty údajů. Omezení tzv. falešných nahlášení (tzv. false positives) je zmírňováno pomocí kontrolních výpočtů a ověřování výsledků a výstupů z jednotlivých aplikací na základě definovaných parametrů či rozmezí, pro které byla aplikace naprogramována.
Intervenabilita	Účast a užívání aplikace lze kdykoli ukončit odinstalováním, vypnutím aplikace nebo celého přístroje.
Transparentnost	Kód aplikace je k dispozici jako otevřený kód, volně přístupný na GitHub.
Nespojitelnost	Historie setkání je chráněna OS a nedostupná aplikaci a uživateli. Dále jde o anonymizovaná/pseudonymizovaná data – viz kapitola 13.4.

13.5.2 Zpracování na straně serveru

Důvěrnost	• Přenos dat mezi serverem a aplikací je chráněn před neoprávněným přístupem pomocí šifrovaného a bezpečného kanálu. • eHRID a klíče nakažených jsou anonymní/pseudonymní, administrátor serveru nemůže identifikovat uživatele a infikované osoby. • Server nevytváří žádné protokoly (IP adresa nebo podobné) procesů odesílání.
Dostupnost	Zaručena skrze SLA Google Cloud Platform.
Integrita	• Přenos dat mezi serverem a aplikací je chráněn před neoprávněným přístupem pomocí šifrovaného a bezpečného kanálu. • Ke všem změnám v rámci chování a nastavení aplikace a její komunikace se serverem dochází na základě administrativního schválení. • Přenos dat je realizován na základě rozhodnutí uživatele.

[63] Aktuálně plně neplatí pro iOS, díky omezení fungování Bluetooth na pozadí.

Intervenabilita	Uvolnění přenosu dat explicitně pouze po stisknutí tlačítka „Anonymně upozornit ostatní“, což také zvyšuje vnímání relevance.
Transparentnost	Tento krok postupu a funkce serveru jsou popsány v dokumentaci zpracování výše. Specifikace, dokumentace a zdrojový kód aplikace a serveru jsou otevřené, takže je možné zkontrolovat certifikační autoritu.
Nespojitelnost	Jde o anonymizovaná/pseudonymizovaná data – viz kapitola 13.4.

13.6 Identifikace dalších požadavků ochrany osobních údajů

Musí být zaveden postup pro pravidelné přezkoumání zpracovatelské činnosti podle čl. 32, odst. 1, písmene d) Obecného nařízení. Konkrétně to znamená, že musí být zavedena ochrana dat a správa zabezpečení IT, pomocí které správce implementuje a vynucuje ochranná a kontrolní opatření. V případě vysokých rizik, které u zpracování osobních údajů zvláštní kategorie hrozí, musí být jmenován pověřenec pro ochranu osobních údajů – pověřenec Ministerstva zdravotnictví. Úkolem pověřence pro ochranu osobních údajů je dohlížet na činnosti managementu, který by měl být integrován do řízení kvality v rámci celého projektu. Úkolem správy IT a ochrany dat je včasné zjištění nedostatků a jejich účinné odstranění. Musí být zajištěna bezpečnost všech zúčastněných součástí IT. K zajištění dostupnosti, musí být alespoň centrální části systému navrženy redundantně a musí být prováděny pravidelné zálohy. Autentičnost zúčastněných serverů, klientů a služeb musí být zajištěna pomocí bezpečnostních certifikátů. Všechna komunikační spojení musí být šifrována end-to-end[64], aby třetí strany nemohly zjistit, jaké osobní údaje se přenášejí. Práva subjektů údajů na informace a zveřejňování, opravy a výmazy (viz čl. 12–22 Obecného nařízení) musí správce účinně uplatňovat, pokud je toho technicky schopen. Musí být umožněno, že v případě pozitivního testu uživatele rozhodne o nahrání informací vždy uživatel sám. Tento základní požadavek je splněn např. tlačítkem „odeslat data“.

13.7 Účastníci

Běžný uživatel. Typický uživatel systému, u kterého se předpokládá, že bude schopen nainstalovat a používat aplikaci pomocí uživatelského rozhraní (UI). Výhradně sleduje informace dostupné prostřednictvím uživatelského rozhraní aplikace a informace o ostatních uživatelích odvozuje z těchto základních dat.

Technicky důvtipný uživatel (hacker Blackhat / Whitehat, nevládní organizace, akademici, vědci atd.). Tento uživatel má přístup do systému prostřednictvím mobilní aplikace. Kromě toho může nastavit (BT, WiFi a mobilní) přijímače tak, aby lokálně odposlouchával data. Aplikaci může dekompilovat / upravovat a má přístup ke zdrojovému kódu.

