NAKIT

Příloha č. 1 – Specifikace Služby Systému

A EPI Dashboard

A.1 Funkcionalita

Aplikace EPI Dashboard je webová aplikace pro analýzu dat a sdílení informací na jednom místě v reálném čase a jejich vizualizaci o průběhu pandemie COVID-19 v ČR i ve vybraných státech světa. Aplikace nabízí uživateli možnost jednoduše měnit parametry vykreslovaných grafů, zobrazovat jednotlivá data na základě vizuálních filtrů (kraje, okresy, městské části Prahy, věkové skupiny ...) a požadovaná data přehledně zobrazit. V mezinárodním srovnání jsou k dispozici předdefinované skupiny zemí (okolní státy, EU) s možností změny na individuální výběr a různé indikátory včetně normování k velikosti populace a poměrového ukazatele počtu případů na 100 testů.

Aplikace EPI Dashboard zahrnuje grafické znázornění využití a kapacity odběrových míst a laboratoří. Data pro tyto přehledy jsou získávána on-line v reálném čase prostřednictvím aplikace Covid Forms App (součinnost AČR, resp. ÚZIS). K dispozici je přehled vytížení po krajích i detailní reporty jednotlivých laboratoří a odběrných míst.

Sledování vyhledávání rizikových kontaktů příslušnými KHS umožňuje modul „Přehled trasování" se třemi reporty. Ty poskytují podrobnou statistiku počtu a typu volaných hovorů v jednotlivých krajích, včetně přehledu o využití vzpomínkových map.

Nástroj poskytuje:

- vizualizace statistických dat o průběhu epidemie,
    - přesná data poskytovaná ÚZIS,
    - přehledy za ČR i zahraničí,
- zobrazení kapacity a vytíženosti laboratoří a odběrových míst,
- přehledy o počtech a typech hovorů KHS a call centra.
- odkazy do mapové aplikace Situační mapa CŘT (součinnost AČR, resp. ÚZIS)

Další funkce systému pracují na pozadí (back-end). Jedná se o:

- Systém správy uživatelů využívající standardní login Microsoft Office 365.
- Datový sklad postavený na technologii Microsoft Data Factory, včetně aktualizačních a integračních mechanismů a processingu přípravy datových kostek pro reporting.
- Datový sklad využívá různé datové zdroje – viz kapitola Architektura a rozhraní

A.2 Uživatelé

Uživateli Aplikace jsou:

- operační a analytické týmy MZ, AČR a ÚZIS.
- externí uživatelé dle určení MZ, např. vybraní zaměstnanci MZ a KHS, členové projektového týmu Chytré karantény 2.0 (MZ, NAKIT, ÚZIS, AČR), členové vlády, hejtmani, ...

Licence k použití Aplikace je množstevně omezená na max 1000 pojmenovaných uživatelů.

A.3 Architektura a rozhraní

Aplikace je založena na následujících SaaS službách Microsoft/Azure, poskytovaných prostřednictvím Internetu:

- Microsoft Power BI PRO
- Microsoft Data Factory Pro
- MS Azure Websites portál

Rozhraní datového skladu pro sběr dat:

- ÚZIS eŽádanka (JSON reporty)
- Nástroje call centra (REST API)
- Covid Forms App (REST API)
- několik zdrojů s daty o pandemii v různých zemích světa (web parsing).

A.4 Zpracování osobních údajů

Nezpracovává osobní údaje s výjimkou emailových adres registrovaných uživatelů.

A.5 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách v souladu s SLA parametry uvedenými v příloze č. 4,
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- vývoj a konfigurace reportů a datového skladu a technická podpora uživatelů v maximálním rozsahu 1 FTE,
- správu uživatelů a přístupových práv
- koordinaci a řízení služeb.

Úpravy Aplikace a podpora uživatelů nad rámec uvedeného rozsahu jsou poskytovány a hrazeny formou Odborných služeb.

Problémy komunikačních sítí (lokální sítě, Internet) mezi uživatelem a místem poskytování SaaS služeb nejsou považovány za problémy Aplikace.

NAKIT

B Komunikační nástroj kontaktního centra

B.1 Funkcionalita

Aplikace Komunikační nástroj kontaktního centra je vystavěna na platformě call centra, (primárně modulu pro kampaně - odchozí volání), včetně rozhraní pro činnost pracovníků KHS. Úzce spolupracuje s nástroji pro vzpomínkové mapy a datovou integraci. Aplikace slouží jako jednotný systém evidence pozitivních pacientů k jejich aktivnímu navolávání a zjišťování jejich kontaktů, dále k navolávání těchto kontaktů a předání informací praktickým lékařům. Nástroj je škálovatelný a umožňuje vzájemnou spolupráci KHS a doplnění kapacit KHS o externí operátory.

K práci v systému je třeba pouze počítač s připojením k internetu a telefonní aplikace s náhlavní soupravou. Pracovní stanice operátorů a náhlavní soupravy nejsou součástí Aplikace.

Aplikace podporuje:

- telekomunikační služby – připojení do veřejné telefonní sítě, přidělení telefonních čísel pro příchozí volání, SMS služby pro posílání notifikačních zpráv - vlastní telefonní hovory a SMS jsou hrazeny formou Mobilních služeb.
- webové rozhraní pro operátory, ve kterém vytáčí infikované a potenciálně infikované kontakty a zapisují získané informace. Trasovači mohou se systémem pracovat a volat vzdáleně, např. na home office.
- software telefon pro operátora TCC a skrz který operátor telefonuje
- nahrávání a archivaci telefonních hovorů
- zpracování dat z epidemiologických šetření za účelem nastavování volacích front
- kompletní přehled šetření od pozitivního pacienta (1. a 2. hovor), přes kontakty (3. hovor) až po informování praktického lékaře (4. hovor),
- předávání zpracování mezi KHS (výpomoc mezi KHS),
- jednotný systém evidence případů.

Proces KHS pro vyhledávání kontaktů

- Hovor 1 (nakažený) - informování o výsledku testů, získání souhlasů s využitím mobilních a bankovních dat
- Hovor 2 (nakažený) - epidemiologické šetření, získání kontaktů, včetně využití Vzpomínkových map
- Hovor 3 (kontakt) - informování o rizikovém kontaktu, nařízení karantény, žádanka na testování
- Hovor 4 (praktický lékař) - oznámení o karanténě

Call skript

Pro operátory call centra je vytvořen a bude udržován call skript schválený MZ, který zohledňuje i potřebná ošetření zpracování osobních dat. Pracovníci KHS pracují se systémem volně na základě schváleného call skriptu a svých odborných zkušeností, externí operátoři budou školeni na používání odsouhlaseného call skriptu, školicí materiály také podléhají schválení MZ.

NAKIT

B.2 Uživatelé

Uživateli Aplikace jsou:

- pracovníci KHS, případně výpomoc z MZ a výpomoc z AČR (armádní medici, armádní KHS)
- v případě nárůstu počtů nakažených také operátoři externího call centra

Přidělování uživatelských práv řídí MZ

Součástí provozních služeb Aplikace a celkové ceny není dodávka operátorů call centra, pouze příprava všech nezbytných systémů a metodik. Předpokládá se, že síly KHS posílené o mediky Armády ČR, nebo jiný proškolený kvalifikovaný personál zvládnou až 300-400 nakažených osob denně. Při překročení tohoto limitu je třeba získat dodatečné financování a začít rychlým tempem doplňovat operátory externího call centra a související SW licence a technické vybavení (sluchátka, pracovní stanice, ...).

Licence k použití Aplikace je množstevně omezená na max 1000 aktivních operátorů (aktivním operátorem se rozumí pojmenovaný uživatel, který v daném měsíci provedl alespoň jednu aktivitu v rámci Aplikace).

Telefonní hovory a SMS jsou hrazeny formou Mobilních služeb dle Smlouvy

Potřebné vybavení uživatelských pracovišť – pracovní stanice a sluchátka nejsou součástí Služby.

B.3 Architektura a rozhraní

Aplikace zahrnuje následující aplikační moduly:

- virtuální telefonní ústřednu s aplikací callcentra, včetně modulu pro kampaně - odchozí volání
- integrace s nástroji pro vzpomínkové mapy a datovou integraci

Aplikace je založena na SaaS službách (zahrnujících telekomunikační služby) poskytovaných prostřednictvím Internetu z datových center v ČR.

Uživatelské rozhraní je poskytováno prostřednictvím browseru na klientských stanicích. Veškeré datově integrační úlohy probíhají asynchronně (v pravidelně schedulovaném dávkovém režimu) prostřednictvím nástrojů pro datovou integraci. Technickým standardem datových rozhraní je REST/JSON.

Integrace s telefonní sítí (aktuálně outcall, možný i incall) je součástí služby.

