MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

DATA PROTECTION IMPACT ASSESMENT (DPIA)

Projekt: IT podpora OČKOVÁNÍ

Verze 3, 18. 2. 2021

Obsah

1 Seznam zkratek (abecedně)

AČR nebo Armáda ČR	Armáda České republiky
CFA	Covid Forms App
CRS	Centrální rezervační systém
ČR	Česká republika
DPIA nebo Posouzení vlivu	Data Protection Impact Assessment – posouzení vlivu dopadu na ochranu osobních údajů
EDPB	Evropský sbor pro ochranu osobních údajů (dříve Pracovní skupina WP29)
EU	Evropská unie
GDPR nebo Obecné nařízení	nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna N016 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)
IISHS	Integrovaný informační systém hygienické služby
ISIN	Informační systém infekčních nemocí
MZ ČR nebo Ministerstvo zdravotnictví	Ministerstvo zdravotnictví České republiky
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OČM	očkovací místo
Posouzení vlivu	posouzení vlivu na ochranu osobních údajů dle čl. 35 Obecného nařízení
RČ	rodné číslo
ROB	Registr obyvatel
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚZIS	Ústav zdravotnických informací a statistiky ČR
zákon o ochraně veřejného zdraví	zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, v platném znění
zákon o kybernetické bezpečnosti	zákon č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění
zákon č. 569/2020 Sb.	zákon č. 569/2020 Sb., o distribuci léčivých přípravků obsahujících očkovací látku pro očkování proti onemocnění COVID-19, o náhradě újmy způsobené očkovaným osobám těmito léčivými přípravky a o změně zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, v platném znění

2 Historie změn

Datum	Verze	Popis změny
9. 1. 2021	1.00	Souhrnná vstupní DPIA
10. 2. 2021	2.00	Upřesnění textu
18. 2. 2021	3.00	Úprava jednotlivých fází očkování

3 Východiska

Při tvorbě tohoto Posouzení vlivu bylo primárně vycházeno z čl. 35 Obecného nařízení a schválených pokynů Evropského sboru pro ochranu osobních údajů.

Toto Posouzení vlivu však vznikalo v současné dynamické době celosvětové pandemie, která vyžaduje rychlé a efektivní rozhodování a změny procesů v kombinaci s technologickým a legislativním vývojem.

Je tedy zřejmé, že budou následovat další verze, které budou odrážet agilní vývoj v oblasti covid-19, zvyšování bezpečnosti zpracování, hodnocení rizik či konzultace s Úřadem pro ochranu osobních údajů.

3.1 Správce

- **Ministerstvo zdravotnictví České republiky**

3.2 Zpracovatel

- **Národní agentura pro komunikační a informační technologie, s. p.**
- **Ústav zdravotnických informací a statistiky ČR**
- **Armáda ČR**

Další zpracovatelé

- **Reservatic s.r.o.,** subzpracovatel pro NAKIT (rezervační modul)
- **KAKTUS Software, spol. s r.o.,** subzpracovatel pro NAKIT (registrační modul)
- **Railsformers s.r.o.,** subzpracovatel pro Reservatic s.r.o. (dílčí vývoj a podpora)
- **SuperNetwork s.r.o.,** subzpracovatel pro Railsformers s.r.o. (dodavatel infrastruktury)

3.3 Cílová skupina

- Ministerstvo zdravotnictví České republiky
- Úřad pro ochranu osobních údajů
- Odborná veřejnost, experti v technické a právní oblasti
- Provozovatel, výrobce a ostatní zúčastněné entity
- Evropská unie

3.4 Dokumenty vztahující se k metodice Posouzení vlivu

- ÚOOÚ – Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů[1]
- ÚOOÚ – Metodika obecného posouzení vlivu na ochranu osobních údajů[2]
- 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)[3]

[1] 10. 5. 2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940
[2] 10. 5. 2020 – https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46487
[3] 9. 5. 2020 – https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 WP 248 rev.01[4]

4 Úvod

Vývoj informačních systémů vztahujících se k očkování respektuje jedno ze základních pravidel GDPR, tedy „**protection by design**“. Jinými slovy již při vývoji aplikace je třeba respektovat právo na ochranu osobních údajů. Součástí takového přístupu je i analýza rizik spojená s užíváním informačních systémů, strukturou dat, jejich uložením apod., což v tomto ohledu respektuje druhé z pravidel, a to „**security by design**“. Kromě těchto technických aspektů vývoje informačních systémů patří k zodpovědnému vývoji i provedení **posouzení vlivu dopadu na ochranu osobních údajů**, tedy tzv. DPIA (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;
- 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.

Hned v úvodu čl. 35 odstavec 1 Obecného nařízení o ochraně osobních údajů uvádí: „*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.*“ Současně se jedná o **rozsáhlé zpracování zvláštní kategorie údajů** dle č. 9 odst. 1 GDPR (čl. 35 odst. 3 písm. b) GDPR) a také se jedná v případě Centrálního rezervačního systému o rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na **automatizovaném zpracování** (čl. 35 odst. 3 písm. a); čl. 22 GDPR). V této souvislosti lze konstatovat, že dle dosavadních zjištění správce u projektu očkování v zásadě vykonává odpovědnost stanovenou Obecným nařízením v čl. 5 odst. 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.

5 Systematický popis zamýšlených operací zpracování a účely zpracování

Z důvodu krizového vývoje epidemiologické situace na území České republiky spojené s výskytem koronaviru SARS-CoV-2, který vyvolává onemocnění covid-19, bylo rozhodnuto **o plošném dobrovolném očkování** obyvatelstva České republiky proti covid-19, protože právě očkování je nejúčinnějším nástrojem kontroly pandemie onemocnění covid-19, resp. zabránění šíření tohoto infekčního a hromadně se vyskytujícího onemocnění. Hlavním cílem očkovací kampaně proti covid-19 je tedy ochránit obyvatele ČR a zamezit dalšímu šíření nákazy v populaci, a to zajištěním prevence onemocnění touto infekcí a prevence reinfekce. Pouze dlouhodobá preventivní ochrana před onemocněním dokáže zabránit vzniku dalších vln pandemie. Tím lze dosáhnout snížení počtu úmrtí,

[4] 8. 1. 2021- wp248 rev.01_cs (uoou.cz)

zabránit přetížení zdravotnických zařízení, přispět k ochraně rizikových skupin obyvatelstva, zdravotnických pracovníků a ochraně klíčových složek kritické infrastruktury.