- (Whitehat hacker) Prozkoumá kód aplikace, informace v telefonu a podívá se, jaké a jak jsou informace vyměňovány se serverem (pomocí antény nebo softwaru nainstalovaného v telefonu) nebo vysílány přes Bluetooth (pasivní).
- (Black hacker) Může realizovat DoS útok na systém (cíleně část nebo celý systém), upravit protokol a aktivně vysílat falešné identifikátory Bluetooth.

Slídil (poskytovatel internetových služeb, místní správce systému, Bluetooth sniffer). Mohou sledovat síťovou komunikaci (tj. zdroj a cíl paketů, zatížení, čas) a/nebo zprávy BTLE.

[64] Jedná se o koncové šifrování mezi dvěma síťovými body – např. mezi dvěma aplikacemi/koncovými uživateli komunikujícími navzájem a skrytím obsahu komunikace před správcem komunikačního kanálu i serveru samotného.

- (Síťař) Může využít odpozorovaného síťového provozu k pokusu o určení stavu uživatele (např. zda je ohrožen, zda je COVID-19 pozitivní atd.).
- (Lokální Bluetooth BTLE Sniffer) Může sledovat lokální Bluetooth přenos (například s výkonnou anténou pokrývající širší oblast) a pokoušet se sledovat lidi v tomto okolí.

V této souvislosti je třeba poznamenat skutečnost, že při takové činnosti osob nebo organizací a využití získaných údajů a dat tímto způsobem nebo shromažďování osobních údajů o kolemjdoucích k pokusu o odhadnutí jejich infekčního stavu na základě přenášených identifikátorů, dochází k porušení celé řady stávající vnitrostátní i evropské legislativy o ochraně osobních údajů, soukromí v oblasti elektronických komunikací a dále ke zneužití výpočetní techniky.

Hygienické stanice. Obdrží informace o pozitivních uživatelích COVID-19 v rámci své běžné diagnostické činnosti pacientů. Hygienická stanice se dozví informace o ohrožených lidech z blízkých kontaktních událostí pouze v případě, že tito infikovaní lidé sami rozhodnou odeslat informaci.

Vývojáři backendu a aplikace. Mají přístup ke všem datům uloženým na serveru(ech). Mohou také změnit programový kód backendu a kód mobilní aplikace (včetně parametrů souvisejících s trasováním). Lze předpokládat, že mobilní aplikaci neupraví, protože taková akce by byla zjistitelná. Mohou kombinovat a porovnávat získané informace, požadovat informace od aplikace, kombinovat s dalšími veřejnými informacemi, a tak získávat informace o poloze subjektů údajů.

Státní entity (bezpečnostní orgány, zpravodajské agentury atd.). Disponují kombinovanými schopnostmi technicky důvtipného uživatele a mají k dispozici různé typy odposlouchávacích a jiných záznamových zařízení. Kromě toho může protivník na úrovni státu disponovat pravomocí, která jim poskytne oprávnění zdravotnického úřadu nebo administrátorské role backendu. Cílem těchto entit je získat informace o populaci nebo cílit na konkrétní jedince. Mohou se zajímat o informace z minulosti, které jsou již v systému uloženy, nebo o budoucí informace, které jim umožní sledovat zájmové osoby na základě odpozorovaných TUID.

Protivník s neomezeným rozpočtem. Např. velké organizace a zahraniční státy, disponují schopností technicky zdatných uživatelů a mohou je nasadit v mnohem větším měřítku. Takový protivník může navíc získat kontrolu nad infrastrukturou projektu, tedy backendem celého systému. Cílem tohoto protivníka by mohlo být získat informace o populaci nebo konkrétních jedincích, případně narušit systém sledování kontaktních událostí, což má za následek nedostupnost služby. Jednou z forem narušení může být pokus rozeslat falešná oznámení o riziku nákazy celé řadě uživatelů pomocí antén rozmístěných na veřejných místech (např. na letištích, na nádražích, v nákupních střediscích nebo v budovách parlamentu) a předávání těchto zpráv v obrovském měřítku.