Integrace s ISIN - předávání informací o vyhledaných kontaktech do ISIN.

Integrace s regionálními systémy - aktuálně realizováno Liberecký kraj (EPIGIS), Moravskoslezský kraj, Plzeňský kraj, rozpracováno Královéhradecký kraj (EPIGIS) a Karlovarský kraj (Medicalc). Integrace automaticky zakládá záznamy pro obvolání, předávány jsou základní údaje (jméno, příjmení, telefonní číslo, indikující lékař, typ testu, datum testu).

Integrace s eRouška a Mapy.cz - viz ostatní kapitoly této přílohy Smlouvy.

Integrace s EPI Dashboard - předávání souhrnných dat o provozu kontaktního centra.

NAKIT

B.4 Zpracování osobních údajů

Kategorie subjektů

Nakažení (infikovaní, osoby s pozitivním výsledkem testu), vyhledané kontakty (osoby s rizikovým kontaktem na nakažené) a praktičtí lékaři těchto kontaktů.

Účel zpracování

Ochrana veřejného zdraví dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, konkrétně provádění epidemiologického šetření dle § 62a a § 67 citovaného zákona. Případně projednávání přestupků dle § 92k citovaného zákona.

Zpracování osobních údajů je prováděno dle čl. 6 odst. 1 písm. c) resp. čl. 9 odst. 2 písm. i) a g) GDPR.

Typ osobních údajů

Nakažení (1. a 2. hovor):

- jméno a příjmení
- rodné číslo
- telefonní číslo
- adresa
- jméno, adresa a telefonní číslo praktického lékaře
- informace o testu a výsledku testu
- informace o zdravotním stavu - informace specifické pro COVID19,
- cestovní anamnéza (navštívené země a termíny návštěv)
- údaje o čase a místě vyhledaných kontaktů získané a zaznamenané v rámci epidemiologického šetření.

Vyhledané kontakty (3. hovor):

- jméno a příjmení
- rodné číslo
- telefonní číslo
- adresa
- jméno, adresa a telefonní číslo praktického lékaře
- datum kontaktu s nakaženým, identifikace nakaženého
- informace o karanténě
- informace o zdravotním stavu - informace specifické pro COVID19,
- informace o testu a výsledku testu
- cestovní anamnéza (navštívené země a termíny návštěv)

Praktičtí lékaři (4. hovor):

- jméno
- adresa ordinace
- telefonní číslo

NAKIT

B.5 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách v souladu s SLA parametry uvedenými v příloze č. 4,
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- drobné rekonfigurace provozních parametrů již implementovaných funkcionalit
- podporu pro operátory formou znalostní báze přímo v systému
- linku technické podpory (slouží i pro vzpomínkové mapy a datové integrace)
- transparentní systém pro příjem a evidenci požadavků na změny
- technickou podporu uživatelů (pro již implementovanou funkcionalitu) v rozsahu max 0,5 FTE
- metodickou podporu uživatelů (pro již implementovanou funkcionalitu) v rozsahu max 1 FTE
- správu uživatelů a přístupových práv
- koordinaci a řízení služeb.

Úpravy Aplikace, zavádění a školení nové funkcionality a podpora uživatelů nad rámec uvedeného rozsahu jsou poskytovány a hrazeny formou Odborných služeb.

Problémy komunikačních sítí (lokální sítě, Internet) mezi uživatelem a místem poskytování SaaS služeb nejsou považovány za problémy Aplikace.

NAKIT

C Vzpomínkové mapy a datové integrace

C.1 Funkcionalita

Vzpomínkové mapy slouží k vizualizaci a k analýze dat nad mapovým podkladem. Na základě lokačních dat mobilních operátorů zobrazují oblasti výskytu nakaženého. Jsou tedy doplňkovým nástrojem pro epidemiologické šetření propojený s nástroji komunikačního centra. Účelem vzpomínkových map je pomoci pozitivnímu pacientovi vzpomenout si na místa, kde se pohyboval.

Datové integrace poskytují výměnu dat s nástroji komunikačního centra, mobilními operátory, aplikacemi eRouška a Mapy.cz, EPI Dashboardem a případně dalšími systémy.

Aplikace podporuje:

- vizualizaci vzpomínkových map, mapová podpora vyhledávání rizikových kontaktů,
- datové integrační nástroje, včetně rozhraní na níže uvedené aplikace a systémy,
- dashboardy pro manažery, metodiky a administrátory kontaktního centra

C.2 Uživatelé

Uživateli Aplikace jsou:

- pracovníci KHS, případně výpomoc z MZ a výpomoc z AČR (armádní medici, armádní KHS)
- v případě nárůstu počtů nakažených také operátoři externího call centra

Přidělování uživatelských práv řídí MZ

Licence k použití Aplikace je množstevně omezená na max 1000 aktivních operátorů (aktivním operátorem se rozumí pojmenovaný uživatel, který v daném měsíci provedl alespoň jednu aktivitu v rámci Aplikace).

C.3 Architektura a rozhraní

Vzpomínkové mapy a datové integrace zahrnují následující aplikační moduly:

- mapovou vizualizační platformu Vzpomínkové mapy
- integrační datová platforma, včetně externích integrací s
    - mobilními operátory
    - aplikací eRouška
    - aplikací Mapy.cz
    - aplikací EPI Dashboard - souhrnná data o provozu kontaktního centra
- dashboardy kontaktního centra

Aplikace dále zahrnuje:

- systém auditu a kontroly dodržování pravidel definovaných v mimořádném opatření MZ č. MZDR 12398/2020-1/MIN/KANNástroje jsou založeny na sadě SaaS služeb poskytovaných prostřednictvím Internetu (aktuálně umístěny v AWS)

Uživatelské rozhraní poskytují moduly Vzpomínkové mapy a Dashboardy kontaktního centra prostřednictvím browseru na klientských stanicích.

Veškeré datově integrační úlohy probíhají asynchronně (v pravidelně schedulovaném dávkovém režimu) prostřednictvím integrační datové platformy. Technickým standardem datových rozhraní je REST/JSON. Datová integrační platforma iniciuje spojení.

Integrace s mobilními operátory

Integrace s mobilními operátory je implementována na základě mimořádného opatření Ministerstva zdravotnictví ze dne 19.3.2020, je možno ji využít pouze pro nakažené osobu a její využití pro určitou osobu vyžaduje souhlas této osoby podle § 91 odst. 2 zákona č. 127/2005 Sb. o elektronických komunikacích.

Nástroje komunikačního centra předávají seznamy telefonních čísel nakažených osob, které poskytly souhlas. Modul datových integrací předává seznamy na zašifrované úložiště, k němuž mají zabezpečený přístup mobilní operátoři. Každý operátor dostává data prostřednictvím samostatného zabezpečeného kanálu.

Následně jsou telefonní čísla zpracována jednotlivými operátory a odpovídající lokalizační data odesílána zabezpečeným kanálem na zašifrované úložiště. Modul datových integrací následně zpracovává a předává zašifrovaná geolokační data do modulu Vzpomínkové mapy.

Data jsou uložena v Aplikaci jen po dobu nezbytně nutnou pro potřeby uživatelů Vzpomínkových dat a v souladu s limity uvedenými v mimořádném opatření maximálně 6 hodin.

C.4 Zpracování osobních údajů

Vzpomínkové mapy

Kategorie subjektů

Nakažení (infikovaní, osoby s pozitivním výsledkem testu).

Účel zpracování

Ochrana veřejného zdraví dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, konkrétně provádění epidemiologického šetření dle § 62a a § 67 citovaného zákona. Případně projednávání přestupků dle § 92k citovaného zákona.

Zpracování osobních údajů je prováděno dle čl. 6 odst. 1 písm. e), resp. čl. 9 odst. 2 písm. i) a g) GDPR.

Souhlas nakažené osoby je vyžadován podle § 91 odst. 2 zákona č. 127/2005 Sb. o elektronických komunikacích.

Typ osobních údajů

Vzpomínkové mapy - mobilní operátoři - Nakažení:

- čas (date, hour, minute)
- telefonní číslo (msisdn)
- lokalizační data (lat, lon)
- přesnost měření (dt, period, precision_code, intensity)
- mobilní operátor

NAKIT

Datové integrace

Datová integrační platforma má přístup ke všem datům nástrojů kontaktního centra i Vzpomínkových map.

Kategorie subjektů

Nakažení (infikovaní, osoby s pozitivním výsledkem testu), vyhledané kontakty (osoby s rizikovým kontaktem na nakažené) a praktičtí lékaři těchto kontaktů.

Účel zpracování

Ochrana veřejného zdraví dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, konkrétně provádění epidemiologického šetření dle § 62a a § 67 citovaného zákona. Případně projednávání přestupků dle § 92k citovaného zákona.

