Smlouva o vzájemné ochraně informací a dodržování bezpečnostní politiky

1. Smluvní strany

Objednatel:

Česká průmyslová zdravotní pojišťovna

Sídlo: Jeremenkova 11, 703 00, Ostrava-Vítkovice

IČO: 47672234

Zastoupena: JUDr. Petrem Vaňkem, Ph.D., generálním ředitelem

Zapsaná u: Krajského soudu v Ostravě, spisová značka A.XIV 545

dále jen ,,ČPZP“ na straně jedné

a

Dodavatel:

Sophia Solutions, s.r.o.

Sídlo: Evropská 2588/33a, 160 00 Praha 6

IČO: 2673 6471

Zastoupena: Mgr. Janem Kadlecem, jednatelem

Zapsaná u: u Městského soudu v Praze, oddíl C, vložka 90534

dále jen ,,Partner“ na straně druhé

sjednali níže uvedeného dne, měsíce a roku tuto smlouvu

takto

2. Předmět smlouvy

2.1 Smluvní strany se zavazují v rámci vzájemné spolupráce zachovat v tajnosti veškeré informace zjištěné při vzájemné spolupráci a neporušovat obchodní tajemství ve smyslu ustanovení § 2985 a § 504 zákona č. 89/2012 Sb., občanský zákoník. Výjimka je možná pouze v rozsahu a za podmínek stanovených zákonem.

2.2 Skutečnosti, které jsou označeny jako veřejné:

- referenční informace o projektech, realizovaných u ČPZP Partnerem, určené k uvádění v seznamu referencí Partnera, a to v rozsahu názvu díla, jména ČPZP a firmy Partnera a jeho subdodavatelů, rok realizace, informace o použité technologii pro vývoj v rozsahu programátorských nástrojů a prostředí, ve kterém byl projekt vytvářen.

- informace v rozsahu Výroční zprávy ČPZP.
- informace z propagačních tiskovin a internetových stránek ČPZP.

Ostatní skutečnosti jsou označeny jako neveřejné, nedohodnou-li se smluvní strany jinak.

2.3 Neveřejné informace, o kterých se Partner zavazuje zachovat mlčenlivost a zajistit, aby mlčenlivost dodržely i osoby jím pověřené prací pro ČPZP, jsou zejména tyto informace týkající se ČPZP:

- strategie a politiky,
- informace o bezpečnosti (zejména aktiva, zranitelnost a přijatá ochranná opatření),
- informační systémy,
- technologie zpracováni dat,
- obsah datové základny,
- obsah pevných disků pracovních stanic,
- metodika zpracování dat,
- interní dokumenty ČPZP.

2.4 Partner se zavazuje přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému zpřístupnění neveřejných informací.

2.5 Partner se zavazuje dodržovat Pravidla informační bezpečnosti uvedená v příloze této Smlouvy. Tato Pravidla tvoří soubor norem, pravidel a postupů, které vymezují způsob a požadovanou úroveň bezpečnosti, vymezení aktiv a způsob jejich zajištění oprávněnými osobami Partnera v rámci vzájemné spolupráce.

2.6 Partner se zavazuje zajistit seznámení svých pověřených pracovníků a oprávněných osob (dále též „zaměstnanci Partnera“) s touto Smlouvou a provede o tom záznam, který bude kdykoliv k dispozici zástupci ČPZP.

2.7 Partner je povinen bez odkladu oznámit ČPZP změny u oprávněných osob, zejména pak ty, mající dopad na přístupy do IS.

2.8 Závazek Partnera dodržovat Pravidla informační bezpečnosti uvedená v příloze této Smlouvy platí pro Partnera po celou dobu vzájemné spolupráce. Závazek o mlčenlivosti platí i po ukončení spolupráce po dobu 5 let a nelze od něj odstoupit.