14 Odpovědnost

Zpracování osobních údajů může být legální, pouze pokud lze určit subjekt odpovědný za zpracování. Porušování práv a svobod fyzických osob v důsledku zpracování osobních údajů by nemělo probíhat bez pravidel (viz 78. bod odůvodnění Obecného nařízení). V čl. 5 odst. 2 ve spojení s čl. 4 odst. 7 Obecné nařízení stanovuje odpovědnost správci, který sám nebo společně s ostatními určuje účel a prostředky zpracování. Dotčená osoba – fyzická nebo právnická osoba, orgán, instituce nebo jiný takto určený subjekt – odpovídá podle čl. 5 odst. 2 Obecného nařízení za zajištění toho, aby zásady zpracování podle čl. 5 odst. 1 Obecného nařízení byly dodržovány a správce musí být toto schopen prokázat. Podle čl. 24 odst. 1 Obecného nařízení musí správce prokazatelně přijmout technická a organizační opatření (74. bod odůvodnění Obecného

nařízení), aby dodržel zásady čl. 5 odst. 1 Obecného nařízení, které zajišťují přiměřenou ochranu práv a svobod subjektů údajů v celém průběhu operace zpracování. Podle čl. 35 Obecného nařízení je správce rovněž povinen implementovat Posouzení vlivu na ochranu osobních údajů.

Stanovení kontroly je zohledněním skutečné, funkční role, kterou správce hraje při zpracování osobních údajů[65]. Ve výjimečných případech může dojít k formálnímu přiřazení správcovství zákonným přidělením.

Podle čl. 4 odst. 7 Obecného nařízení, je správce definován jako:

„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;“

Správcem může být jakákoli fyzická nebo právnická osoba, orgán veřejné moci nebo jiný subjekt. Proto by mohli být všichni aktéři zapojení do zpracování (viz kapitola **Chyba! Nenalezen zdroj odkazů.**) považováni za správce. Protože neexistují žádná právní ustanovení o aplikaci nebo jejím užití, je důležité určit, zda a do jaké míry každý ze zúčastněných subjektů rozhoduje o účelech a prostředcích zpracování.

Podle čl. 5 odst. 1 písm. b Obecného nařízení, účely musí být stanoveny před zpracováním a musí být výslovně vyjádřené a legitimní. Způsoby jsou postupy a procesy, jakými má být účelu dosaženo.

V tomto ohledu je rozhodujícím kritériem skutečná pravomoc rozhodovat o základních prvcích zpracování. Správce musí vždy rozhodovat o účelu i o základních způsobech zpracování. Schopnost rozhodovat pouze o účelech není dostačující. Rozhodnutí o základních způsobech, jsou rozhodnutí o tom, která data jsou zpracovávána, o jejich době zpracování a o tom, kdo může k údajům získat přístup. Například rozhodnutí o výběru konkrétního hardwaru a softwaru nelze chápat jako základní a nezbytné rozhodnutí. Rozhodovací pravomoc může také nastat ze zákonných důvodů, pokud zákon stanoví kritéria pro určení toho, kdo představuje skutečnou rozhodovací pravomoc. Pokud se účel zpracování objeví v důsledku zákonného zadání úkolů, může být také údajem o skutečné rozhodovací pravomoci.

Pro určení toho, kdo má rozhodovací pravomoc, je třeba vzít v úvahu skutečné okolnosti zpracování. Toho lze dosáhnout položením otázky „Proč se toto zpracování provádí?“ a „Kdo zpracování inicioval?“[66]. Je třeba poznamenat, že operace zpracování se může skládat z více dílčích operací zpracování, a to buď samostatně, nebo pokud jsou propojeny takovým způsobem, že je lze považovat za koherentní operaci zpracování, pokud jsou vzájemně kombinovány. V tomto ohledu je třeba rozlišovat mezi různými operacemi zpracování. Indikace jediné operace zpracování je dána účelem zpracování. Operace zpracování sloužící stejnému účelu by měly být obvykle považovány za jednu operaci nebo soubor operací. Rozhodujícím faktorem je rozhodující vliv na konkrétní kontext zpracování. Schopnost rozhodovat o důvodech zpracování, a tedy o jeho účelu, je charakteristická pro skutečnou rozhodovací pravomoc ohledně zpracování.

Fyzické osoby, uživatelé, nejsou od samého počátku vyloučeny z pojmu správcovství. S ohledem na účely zpracování a poskytování aplikace uživatelům, mají uživatelé možnost uplatnit rozhodovací pravomoc, pokud jde o to „jak“ – mohou v nastavení profilu některé věci změnit a ovlivnit tak chování aplikace, ale také může nastat situace, kdy nemohou chování aplikace ovlivnit, protože neexistuje dostatek možností konfigurace.