Samotné očkování je zcela DOBROVOLNÉ a je na rozhodnutí subjektu údajů, zda jej využije. V návaznosti na to je také dobrovolné využití IT systému, které k registraci očkování slouží.

Koncept IT podpory vychází z dokumentu "**Strategie očkování proti covid-19 v České republice**" (vzata na vědomí vládou ČR 7. 12. 2020 – aktualizována 22. 12. 2020).[5] Hlavním cílem očkovací kampaně proti covid-19 je ochránit obyvatele ČR a zabránit dalšímu šíření nákazy v populaci, a to zajištěním prevence vzniku onemocnění způsobeného touto infekcí a prevence reinfekce. IT podpora byla vytvořena v návaznosti na implementaci **zákona č. 569/2020 Sb.** a dále v návaznosti na **zákon o ochraně veřejného zdraví**.

Účelem IT podpory očkování je zabezpečit podporu procesů a provoz řídících a koordinačních struktur, a subjektů participujících na procesu očkování.

IT podpora pro zabezpečení procesů očkování sestává ze tří bloků:

1. **Centrální rezervační systém**, který svými komponentami plní role registrace a rezervace.
2. **ISIN/Vakcinační modul OČKO**, který svými komponentami plní role evidence provedeného očkování a vystavení certifikátu o provedeném očkování.
3. Aplikace a systémy podporující řídící a logistické procesy, jedná se o systémy a aplikace Chytré karantény jako jsou **CFA, EPI Dashboard** a další.

V rámci DPIA bude samostatně popsán zejména informační systém CRS a OČKO.

Z hlediska IT podpory lze postup očkování rozdělit na tyto procesní bloky:

1. **Registrace** – online registrační formulář pro osoby indikující jejich zájem a souhlas s očkováním, s nutným vyplnění atributů pro prioritizaci (zařazení osoby do příslušné skupiny).
2. **Prioritizace**, kapacitní plánování a výzva osoby k rezervaci termínů – z registrací je vypočteno bodové skóre, které spolu s plánem dodávek vakcín určuje, kdy je osoba vyzvána k rezervaci konkrétního termínu.
3. **Rezervace termínů** – na základě PIN kódu zaslaného notifikací bude osobě umožněna rezervace obou termínů očkování v CRS.
4. **Očkování** – vlastní očkovací úkon a jeho dokumentace (zapsání úkonu do registru ISIN a potvrzení o očkování pro osobu).

Systém je navržen tak, aby **registraci a rezervaci seniorů** (která vyžaduje znalost práce s internetem) mohli provádět **rodinní příslušníci, sociální pracovníci i pracovníci informační linky 1221**.

Proces očkování je postaven na čtyřech fázích:

- **Přípravná fáze** – vytvoření základních podmínek pro průběh očkování;
- **Fáze IA** – očkování nejrizikovějších skupin obyvatelstva – zabránění růstu nemocnosti a úmrtnosti u seniorů (80+) a u institucionalizovaných osob, ochrana určeného zdravotnického personálu a osob zajišťujících péči u vybraných poskytovatelů sociálních služeb;
- **Fáze IB** – očkování prioritních skupin obyvatelstva – zabránění růstu nemocnosti a úmrtnosti u osob s vybranými chronickými onemocněními, senioři (65+), ochrana osob zajišťujících kritickou infrastrukturu státu;
- **Fáze II** – očkování dalších skupin obyvatelstva – zabránění růstu nemocnosti a úmrtnosti ostatní populace ČR.