2.9 V případě, že Partner bude využívat služeb subdodavatele

- platí pro něj a pro jeho zaměstnance stejná bezpečnostní pravidla jako pro Partnera včetně požadavku mlčenlivosti,
- o úmyslu použít služeb subdodavatele je Partner povinen předem písemně informovat ČPZP včetně rozsahu využívaných služeb a je povinen požádat ČPZP o povolení takového postupu,
- Partner nese plnou odpovědnost za činnost svého subdodavatele i v případě porušení povinností vyplývajících z této Smlouvy,

- Partner je povinen smluvně zavázat subdodavatele tak, aby pro něj a pro jeho zaměstnance platila stejná bezpečnostní pravidla jako pro Partnera, včetně sjednání závazků zachovávat za stejných podmínek mlčenlivost.

3. Ostatní a závěrečná ujednání

a) Tato smlouva je uzavřena a nabývá účinnosti dnem jejího podpisu oběma smluvními stranami. Smlouva je sjednána na dobu určitou do 31. 12. 2021 a nelze od ní odstoupit. Smluvní strany sjednávají, že tato smlouva nahrazuje všechny předchozí smlouvy o vzájemné ochraně informací uzavřené mezi oběma smluvními stranami.

b) Pokud po ukončení platnosti této smlouvy nebude podepsána nová smlouva o vzájemné ochraně informací, zavazuje se Partner zachovat mlčenlivost o všech skutečnostech, které nebudou označeny jako veřejné, i po skončení této smlouvy po dobu 5 let.

c) V případě prokazatelného porušení povinností sjednaných touto smlouvou se Partner zavazuje k úhradě smluvní pokuty ve výši 100 000 Kč (slovy: jednostotisíc korun českých) za každý jednotlivý případ. Náhrada škody, která by z takovéhoto porušení vznikla, není tímto dotčena.

d) Tato smlouva je vypracována ve dvou vyhotoveních rovné právní síly, z nichž každá strana obdrží po jednom vyhotovení a je ji možné měnit pouze písemnými dodatky podepsanými oprávněnými zástupci obou smluvních stran.

V Ostravě dne 24.11.2017

……	……
JUDr. Petr Vaněk, Ph.D.	partner
generální ředitel	Mgr. Jan Kadlec, jednatel
Česká průmyslová zdravotní pojišťovna	

Příloha ke Smlouvě o vzájemné ochraně informací a dodržování bezpečnostní politiky: **Pravidla informační bezpečnosti**

1. Obecné povinnosti

a) Zaměstnanci Partnera jsou povinni chránit aktiva ČPZP, která používají ke své práci pro ČPZP anebo k nim mají přístup, a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití nebo odcizení.

b) Povinnosti zaměstnanců Partnera při ochraně informací a aktiv ČPZP:

- dodržovat platnou obecně závaznou legislativu,
- využívat uživatelské systémy tak, jak bylo stanoveno vlastníkem informací,
- používat informační aktiva pouze v souladu s rozsahem přidělených přístupových oprávnění a pouze ke schváleným účelům,
- zajistit ochranu svých autentizačních údajů (login, heslo, identifikační předmět),
- odpovědnost za každý přístup k informacím ČPZP, provedený prostřednictvím přidělených autentizačních údajů,
- respektovat všechna bezpečnostní opatření a procedury určené vlastníkem informací,
- nerozšiřovat data bez souhlasu ČPZP.

2. Pracovní stanice, mobilní prostředky

Při práci na koncových uživatelských pracovištích ČPZP musí být splněny nejméně následující bezpečnostní zásady:

a) Použití počítače ČPZP je povoleno pouze oprávněné osobě Partnera.

b) Zaměstnancům Partnera je zakázáno připojovat vlastní počítače a mobilní prostředky včetně mobilních telefonů do vnitřní sítě ČPZP bez vědomí vedoucího odboru technické a systémové podpory ČPZP.

c) Pracovní stanice a mobilní prostředky nesmí být ponechány bez dozoru zapnuté a s přihlášeným uživatelem. Je nutné přinejmenším použít heslem chráněného spořiče obrazovky.

d) Počítač Partnera, který má být připojen do vnitřní sítě ČPZP, musí mít instalován a spuštěn antivirový program v nejnovější verzi programu i virové databáze.