[65] WP29 – Opinion 1/2010 on the concepts of "controller" and "processor" – 4.5.2020 – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf..
[66] WP29 – Opinion 1/2010 on the concepts of "controller" and "processor" – 4.5.2020.

Přestože se uživatelé mohou de-facto rozhodnout, „zda“ zpracování zahájí instalací aplikace, tak následně už nemohou ovlivnit účel zpracování. Výměna klíčů mezi uživateli nepředstavuje samotnou operaci zpracování, protože dotyčný účel je jiným účelem než pouhou výměnou, jmenovitě porovnáváním informací. Uživatel není odpovědný, protože to již nezávisí na jeho rozhodnutí.

Pokud je aplikace provozována na základě právní povinnosti orgánem veřejné moci, např. ministerstvo zdravotnictví (MZ ČR) nebo jiný veřejný subjekt, např. stanice hygienické kontroly, bude vztah s uživateli charakterizován nejen informační asymetrií moci, ale také vztahem podřízenosti, který ukazuje na skutečnost, že odpovědným je orgán veřejné moci. Pokud provozovatel rozhoduje o tom, proč a jak se osobní údaje zpracovávají, pak je de facto rozhodovací pravomoc na provozovateli a je tedy za zpracování odpovědný. To platí i v případě, kdy jako provozovatel aplikace jedná soukromý subjekt. Není důležité, zda je to také výrobcem aplikace. Výrobce aplikace má rozhodovací pravomoc, pouze pokud rozhoduje o základních prostředcích a účelech zpracování. Přestože výrobce aplikace konfiguruje technický systém a má tedy vliv na jeho fungování, v konečném důsledku nerozhoduje o účelech skutečného zpracování, pro které se aplikace využívá.

Jsou-li aplikace a server(y) nezbytné pro funkčnost služby spravovány různými právnickými osobami, pak správcovství závisí na tom, kdo má skutečnou pravomoc rozhodovat o zpracování osobních údajů. Závisí to na typu aplikace (viz kapitola 4.1). Pokud k porovnávání a párování dochází na serveru (serverech) operátora a provozovatel rozhoduje o postupu pro porovnávání a párování a / nebo oznámení příjemci (kategorie 1 a 2), nebo pokud provozovatel uloží seznamy ID a dále je zpracuje, například pro výpočet dalších výsledků, které mohou být agregovány (např. statistika), má pro tyto operace zpracování skutečnou rozhodovací pravomoc. Pokud je přiřazení provedeno na koncovém zařízení (typ 3), znamená to skutečnou rozhodovací pravomoc, a odpovědnost tedy leží na straně provozovatele aplikace. Pokud je server provozován jinou právnickou osobou, lze v této konstelaci uvažovat o takovém zpracování, kde se v roli správce nachází provozovatel serveru.

Není nezbytné, aby správce měl přístup k osobním údajům. Podstatné je, že správce určuje, že ke zpracování osobních údajů v souvislosti s aplikací dochází na uživatelských zařízeních a také rozhoduje, které osobní údaje jsou v tomto ohledu zpracovávány.

Kromě toho nemusí být kontrola správce nad operací zpracování během celého postupu; stačí, že se týká konkrétních operací zpracování a že za jiné operace odpovídá jiný subjekt[67]. Provozovatelé aplikace a serveru (serverů) jsou považováni za společně odpovědné, pokud společně rozhodují o účelech a prostředcích zpracování[68].

Uživatelé nemohou nést odpovědnost jako společní správci s provozovateli. Vyloučení věcného rozsahu působnosti Obecného nařízení, které by se mohlo zvážit, pokud by zpracování osobních údajů fyzickými osobami bylo provedeno pro čistě osobní nebo domácí činnosti v souladu s čl. 2 odst. 2 písm. 2 písm. c) Obecného nařízení, nelze považovat za možné. Výměna klíčů není čistě osobní nebo rodinnou činností, ale slouží k účelům kontroly infekce nebo pandemické karantény (viz kapitola 5.3). V závěru však tato otázka

[67] Fashion ID GmbH & Co. KG vs Verbraucherzentrale NRW eV, C-40/17, bod 74. – 16.5.2020 – http://curia.europa.eu/juris/document/document_print.jsf?docid=216555&text=&doclang=CS&pageIndex=0&cid=434832.