[5] 8.1.2021 - zVlády – Jednání vlády – Portál Aplikace ODok

5.1 IT podpora ve vazbě na proces očkování

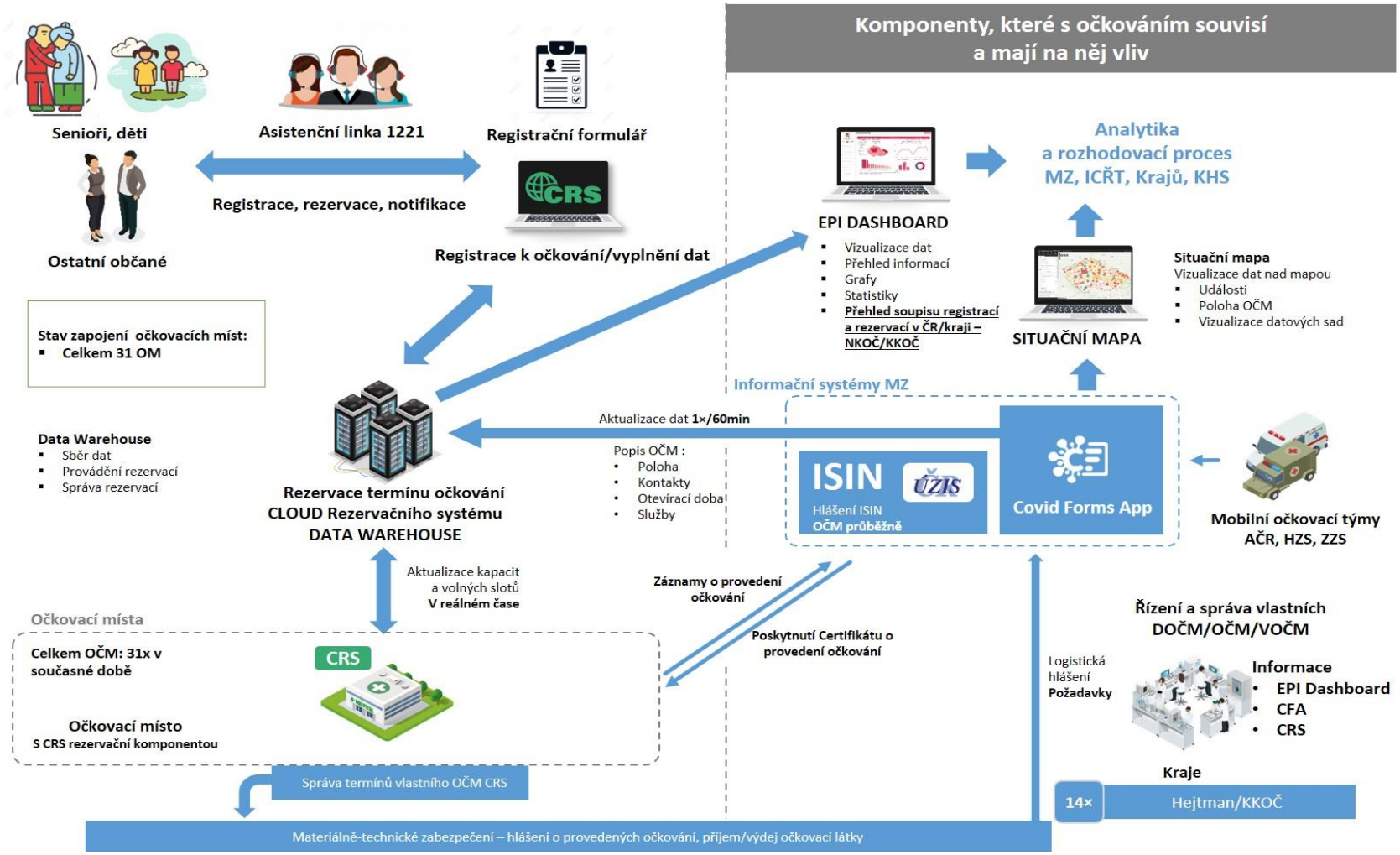


Schéma 1 - IT podpora ve vazbě na proces očkování

6 Centrální rezervační systém

6.1 Základní popis CRS

Formulář je počáteční bod pro vstup do procesu očkování. Poskytuje přístup k registraci na očkování z jednoho místa (formulář/web MZ ČR). Vyplněním formuláře vyjadřuje osoba svůj **dobrovolný zájem o provedení očkování** a poskytuje **o své osobě údaje**, které jsou pro provedení **nezbytné** (viz níže v podkapitole 6.2.)

1. Vyplnění registračního formuláře – osoba na CRS registrace
    a. registraci provede osoba přímo na webu, nebo asistenčně přes informační linku 1221, nebo v zastoupení za seniora
    b. registraci může rovněž provést praktický lékař (není jeho povinností), nebo alespoň poskytnout osobě údaje nutné pro správnou indikaci,
    c. CRS registrace zašle data do ISIN – podle samo-indikace ve formuláři se vyplní příslušná pole případu v ISIN.

Při vstupu do registračního formuláře je osoba vyzvána k zadání telefonního čísla a následně kódu (PIN1). Touto metodou je omezena možnost útoku na web Registrační formulář. Osoba vyplní např. věk, rodné číslo, zdravotní pojišťovnu a základní informace o svém zdravotním stavu. Není-li si sama osoba jista svým zdravotním stavem ve vztahu k očkování, provede konzultaci se svým lékařem.

Při registraci dále provede volbu preferovaného OČM (jedná se pouze o preferenci, z důvodu enormního vytížení OČM mohou být termíny preferovaného OČM vyčerpány).

2. Systém provede kalkulace priority dle vyplněného formuláře a kapacitního plánu – CRS registrace (prioritizace).
3. Systém zajistí notifikaci osoby o přijetí registrace. Po zahájení očkování skupiny, do které osoba náleží, je mu poskytnut přístup k provedení rezervace. Tuto informaci doplňuje kód (PIN2) pro přístup do rezervační komponenty.
4. Rezervace termínu očkování – osoba v CRS Rezervační komponentě.

Rezervační komponenta poskytuje osobě nástroj k provedení rezervace na přesné datum v rámci časového období skupiny, do které je zařazen. K rezervační komponentě má osoba přístup odkazem získaným při provádění registrace a rovněž je nutné **použít získaný kód (PIN2)**.

Rezervační komponenta získává data nezbytná pro vedení rezervace z registračního formuláře a nabízí osobě výběr OČM, data a času – vše dle dostupných kapacit OČM. Zájemce o očkování provádí rezervaci na první termín očkování. Rezervace pro 2. termín se vytvoří a distribuuje občanovi automaticky až na základě záznamu v ISIN o typu aplikované vakcíny v prvním termínu (s požadovaným intervalem dle typu užité vakcíny). Osobě je poskytnuto potvrzení rezervace. Změny termínu jsou možné v omezeném rozsahu, zejména z důvodu předpokládaného vytížení OČM a závislosti na dodávkách vakcín.

6.2 Výčet zpracovávaných osobních údajů

V rámci formuláře jsou vyžadovány následující údaje:

Období od 15. 1. 2021

Registrační modul:

- Jméno
- Příjmení
- Číslo pojištěnce
- Číslo pojišťovny
- Místo trvalého pobytu
- E-mail (variantně)
- Telefon
- Preferované OČM
- Dosažená věkové hranice
- Profesní příslušnost

Rezervační modul:

- Číslo pojištěnce
- Jméno
- Příjmení
- Adresa trvalého pobytu
- Číslo pojišťovny
- Vybrané OČM
- Telefon
- E-mail (nepovinný)

Následné rozšířené registrace

- Jméno
- Příjmení
- Číslo pojištěnce
- Číslo pojišťovny
- Místo trvalého pobytu
- E-mail (variantně)
- Telefon
- Preferované OČM
- Dosažená věkové hranice
- Profesní příslušnost
- Zdravotní stav

6.2.1 Ztotožnění osoby

Rozsah vyžadovaných identifikačních údajů je vyžadován v návaznosti na nutnost ztotožnění konkrétní osoby prostřednictvím ISIN, respektive základních registrů (např. v rámci ROB).

- Jméno
- Příjmení
- Datum narození

6.2.2 Ověření správnosti dat uvedených v CRS

Údaje uvedené v CRS jsou ověřovány na očkovacím místě. Jsou ověřovány jak identifikační údaje, tak údaje o zdravotním stavu a profesní příslušnosti.

6.3 Právní titul zpracování osobních údajů

V rámci CRS dochází ke zpracování osobních údajů dle čl. 4 bodu 1, 2 Obecného nařízení a je také zpracovávána zvláštní kategorie osobních údajů. Současně je využíváno **automatizované rozhodování** dle čl. 22 Obecného nařízení **pro prioritizaci osob** v rámci očkování. Správce vyhodnotil veškeré jiné možnosti řešení, ale vzhledem k počtu očkovaných osob a počtu očkovacích dávek muselo být přistoupeno k automatizované prioritizaci rizikových skupin osob. Vzhledem k nutnosti zajištění funkčního a efektivního rezervačního systému bylo přistoupeno k tomuto řešení, které bylo vyhodnoceno jako procesně nejvhodnější a zároveň efektivní řešení z pohledu managementu očkování a jeho logistického zabezpečení.

