

## DODATEK Č. 2

(dále jen „dodatek“)

k Rámcové dohodě na dodávku díla a služeb „Technická podpora a strategický rozvoj Core systému VoZP“ uzavřené dne 29. 1. 2019

(dále jen „Rámcová dohoda“)

### **Vojenská zdravotní pojišťovna České republiky**

se sídlem: Drahobejlova 1404/4, 190 03 Praha 9  
IČO: 471 14 975  
zastoupena: Ing. Josefem Diesslem, generálním ředitelem  
zapsána v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl A, vložka 7564

(dále jen „VoZP“)

a

### **Konsorcium KOMIX – Solitea**

Účastník 1:

#### **KOMIX s.r.o.**

se sídlem: Drtinova 467/2a, 150 00 Praha 5  
IČO: 47117087  
jejímž jménem jedná: Ing. Tomáš Rutrle a Ing. Jaromír Babinec, jednatelé  
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 12440

Účastník 2:

#### **Solitea, a.s.**

se sídlem: Drobného 555/49, Ponava, 602 00 Brno  
IČO: 01572377  
jejímž jménem jedná: ■■■■■ ■■■■■ ředitel, zakázkové aplikace, na základě plné moci  
zapsána v obchodním rejstříku vedeném u Krajského soudu v Brně, oddíl B, vložka 7072

(dále jen „Dodavatel“);

(VoZP a Dodavatel dále společně jen jako „smluvní strany“, nebo samostatně jako „smluvní strana“)

## I. Základní ustanovení a prohlášení smluvních stran

1. VoZP dne 29. 1. 2019 uzavřela s Dodavatelem na základě zadávacího řízení Rámcovou dohodu na dodávku díla a služeb, jejímž předmětem je zajištění technické podpory provozu stávajícího Core systému na VoZP.
2. VoZP prohlašuje, že IIS VoZP<sup>1</sup> je významným informačním systémem dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon č. 181/2014 Sb.“), jehož součástí je Core systém, jehož podpora a rozvoj jsou předmětem Rámcové dohody na dodávku díla a služeb Technické podpory a strategického rozvoje Core systému VoZP ze dne 29.1.2019.
3. VoZP prohlašuje, že je správcem významného informačního systému dle zákona č. 181/2014 Sb.
4. VoZP prohlašuje, že je provozovatelem významného informačního systému dle zákona č. 181/2014 Sb. vyjma Portálu zdravotních pojišťoven (dále jen „PZP“).
5. Vzhledem k výše uvedenému je VoZP povinna dle § 4 odst. 4 zákona č. 181/2014 Sb. zohlednit požadavky vyplývající z bezpečnostních opatření při výběru Dodavatele pro informační nebo komunikační systém a tyto požadavky zahrnout do smluvního vztahu s vybraným Dodavatelem.
6. VoZP dále prohlašuje, že Dodavatel je významným Dodavatelem dle zákona č. 181/2014 Sb. a vyhlášky 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška č. 82/2018 Sb.“).
7. VoZP prohlašuje, že má zavedena všechna organizační a technická opatření včetně schválených politik a bezpečnostní dokumentace dle požadavků zákona č. 181/2014 Sb. a navazujících právních předpisů, zejména vyhlášky č. 82/2018 Sb.
8. Dodavatel prohlašuje, že má zavedena všechna relevantní organizační a technická opatření včetně schválených politik a bezpečnostní dokumentace odpovídající plnění požadavků zákona č. 181/2014 Sb. a navazujících právních předpisů týkajících se požadavků na významného Dodavatele. Zavedená relevantní technická a organizační opatření se vztahují výlučně k Seznamu podpůrných aktiv, který je veden v rámci projektové dokumentace a jejichž garantem je Dodavatel.
9. Dodavatel je v souladu se zákonem č. 181/2014 Sb. a vyhláškou č. 82/2018 Sb. povinen informovat VoZP o způsobu řízení rizik, o významné změně ovládaní Dodavatele dle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech, ve znění pozdějších předpisů, nebo o změně vlastnictví zásadních aktiv využívaných Dodavatelem k plnění podle Rámcové dohody.
10. S ohledem na výše uvedené doplňují smluvní strany Rámcovou dohodu o tento článek I. Základní ustanovení a prohlášení smluvních stran a dále o novou Přílohu č. 3 – Bezpečnostní opatření a Přílohu č. 4 – Pravidla informační bezpečnosti, jejichž text je uveden v přílohách tohoto dodatku.