[68] Kühling, Jürgen and Benedikt Buchner, eds. (2018). Datenschutz-Grundverordnung / BDSG. 2nd ed. München: C.H.Beck.

může zůstat nevyřešena, protože na jedné straně potvrzení výlučně osobních nebo rodinných činností nevylučuje, že provozovatel může mít odpovědnost (viz 18. bod odůvodnění Obecného nařízení), a na druhé straně uživatelé nemají právní ani faktický vliv na účel a rozhodnutí o tom, jak jsou osobní údaje zpracovávány na jejich zařízeních, a proto by se také nikdy neměly tyto osoby považovat za správce.

14.1 Proporcionalita

Všechny právní základy vyžadují, aby zpracování osobních údajů bylo přiměřené a adekvátní ve vztahu k účelům, pro které jsou osobní údaje zpracovávány. Operaci zpracování lze považovat za přiměřenou pouze tehdy, pokud bez ní nelze účelu dosáhnout, nebo jej nelze dosáhnout spolehlivě případně pouze s nepřiměřeným úsilím. To je třeba posoudit podle objektivních kritérií a musí existovat souvislost mezi zpracovávanými osobními údaji a účelem sledovaným jejich zpracováním.

Princip proporcionality, resp. nutnost aplikace třístupňového testu (zákonný podklad – legitimní cíl – nezbytnost/přiměřenost), používají při své rozhodovací činnosti Evropský soud pro lidská práva, Soudní dvůr Evropské unie (resp. Evropský soudní dvůr), např. rozsudek ze dne 20. května 2003 ve spojených věcech Österreichischer Rundfunk a další (C-465/00, C-38/01 a C-139/01) nebo rozsudek ze dne 9. listopadu 2010 Volker a Markus Schecke GbR (C-92/09) a Hartmut Eifert (C-93/09) vs. spolková země Hessensko, ale i Ústavní soud, např. nález zn. Pl. ÚS 4/94 ze dne 12. října 1994, zn. Pl. ÚS 15/96 ze dne 9. října 1996, či zn. Pl. ÚS 40/08 ze dne 26. května 2009 a Nejvyšší správní soud (např. rozsudek čj. 1 Afs 60/2009-119)[69].

Omezení základních práv a svobod je podle testu proporcionality možné pouze tehdy, jedná-li se o zásah, který je pro dosažení sledovaného cíle vhodný, nutný a přiměřený. Za přiměřený je považován takový zásah, kdy je možno očekávat, že dosažený prospěch realizací dané činnosti bude větší, nežli nepříznivý následek jí způsobený – v tomto případě zejména v podobě míry zásahu do osobnosti dotčených subjektů údajů.

V případech, kdy jsou vzájemně protichůdná základní práva vyvážena, musí být toto vyvážení vždy provedeno s ohledem na velmi specifické operace zpracování a jejich konkrétní formy. Předtím, než může být přijato rozhodnutí o zákonném nařízení, kterým se stanoví a legitimizuje konkrétní účel a operace zpracování, které mají být použity, musí být projednány účely, operace zpracování a souvislosti mezi nimi. K projednání musí dojít nejen na právním, ale i technickém základě, protože způsob využití technologie může mít zásadní vliv na výsledek, a tedy dopad na subjekt údajů.

Zásada proporcionality vyžaduje, aby zpracování osobních údajů

- sloužilo k legitimnímu účelu;
- bylo k dosažení tohoto účelu vhodné;
- bylo nezbytné k dosažení tohoto účelu (tzn. neexistují mírnější, stejně účinné prostředky); a
- bylo vhodné, tj. přiměřené v užším smyslu.

Operace zpracování je legitimní, pokud je účel zpracování v rámci úkolů svěřených státu. Je vhodné, pokud může v zásadě sloužit tomuto účelu přímo. Je nezbytné, pokud žádné mírnější prostředky nejsou pro tento účel srovnatelně účelné. Zpracování je vhodné nebo přiměřené, pokud závažnost zásahu do základních práv subjektu údajů není nepřiměřená vzhledem k závažnosti důvodů vedoucích k potřebě vzniku operace zpracování. Vždy je vyžadováno vyvážení právních zájmů.

[69] (ÚOOÚ, 2013).

14.1.1 Legitimní účel

Celkový účel aplikace souvisí nepřímo s ochranou života a fyzickou integritou osob během pandemie; tedy, jako celek, slouží k omezení a kontrole pandemie, konkrétně k zabránění šíření nových infekcí a k eliminaci rizika přetížení kapacity systému zdravotní péče. Jinými slovy slouží ke zploštění křivky nákazy. Jednotlivci nemohou tohoto cíle sami dosáhnout, je to tedy legitimní účel, který může sloužit jako základ pro právní povinnost nebo jako úkol ve veřejném zájmu.