Zpracování osobních údajů je prováděno dle čl. 6 odst. 1 písm. c) a e), resp. čl. 9 odst. 2 písm. i) a g) GDPR.

.

Typ osobních údajů

Nástroje kontaktního centra - Nakažení (1. a 2. hovor):

- jméno a příjmení
- rodné číslo
- telefonní číslo
- adresa
- jméno, adresa a telefonní číslo praktického lékaře
- informace o testu a výsledku testu
- informace o zdravotním stavu - informace specifické pro COVID19,
- cestovní anamnéza (navštívené země a termíny návštěv)
- údaje o čase a místě vyhledaných kontaktů získané a zaznamenané v rámci epidemiologického šetření.

Nástroje kontaktního centra - Vyhledané kontakty (3. hovor):

- jméno a příjmení
- rodné číslo
- telefonní číslo
- adresa
- jméno, adresa a telefonní číslo praktického lékaře
- datum kontaktu s nakaženým, identifikace nakaženého
- informace o karanténě
- informace o zdravotním stavu - informace specifické pro COVID19,
- informace o testu a výsledku testu
- cestovní anamnéza (navštívené země a termíny návštěv)

Nástroje kontaktního centra - Praktičtí lékaři (4. hovor):

- jméno
- adresa ordinace
- telefonní číslo

Vzpomínkové mapy - mobilní operátoři - Nakažení:

- čas (date, hour, minute)
- telefonní číslo (msisdn)
- lokalizační data (lat, lon)
- přesnost měření (dt, period, precision_code, intensity)
- mobilní operátor

C.5 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách v souladu s SLA parametry uvedenými v příloze č. 4,
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- drobné rekonfigurace provozních parametrů již implementovaných funkcionalit
- technickou a metodickou podporu uživatelů (pro již implementovanou funkcionalitu) v rozsahu max 0,5 FTE
- správu uživatelů a přístupových práv
- koordinaci a řízení služeb.

Úpravy Aplikace, zavádění a školení nové funkcionality a podpora uživatelů nad rámec uvedeného rozsahu jsou poskytovány a hrazeny formou Odborných služeb.

Problémy komunikačních sítí (lokální sítě, Internet) mezi uživatelem a místem poskytování SaaS služeb nejsou považovány za problémy Aplikace.

D eRouška

D.1 Funkcionalita

eRouška je mobilní aplikace pro chytré telefony, určená pro automatické vyhledávání rizikových kontaktů nakažených osob s využitím Bluetooth protokolu. eRouška nesleduje a nesbírá informace o poloze uživatele. Aplikace k detekci rizikových kontaktů nepotřebuje připojení k Internetu, takže funguje například i v metru.

Identifikace uživatelů aplikace je založena na pseudoanonymizovaných identifikátorech. Pseudonymizace probíhá na serveru, na mobilu nelze určit skutečnou identitu osob. Kontakty nakaženého jsou v případě jeho souhlasu odeslány na back-end server, kde je vyhodnocena jejich rizikovost a jsou namapovány na konkrétní telefonní čísla.

Všichni uživatelé jsou hned po instalaci aplikace povinně registrováni na back-end (s využitím jednorázového hesla v SMS). Telefonní číslo zadané při registraci může využít KHS k identifikaci kontaktů a jejich navolávání, ostatní uživatelé eRouška ho zjistit nemohou.

Aplikace je dostupná pro mobilní telefony s operačním systémem Android a iOS.

D.2 Uživatelé

Veřejní uživatelé, kteří si aplikaci nainstalují na vlastní mobilní telefon z Google Play nebo Apple Store. Počet uživatelů není omezen.

D.3 Architektura a rozhraní

Aplikace eRouška obsahuje:

- mobilní aplikaci eRouška pro Android a iOS
- serverovou část (back-end) spravující registrace instalovaných aplikací a unikátní kódy, které mobilní telefony vysílají do svého okolí

Back-end aplikace jsou provozovány v Google Cloud na platformě Google Firebase,

Na straně serveru je připravena integrace do procesů KHS prostřednictvím Nástrojů datové integrace.

D.4 Zpracování osobních údajů

Při registraci aplikace eRouška vznikne na back-end serveru vazba mezi telefonním číslem uživatele eRouška a sadou pseudonymních identifikátorů, přidělených danému uživateli aplikace eRouška. Back-end server eRouška nemá k dispozici informace o kontaktech uživatelů aplikace eRouška, dokud uživatel aplikace dobrovolně neodešle data na server. Takto předaná data se z back-end serveru eRouška smažou po 6 hodinách od odeslání.

Kategorie subjektů

Všichni uživatelé mobilní aplikace eRouška, kteří si jí dobrovolně stáhnou a nainstalují. Nakažení (infikovaní, osoby s pozitivním výsledkem testu.

Účel zpracování

Ochrana veřejného zdraví dle zákona č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, konkrétně provádění epidemiologického šetření dle § 62a a § 67 citovaného zákona.

Zpracování osobních údajů je prováděno na základě souhlasu dle čl. 6 odst. 1 písm. a), GDPR.

Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů vyjadřuje každý uživatel dobrovolným stažením a instalací aplikace a registrací do back-end systému. Nakažený dále vyjadřuje souhlas dobrovolným odesláním dat o kontaktech.

Typ osobních údajů

Uživatelé aplikace eRouška

- telefonní číslo

Nakažení:

- telefonní číslo
- datum a čas setkání s jinými uživateli eRouška
- síla Bluetooth signálu při setkání s jinými uživateli eRouška
- seznam vyhledaných kontaktů

Vyhledané kontakty:

- telefonní číslo
- datum a čas setkání s nakaženým
- síla Bluetooth signálu při setkání nakaženým

D.5 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách v souladu s SLA parametry uvedenými v příloze č. 4,
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- vydávání nových verzí aplikace formou instalačních balíků Google Play a Apple Store
- administraci serverové části,
- podporu veřejných uživatelů prostřednictvím různých kanálů – přímo na Google Play a Apple Store, na webu erouska.cz, Facebook, Twitter, chatbot - viz níže
- koordinaci a řízení služeb.

Úpravy Aplikace a podpora uživatelů nad rámec uvedeného rozsahu jsou poskytovány a hrazeny formou Odborných služeb.

Mobilní aplikace eRouška je poskytována formou instalačních balíků na Apple Store a Google Play, povinností Objednatele je zajistit a poskytnout Poskytovateli přístup k účtu Ministerstva zdravotnictví na těchto platformách.

Problémy komunikačních sítí (mobilní sítě, Internet) mezi mobilním telefonem uživatele a místem poskytování SaaS služeb serverové části aplikace nejsou považovány za problémy Aplikace. Poskytovatel není odpovědný za funkcionalitu operačních systémů mobilních telefonů. Poskytovatel není odpovědný za funkcionalitu Apple Store a Google Play – aplikace jsou publikovány pod účty Ministerstva zdravotnictví a Objednatel zajišťuje i komunikaci s Apple/Google a případné eskalace.

Podpora veřejných uživatelů

Podpora veřejných uživatelů probíhá prostřednictvím různých veřejných komunikačních kanálů – přímo na Google Play a Apple Store, na webu erouska.cz, Facebook, Twitter.

S výjimkou těch nejsložitějších budou dotazy a stížnosti uživatelů vyřizovány do následujícího pracovního dne. V případě nárůstu požadavků na podporu od veřejných uživatelů je nutno brát v úvahu limit kapacity týmu eRouška – podpoře uživatelů může být věnována kapacita max 2FTE.

Předpokladem, resp. významným faktorem pro vyšší efektivitu poskytování podpory vyšších počtů veřejných uživatelů je provozování chatbota Anežka (IBM) ze strany MZ. Chatbot Anežka je aktuálně integrován i do webu erouska.cz. V případě nedostupnosti chatbota Anežka může být dříve dosaženo limitů kapacit týmu, zejména v případě náhlého nárůstu uživatelů v souvislosti s PR kampaněmi apod.

NAKIT

E Integrace Mapy.cz

E.1 Funkcionalita

Integrace mobilní aplikace Mapy.cz. Aplikace Mapy.cz je vyvíjena, spravována a provozována společností Seznam.cz. MZ a Seznam.cz mají uzavřenu partnerskou smlouvu o bezúplatné spolupráci. MZ potvrzuje Seznam.cz pomocí identifikátoru HRID nakaženou osobu, aby mohly být upozorněny potenciálně nakažené osoby. HRID není nikde párován na identifikátor přihlášeného uživatele aplikace Mapy.cz ani na jiné identifikátory uživatele či jeho osobní údaje.

E.2 Uživatelé

Veřejní uživatelé aplikace Mapy.cz, kteří si dobrovolně zapnou sledování polohy. Vzhledem k partnerskému charakteru integrace s Mapy.cz jsou uživatele podporováni přímo ze strany Seznamu.