e) Zaměstnanec Partnera je povinen chránit vybavení ČPZP a udržovat bezpečné pracovní prostředí.

f) V případě ukončení práce se zařízením je zaměstnanec Partnera povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

3. Využívání internetu

a) Systémy v ČPZP vztahující se k počítačové síti, internetu a intranetu, včetně počítačového vybavení, programů, operačních systémů, medií pro ukládání dat, schránek elektronické pošty ČPZP, možností prohlížení internetových stránek a zdrojů přístupných na FTP jsou vlastnictvím ČPZP. Tyto systémy jsou používány pro pracovní účely tak, aby sloužily zájmům ČPZP.

b) Zaměstnanci Partnera mají dovoleno používat internetové připojení do a z vnitřní sítě ČPZP pouze za účelem naplnění předmětu smlouvy. Způsob připojení do vnitřní sítě ČPZP a jejich autentizace musí být předem dohodnuta s útvarem pro ICT. Není-li smluvně dohodnuto jinak, jsou zaměstnanci Partnera povinni oznámit předem datum a čas přihlášení k vnitřnímu prostředí ČPZP a následně ukončení práce.

4. Bezpečnost systémů IT

U vyvíjených nebo dodávaných informačních systémů musí Partner zajistit níže uvedená pravidla.

a) Používání hesel v aplikaci

- Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla.
- Hesla nesmí být v aplikaci uložena v otevřené (čitelné) podobě.
- Uživatel aplikace musí být nucen si heslo pravidelně měnit nejméně po 100 dnech.
- V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je nutné, aby aplikace umožnila vynutit změnu inicializačního hesla.
- Heslo musí být kontrolováno aplikací, zda má alespoň 8 znaků a splňuje alespoň tři ze čtyř pravidel:
    - alespoň jedno malé písmeno,
    - alespoň jedno velké písmeno,
    - alespoň jednu číslici,
    - alespoň jeden speciální znak odlišný od znaků uvedených v prvních třech bodech (např. !, -, :, mezera).
- V případě požadavku ČPZP na zahrnutí aplikace do interního systému single sign on se použijí jen adekvátní pravidla.

b) Monitorování používání a přístupu k systému

V informačních systémech musí být pořizovány kontrolní záznamy pro nepopiratelnost odpovědnosti uživatelů obsahující:

- identifikaci uživatele,
- datum a čas přihlášení a odhlášení,
- identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné),

- záznamy o přístupu (úspěšném i neúspěšném),
- monitorování důležitých aktivit a operací s daty a jinými zdroji systému.

c) Řízení přístupu k informačnímu systému

- Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti. Není-li možné pro daný účel (např. pro automatizovanou synchronizaci dat mezi dvěma systémy) vytvořit účet personalizovaný, je možné vytvořit účet technický. Vytvoření technického účtu schvaluje a povoluje manažer kybernetické bezpečnosti ČPZP po dodání všech jím požadovaných údajů do evidence technických účtů ČPZP. Změny v rozsahu oprávnění podléhají rovněž schválení a povolení manažerem kybernetické bezpečnosti ČPZP.
- Před umožněním přístupu musí být každý uživatel identifikován a autentizován.
- Informační systém by měl po určité době nečinnosti uživatele (doporučeno 20 minut) tohoto uživatele odhlásit.
- Aplikace musí být vytvořena tak, aby počet neúspěšných pokusů o přihlášení byl omezen. Po třech neúspěšných pokusech o přihlášení musí být další zadávání na určitou dobu omezeno nebo spojení rozpojeno.
- Pokud je při přihlašování do aplikace některá část chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.
- Pro každého uživatele systému musí být možné identifikovat, jaká má přístupová práva.
- Pro každý prostředek (funkce, nabídka v menu, tabulka atd.) musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.)
- Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

5. Bezpečnost dat

a) Data vstupující do IS ČPZP

- Musí být zabezpečena proti neautorizovanému přístupu a musí být dostupná oprávněným uživatelům.
- Musí být navržen zálohovací mechanismus včetně kontroly integrity dat na zálohovacím médiu a způsob obnovy dat ze zálohy. Zálohování nesmí omezit uživatele IS.
- Integrita dat musí být zajištěna transakčním zpracováním.
- Data vstupující do IS musí být kontrolována (neplatné znaky, rozsah, přetečení, formát, kompletnost, souvislost…), zjištěná chyba musí být srozumitelně popsána.

