

Dodatek č. 1
k servisní smlouvě, uzavřené dne 4. 11. 2021

mezi stranami:

Česká republika - Státní ústav pro kontrolu léčiv, organizační složka státu

IČ: 00023817

se sídlem: Šrobárova 48, PSČ: 100 41, Praha 10

zastoupena: Mgr. Irenou Storovou, MHA, ředitelkou

bankovní spojení: 623101/0710 (veden u ČNB)

(dále jen "**Objednatel**")

a

ORSIA, spol. s r.o.

IČ: 15030261

DIČ: CZ15030261

se sídlem: Čs. armády 1181, 562 01 Ústí nad Orlicí

zastoupen: XXX

bankovní spojení, č.ú.: XXX

(dále jen „**Poskytovatel**“)

(Objednatel a Poskytovatel dále společně také jen jako „**smluvní strany**“)

Článek 1.

Úvodní ustanovení

1.01 Dne 4. 11. 2021 uzavřely smluvní strany servisní smlouvu, jejímž předmětem je povinnost Poskytovatele poskytovat Objednateli servisní podporu informačního systému Centrální databáze nežádoucích účinků (dále jen „**Smlouva**“).

1.02 Tímto dodatkem se Smlouva mění tak, jak je uvedeno v Článku 2. tohoto dodatku.

Článek 2.

Změny Smlouvy

2.01 Dosavadní znění odst. 1.03 Smlouvy se vypouští a nahrazuje se následujícím ustanovením:

*„1.03 Objednatel v souladu s § 4a odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**“) informuje Poskytovatele, že Systém je významným informačním systémem ve smyslu § 2 písm. d) ZoKB a Objednatel je ve smyslu § 2 písm. e) ZoKB správcem tohoto Systému, přičemž Poskytovatel bere toto na vědomí. V tomto smyslu se Poskytovatel stává významným dodavatelem dle § 2 písm. n)*

vyhlášky č. 82/2018 Sb. a při plnění této Smlouvy je povinen plnit Bezpečnostní pravidla pro významné dodavatele, které tvoří Přílohu č. 4 této Smlouvy. V případě rozporu mezi ustanovením Smlouvy a ustanovením Přílohy č. 4 je rozhodující ustanovení Smlouvy. V případě rozporu mezi ustanovením Přílohy č. 1 a ustanovením Přílohy č. 4 je rozhodující ustanovení Přílohy č. 1.“

2.02 Dosavadní znění odst. 16.02 Smlouvy se vypouští a nahrazuje se následujícím ustanovením:

„16.02 Nedílnou součástí této Smlouvy je:

Příloha č. 1 - Specifikace Služeb

Příloha č. 2 - Specifikace Systému

Příloha č. 3 - Formulář žádosti o přístup/ukončení přístupu do informačního systému Objednatele

Příloha č. 4 – Bezpečnostní pravidla pro významné dodavatele“

2.03 Doplnuje se nová Příloha č. 4 Smlouvy – Bezpečnostní pravidla pro významné dodavatele, která je přílohou tohoto dodatku.

Článek 3.

Závěrečná ustanovení

3.01 Ostatní ustanovení Smlouvy, neuvedená v Článku 2. tohoto dodatku, zůstávají tímto dodatkem nedotčena.

3.02 Nedílnou součástí tohoto dodatku je příloha Bezpečnostní pravidla pro významné dodavatele, která se doplňuje jako nová Příloha č. 4 Smlouvy.

3.03 Tento dodatek nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

3.04 Na důkaz toho, že celý obsah tohoto dodatku je projevem jejich pravé, vážné a svobodné vůle, připojují osoby oprávněné za smluvní strany uzavírat tento dodatek své podpisy.

V Praze dne 16.12.2021

V Ústí nad Orlicí dne 10.12.2021

Objednatel:

Poskytovatel:

.....
Mgr. Irena Storová, MHA
ředitelka Státního ústavu pro kontrolu léčiv

.....
XXX
jednatel ORSIA, spol. s r.o.

BEZPEČNOSTNÍ PRAVIDLA PRO VÝZNAMNÉ DODAVATELE dle ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI (č. 181/2014 Sb.) a VYHLÁŠKY č. 82/2018 Sb.