E.3 Architektura a rozhraní

Integrace do procesu KHS

Aktuálně v přípravě.

Aplikaci (Mapy.cz) mají uživatelé nainstalovanou v mobilním telefonu. Každý uživatel může ve své aplikaci zapnout sdílení polohy a následné využití nasbíraných dat pro výpočet pravděpodobnosti nákazy podle toho, zda se po významnou dobu mohl nacházet na stejném místě jako nakažená osoba. Ke každé aplikaci má Seznam.cz uložené pouze unikátní ID aplikace (HRID), které není vázáno na identitu uživatele, a k němu v čase zaznamenanou polohu. Data jsou uložena pouze v datových centrech Seznam.cz v ČR.

Druhým krokem je získání informací o nakaženém. Operátor kontaktního centra KHS ověří, zda má pozitivně testovaný člověk aplikaci Mapy.cz a pokud ano, vyzve jej k přečtení identifikačního čísla aplikace (HRID) přímo z jeho mobilního telefonu. Zároveň operátor požádá o souhlas nakaženého s předáním HRID a o datum prvních příznaků nebo datum od kdy má potvrzenou diagnózu, společnosti Seznam.cz pro trasování nákazy. Seznam.cz dostává pouze sadu HRID nakažených osob.

Když algoritmus vyhodnotí rizikový kontakt uživatele aplikace s nakaženou osobou, odešle uživateli upozornění ve znění určeném MZ.

E.4 Zpracování osobních údajů

Na straně MZ nejsou zpracovávány osobní údaje v rámci aplikace MAPY.CZ.

Předávané údaje:

HRID – unikátní identifikátor instalace mobilní aplikace Mapy.cz

Infekční období (datum prvních příznaků/infekčnosti)

KHS neposkytuje společnosti Seznam.cz žádné další osobní údaje nakaženého.

HRID slouží k identifikaci sady polohových dat z daného zařízení a ke zpětnému zaslání notifikace v případě, že algoritmus vyhodnotí dané zařízení jako "rizikový kontakt nakažené osoby".

HRID není nikde párován na identifikátor přihlášeného uživatele aplikace Mapy.cz. Tato vazba tedy stranám není známa. Systém funguje nezávisle na tom, zda je uživatel přihlášen, či nikoliv. HRID není párován ani na jiné identifikátory uživatele či jeho osobní údaje.

HRID a polohová data jsou uložena v infrastruktuře Seznam.cz v ČR a jsou v rámci virtualizované infrastruktury oddělena od ostatních zpracovávaných dat a dalších běžících aktivit využitých pro Mapy.cz a Seznam.cz obecně. Identifikátor HRID je vytvořen a použit pouze pro účely sledování kontaktů COVID19. Po skončení epidemie C19 budou všechna data související s sledování kontaktů COVID19 ze systémů Seznam.cz odstraněna.

NAKIT

F Nástroje EA

F.1 Funkcionalita

Aplikace pro správu modelu enterprise architektury (EA) celého řešení Chytré karantény 2.0 (ve smyslu usnesení vlády) a systému správy grafových dat (objektové databáze), včetně podpory řízení katalogu požadavků na různé komponenty systému a jejich funkce.

Nástroje a model EA sestávají z:

- modelu Enterprise architektury celého řešení Chytré karantény 2.0
- aplikační služby systému ArchiREPO
- aplikační služby systému ArchiREPO Tracker

Model enterprise architektury je aktuálně zpracován v rozsahu cca 400 elementů, cca 600 vazeb a cca 20 diagramů v jazyce ArchiMate 3.0. Forma případného předání modelu je transportní soubor ve formátu XML dle specifikace The Open Group.

Poskytnutí aplikační služby systému ArchiREPO (SAAS služba)

Předmětem je poskytnutí služby projektového repozitory EA modelu Chytré karantény prostřednictvím cloudové verze systému ArchiREPO (www.archirepo.com). Služba zahrnuje provoz v cloudu, nahrání EA modelu do systému, vytvoření navigačních struktur a základních reportů a založení uživatelských účtů.

Systém ArchiREPO je přednastaven k podpoře řízení a ke správě EA modelu „Chytré karantény". Jde o platformové řešení pro tvorbu, optimalizaci, užití a správu modelu organizace (DTO – Digital Twin of Organization), nebo dílčí části (systému, programu, projektu, ...). Jako modelový základ je využit standard pro „Enterprise Architekturu" ArchiMate sdružení www.opengroup.org. Možnosti užití platformy jsou širší než jen prosté sdílené úložiště EA modelů (Enterprise Architecture repository). Možnosti zahrnují:

- Agregace dat z externích systémů do objektové/grafové znalostní báze (platforma může sloužit pro správu dat a anayltické úlohy ne-relační povahy, kterých může být v systému zdravotních hrozeb celá řada).
- Systém převádějící digitální model do intranetu/extranetu.
- Umožňuje efektivní strategické, procesní a projektové řízení, včetně řízení IT a správy bezpečnostní dokumentace dle požadavků legislativy (správa IT aktiv dle požadavků na kybernetickou bezpečnost).
- Sdílení znalostí o fungování projektu a okolního prostředí.
- Možnost plnohodnotného využití platformy jako centrálního systému správy aktiv.

Platformu využívá Ministerstvo zdravotnictví jako úložiště modelů eHealth. Model Chytré karantény v projektovém repository lze synchronizovat s modelem v repository MZ ČR.

Poskytnutí aplikační služby systému ArchiREPO Tracker (SAAS služba)

Předmětem je poskytnutí služby řídícího modulu správy katalogu požadavků a podpory řídících procesů Chytré karantény prostřednictvím cloudové verze systému Tracker. Služba zahrnuje provoz v cloudu, naplnění katalogů požadavků pro klíčové komponenty Chytré karantény, nastavení formulářů a pracovních toků a vytvoření základních reportů.

- Modul „Tracker" disponuje pokročilou obousměrnou integrací s jádrem ArchiREPO. Ta se neomezuje jen na podporu provázání prvků modelu s formuláři úloh a jejich workflow. Podporovány jsou rovněž scénáře automatického založení ticketu/formuláře při změně stavu prvku modelu (detekce poruchy nebo chyby), nebo obráceně, pracovní tok formuláře může vytvořit nebo aktualizovat soubor prvků v modelu včetně jejich vazeb.
- Součástí systému jsou pokročilé funkce podpory řízení projektu (portfolia). Včetně sdílení úkolů s rozpadem do harmonogramů.

Služby **aktualizace EA modelu** a aktualizace vazeb na katalog požadavků jsou poskytovány formou Konzultačních služeb dle Smlouvy. Součástí služeb je aktualizace navigačních struktur repository a provázání požadavků (položek katalogu požadavků) s prvky a diagramy EA modelu.

F.2 Uživatelé

Členové projektového týmu Chytré karantény 2.0 (MZ, NAKIT, ÚZIS, AČR, SZÚ), klíčoví uživatelé z KHS.

Přidělování uživatelských práv řídí MZ.

Licence k použití Aplikace je množstevně omezená na max 500 pojmenovaných uživatelů.

F.3 Architektura a rozhraní

Služba je realizována prostřednictvím SaaS služeb ArchiREPO, poskytovaných prostřednictvím Internetu.

F.4 Zpracování osobních údajů

Nezpracovává osobní údaje, s výjimkou údajů nezbytných pro správu registrovaných uživatelů (jméno, příjmení, emailová adresa).

F.5 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách v souladu s SLA parametry uvedenými v příloze č. 4,
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- úpravy konfigurace nástrojů a technická podpora uživatelů v maximálním rozsahu 0,25 FTE,
- správu uživatelů a přístupových práv
- koordinaci a řízení služeb.

Úpravy Aplikace a podpora uživatelů nad rámec uvedeného rozsahu jsou poskytovány a hrazeny formou Odborných služeb.

Problémy komunikačních sítí (lokální sítě, Internet) mezi uživatelem a místem poskytování SaaS služeb nejsou považovány za problémy Aplikace.

G COVID mobilní info karta

G.1 Funkcionalita

Aplikace je mobilní info kartou pro operační systémy Android a iOS. Aplikace zobrazuje

- Aktuální informace o vývoji epidemie
- Důležité kontakty a infolinky
- Oficiální pokyny a doporučení z MZČR

Aplikace poskytne podporu integrace a propagace Aplikace eRouška:

- pro variantu karty pro iOS napojení aplikace eRouska přímo na digitální kartu, tj. možnost spuštění (či stažení) eRousky přímo z digitální karty
- pro variantu karty pro Android propojení s aplikací eRouska pomocí aktivního linku na zadní straně karty (technologie Android neumožňuje přímé spuštění jiné aplikace)
- pravidelné aktivní upozornění uživatelů digitální karty na stažení či používání aplikace eRouska

G.2 Uživatelé

Veřejní uživatelé, kteří si aplikaci nainstalují na vlastní mobilní telefon (například prostřednictvím https://koronavirus.mzcr.cz/digitalni-karta-covid19/). Počet uživatelů není omezen.