Vzhledem k tomu, že k vyvážení musí dojít v konkrétním případě, je třeba v souvislosti s tímto DPIA považovat za příklady následující účely:

Účelem je informovat potenciálně infikované (exponované) osoby, tj. varovat osoby, které byly v kontaktu s infikovanými osobami a hrozí jim nebezpečí nákazy, obecně zastavit šíření nákazy.

Uvedených cílů lze dosáhnout, buďto bez použití technologie anebo právě využitím různých technologií. Samotný účel zpracování však není technickou otázkou.

14.1.2 Přiměřenost

Otázka přiměřenosti zpracování má technický aspekt, protože pokud určitá technologie nemůže být pro daný účel využita, pak nesmí být ani použita.

Technické vyhodnocení metadat GPS nebo mobilního telefonu ukazují, že tato data nejsou dostatečně přesná k identifikaci epidemiologicky významných kontaktních událostí. Tyto technologie jsou proto vyloučeny. Na druhé straně jsou vhodné technologie krátkého dosahu, jako je Bluetooth, protože jsou mimo jiné dokonce schopny měřit vzdálenost v dosahu přístroje.

Nadto zpracování údajů s využitím některých speciálních kategorií osobních údajů (jako je např. informace o potvrzené nákaze či infekční rizikovost) přesně splňují účel sledovaný správcem aplikace eRouška, přičemž na základě vyhodnocování těchto parametrů dochází ke zlepšení algoritmických výpočtů v samotné aplikaci a zkvalitnění výstupů pro další epidemiologický postup na to navázaný. Proto je nastavené zpracování datových parametrů pro sažení sledovaného účelu nezbytné, ale i dostatečně přiměřené.

14.1.3 Nezbytnost

Nezbytnost zpracování je jedním ze základních předpokladů zákonnosti. Při zvažování nezbytnosti zpracování je třeba zohlednit i technický aspekt. Pokud lze cíle dosáhnout pomocí „mírnějších“ technických prostředků, protože takový postup má z technických důvodů nižší míru zásahu do základních práv a svobod, pak musí být zvoleny tyto mírnější prostředky. Aby bylo možné posoudit, zda existují nebo jaké jsou mírnější prostředky, je obvykle nutné technické posouzení. V tomto ohledu je třeba zohlednit také požadavky článku 25 Obecného nařízení (Záměrná a standardní ochrana osobních údajů). To mimo jiné znamená, že je třeba zohlednit nejmodernější technologie a dodržovat zásadu minimalizace dat.

Používání technologií krátkého dosahu, jako je Bluetooth, by mohlo být nezbytné, pokud by úkol orgánů hygieny rychle a účinně detekovat řetězce infekce mohl být splněn mnohem rychleji a přesněji pomocí aplikace než prostřednictvím dotazníků a telefonických hovorů.

Zároveň při použití pseudonymizovaných ID je omezeno zjištění reálné totožnosti fyzických osob, čímž dochází k legitimizaci takovéhoto zpracování v jeho nezbytné a minimální míře.

14.1.4 Vhodnost

Zpracování je pro dosažení účelu dostatečné, pouze pokud je konkrétní rovnováha zájmů ve prospěch správce v kontextu s poměrem účelu a použitých prostředků. Při zpracování je třeba zájmy subjektů údajů porovnat se zájmy správce. Tento balanční test musí zohlednit i vedlejší účinky na společnost jako celek. Obecně se může jednat nejen o zdravotní záležitosti, ale také o sociální, ekonomické nebo psychologické dopady, přičemž tyto aspekty mohou být i vzájemně propojeny.

Z technického hlediska lze cíle dosáhnout pomocí technologií krátkého dosahu Bluetooth. Vše závisí na vhodnosti a podrobnostech technické implementace. I malé změny však mohou vést k jinému výsledku či výstupům zpracování údajů.

Povolení sdílení údajů v rámci interoperability mezi jednotlivými členskými státy EU umožňuje rychlejší a efektivnější snižování karanténních opatření, jenž omezují pohyb uvnitř EU.