Pokud ČPZP usoudí, že vytvářená aplikace by měla pro ochranu dat využívat kryptografii, je nezbytné, aby byly aplikovány mezinárodně uznávané standardy a dodržena obecně závazná legislativa.

b) Data předávaná Partnerům

- Předáváním dat Partnerům se rozumí předávání informací z ČPZP smluvnímu partnerovi na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty ČPZP, CD-ROM, diskety, pevné disky počítačů a jiné nebo zasílané e-mailem, datovou schránkou, na datové úložiště Partnera nebo jiným elektronickým způsobem. Partner je povinen nakládat s předanými daty dle tohoto dokumentu.
- Předávání dat musí být vymezeno ve smlouvě (popis a struktura dat, způsob předávání, způsob ochrany, periodicita, oprávněné osoby, atp.) a musí probíhat bezpečným způsobem.
- Uchovávání a případné zpracování dat u Partnera musí být prováděno tak, aby byla zajištěna jejich dostatečná ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití nebo poškození.
- Zodpovědnost za dostatečnou ochranu předávaných dat má Partner
- Partner je povinen dbát na bezpečnost likvidace již nepotřebných dat, případně médií s daty. Pro likvidaci medií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možné běžně dostupnými prostředky obnovit (skartovačka, SW skartovačka).
- Partner si nesmí sám stahovat žádná data z IS ČPZP; vytváření souborů musí provést oprávněný zaměstnanec ČPZP a teprve takto vytvořená data smí být (na smluvním základě) předána Partnerovi. Toto opatření neplatí pro soubory vytvářené na žádost oprávněných zaměstnanců ČPZP z IS, které Partner na smluvním základě udržuje.
- Pokud budou zasílána neveřejná data e-mailem, musí být šifrována a to v obou směrech komunikace.

6. Bezpečnost dodávek a služeb

a) Vývoj a údržba software smluvními partnery

- Vývoj software musí probíhat na vývojovém prostředí u Partnera, který je povinen je udržovat po celou dobu trvání smluvního vztahu souvisejícího s vývojem software. Poté musí být software otestován v testovacím prostředí ČPZP, které je oddělené od produkčního prostředí. Vývoj musí probíhat:
    - legálním software,
    - na testovacích datech, která nejsou převzata z provozní databáze (pokud je nutno použít data z provozní databáze, je nutno je anonymizovat),

    - tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení.

- Partner musí zajistit důsledné verzování a archivaci všech zdrojových kódů a dalších výstupů vývoje tak, aby bylo možné se v případě potřeby vrátit k předchozímu stavu.
- Nedílnou součástí dodávky software je bezpečnostní dokumentace.
- Přístup Partnera do IS ČPZP (testovacího i provozního prostředí) může být použit pouze pro činnosti směřující k naplnění předmětu smlouvy.
- Pro realizaci údržby systémů platí tytéž bezpečnostní požadavky, jako v případě jejich vývoje.

b) <u>Dodávka software</u>

- Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována.
- U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice.
- Každý nový software musí být otestován, než bude akceptován a zařazen do produkčního prostředí, přičemž je nutné dbát na zjištění shody dodaného produktu s dokumentací a na vyloučení možnosti zavlečení škodlivého kódu.

c) <u>Dodávka hardware</u>

- Dodávka hardware musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. O každé dodávce musí existovat kromě účetních dokladů i předávací protokol podepsaný Partnerem (dodavatelem) a ČPZP (odběratelem). Způsob předání závisí na konkrétním produktu a na smlouvě s Partnerem.
- Každé nové zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí.

d) <u>Dodávka služeb</u>

- Dodávka služeb musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Způsob předání závisí na konkrétní službě a na smlouvě s Partnerem (dodavatelem).
- Součástí dodávky služeb musí být jednoznačná deklarace požadované služby a musí být nastaveny její kvalitativní parametry.
- Je-li součástí dodávky služeb údržba IS nebo aplikací ČPZP a je-li tato údržba prováděna zaměstnanci Partnera, nelze ji zahájit bez souhlasu oprávněného zaměstnance útvaru pro ICT.
- **<u>Servis hardware a software</u>**

  Partneři, zajišťující servis hardware nebo software, jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech v ČPZP pouze s vědomím útvaru pro ICT ČPZP.