1 PERSONÁLNÍ BEZPEČNOST

1.1 Smluvní partner Státního ústavu pro kontrolu léčiv (dále jen „SÚKL“) a jeho případní subdodavatelé (smluvní partner a subdodavatelé dále jen souhrnně „dodavatel“) mají povinnost ve svých interních procesech realizovat tato opatření:

- a) mít stanoven vlastní plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah:
 - i. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
 - ii. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role, nebo zajišťujících podporu provozu informačního systému SÚKL;
- b) mít určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;
- c) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
- d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;
- e) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
- f) zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
- g) v případě ukončení smluvního vztahu s administrátory a osobami podílejících se na podpoře vývoje či provozu systému SÚKL či jakékoliv jeho infrastrukturní části, zajišťovat předání odpovědností, zrušení jejich přístupových účtů a informovat SÚKL o této skutečnosti;
- h) stanovit interní pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany administrátorů a osob zastávajících bezpečnostní role;
- i) vést o provedených školeních přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.2 SÚKL si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“). Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele, zejména při situacích vzniklých bezpečnostních incidentů. V případě identifikovaného rizika oznámí SÚKL nesoulad dodavateli a obě strany vejdou v jednání pro řešení této situace.

1.3 Kvalifikace zaměstnanců dodavatele musí odpovídat vykonávané pracovní pozici (vykonávané práci a úrovni zabezpečení).

2 FYZICKÁ BEZPEČNOST, POŽÁRNÍ OCHRANA A BOZP

2.1 Dodavatel jako zaměstnavatel při provádění prací při plnění smlouvy odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci v prostorách SÚKL, popř. dalšími fyzickými osobami vykonávajícími práci v jeho prospěch a odpovídá za dodržování podmínek vstupu osob a vjezdu vozidel do areálů, objektů a na pozemky SÚKL a bezpečnostního režimu pro ně stanoveného.

3 BEZPEČNOSTNÍ POVĚDOMÍ

3.1 Každý zaměstnanec dodavatele musí být prokazatelně proškolen a mít znalosti příslušných interních předpisů SÚKL souvisejících s předmětem plnění smlouvy. Za proškolení zaměstnanců dodavatele (v roli provozovatele) a za jejich prokazatelné seznámení s požadavky smlouvy a jejích příloh odpovídá dodavatel.

4 IDENTIFIKACE

4.1 Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji. Na technická zařízení, se kterými zaměstnanci dodavatele přistupují do vymezených částí vnitřní infrastruktury SÚKL, se ze strany SÚKL pohlíží jako na BYOD a pro jejich konfiguraci se vyžaduje dodržování minima dle vnitřního předpisu SÚKL S-069, který je dodavateli předán.

4.2 Každý zaměstnanec dodavatele, pokud přistupuje k interním systémům SÚKL, má u SÚKL veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.

5 AUTENTIZACE

5.1 Podmínky pro autentizaci při využití ICT infrastruktury SÚKL:

a) k jednoznačné identifikaci privilegovaných uživatelů určených systémů se preferovaně využívá vícefaktorová autentizace;

b) ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace heslem o minimální délce 17 znaků, kdy mezi znaky musí být minimálně jedno velké písmeno, jedno malé písmeno, jedna číslice a **jeden metaznak z možností: #, \$, &, %, !, ?, +, -**. Heslo musí být měněno nejpozději po **12 / 18 měsících** a nesmí se následně zopakovat v následných 12ti změnách.

5.2 Pro vzdálený přístup zaměstnanců dodavatele předkládá dodavatel podklady pro vyplnění žádosti o vzdálený přístup, podle které jsou poté nastavena oprávnění. Žádost podepisuje oprávněná osoba dodavatele jednat ve věcech plnění smlouvy.

5.3 Dodavatel odpovídá za činnosti svých zaměstnanců, popřípadě dalších fyzických osob vykonávajících práci v jeho prospěch, které musí být v souladu s pravidly, předanými ze strany SÚKL.

Veškeré škody, které vzniknou porušením těchto pravidel zaměstnanci dodavatele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k tíži dodavatele, který je povinen tyto škody v plném rozsahu SÚKL nahradit.

6 AUTORIZACE

6.1 Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře SÚKL využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou určeného systému a v žádném případě nesmí umožnit pracovat pod tímto účtem jiným osobám.

6.2 Zaměstnanci dodavatele jsou informováni SÚKL, ke kterým chráněným informacím SÚKL mají při plnění smlouvy přístup a jak s nimi mohou nakládat. Tyto informace vyplývají ze smlouvy a dodavatel je oprávněn a povinen své zaměstnance s příslušnými částmi smlouvy prokazatelně seznámit. Jakékoliv manipulace a další operace s chráněnými informacemi SÚKL, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

7 KONCOVÁ PRACOVNÍ STANICE

7.1 Pro přístup k systémům SÚKL jsou standardně použity vlastní prostředky dodavatele (HW, SW). Dodavatel odpovídá za to, že nejsou používány v rozporu s licenčními podmínkami produktů.