G.3 Zpracování osobních údajů

Nezpracovává osobní údaje.

G.4 Rozsah provozních služeb

Měsíční cena Služby systému pro Aplikaci zahrnuje:

- provoz Aplikace v rozsahu funkcionality popsané v předchozích kapitolách
- řešení problémů a chyb v Aplikaci nebo způsobených Poskytovatelem při provozu Aplikace
- aktualizaci údajů minimálně 1x denně

H Mobilní služby

Zahrnuje mobilní a telekomunikační služby využívané v rámci aplikací Služeb Systému.

Služby Telefonní hovory call centra a SMS call centra (písm. a) a b) níže) jsou integrovány s nástroji kontaktního centra a vztahují se na ně podmínky provozu nástrojů call centra uvedené v příloze č.4 Smlouvy. Služby jsou poskytovány na základě Všeobecných podmínek poskytování telekomunikačních služeb uvedených na https://www.daktela.com/downloads/Vseobecne_Obchodni_Podminky.pdf

Telefonní hovory call centra (Komunikační nástroj kontaktního centra)

Odchozí telefonní hovory při volání nakaženým, jejich kontaktům a praktickým lékařům, případně další související odchozí telefonní hovory.

SMS call centra (Komunikační nástroj kontaktního centra)

Odchozí SMS při činnosti operátorů call centra. Aktuálně jsou používány jen minimálně.

NAKIT

Příloha č. 2 – Specifikace Rolí

Specifikace a ceník rolí

Pro zajištění poměrně rozsáhlého týmu pro projekt Chytré karantény 2.0 se specializací v několika různých oblastech je třeba využít kombinaci zaměstnanců NAKIT a expertů, dodaných externími dodavateli. Z důvodu udržení kontinuity a know-how dodávaného plnění je dále nutné doplnit tým o externí experty, kteří se na vývoji dílčích plnění Chytré karantény 2.0 v minulosti podíleli.

A Role zajištěné interními zdroji NAKIT

Role	Cena za MD bez DPH
Architekt	11 821
Bezpečnostní manažer	10 336
Bezpečnostní architekt	12 848
Projektový manažer senior	14 107
Projektový administrátor	6 377
Vývojář	9 070
Projektový manažer	10 403
Konzultant ICT	11 686
Analytik senior	11 183

B Role zajištěné subdodavateli

B.1 Specifikace rolí Keboola

Role	Cena za MD bez DPH
Vývojář/Specialista	15000
Bezpečnostní architekt	15000

B.2 Specifikace rolí Daktela

Role	Cena za MD bez DPH
Architekt	14400
Vývojář/Specialista	14400
Bezpečnostní architekt	14400
Technická podpora	10400

B.3 Specifikace externí rolí Intelligent Technologies

Role	Cena za MD bez DPH
Dashboard specialista	9600

C Popis rolí

C.1 Role zajištěné interními zdroji NAKIT

Role	Specifikace
Architekt	• Realizuje analytickou a dokumentační činnost nad infrastrukturou a aplikacemi. • Řídí, nebo se podílí na procesu návrhu a implementace úprav. Připravuje technická řešení a prováděcí projekty. • Účastní se anebo řídí implementaci úprav. • Komunikuje s příslušnými organizačními celky v rámci řešené problematiky, se specialisty zodpovědnými za aplikace a technologie v projektech.
Bezpečnostní manažer	• Navrhuje a zajišťuje implementaci bezpečnostních pravidel ve fázi návrhu i realizace úprav i provozu • Odpovídá za dodržování pravidel bezpečnosti dle platné dokumentace (interní/projektová) • Odpovídá za soulad bezpečnostní dokumentace pro svěřenou část provozu/projektu s platnou bezpečnostní dokumentací Objednatele • V průběhu realizace projektu kontroluje shodu implementace bezpečnostních nástrojů a opatření dle schváleného návrhu bezpečnostního architekta a konzultuje případné změny a odchylky • Zpracovává potřebné analýzy z oblasti bezpečnosti (řízení rizik, řízení kontinuity, shoda s požadavky ZoKB atd.) a prezentuje Objednateli výstupy, navrhuje opatření a dohlíží na realizaci schválených opatření • Navrhuje a zpracovává strategické dokumenty v oblasti bezpečnosti dle zadání Objednatele • Navrhuje a zpracovává bezpečnostní dokumentaci pro konkrétní projekt/provoz, kontroluje shodu provozní a procesní dokumentace s bezpečnostními pravidly • Zajišťuje řízení rizik, řešení bezpečnostních incidentů a komunikuje s manažerem kybernetické bezpečnosti Objednatele • Koordinuje detekci, analýzu a vyhodnocení bezpečnostních událostí a incidentů. Koordinuje řešení bezpečnostních incidentů. • Definuje a optimalizuje procesy detekce, analýzy a vyhodnocování bezpečnostních událostí a incidentů • Definuje a optimalizuje proces řešení bezpečnostních incidentů

Bezpečnostní architekt	• Odpovídá za architekturu bezpečnostních prvků a nástrojů u projektů/provozu a jejich shodu s požadavky Objednatele, formuluje požadavky na budoucí stav zajištění kybernetické bezpečnosti v rámci projektů a identifikuje kroky vedoucí k dosažení požadovaného budoucího stavu. • Provádí analýzy úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Vytváří plány implementace architektury kybernetické bezpečnosti a určuje milníky dosažení očekávaného cílového stavu. • Formuluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů a podílí se na aktualizaci strategie kybernetické bezpečnosti organizace vyplývající z projektů. • Tvoří a aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Průběžné vyhodnocuje aktuální stav úrovně bezpečnostní politiky projektů podle stanovených metrik. • Aktivně se účastní oponentních řízení. • Provádí kontroly úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Spolupracuje na přípravě plánů implementace architektury kybernetické bezpečnosti a kontroluje milníky k dosažení očekávaného cílového stavu. • Kontroluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů. • Průběžně aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Připravuje podklady pro hodnocení aktuálního stavu úrovně bezpečnostní politiky projektů podle stanovených metrik. • Připravuje podklady pro oponentní řízení.
Projektový manažer senior	• Projektový manažer zodpovídá za plánování, organizování, řízení a kontrolu realizace projektu tak, aby bylo dosaženo stanovených projektových cílů, a to ve stanoveném termínu a v rámci stanoveného rozpočtu projektu. Činnosti: • řízení projektu ve všech jeho fázích - inicializace, plánování, realizace, monitoring a reporting, prezentace výstupů, vyhodnocení a uzavření • řídí změnový management, management rizik a případný krizový management v projektech, včetně implementace nápravných opatření • stanovení časového a finančního plánu realizace projektu • sestavení, vedení a řízení projektového týmu • řízení finančních zdrojů, nákladů, výnosů a cash flow projektu • koordinace postupů prací a návazností činností v jednotlivých úkolech • řízení komunikace v projektu, podpora a motivování členů projektu k efektivnímu výkonu • analýza a řízení rizik a příležitostí v projektu • řízení kvality projektu • řízení všech dostupných zdrojů v projektu • koordinace a spolupráce při tvorbě vstupních analýz předmětu a cílů projektu • spolupráce na výběrovém řízení a smluvním zabezpečení projektu • řízení změn v projektu • kontrola dodržování harmonogramu prací, výstupů z projektu a jejich akceptace zúčastněnými stranami • řízení a kontrola kompletní dokumentace k projektu • reportování stavu realizace projektu směrem dovnitř projektového týmu i směrem ven na stranu zadavatele projektu