Osobní údaje jsou zpracovávány dle čl. 6 odst. 1 písm. a), c), čl. 9 odst. 2 písm. a), čl. 22 odst. 2 písm. c) Obecného nařízení.

Očkování proti onemocnění covid-19 je dobrovolné, stejně tak rezervace na jeho provedení. K jejich absolvování tedy osoba projeví svobodný projev vůle.

Před započetím je zájemce o registraci k očkování informován o podmínkách nakládání s jeho osobními údaji, a to přímo na registračním webu, nebo v případě asistence pomocí linky 1221 na této lince.

Rezervující osoba je dále poučena o automatizovaném zpracování, neboť součástí rezervace je také automatické rozdělování skupin osob dle prioritizace (*věk, zdravotní stav, profese*).

Souhlas subjektu údajů může být kdykoliv odvolán. Registrující osoba je před započetím zpracování informována, že může kdykoliv svůj souhlas odvolat dle čl. 7 odst. 3 Obecného nařízení. V případě odvolání souhlasu (*v době od započetí rezervace až do dostavení se k poslední dávce očkování*) jsou její osobní údaje bezodkladně vymazány.

S registrací může pomoci seniorům další osoba (*například rodinný příslušník, ošetřovatel atd.*). V případě vyplnění formuláře cestou linky 1221 je právní titul k vyplnění čl. 6 odst. 1 písm. b) Obecného nařízení pro plnění smluvního vztahu a následně je vyžádán souhlas se zpracováním osobních údajů ve formuláři CSR a s profilováním/automatizovaným zpracováním dle čl. 22 odst. 2 písm. c) Obecného nařízení.

6.4 Doba uložení údajů

Údaje z registračního modulu aktuálně nejsou mazány.

Údaje z rezervačního modulu budou mazány standardně nastavenou automatickou anonymizací dat 365 dní po proběhlé rezervaci. Očkovací místo má možnost si tento interval změnit.

Tato lhůta bude upravena/zkrácena.

V případě odvolání souhlasu dojde okamžitě k výmazu dat z CRS, současně není možné se účastnit očkování, protože jsou současně odstraněny i rezervované termíny očkování.

6.5 Cookies

Cookies registrace
V rámci registračního procesu nejsou v registrační aplikací pro registraci občany vkládány a využívány Cookies. Systém může obsahovat systémová Cookies, která jsou do stránek vkládána dalšími systémy, kterými jsou běhové prostředí Microsoft .Net Core, Google reCaptcha a Google Analytics.

Cookies rezervace
Aktuálně ukládané Cookies

- Aktuální časové razítko
- Interní ID uživatele (pokud má uživatel zřízen účet v systému Reservatic a je přihlášen)
- Naposledy používaná jazyková verze
- Potvrzení Cookies
- Samotné ID session

Registrace ani rezervace není z technického pohledu funkční v případě zakázání Cookies. Cookies jsou využívány na základě oprávněného zájmu.

6.6 Využití Google Analytics

V rámci Google Analytics jsou v rámci registrací a rezervací sbírány pouze:

- Obecné analytické údaje
- Obecné technické informace o prohlížeči
- Geografické údaje do úrovně krajských měst

IP adresa je anonymizována, je vypnutý remarketing, v URL není sbíráno RČ ani e-mail, přístupy jsou řízeny – pouze pro odpovědné zaměstnance MZ ČR, ÚZIS a Reservatic.

Odkaz na Ochranu soukromí a smluvní podmínky v rámci využití Google Analytics:

https://policies.google.com/privacy?hl=cs

https://marketingplatform.google.com/about/analytics/terms/cz/

7 ISIN/Vakcinační modul OČKO

7.1 Základní popis modulu OČKO

ÚZIS je provozovatelem Integrovaného infomačního systému hygienické služby IISHS, jehož součástí je ISIN. Tyto infomační systémy jsou provozovány v unikátním prostředí resortních zdravotnických registrů, jehož základní komponenta **Jednotná technologická platforma je součástí kritické infrastruktury státu** dle zákona o kybernetické bezpečnosti. Prostředí resortních zdravotnických registrů umožňuje standardizovaný a snadný vývoj nových komponent registrů v souladu s požadavky zákona o kybernetické bezpečnosti a ochrany osobních údajů.