- **Ostatní služby**

  Partneři zajišťující ostatní služby (např. úklid, ostrahu atd.) jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech v ČPZP. Při svém pohybu musí dbát bezpečnostních pravidel a pokynů útvaru pro provoz.

e) Dokumentace o provedené práci

Nedílnou součástí dodávky hardware, software nebo služeb tam, kde to má smysl, je projektová a bezpečnostní dokumentace. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v krajním případě odstoupení od smlouvy z důvodu jejího nenaplnění ze strany Partnera (dodavatele).

f) Akceptace

- Každý dodaný software musí být plně a široce otestován, zda splňuje očekávané a smluvně definované parametry a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika. Než bude systém předán do rutinního provozu, musí být formálně akceptován útvarem pro ICT ČPZP.
- Součástí akceptačních testů musí být minimálně test jednotlivých funkcí, zátěžový test a test obnovy IS.
- O provedení akceptačních testů provede Partner záznam a v podobě Akceptačního protokolu jej předloží ČPZP ke schválení.

g) Externí zpracování dat

Externí zpracování dat musí být řádně smluvně zajištěno a průběžně kontrolováno a dokumentováno. Všechna externí zpracování neveřejných informací ČPZP musí být smluvně zajištěna tak, aby byla zachována úroveň ochrany ve všech aspektech informační bezpečnosti podle požadavkům ČPZP a platných právních předpisů.

7. Fyzická bezpečnost

a) Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva ČPZP, zabránit náhodnému i cílenému neautorizovanému přístupu, poškození nebo narušení aktiv v prostorách ČPZP.

b) V ČPZP jsou všechny prostory rozděleny na prostory pro veřejnost a prostory neveřejné. V neveřejných prostorách není dovolen pohyb cizích osob bez doprovodu zaměstnance ČPZP a cizí osoba nesmí být také zanechána bez dozoru v neveřejném prostoru, pokud tyto případy nejsou zajištěny smlouvou.

c) Zaměstnanci Partnera mají povinnost pohybovat se jen v prostorách určených mu oprávněným zaměstnancem ČPZP a nesmí vstupovat do jiných neveřejných prostor ČPZP.

8. Poskytování informací třetím stranám

Zaměstnanci Partnera jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při své práci v ČPZP.

Každé veřejné použití neveřejných informací ČPZP (např. na veřejných vystoupeních, do publikací) musí být schváleno oprávněným zaměstnancem ČPZP (vlastník informace).

9. Řešení kybernetických bezpečnostních událostí a incidentů

a) Kybernetický bezpečnostní incident je každá nestandardní bezpečnostní situace, při které došlo k ohrožení bezpečnosti (dostupnosti, integrity a/nebo důvěrnosti) neveřejných dat ČPZP.

b) Partner musí informovat ČPZP neprodleně poté, jakmile zjistí, že ke kybernetickému bezpečnostnímu incidentu došlo.

c) Každý kybernetický bezpečnostní incident musí být na straně ČPZP zaevidován a vyšetřen, aby mohlo být zabráněno stejným situacím v budoucnu.

d) Zaměstnanci Partnera jsou povinni v rámci svých možností poskytnout součinnost při vyšetřování a odstraňování následků kybernetického bezpečnostního incidentu.

Ohlašovací povinnost partnera vůči ČPZP platí také v případě kybernetických bezpečnostních událostí (nestandardní bezpečnostní situace, při které mohlo dojít, ale nedošlo k ohrožení bezpečnosti neveřejných dat ČPZP).