7.2 Přístup výpočetní techniky dodavatele (PC, notebooky) k chráněným interním informacím a k informačním a telekomunikačním systémům je podmíněn schválením příslušného pracoviště SÚKL a odpovědnou osobou systému.

7.3 Pracovní stanice dodavatele přistupující prostřednictvím VPN musí splňovat podmínky uvedené pro používání BYOD v interní směrnici SÚKL S-069.

8 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

8.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:

- a) užití pouze kryptografických prostředků podle doporučení vydávaných a aktualizovaných NÚKIB
- b) šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;
- c) pro webové servery prezentující data pocházející z určených informačních systémů mimo samotný systém používat HTTPS protokol;
- d) pro webové servery prezentující data pocházející z určených systémů pro uživatele mimo SÚKL se používá certifikát obecně uznávané certifikační autority.

9 MONITORING

9.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům SÚKL může být nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události v systémech jsou SÚKL zaznamenávány do logů.

9.2 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

9.3 V souladu s příslušnými ustanoveními smlouvy je dodavatel povinen neprodleně po zjištění hlásit SÚKL každý nastalý bezpečnostní incident.

10 OCHRANA MÉDIÍ

10.1 Uložení chráněných informací SÚKL na přenosná média a případný transport médií mimo prostory SÚKL podléhá jeho schválení.

10.2 V případě ukládání chráněných informací SÚKL na přenosná média má dodavatel povinnost, pokud je to technicky možné, ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

10.3 Dodavatel je povinen zajistit likvidaci operativních dat obsahujících chráněné informace SÚKL ihned po pominutí účelu jejich zpracování a/nebo uložení způsobem dle právních předpisů či metodik vydaných NÚKIB, případně ÚOOÚ. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

11 BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

11.1 Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události:

a) odpovědné osobě SÚKL (osoba oprávněná jednat ve věcech plnění smlouvy a manager kybernetické bezpečnosti). Ohlášení provede mailem (případně telefonicky) v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu.

b) v ohlášení uvede:

- i. datum a čas zjištění;
- ii. povahu události / incidentu;
- iii. zdroje události;
- iv. cíle / oběti události;
- v. okamžité i potencionální dopady;
- vi. přijatá či navrhovaná opatření k omezení dopadů, případně eliminaci opakování.

12 AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)

12.1 OPRÁVNĚNÍ K PROVEDENÍ AUDITU DODAVATELE

a) SÚKL si v souladu s ustanovením smlouvy vyhrazuje právo provádět audity dodavatele.

b) SÚKL s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že SÚKL se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.

c) SÚKL si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.

d) Dokumentace auditů prováděných SÚKL tvoří pro každý audit:

- i. oznámení o auditu a plán auditu;
- ii. dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
- iii. zpráva z auditu;
- iv. písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
- v. záznam o zjištění (nápravných opatřeních a následné kontrole).

f) Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění:

- i. dodavatel navrhne na základě zjištění uvedených v závěrečné auditní zprávě návrh opatření a termíny řešení a předá jejich seznam SÚKL k odsouhlasení;
- ii. SÚKL potvrdí souhlas s navrženými opatřeními. Souhlas vydává osoba oprávněná jednat ve věcech smlouvy.

12.2 NÁPRAVNÁ OPATŘENÍ

a) Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření;

b) Zprávu o realizovaných opatřeních dodavatel oznamuje a předává SÚKL cestou člena jeho auditního týmu.

13 PODMÍNKY PŘI UKONČENÍ SMLOUVY

13.1 V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům společnosti (VPN, systémy, informace) nejpozději k termínu ukončení smluvního vztahu.

13.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva SÚKL, musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.

13.3 Pokud byla dodavateli poskytnuta informační aktiva (data) SÚKL, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem určeným v právních předpisech o kybernetické bezpečnosti, či metodice NÚKIB, resp. ÚOOÚ, ze všech systémů dodavatele a nosičů dodavatele taková aktiva obsahujících. O smazání či předání takových aktiv musí být vypracován protokol, který je předán SÚKL.

13.4 V případě předčasného ukončení smluvního vztahu jiným způsobem než splněním závazku (např. výpovědí, odstoupením od smlouvy, dohodou o ukončení smlouvy apod.), mohou být přístupy dodavatele, pokud je to nutné, ze strany SÚKL ukončeny před uplynutím doby trvání smluvního vztahu.