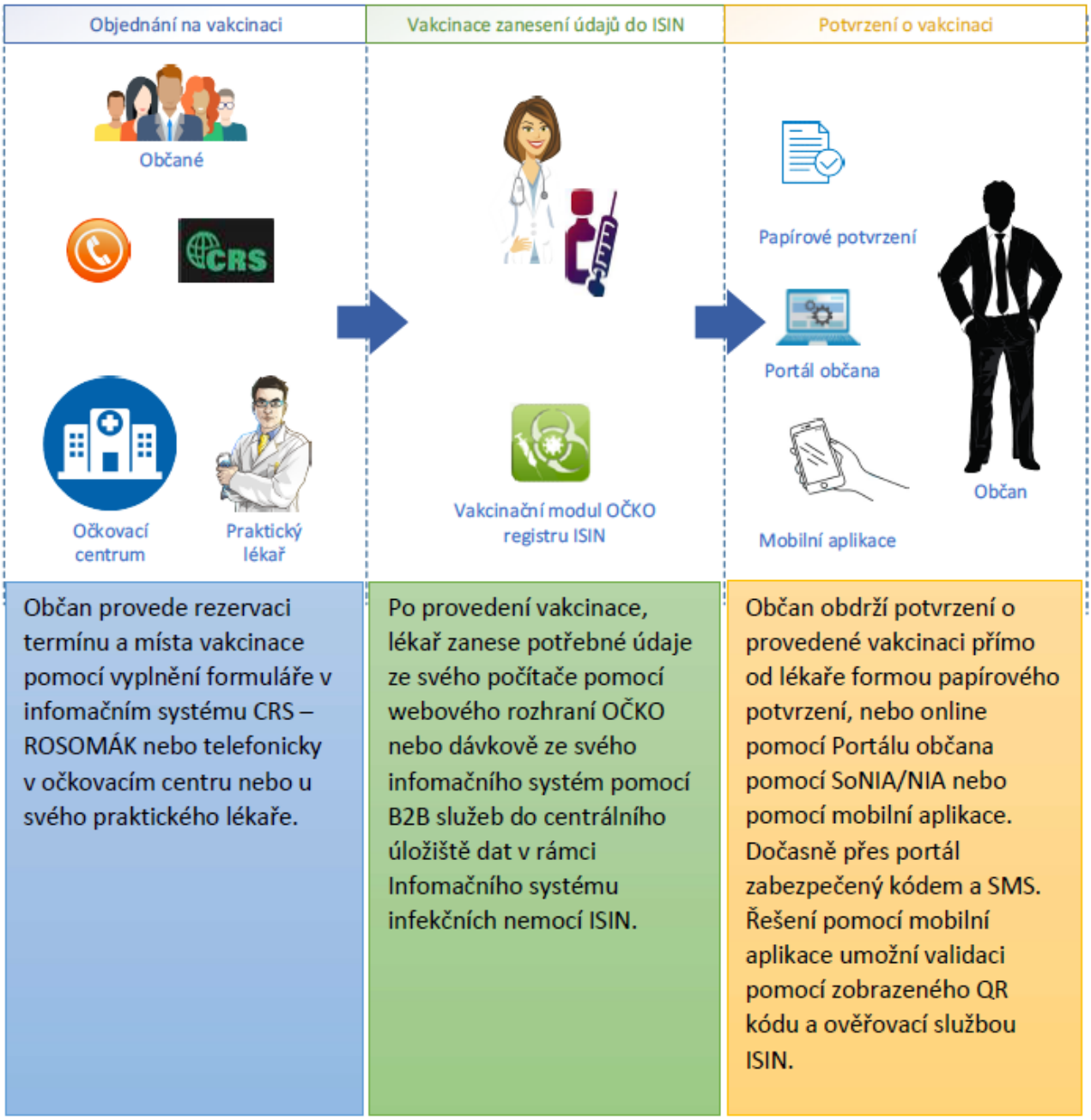
Vakcinační modul OČKO byl navržen jako logické rozšíření modulu ISIN a centrálního úložiště dat, modul byl vytvořen zejména pro zpřístupnění výsledků očkování praktickým lékařům, hygienickým stanicím a pro statistické zpracování dat pak Ministerstvu zdravotnictví. Využívá připravené komponenty, naplněné datové struktury a dostupné další datové zdroje ISIN, ÚZIS a MZ ČR. Využívá infrastrukturu eREG včetně existujícího administrativního zázemí (procesy registrace, podpory uživatelů) a již existující uživatelské přístupy většiny zdravotnických pracovníků. Systém je modulární a umožní v postupných krocích dosáhnutí cílového stavu, podle plánu a operativně podle priorit dle aktuální epidemiologické situace. Systém je provozován na základě legislativního zmocnění **dle zákona o ochraně veřejného zdraví**.

Vakcinační modul OČKO je moderní platformou pro centralizované uchovávání informací o provedené vakcinaci. Přestavuje praktickou aplikaci **koncepce Elektronizace zdravotnictví České republiky,** jejímž hlavním nositelem je MZ ČR.

Základní přehled funkcí vakcinačního modulu:

- Vyhledání a ztotožnění pacienta.
- Informace o pacientovi – dohledání údajů včetně COVID testů a informací ze žádanek, karantén a izolace.
- Evidence provedeného očkování pacienta.
- Přístup k historii všech očkování pacienta.
- Notifikace uživatelům a pacientům o provedených vakcinacích, termínech apod.
- Vystavování a ověření potvrzení o provedeném očkování.
- Přístup webovou službou pro software lékařů a dalších institucí.
- Poskytnutí informací pro pacienta a zákonného zástupce na portál občana.
- Poskytnutí informací pro zahraniční informační systémy v rámci NCP.
- Vedení elektronického očkovacího průkazu občana.
- Reporty a exporty (pouze základní přehledové reporty a exporty pacientů), dle potřeb.

Příklad využití vakcinačního modelu:



7.2 Výčet zpracovávaných osobních údajů

V rámci modulu OČKO jsou evidovány následující údaje:

- Jméno
- Příjmení
- Rodné číslo/datum narození/místo narození/občanství (pro cizince)
- Číslo pojištěnce

Informace k očkování:

- Typ: Očkování proti covid-19
- Číslo
- Stav: Indikováno
- Indikace např. věk
- Očkovací látka
- Aplikační cesta
- Datum vakcinace
- Typ výkonu
- Šarže
- Expirace
- Místo aplikace – končetina
- Místo aplikace – strana
- Místo aplikace – pozice
- Poznámka
- Reakce
- Subjekt, který očkování provedl

7.3 Právní titul zpracování osobních údajů

Ministerstvo zdravotnictví plní povinnosti stanovené zákonem v oblasti prevence vzniku a šíření infekčních onemocnění. Zákon o ochraně veřejného zdraví zároveň ve vymezuje některé pojmy, které jsou podstatné pro práci orgánů ochrany veřejného zdraví, jsou jimi zejména tyto pojmy:

Veřejným zdravím je zdravotní stav obyvatelstva a jeho skupin. Tento zdravotní stav je určován souhrnem přírodních, životních a pracovních podmínek a způsobem života.

Ochrana veřejného zdraví je souhrn činností a opatření k vytváření a ochraně zdravých životních a pracovních podmínek a **zabránění šíření infekčních a hromadně se vyskytujících onemocnění,** ohrožení zdraví v souvislosti s vykonávanou prací, vzniku nemocí souvisejících s prací a jiných významných poruch zdraví a dozoru nad jejich zachováním. Ohrožením veřejného zdraví je stav, při kterém jsou obyvatelstvo nebo jeho skupiny vystaveny nebezpečí, z něhož míra zátěže rizikovými faktory přírodních, životních nebo pracovních podmínek překračuje obecně přijatelnou úroveň a představuje významné riziko poškození zdraví.

Podpora veřejného zdraví je souhrn činností pomáhajících fyzickým osobám zachovat a zlepšovat své zdraví a zvyšovat kontrolu nad faktory ovlivňujícími zdraví. Zahrnuje činnosti k zajištění sociálních, ekonomických a environmentálních podmínek pro rozvoj individuálního i veřejného zdraví, zdravotního stavu a zdravého životního stylu.

K plnění těchto úkolů využívají ve smyslu ustanovení **§ 47b zákona o ochraně veřejného zdraví** tyto **zdroje údajů**:
a) referenční údaje ze základního registru obyvatel
b) údaje z agendového informačního systému evidence obyvatel,
c) údaje z agendového informačního systému cizinců.