14.2 Právo na informace a další uplatňovaná práva

Za účelem dodržení zásad zpracování podle čl. 5 odst. 1 Obecného nařízení, správce musí zajistit, aby zpracování bylo provedeno způsobem, který je pochopitelný a srozumitelný pro subjekty údajů. Transparentnost může být zajištěna plněním informační povinnosti. Správce nebo provozovatel proto musí subjektům údajů poskytnout veškeré informace podle článků 13 a 14 a všechna oznámení podle článků 15 až 22 a článku 34, které se vztahují ke zpracování v přesné, transparentní, srozumitelné a snadno dostupné formě psané jasným a srozumitelným jazykem (čl. 12, odst. 1 Obecného nařízení). Výše uvedené by mělo být uvedeno v prohlášení o ochraně osobních údajů, které by mělo být přístupné i z aplikace. Konkrétně by prohlášení o ochraně osobních údajů mělo zahrnovat informace o účelech zpracování, o použitých opatřeních, zejména o délce uchovávání osobních údajů, přenosech dat a jejich příjemcích a o tom, jak mohou subjekty údajů účinně uplatňovat svá práva vůči správci, a to i prostřednictvím odvolání u ÚOOÚ.

Transparentnost je zajištěna i kompletním zveřejněním kódu aplikace. K dispozici je na adrese https://github.com/covid19cz/. Struktura je rozdělena na následující části:

- erouska-firebase
- erouska-backend
- erouska-ios
- erouska-android
- erouska-homepage
- erouska-webapp

Veškeré informace pro subjekty údajů jsou uvedeny na adrese: https://erouska.cz, informace o podmínkách jejího užívání pak zde: https://erouska.cz/podminky-pouzivani.

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

ID, správce serveru i samotné aplikace není schopen z těchto údajů odvodit jednoznačnou identitu fyzické osoby, tak aby mohl technicky provést výmaz (např. z konkrétní databáze uložených user ID).

Pro podrobnosti ohledně uplatnění tohoto práva lze kontaktovat 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

14.3 Technická a organizační opatření

Čl. 24, odst. 1 Obecného nařízení vyžaduje, aby správce – s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Zásady ochrany osobních údajů splňuje za předpokladu, že je správce v souladu s čl. 5 Obecného nařízení, účinně realizuje požadavky postulované v čl. 32 Obecného nařízení, účinně zaručuje práva subjektů údajů v souladu s čl. 12 až 22 Obecného nařízení. Toto je prováděno prostřednictvím technického návrhu, výchozích nastavení a je doprovázeno řádnou správou ochrany osobních údajů.

15 Audity a nezávislé posouzení

15.1 Vyjádření Spolku pro ochranu osobních údajů

V rámci zvýšení ochrany práv subjektů osobních údajů byla navázána spolupráce se Spolkem pro ochranu osobních údajů, jenž je organizace zabývající se otázkami ochrany a zpracování osobních údajů, která sdružuje zájemce o tuto problematiku a profesionály zabývajících se zpracováním a ochranou osobních údajů v soukromém podnikání, samosprávě a veřejné správě. Zároveň se jedná o profesní organizaci sdružující pověřence pro ochranu osobních údajů, a to zejména pověřence, kteří jsou jmenováni k naplnění povinností dle článku 37 Nařízení Evropského parlamentu a Rady (EU) č. 2016/679. Členy spolku však mohou být i jiné osoby zajímající se o ochranu osobních údajů. Spolek je také členem European Federation of Data Protection Officers.[70]

Následně Spolek pro ochranu osobních údajů vydal vyjádření názoru, že v rámci nastavení aplikace eRouška 2.0 byly dodrženy veškeré základní zásady ke zpracování osobních údajů podle GDPR, zejména minimalizace zpracovávaných osobních údajů a minimalizace doby zpracování.[71]

[70] Spolek pro ochranu osobních údajů – 19.10.2020: https://www.ochranaudaju.cz/kdo-jsme/.
[71] eRouška 2.0 audity a posudky - 21.10.2020: https://erouska.cz/audit-kod.

15.2 Posudek Českého učení technického v Praze mobilní aplikace eRouška 2.0.

Dále tak jako v případě eRoušky verze 1.0, byla požádána univerzita Českého učení technického v Praze (ČVÚT) o spolupráci a zpracování posudku, v němž zástupci ČVÚT prohlásili, že eRouška 2.0 ve specifikované verzi:

„1. Aplikace neodesílá data o setkáních uživatele mimo zařízení. Ve chvíli, kdy je uživatel prohlášen za nakaženého, odesílá se, na základě pokynu uživatele zadáním kódu, anonymní identifikátory aplikace – tzv. TEK – na server.
2. Aplikace nesbírá údaje o GPS poloze telefonu.
3. Informace o setkáních jsou na telefonu uloženy v úložišti plně pod kontrolou Apple/Google API. Nejsou k dispozici uživateli ani není možné je zobrazit lokálním vývojářům aplikace.“[72]