	Odborné zkušenosti: • praxe v projektovém managementu více než 8 let. • dokončení min. 5 projektů • hodnota řízeného projektu min. 30 mio
Projektový administrátor	Projektový administrátor spolupracuje s manažerem projektu na organizování a zajišťování realizace projektu tak, aby bylo dosaženo stanovených projektových cílů, a to ve stanoveném termínu a v rámci stanoveného rozpočtu projektu. Činnosti: • Podpora manažera projektu po celý životní cyklus projektu, nebo ve vybraných fázích projektu. • Tvorba dílčích částí vstupních analýz předmětu a cílů projektu. • Spolupráce na sestavení projektového týmu. • Koordinování práce projektového týmu. • Spolupráce při řízení komunikace mezi subjekty zainteresovanými v projektu. • Koordinace postupů prací a návazností činností v jednotlivých úkolech. • Spolupráce na analýze a řízení rizik a příležitostí v projektu. • Spolupráce při řízení kvality projektu. • Příprava reportů o stavu realizace projektu pro projektový tým i pro zadavatele projektu a vedení zainteresovaných subjektů. • Zajištění dílčích činností při řízení změn v projektu. • Spolupráce při zajištění předání výstupů z projektu a při jejich akceptaci zúčastněnými stranami. • Spolupráce při řízení a kontrole zpracování kompletní dokumentace k projektu. • Spolupráce při řízení finančních zdrojů, nákladů, výnosů a cashflow projektu.
Vývojář/Specialista	• Pracuje v projektovém týmu na externím či interním projektu v roli specialisty zodpovědného za vývoj v příslušném programovacím jazyce. • Podílí se na tvorbě designu aplikací a architektury systémů. • Má podíl na navrhování databází. Podíl na navrhování a tvorbě datového modelu pro aplikaci. Podíl na přípravě a školení daných technologií. • Znalost analytických datových modelů. • Podíl na přípravě technické a programátorské dokumentace. • Podíl na přípravě automatizovaných a/nebo performance testů. • Podíl na přípravě technické a programátorské dokumentace.
Projektový manažer	• Projektový manažer zodpovídá za plánování, organizování, řízení a kontrolu realizace projektu tak, aby bylo dosaženo stanovených projektových cílů, a to ve stanoveném termínu a v rámci stanoveného rozpočtu projektu. Činnosti: • řízení projektu ve všech jeho fázích - inicializace, plánování, realizace, monitoring a reporting, prezentace výstupů, vyhodnocení a uzavření • stanovení časového a finančního plánu realizace projektu • sestavení, vedení a řízení projektového týmu • řízení finančních zdrojů, nákladů, výnosů a cash flow projektu • koordinace postupů prací a návazností činností v jednotlivých úkolech • řízení komunikace v projektu, podpora a motivování členů projektu k efektivnímu výkonu • analýza a řízení rizik a příležitostí v projektu • řízení kvality projektu • řízení všech dostupných zdrojů v projektu • koordinace a spolupráce při tvorbě vstupních analýz předmětu a cílů projektu • spolupráce na výběrovém řízení a smluvním zabezpečení projektu • řízení změn v projektu

	• kontrola dodržování harmonogramu prací, výstupů z projektu a jejich akceptace zúčastněnými stranami • řízení a kontrola kompletní dokumentace k projektu • reportování stavu realizace projektu směrem dovnitř projektového týmu i směrem ven na stranu zadavatele projektu Odborné zkušenosti: • praxe v projektovém managementu více než 5 let. • dokončení min. 3 projektů • hodnota řízeného projektu min. 10 mio
Konzultant ICT	• Soustřeďuje dostupné technické informace o provozu informačních a komunikačních systémů • Identifikuje možnosti zlepšování provozu, posuzuje jejich proveditelnost a koordinuje servisní a rozvojové činnosti ICT • Provádí konzultační poradenství v ICT • Provádí rozbory a analýzy požadavků návrhů z ekonomicko-legislativního pohledu pro realizaci a provoz ICT systémů. • Vypracovává podklady technického, procesního, bezpečnostního, ekonomického a legislativního rázu pro jednotlivé oblasti životního cyklu IT systémů. • Posuzuje proveditelnost ICT projektů z hlediska jejich realizace i provozu.
Analytik senior	• Realizuje sběr business požadavků; • Analyzuje business požadavky a vstupní data; • Zajišťuje vstupy pro přípravu návrhu analytického řešení; • Podílí se na přípravě analytických materiálů; • Spolupracuje s realizačním týmem zajišťujícím návrh a přípravu analytického řešení a na jeho následné realizaci. • Provádí mapování a analýzu business požadavků a vstupních dat zákazníka v rámci definovaného projektu; • Připravuje vstupy pro návrh analytického řešení a spolupracuje na zpracování návrhu, prezentaci analytického řešení (návrh datového modelu, UC diagramy, business analýzy, procesní modely apod.) a jeho následné realizaci; • Zpracovává relevantní analytické materiály (dokumentace, schématické diagramy apod.).

C.2 Role zajištěné externími zdroji

Ext. Zdroje	Role	Specifikace
Keboola	Vývojář	• Pracuje v projektovém týmu Keboola v roli specialisty zodpovědného za analýzu, vývoj a testování úprav. • Podílí se na tvorbě designu aplikací a architektury systémů. • Má podíl na navrhování databází. Podíl na navrhování a tvorbě datového modelu pro aplikaci. Podíl na přípravě a školení daných technologií. • Znalost analytických datových modelů.

		• Podíl na přípravě technické a programátorské dokumentace. • Podíl na přípravě automatizovaných a/nebo performance testů.
	Bezpečnostní architekt	• Odpovídá za architekturu bezpečnostních prvků a nástrojů u projektů/provozu a jejich shodu s požadavky Objednatele, formuluje požadavky na budoucí stav zajištění kybernetické bezpečnosti v rámci projektů a identifikuje kroky vedoucí k dosažení požadovaného budoucího stavu. • Provádí analýzy úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Vytváří plány implementace architektury kybernetické bezpečnosti a určuje milníky dosažení očekávaného cílového stavu. • Formuluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů a podílí se na aktualizaci strategie kybernetické bezpečnosti organizace vyplývající z projektů. • Tvoří a aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Průběžné vyhodnocuje aktuální stav úrovně bezpečnostní politiky projektů podle stanovených metrik. • Aktivně se účastní oponentních řízení. • Provádí kontroly úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Spolupracuje na přípravě plánů implementace architektury kybernetické bezpečnosti a kontroluje milníky k dosažení očekávaného cílového stavu. • Kontroluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů. • Průběžně aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Připravuje podklady pro hodnocení aktuálního stavu úrovně bezpečnostní politiky projektů podle stanovených metrik. • Připravuje podklady pro oponentní řízení.
Daktela	Architekt	• Realizuje analytickou a dokumentační činnost nad aplikacemi v prostředí infrastruktury a projektů. • Zajišťuje návrh technických řešení a prováděcí projekty • Připravuje návrhy pro rozvojové činnosti a projekty • Komunikuje s příslušnými organizačními celky v rámci řešené problematiky, se specialisty

		zodpovědnými za aplikace a technologie v projektech•
	Vývojář/Specialista	• Pracuje v projektovém týmu Daktela v roli specialisty zodpovědného za vývoj v příslušném programovacím jazyce a prostředí. • Podílí se na tvorbě designu aplikací a architektury systémů. • Má podíl na navrhování databází. Podíl na navrhování a tvorbě datového modelu pro aplikaci. Podíl na přípravě a školení daných technologií. • Znalost analytických datových modelů. • Podíl na přípravě technické a programátorské dokumentace. • Podíl na přípravě automatizovaných a/nebo performance testů.
	Bezpečnostní architekt	• Odpovídá za architekturu bezpečnostních prvků a nástrojů u projektů/provozu a jejich shodu s požadavky Objednatele, formuluje požadavky na budoucí stav zajištění kybernetické bezpečnosti v rámci projektů a identifikuje kroky vedoucí k dosažení požadovaného budoucího stavu. • Provádí analýzy úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Vytváří plány implementace architektury kybernetické bezpečnosti a určuje milníky dosažení očekávaného cílového stavu. • Formuluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů a podílí se na aktualizaci strategie kybernetické bezpečnosti organizace vyplývající z projektů. • Tvoří a aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Průběžné vyhodnocuje aktuální stav úrovně bezpečnostní politiky projektů podle stanovených metrik. • Aktivně se účastní oponentních řízení. • Provádí kontroly úrovně architektury kybernetické bezpečnosti projektů, definuje metriky a identifikuje existující rizika a navrhuje strategii a bezpečnostní opatření na zmírnění identifikovaných rizik. • Spolupracuje na přípravě plánů implementace architektury kybernetické bezpečnosti a kontroluje milníky k dosažení očekávaného cílového stavu. • Kontroluje pravidla a standardy pro oblast kybernetické bezpečnosti projektů. • Průběžně aktualizuje model projektové architektury kybernetické bezpečnosti dle požadavků Objednatele. • Připravuje podklady pro hodnocení aktuálního stavu

		úrovně bezpečnostní politiky projektů podle stanovených metrik. • Připravuje podklady pro oponentní řízení.
	Technická podpora	Pracuje v projektovém týmu Daktela a poskytuje telefonní a emailovou technickou podporu uživatelům systému Implementuje nastavení a konfiguraci systému dle požadavků Objednatele Školí uživatele na nové nastavení Spolupracuje a komunikuje s Objednavatelem ohledně možností konfigurace systému Je zodpovědný za dokumentaci základního nastavení pro interní učely Provozovatele Provádí pravidelné kontroly systému, je zodpovědný za řešení alertů v monitorovacím systému V případě potřeby analyzuje logy a debugovací informace a předává je v přehledné formě na vývojové oddělení Zadavatele
Intelligent Technologies	Dashboard specialista	• Zajišťuje metodické vedení provozu Dashboardu. • Zajišťuje dohled nad provozem Dashboardu. • Realizuje návrhovou a dokumentační činnost Dashoardu • Řídí, nebo se podílí na procesu návrhu a implementace úprav Dashboardu. Připravuje technická řešení. • Účastní se anebo řídí implementaci úprav Dashboardu. • Komunikuje s příslušnými organizačními celky v rámci řešené problematiky, se specialisty zodpovědnými za aplikace a technologie v projektech

NAKIT

Příloha č. 3 – Akceptační protokol

Dodavatel	*Národní agentura pro informační a komunikační technologie, s.p.*
Objednatel	*Česká republika – Ministerstvo zdravotnictví*
Smlouva	*Číslo Smlouvy*
Název Projektu	*Chytrá karanténa 2.0*
Datum předání	*Datum*

Předmět akceptace

Číslo	Popis	Akceptováno	Neakceptováno
01			

Seznam příloh

Závěrečná ustanovení

Poskytovatel a Objednatel svým podpisem stvrzují akceptaci dle výše specifikované Smlouvy.