Konkrétními využívanými údaji podle písm. a) jsou
a) příjmení,
b) jméno, popřípadě jména,

c) adresa místa pobytu,
d) státní občanství, popřípadě více státních občanství.

Konkrétními využívanými údaji podle písm. b) jsou
a) jméno, popřípadě jména, příjmení, popřípadě jejich změna, rodné příjmení,
b) adresa místa trvalého pobytu,
c) státní občanství, popřípadě více státních občanství,
d) počátek trvalého pobytu, popřípadě datum zrušení údaje o místu trvalého pobytu nebo datum ukončení trvalého pobytu na území České republiky.

Konkrétními využívanými údaji podle písm. c) jsou
a) jméno, popřípadě jména, příjmení, jejich změna, rodné příjmení,
b) státní občanství, popřípadě více státních občanství,
c) druh a adresa místa pobytu,
d) počátek pobytu, popřípadě datum ukončení pobytu.

V souladu s ustanovením § 79 zákona o ochraně veřejného zdraví jsou orgány ochrany veřejného zdraví oprávněny ke sběru a zpracování osobních a citlivých údajů. Orgány ochrany veřejného zdraví jsou ve smyslu ustanovení § 78 zákona o ochraně veřejného zdraví Ministerstvo zdravotnictví, krajské hygienické stanice, Ministerstvo vnitra a Ministerstvo obrany. Konkrétními údaji, vedenými v registrech, které jsou oprávněny vést orgány ochrany veřejného zdraví jsou:

osobní údaje:	V rozsahu jméno, příjmení, rodné číslo, je-li přiděleno, jinak datum narození, místo pobytu fyzických osob, místo jejich podnikání nebo označení jejich zaměstnavatele, údaje související s kategorizací prací a s nařízenými lékařskými preventivními prohlídkami a osobní údaje podle § 40 písm. a) zákona o ochraně veřejného zdraví;	Jde-li o mladistvé a studenty, označení zařízení pro výchovu a vzdělávání nebo označení dětského domova pro děti do 3 let věku.

citlivé údaje: vypovídající o zdravotním stavu fyzických osob, zahrnující diagnózy onemocnění, údaje o rizikovém chování, o splnění povinnosti podrobit se léčení, o počtu, druhu a závěrech lékařských prohlídek, údaje o expozici fyzických osob faktorům pracovního a životního prostředí, údaje o epidemiologii drogových závislostí a citlivé údaje podle § 40 písm. a) zákona o ochraně veřejného zdraví.

Podle § 79 odst. 2 věty druhé zákona o ochraně veřejného zdraví **může být rozsah zpracovávaných údajů rozšířen pouze výjimečně v zájmu splnění povinnosti orgánu ochrany veřejného zdraví, stanovené právním předpisem a za podmínek stanovených zvláštním zákonem.** Tímto zvláštním zákonem byl zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Tento zákon byl zrušen zákonem č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.

MZ ČR je ústředním orgánem státní správy pro rezort zdravotnictví a v souladu s výkonem státní správy a plnění úkolů v ochraně a podpoře veřejného zdraví ve smyslu zákona o ochraně veřejného zdraví spolu s Krajskými hygienickými stanicemi vytvořilo program k zajištění povinného hlášení, evidence a analýzy výskytu infekčních nemocí v České republice v ISIN.

KHS jsou **společnými správci** spolu s MZ ČR, který je **centrálním správcem** osobních a zvláštních kategorií osobních údajů – citlivých údajů vedených v systému ISIN.

Orgány ochrany veřejného zdraví mohou vést v registrech osobní údaje, vč. citlivých údajů, zahrnující údaje o zdravotním stavu. Explicitně však není zmíněna aplikace očkovací látky. Ve smyslu ustanovení § 79 odst. 2 věta druhá lze však v zájmu plnění úkolů orgánů ochrany veřejného zdraví rozšířit rozsah údajů v registrech vedených.

Nový modul OČKO je provozován na základě veřejného zájmu dle čl. 6 odst. 1 písm. e) a čl. 9 odst. 2 písm. i) GDPR. Toto zpracování osobních údajů je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, kterým je pověřen správce v oblasti veřejného zdraví, při ochraně před vážnými přeshraničními zdravotními hrozbami. Postupujeme při tom jako ústřední orgán státní správy, a stejně jako krajské hygienické stanice plníme své úkoly dle zákona o ochraně veřejného zdraví.

7.4 Přístupy do modulu OČKO

Pro řízení přístupů slouží **jednotná správa uživatelů**, jež je komponentou rezortních zdravotnických registrů Ministerstva zdravotnictví. O přístup mohou žádat pouze uživatelé, kteří jednoznačně prokážou svoji identitu prostřednictvím svých osobních údajů. Za subjekt údajů podává prvotní žádost o přístup statutární zástupce daného IČ. Po zřízení prvotního přístupu může uvedená osoba v oficiální žádosti přidávat řízeným způsobem přístupy pro další zaměstnance ve své organizaci. Přístupy jsou tímto zabezpečeným přístupem přidělovány definovaným subjektům, které mohou mít dle zákona zajištěný přístup. Jde zejména o poskytovatele zdravotních služeb (praktičtí lékaři, poskytovatelé lůžkové péče), hygienické stanice a Ministerstvo zdravotnictví.

Při přístupu k registru OČKO musí každý uživatel provést dvoufázovou autentifikaci.[6] Veškeré akce přihlášeného uživatele jsou pak logovány pro případnou kontrolu.

8 Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů

Rezervační systém byl posouzen z hlediska jeho proporcionality a požadované i zpracovávané osobní údaje byly shledány jako adekvátními vzhledem k současné akutní potřebě v oblasti ochrany obyvatelstva a stabilizace celkové epidemiologické situace.

Rezervační systém je současně navržen takovým způsobem, aby při jednotlivých operacích zpracovávání osobních údajů bylo dosaženo co největší minimalizace takovýchto údajů v rámci jednotlivých dílčích procesů zpracování (viz výše) a bylo přitom dosaženo legitimního zájmu správce na efektivním průběhu celého procesu registrace a následné rezervace v rámci očkovací strategie.

8.1 Posouzení právních titulů zpracování

Správce se před započetím samotného zpracování údajů zamýšlel a následně posoudil vhodné právní tituly k zákonnému zpracování.