16 Doporučení

16.1 Doporučení plynoucí z DPIA k aplikaci eRouška 2.0

1. Zakotvení provozování aplikace do povinné legislativy v oblasti veřejného zdraví
2. Případná změna v oblasti právního titulu pro přeshraniční zpracování údajů v souvislosti s interoperabilitou

16.2 Vyjádření osoby odpovědné za ochranu údajů

Pověřenec pro ochranu osobních údajů MZ ČR vydal následující stanovisko týkající se provedení zpracování a studie posouzení dopadu na soukromí:

Se závěry DPIA se lze ztotožnit. Za podstatné považuji zejména zakotvení v legislativě dle doporučení plynoucích z DPIA a od ÚOOÚ. Změny a předpokládaný budoucí vývoj je nezbytné nadále monitorovat z pohledu ochrany osobních údajů.

Aplikace kontrolních mechanismů plánovaná pro dodržování základních zásad ochrany soukromí a pro řešení rizik ohrožujících soukromí subjektů údajů je vzhledem k celkové situaci a uplatňovanému významnému veřejnému zájmu považována za přijatelnou.

17 Přílohy

Příloha č. 1 - Information from the processor to the joint controllers regarding the European Federation Gateway Service for the purpose of their Data Protection Impact Assessments (DPIA-Draft)

[72] eRouška 2.0 audity a posudky - 21.10.2020: https://erouska.cz/audit-kod.

18 Zdroje[73]

Aktuálně o koronaviru. (14. 5 2020). Načteno z https://koronavirus.mzcr.cz/

Cannataci, A. J. (2016). *The Individual and Privacy: Volume I.* : Routledge.

DATENSCHUTZ PEPP PT. (20. 4 2020). Načteno z https://www.pepp-pt.org/datenschutz

DP-3T Whitepaper. (22. 4 2020). Načteno z https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

eHealth Network. (15. 04 2020). Mobile applications to support contact tracing in the EU's fight against COVID-19.

Evropská komise. (4. 16 2020). Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection. Brusel.

Evropská komise. (8. 4 2020). on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Brusel.

Evropská komise. (20. 05 2020). *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).* Načteno z Úřední věstník EU: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32002L0058&from=DE

Fashion ID GmbH & Co. KG vs Verbraucherzentrale NRW eV, C-40/17. (29. 7 2019). Načteno z InfoCuria: http://curia.europa.eu/juris/document/document_print.jsf?docid=216555&text=&doclang=CS&pageIndex=0&cid=434832

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf. (2. 10 2019). Načteno z https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure. (12. 7 2020). Načteno z https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_en.pdf

Kühne, C. R., Bock, K., Mühlhoff, R., Ost, M. R., Pohle, J., & Rainer, R. (29. 4 2020). Data Protection Impact Assessment for the Corona App.

Länder, A. T. (17. 4 2020). The Standard Data Protection Model v. 2.0b. Kiel, Německo.

Neumann, L. (9. 5 2020). *„Corona-Apps": Sinn und Unsinn von Tracking.* Načteno z https://linus-neumann.de/2020/03/corona-apps-sinn-und-unsinn-von-tracking/

[73] Všechny zde uvedené zdroje jsou platné ke dni 8. 2. 2021.

PARTY, A. 2. (16. 2 2010). Opinion 1/2010 on the concepts of "controller" and "processor" .

Ryder, J. (6. 5 2020). DPIA NHS COVID-19 App PILOT LIVE.

Stanovisko Asociace pověřenců ČR k ochraně osobních údajů v souvislosti s Chytrou karanténou. (31. 3 2020).

Tang, Q. (nedatováno). Privacy-Preserving Contact Tracing: current. Luxembourg .

Toužimská, E. (15. 10 2015). *Nakládání s informacemi o zdravotním stavu pacienta*. Načteno z Právní prostor: https://www.pravniprostor.cz/clanky/obcanske-pravo/nakladani-s-informacemi-o-zdravotnim-stavu-pacienta

ÚOOÚ. (13. 11 2013). *K principu proporcionality při zpracování osobních údajů na základě zákona o svobodném přístupu k informacím*. Načteno z ÚOOÚ: https://www.uoou.cz/k-nbsp-principu-proporcionality-pri-nbsp-zpracovani-osobnich-udaju-na-zaklade-zakona-o-nbsp-svobodnem-pristupu-k-nbsp-informacim/d-5511/p1=1099

WP 29. (20. 5 2020). Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018. Načteno z EC: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051