	Jméno a příjmení	Datum	Podpis
Akceptoval za Poskytovatele			
Akceptoval za Objednatele			

NAKIT

Příloha č. 4 – SLA Služby Systému

A EPI Dashboard

SLA

Provozní doba Aplikace je 7x24, **servisní podpora** (příjem servisních požadavků, řešení provozních problémů) je vykonávána v hodinách 8:00-20:00 každý kalendářní den včetně víkendů a svátků.

Poskytovatel je povinen hlásit minimálně 48 hodin předem plánované odstávky, které by mohly ovlivnit kvalitu a rozsah provozních služeb. Plánované odstávky jsou prováděny primárně mimo dobu servisní podpory (v nočních hodinách). Plánovanou odstávku v době servisní podpory je možno provést pouze se souhlasem Objednatele.

Řešení problémů a sankce:

Stupeň 1 (velmi vysoká priorita)

(Nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba se projevuje u více než 5 % uživatelů)

Doba garantované opravy je 24 hodin od nahlášení. Problémy hlásí zástupce Objednatele na určeném telefonním čísle nebo e-mailu.

Za nedodržení doby opravy je stanovena sankce ve výši 1000,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankcí za všechny problémy Stupně 1 může být maximálně 50 % paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. a) Smlouvy.

B Komunikační nástroj kontaktního centra

SLA

Provozní doba Aplikace je 7x24, **servisní podpora** (příjem servisních požadavků, řešení provozních problémů) je vykonávána v hodinách 8:00-20:00 každý kalendářní den včetně víkendů a svátků.

Poskytovatel je povinen hlásit minimálně 48 hodin předem plánované odstávky, které by mohly ovlivnit kvalitu a rozsah provozních služeb. Plánované odstávky jsou prováděny primárně mimo dobu servisní podpory (v nočních hodinách). Plánovanou odstávku v době servisní podpory je možno provést pouze se souhlasem Objednatele.

Řešení problémů a sankce:

Problémy hlásí zástupce Objednatele nebo uživatelé prostřednictvím linky technické podpory (viz popis níže).

Stupeň 1 (velmi vysoká priorita)

(Základní vlastnosti hlasového připojení jsou nefunkční, např. nelze provádět odchozí telefonické hovory, nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba znemožňuje činnost jedné nebo více KHS.)

Doba garantované opravy je 8 hodin od nahlášení v průběhu doby servisní podpory. V případě nahlášení po 12:00 je doba garantované opravy do 10:00 následujícího dne.

Za nedodržení doby opravy je stanovena sankce ve výši 1000,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankcí za všechny problémy Stupně 1 může být maximálně 50% paušální měsíční ceny Aplikace.

Stupeň 2 (střední priorita)

(Základní vlastnosti hlasového připojení jsou nefunkční, např. nelze provádět odchozí telefonické hovory, nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba se projevuje u méně než 10 % operátorů)

Doba garantované opravy je dohodnuta na 48 hodin od nahlášení.

Za nedodržení doby opravy je stanovena sankce ve výši 500,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankcí za všechny problémy Stupně 2 může být maximálně 25% paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. b) Smlouvy.

Stupeň 3 (nízká priorita)

(Základní vlastnosti telefonie a webové aplikace jsou funkční, chyba je v běžných telefonních operacích (telefon nezvoní, nelze přepojit nebo přesměrovat hovor) nebo jednotlivých funkcionalitách aplikace.

Doba garantované opravy je dohodnuta na 96 hodin od nahlášení.

Za nedodržení doby opravy je stanovena sankce ve výši 100,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy, nejvýše však 500,- za každý jednotlivý servisní problém.

Linka technické podpory

Jednotné telefonní číslo pro hlášení servisních požadavků. Na čísle je implementován rozdělovací hlasový automat pro přesměrování hovoru na servisní hotlinku konkrétní aplikace nebo modulu – nástroje komunikačního centra, vzpomínkové mapy, datové integrace. Hovory jsou monitorovány a je k dispozici reporting a základní statistiky o využití.

Jednotný e-mail pro servisní požadavky E-maily se budou stahovat do samostatné instance helpdeskového systému.

NAKIT

C Vzpomínkové mapy a datové integrace

SLA

Provozní doba Aplikace je 7x24, **servisní podpora** (příjem servisních požadavků, řešení provozních problémů) je vykonávána v hodinách 8:00-20:00 každý kalendářní den včetně víkendů a svátků.

Poskytovatel je povinen hlásit minimálně 48 hodin předem plánované odstávky, které by mohly ovlivnit kvalitu a rozsah provozních služeb. Plánované odstávky jsou prováděny primárně mimo dobu servisní podpory (v nočních hodinách). Plánovanou odstávku v době servisní podpory je možno provést pouze se souhlasem Objednatele.

Řešení problémů a sankce:

Problémy hlásí zástupce Objednatele nebo uživatelé prostřednictvím linky technické podpory (viz kapitola Nástroje call centra).

Stupeň 1 (velmi vysoká priorita)

(Základní vlastnosti hlasového připojení jsou nefunkční, např. nelze provádět odchozí telefonické hovory, nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba znemožňuje činnost jedné nebo více KHS.)

Doba garantované opravy je 8 hodin od nahlášení v průběhu doby servisní podpory. V případě nahlášení po 12:00 je doba garantované opravy do 10:00 následujícího dne.

Za nedodržení doby opravy je stanovena sankce ve výši 1000,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankcí za všechny problémy Stupně 1 může být maximálně 50% paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. c) Smlouvy.

Stupeň 2 (střední priorita)

(Základní vlastnosti hlasového připojení jsou nefunkční, např. nelze provádět odchozí telefonické hovory, nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba se projevuje u méně než 10 % operátorů)

Doba garantované opravy je dohodnuta na 48 hodin od nahlášení.

Za nedodržení doby opravy je stanovena sankce ve výši 500,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankcí za všechny problémy Stupně 2 může být maximálně 25% paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. c) Smlouvy.

Stupeň 3 (nízká priorita)

(Základní vlastnosti telefonie a webové aplikace jsou funkční, chyba je v běžných telefonních operacích (telefon nezvoní, nelze přepojit nebo přesměrovat hovor) nebo jednotlivých funkcionalitách aplikace.

Doba garantované opravy je dohodnuta na 96 hodin od nahlášení.

(Nefunkčnost jednoho z výše uvedených základních procesů, která se projevuje u 5-10% uživatelů)

Doba garantované opravy je 3 kalendářní dny od nahlášení.

Za nedodržení doby opravy je stanovena sankce ve výši 500,- Kč za každou i započatou hodinu nad rámec doby opravy. Celková výše sankce za všechny problémy Stupně 2 může být maximálně 25% paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. d) Smlouvy.

Stupeň 3 (nízká priorita)

(Nefunkčnost jednoho z výše uvedených základních procesů, která se projevuje u 1-5% uživatelů)

Doba garantované opravy je 7 kalendářních dnů od nahlášení.

Za nedodržení doby opravy je stanovena sankce ve výši 100,- Kč za každou i započatou hodinu nad rámec doby opravy, nejvýše však 500,- za každý jednotlivý servisní problém.

Stupeň 4 (marginální)

(Nefunkčnost jednoho z výše uvedených základních procesů, která se projevuje u méně než 1% uživatelů)

Pro tuto závažnost není stanoveno SLA a Poskytovatel má v odůvodněných případech aplikaci neopravovat.

E Integrace Mapy.cz

Provozní služby integrace Mapy.cz jsou součástí provozních služeb komunikačních nástrojů kontaktního centra a nástrojů datové integrace.