[6] Prostřednictvím webového rozhraní a sms.

Jako právní titul ke zpracování osobních údajů se jevil jako nejpříhodnější **čl. 6 odst. 1 písm. e) plnění úkolu ve veřejném zájmu,** jímž je správce pověřen a **čl. 9 odst. 2 písm. i) nezbytné zpracování ve veřejném zájmu v oblasti veřejného zdraví**, jako je ochrana před vážnými přeshraničními zdravotními hrozbami[7], čímž pandemie covid-19 bezpochyby je.[8]

Rychlé, bezproblémové a efektivní proočkování společnosti je důležité k ochraně životů a zdraví osob. Opatření proti covid-19 však také způsobují značné ekonomické ztráty. Jelikož se jedná o jednu z nejnáročnějších logistických operací České republiky, je z toho důvodu rezervační systém koncipován s počátečním automatickým profilováním osob, aby mohl co nejrychleji a nejefektivněji provést rezervaci potřebným skupinám obyvatel a zajistit jim nezbytné očkování. Jelikož **zákon č. 569/2020 Sb., zákon o ochraně veřejného zdraví** ani **jiná právní norma Evropské unie či České republiky** nestanovují podmínky automatizovaného zpracování v této souvislosti, **nelze tedy aplikovat čl. 22 odst. 3 Obecného nařízení**.

Správce v tomto směru přihlédnul ke stanovisku EDPB č. WP251rev.01,[9] bod č. 5 str. 14:

„*Čl. 6 odst. 1 písm. e) – nezbytnost pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci Článek 6 odst. 1 písm. e) může být za určitých okolností vhodným základem pro profilování ve veřejném sektoru. Úkol nebo funkce musí mít jasný základ v právu*.“

A dále na str. 22 jako vzorové rozhodnutí, které se fyzické osoby významně dotýká jako:

„*rozhodnutí, která se dotýkají přístupu určité osoby ke zdravotním službám*“ .

Správce tedy adekvátně stanovil zpracování v CRS dle čl. 6 odst. 1 písm. a), c), čl. 9 odst. 2 písm. a), čl. 22 odst. 2 písm. c) Obecného nařízení.

8.2 Posouzení přiměřenosti rozsahu osobních údajů

Správce se zamýšlel a posoudil vhodný rozsah zpracovávaných osobních údajů v souladu se zásadou přiměřenosti dle ust. čl. 5 odst. 1 písm. c) Obecného nařízení: „c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“).“

Správce stanovil pro provedení rezervace a očkování rozsah osobních údajů uvedených v kapitolách, a to v části 6.2 pro rezervaci a registraci a části 7.2 pro očkování.

Funkcionalita systému je rozdělena do několika fází, které odráží aktuální stav *(zejména množství vakcín a rizikovost ohrožených skupin obyvatel*). Z toho důvodu ve fázi IA bude od 15. 1. 2021 služba dostupná pouze pro nejrizikovější skupiny osob. **Další výběr nebude možný a nebude tedy probíhat automatické profilování**. Pro potřebu rezervace a registraci jsou požadovány běžné osobní údaje (*jméno, příjmení, preferované očkovací místo*), důležité pro ztotožnění osoby pro potřeby rezervace, víceúrovňové verifikace (*telefon*) a zdravotních systémů (*číslo pojištěnce, číslo pojišťovny, místo trvalého pobytu, dosažená věkové hranice, profesní příslušnost*).

[7] 8.1.2021-NATO – COVID-19
[8] 8.1.2021-WHO Coronavirus Disease (COVID-19) Dashboard | WHO Coronavirus Disease (COVID-19) Dashboard
[9] 8.1.2021-wp251rev_en (uoou.cz)

Jako alternativní a nepovinný je email, díky čemuž plynou pro registrované výhody *(například možnost zaslání potvrzení o očkování v PDF formátu, nebo alternativní možnost kontaktu v případě uvedeného špatného telefonního čísla*).

Ve fázi IB přibude **informace o zdravotním stavu a profesní příslušnosti (mimo zdravotní specializaci), která je nutná k prioritizaci rizikových skupin obyvatel.**

Po příchodu na očkovací místa proběhne ztotožnění osob dle platného dokladu totožnosti, aby nedošlo k záměně osob a posouzení informací zdravotním personálem, aby nedošlo k zneužití či neúmyslnému uvedení mylných informací, které by měly za následek zdravotní riziko pro očkované osoby. Příchodem osoby na očkovací místo, **končí funkce rezervace a veškerý tok dat (*včetně osobních údajů*) probíhá v rámci ISIN**, který pak případně komunikuje s dalšími IS či registry údajů (*například základními registry, které ke ztotožnění vyžadují jméno, příjmení, datum narození*). Celý systém je navržen tak, aby nebyly zahlceny očkovací místa a nedocházelo při očkování k nadměrnému shlukování osob, avšak při plném respektování práv a svobod očkovaných osob a implementaci přísných bezpečnostních pravidel.

9 Posouzení rizik pro práva a svobody subjektů údajů

Správce identifikoval hlavní rizika, která by při využití informačních systémů pro zabezpečení procesů očkování mohly narušit práva a svobody osob.

9.1 Zneužití identity – úmyslné uvedení cizích osobních údajů

Rezervační systém provádí vícefaktorovou autentizaci uživatele pomocí mobilního telefonu. Tímto se zabrání například robotickému přetěžování informačního systému i očkovacích kapacit. Veškeré informace k osobě jsou **následně ověřovány na očkovacích místech zdravotním personálem**. Zde jsou osoby ztotožňovány pomocí dokladů totožnosti, průkazů pojištěnce či dalších potřebných dokumentů (*například lékařské zprávy*). Zde již běží standardní proces v oblasti lékařských úkonů. Pokud by tedy při úvodním vyplnění registračního formuláře uživatel zneužil cizí identitu, nebo uvedl smyšlené osobní údaje, dojde pouze ke zneužití rezervačního termínu, nikoliv však ke zneužití či nesprávné aplikaci samotného očkování.

9.2 Neúmyslné uvedení nesprávných informací

Výše popsaný systém vícefaktorové validace osoby odhalí nesprávně uvedené informace, ať již uvedené úmyslně či neúmyslně (*například osoba se překlepne při zadávání svých osobních údajů v rámci zadávání svého místa bydliště nebo u své zdravotní anamnézy*). Tímto se zamezí riziku odmítnutí služby nebo poskytnutí nesprávného lékařského úkonu (*například alergická reakce na očkování*), což by pro osobu mohlo mít za následek vysoké zdravotní riziko.

9.3 Linka 1221 jako lidský faktor k automatizovanému zpracování

Aby systém rezervací byl komfortní a dostupný i pro osoby, které z jakékoliv důvodu nedisponují možností provedení rezervace pomocí webového formuláře a mobilního telefonu, je těmto osobám nabídnuta **možnost využít linky 1221**, kde je registrací provedou proškolení operátoři. Tuto možnost mohou využít také osoby, které se domnívají, že jsou automatickým profilováním rezervačního systému značně znevýhodněny *(například i když je rezervační systém vyhodnotil jako nevhodné v rámci prioritizace, ale mají zvláštní*

kombinace zdravotních komplikací). Tímto úkonem vstupuje do systému lidský faktor, aby stejně jako v bodě 9.1 a 9.2 přehodnotil veškeré dostupné informace a případně stanovil mimořádné postupy.

9.4 Důvěrnost, integrita a dostupnost

Správce si je vědom vysokého rizika informačních systémů, které může mít za následek únik dat, narušení jejich struktury či nedostupnost služby dat včetně osobních údajů (*například v případě kybernetického incidentu nebo události, úmyslné chyby administrátora, výpadku sítě*). A již od počátku vývoje věnoval značnou pozornost bezpečnosti. I v případě rezervačního systému jsou splněny vysoké bezpečnostní standardy. ISIN je současně v plné jurisdikci zákona o kybernetické bezpečnosti. Pro oba systémy jsou správcem přijata vhodná organizační a technická opatření k zajištění jejich důvěrnosti, integrity a dostupnosti. Tímto správce snížil úroveň tohoto rizika na akceptovatelnou úroveň.

10 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

10.1 Kybernetická bezpečnost

Veškeré datové toky včetně osobních údajů jsou transferovány do vnitřní infrastruktury Ministerstva zdravotnictví a ISIN, který je pod jurisdikcí zákona o kybernetické bezpečnosti. Provoz této infrastruktury tedy podléhá přísným bezpečnostním pravidlům stanoveným prováděcími právními předpisy v oblasti kybernetické bezpečnosti a dozoru Národního úřadu pro kybernetickou a informační bezpečnost.[10]

Celková bezpečnostní architektura je dostatečně robustní, odolná a dedikována takovým způsobem, aby při výpadků jedné z částí infrastruktury došlo k efektivní redundanci do zálohového datového uložiště.

V rámci bezpečnostní architektury jsou využívány prvky SOC, analýzy SIEM a Log managementu.

10.2 Politika systému řízení bezpečnosti informací MZ ČR

Ministerstvo zdravotnictví je ústředním orgánem státní správy pro zdravotní služby, ochranu veřejného zdraví, zdravotnickou vědecko-výzkumnou činnost, poskytovatele **zdravotních služeb v přímé řídící působnosti, zacházení s návykovými látkami, přípravky,** prekursory a pomocnými látkami, vyhledávání, ochranu a využívání přírodních léčivých zdrojů, přírodních léčebných lázní a zdrojů přírodních minerálních vod, léčiva a prostředky zdravotnické techniky pro prevenci, diagnostiku a léčení lidí, zdravotní pojištění a zdravotnický informační systém, pro používání biocidních přípravků a uvádění biocidních přípravků a účinných látek na trh.

[10] 8.1.2020 - Národní úřad pro kybernetickou a informační bezpečnost – O NÚKIB (nukib.cz)

Jako takové vyhlašuje zásady bezpečnosti informací platné pro resort zdravotnictví pro uplatnění vhodných technických a organizačních opatření.

Aktuálně je platná Verze: v2/01.

Tato Politika systému řízení bezpečnosti informací je vypracována v souladu s požadavky definovanými v zákona o kybernetické bezpečnosti a jeho prováděcích předpisech.

Záměrem vedení MZ ČR je udržovat přiměřenou ochranu informačních aktiv (včetně ochrany osobních údajů) v souladu se zákony a jinými právními předpisy ČR, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na spolupracující organizace.

10.3 Spolupráce s odbornou veřejností – Spolek pro ochranu osobních údajů

V rámci zajištění vysoké ochrany práv subjektů údajů MZ ČR a NAKIT konzultují některé aspekty projektu CHK 2.0 také s odbornou veřejností. Za tímto účelem byla zahájena aktivní spolupráce se Spolkem pro ochranu osobních údajů, jenž je organizací 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.[11] Spolek je členem European Federation of Data Protection Officers.[12]

10.4 eHealth network – Joint Controller Subgroup

V souladu s právem Evropské unie a vydanými dokumenty je v rámci ochrany před vážnou přeshraniční zdravotní hrozbou covid-19 založena skupina eHealth network – Joint Controller Subgroup. Zde je také například řešena následná jednotná podoba certifikátu o provedeném očkování.

11 Dokumentace doporučení

11.1 Doporučení plynoucí z DPIA

1. Konzultovat s ÚOOÚ
2. Pokračovat v konzultacích s odbornou veřejností (například Spolek pro ochranu osobních údajů)
3. Spolupracovat se skupinou eHealth – Joint Controller Subgroup
4. Při technologických, nebo procesních změnách provést posouzení rizik a přiměřenosti zpracování včetně kontroly právní opodstatněnosti a celkové legitimity zpracování.
5. Neustálé zvyšování bezpečnostních standardů (například skrze penetrační testování); dle doporučení EDPB WP č.248.

[11] https://www.ochranaudaju.cz/kdo-jsme/
[12] https://www.efdpo.eu/

11.2 Dokumentace doporučení od osoby odpovědné za ochranu údajů

Se závěry DPIA a uvedenými doporučeními se lze ztotožnit.

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

Současně je nutné dále pracovat na detailním dopracování dokumentace v návaznosti na případné úpravy systému, ke kterým bude při implementaci docházet. Zároveň je nutná spolupráce se Spolkem pro ochranu osobních údajů a aktivní komunikace s ÚOOÚ.

MZ musí taktéž nadále aktivně přistupovat a vyhodnocovat možné kybernetické hrozby a rizika v oblasti informační bezpečnosti v rámci úzké spolupráce se zástupci NÚKIB.