Poskytovatel neodpovídá za problémy na straně aplikací Seznam.cz.

F Nástroje EA

SLA

Provozní doba Aplikace je 7x24, **servisní podpora** (příjem servisních požadavků, řešení provozních problémů) je vykonávána v pracovních dnech 8:00-17:00.

Poskytovatel je povinen hlásit minimálně 48 hodin předem plánované odstávky, které by mohly ovlivnit kvalitu a rozsah provozních služeb. Plánované odstávky jsou prováděny primárně mimo dobu servisní podpory (v nočních hodinách). Plánovanou odstávku v době servisní podpory je možno provést pouze se souhlasem Objednatele.

Řešení problémů a sankce:

Stupeň 1 (velmi vysoká priorita)

(Nelze se připojit k webovému rozhraní nebo webové rozhraní neumožňuje provádět základní úkony, a chyba se projevuje u více než 10 % uživatelů)

Doba garantované opravy je do konce příštího pracovního dne od nahlášení. Problémy hlásí zástupce Objednatele na určeném telefonním čísle nebo e-mailu.

Za nedodržení doby opravy je stanovena sankce ve výši 1000,- Kč za každou i započatou hodinu doby servisní podpory nad rámec doby opravy. Celková výše sankce za všechny problémy Stupně 1 může být maximálně 50 % paušální měsíční ceny Aplikace uvedené v čl. 2 odst. 2.8 písm. f) Smlouvy.

G COVID mobilní info karta

Pro Aplikaci kartu není stanoveno SLA.

NAKIT

Příloha č. 5 - Bezpečnostní požadavky

1. Služba Systému musí splňovat požadavky na řízení bezpečnosti informací v souladu platnou legislativou, standardy v oblasti řízení bezpečnosti informací. Především dle zákona 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve stejném rozsahu, jako je požadováno pro významný informační systém. Pro vyloučení pochybností se sjednává, že tyto bezpečnostní požadavky se vztahují i na jednotlivé Aplikace zvlášť. Pro Systém a jednotlivé Aplikace bude rovněž Poskytovatelem v rámci poskytování Odborných služeb zpracována bezpečnostní dokumentace v souladu s požadavky vyhlášky o kybernetické bezpečnosti a další řídící dokumentací v oblasti kybernetické bezpečnosti Objednatele, byla-li prokazatelně zpřístupněna Poskytovateli.

2. V rámci poskytování Odborných služeb bude Poskytovatelem zpracována provozní a bezpečnostní dokumentace v souladu s vyhláškou č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

3. Dokumentace podle bodů 1. a 2. výše bude zpracována s ohledem na níže uvedené požadavky na strukturu, rozsah a kvalitu:

   3.1 Bezpečnostní dokumentace systému KII (nebo VIS):

      3.1.1 bezpečnostní politika,

      3.1.2 bezpečnostní směrnice pro činnost bezpečnostního správce systému,

      3.1.3 bezpečnostní a provozní postupy definující požadavky, procesní pravidla, role a odpovědnost v rámci jednotlivých procesů v rámci celého životního cyklu IS (od zajištění vývoje a rozvoje nových funkčností IS, následného předání do provozu, provozování a správy IS, nebo zařízení v produkci až po jeho vyřazení z používání).

   3.2 Systémová příručka obsahující

      3.2.1 popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy a návod na používání těchto funkcí,

      3.2.2 parametry kvality vycházejí z požadavků na kvalitu,

      3.2.3 podrobný popis IS nebo odkaz na dokument, ve kterém je popis uveden a který je Objednateli dostupný,

      3.2.4 popis jednotlivých činností vykonávaných při správě IS, včetně činností definovaných pro role, určení fyzických osob, které tyto činnosti vykonávají a oprávnění nezbytných pro výkon těchto činností,

3.2.5 definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání IS.

3.3 Uživatelská příručka obsahující

3.3.1 popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost v IS a návod na použití těchto funkcí,

3.3.2 vymezení oprávnění a povinností uživatelů ve vztahu k IS.

3.4 Dokumentace k integraci řešení, a to včetně identifikovaných datových struktur a toků, protokolů, architektonického nákresu komponent a jejich spolupráce, diagramů logického a fyzického zapojení.

3.5 Další dokumentaci v souladu s bezpečnostními politikami a standardy Objednatele, byla-li prokazatelně zpřístupněna Poskytovateli.

3.6 Poskytovatel se v rámci poskytovaného plnění pro Objednatele zavazuje předat Objednateli také provozní dokumentaci v obdobném rozsahu dle předmětu a povahy Smlouvy:

3.6.1 dokumentaci strategie obnovy,

3.6.2 dokumentaci skutečného provedení,

3.6.3 dokumentaci obsahující popis autorizačního konceptu a oprávnění,

3.6.4 dokumentaci obsahující zálohovací a archivační postupy,

3.6.5 dokumentaci obsahující instalační a konfigurační postupy,

3.6.6 dokumentaci obsahující bezpečností nastavení související s předmětem plnění Smlouvy.

4. Auditovatelnost a nepopiratelnost

4.1 Všechny úspěšné i neúspěšné přístupy ke Službě Systému musí být logovány. Záznamy o neúspěšných přístupech musí být monitorovány a v případě zvýšeného počtu neúspěšných pokusů se požaduje vyvolání odpovídající akce. Veškeré změny dat ve Službě Systému musí být logovány tak, aby bylo možné zjistit kdo, kdy, jak a která data ve Službě Systému modifikoval:

4.1.1 u nově založených záznamů (operace INSERT) musí být možno dohledat informace kdo, kdy a v jakém stavu (obsahu dat) záznam založil;

4.1.2 u změněného záznamu (při každé operaci UPDATE) musí být umožněno zjištění kdo, kdy a jakým způsobem data změnil, a to v plné šíři datové věty a plné historii změn;

4.1.3 u smazaného záznamu nesmí dojít k trvalému odstranění dat („nepodporovat fyzickou operaci DELETE“), ale pouze k logickému zneplatnění záznamu (provést operaci UPDATE s nastavením

ukončení platnosti) a musí být zaznamenáno kdo, kdy a v jakém stavu dat záznam logicky zneplatnil.

4.2 Ze záznamů musí být možné zrekonstruovat kompletní historii každého datového objektu včetně časové specifikace jeho změn, včetně historie všech datových vazeb na ostatní datové objekty. Ke každé změně dat musí být možné identifikovat jejího původce (uživatel / Služba Systému).

4.3 Služba Systému musí zajistit důvěrnost a integritu dat na celé cestě mezi databázovým serverem a klientem, tedy je požadováno zabezpečené propojení mezi všemi architektonickými vrstvami systému vyjma zásahů a úprav realizovaných administrátory DB.

4.4 Důvěrnost a integrita dat musí být zachována i při zálohování a archivaci, a to jak při vlastním procesu, tak i následně vzhledem k médiím, na nichž jsou zálohy a archivní data uloženy vyjma zásahů a úprav realizovaných administrátory DB.

5. Služba Systému musí splňovat požadavky na řízení bezpečnosti informací v souladu platnou legislativou, standardy v oblasti řízení bezpečnosti informací. Služba Systému musí být odolný proti známým bezpečnostním hrozbám a útokům. Podrobnosti budou upraveny v bezpečnostní dokumentaci dle bodu 2 této přílohy.

6. V případě realizace penetračních testů, skenu zranitelnosti a dalších bezpečnostních testů Služby Systému a/nebo Aplikace Objednatelem, se Poskytovatel zavazuje poskytnout Objednateli veškerou součinnost potřebnou pro úspěšné provedení testů.

7. Poskytovatel je povinen dodržovat při plnění předmětu Smlouvy příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Poskytovateli Objednatelem, resp. platné řídící dokumentace Objednatele, či její části anebo platné řídící dokumentace, k jejímuž dodržování se zavázal, pokud byl Poskytovatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Poskytovateli, elektronickým předáním prostřednictvím e-mailu, zřízením přístupu Poskytovatele na sdílené úložiště aj.)

8. Poskytovatel umožní Objednateli provedení zákaznického auditu u Poskytovatele a poskytnout mu k němu nezbytnou součinnost (dále jen „zákaznický audit"). Objednatel je oprávněn provést zákaznický audit v případě auditu kybernetické bezpečnosti, dle § 16 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), Dále lze provést zákaznický audit v případě řešení kybernetického bezpečnostního incidentu v přímé souvislosti s plněním dle této Smlouvy. Zákaznický audit může za Objednatele provést pověřený zaměstnanec Objednatele nebo jiná pověřená osoba. Objednatel je oprávněn pověřit provedením zákaznického auditu třetí stranu. Rozsah auditu musí být rozsahem relevantní k předmětu a účelu této Smlouvy.