## II. Závěrečná ustanovení

1. Tento dodatek je sepsán ve třech vyhotoveních, z nichž VoZP obdrží jedno vyhotovení a Dodavatel dvě vyhotovení.

<sup>1</sup> IIS VoZP je tvořen: IS VoZP – informačním systémem pro plnění povinností dle zákona č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, který slouží pro výkon činností v oblasti výběru a kontroly pojistného a úhrady zdravotních služeb; RIS2000 – informační systém pro plnění povinností dle zákona č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách, ve znění pozdějších předpisů, pro vedení účetnictví, evidence majetku a fondové hospodaření; EZOP – systém spisové a archivní služby pro plnění povinností dle zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů; Portál zdravotních pojišťoven – internetová aplikace zajišťující uživatelům vyřízení agendy se zdravotními pojišťovnami zapojenými do PZP. PZP je propojen s Core systémem VoZP.

2. Smluvní strany shodně prohlašují, že si tento dodatek před jejím podpisem přečetly a že byl uzavřen po vzájemném projednání podle jejich pravé a svobodné vůle určitě, vážně a srozumitelně, a že se dohodly o celém jeho obsahu, což stvrzují svými podpisy.
3. Právní vztahy vzniklé z tohoto dodatku, stejně jako Rámcová dohoda samotná, se řídí právním řádem České republiky, zejména ustanoveními občanského zákoníku.
4. Závazky stanovené tímto dodatkem k ochraně skutečností tvořících obchodní tajemství a informací uvedených v Příloze č. 1, odst. I. tohoto dodatku, které byly předány přede dnem ukončení účinnosti Rámcové smlouvy, kterou tento dodatek rozšiřuje, platí i nadále po dobu pěti let po ukončení účinnosti Rámcové smlouvy.
5. Tento dodatek nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v Registru smluv. Smluvní strany výslovně souhlasí s tím, že tento dodatek bude uveřejněn v Registru smluv bez jakýchkoliv omezení s přihlédnutím k ochraně osobních údajů.

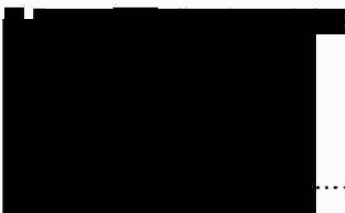
### III. Přílohy

Příloha č. 1 – Bezpečnostní opatření  
Příloha č. 2 – Pravidla informační bezpečnosti

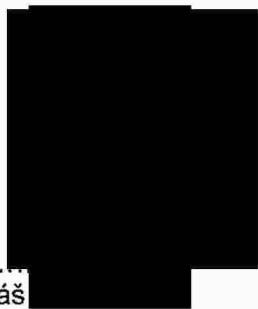
Za VoZP:

Za Dodavatele:


V Praze dne dle el. podpisu

  
Ing. Josef Diessl  
generální ředitel VoZP

24-09-2021

  
Ing. Tomáš  
jednatel  
KOMIX s.r.o.

  
Ing. Jaromír Sabinec

  
Ředitel, zakázkové aplikace, na základě plné moci  
Solitea, a.s.

Příloha č. 1 dodatku – Bezpečnostní opatření

Příloha č. 3 Rámcové dohody – Bezpečnostní opatření

## I. Bezpečnost informací a dat

1. Informace **určené ke zveřejnění** jsou takové, které byly nebo mohou být zveřejněny, nebo se jedná o informace získané prokazatelně z veřejných zdrojů. Přístup k těmto informacím mají všichni zaměstnanci VoZP. Patří sem například:

- referenční informace o projektech, realizovaných u VoZP Dodavatelem, určené k uvádění v seznamu referencí Dodavatele, a to v rozsahu názvu projektu, jména VoZP a firmy Dodavatele a jeho poddodavatelů, rok realizace, informace o použité technologii pro vývoj v rozsahu programátorských nástrojů a prostředí, ve kterém byl projekt vytvářen;
- informace v rozsahu výroční zprávy VoZP;
- informace z propagačních tiskovin a internetových stránek VoZP.

2. Informace **pro vnitřní potřebu** tvoří většinu informací, se kterými se pracuje ve VoZP. Přístup k těmto informacím je řízen podle zásady „potřeba vědět“, tj. jsou poskytovány všem, kdo je potřebují znát ke své práci.

3. **Citlivé informace** jsou představovány omezeným okruhem velmi důvěrných až strategických informací definovaných ve vnitřním předpise VoZP. Přístup k těmto informacím je co nejvíce omezován.

Citlivé informace tvoří obchodní tajemství VoZP, přičemž Dodavatel se zavazuje zachovat o nich mlčenlivost a zajistit, aby mlčenlivost dodržely i osoby jím pověřené prací pro VoZP. Citlivé jsou zejména tyto informace týkající se VoZP:

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

4. Všechny **informace pro vnitřní potřebu a citlivé informace** budou příslušným stupněm důvěrnosti označeny. Neoznačené informace budou automaticky považovány za Informace určené ke zveřejnění. Dodavatel se zavazuje přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému zpřístupnění **informací pro vnitřní potřebu a citlivých informací** třetím osobám.

5. Dodavatel se zavazuje dodržovat Pravidla informační bezpečnosti (dále jen „Pravidla“) uvedená v příloze tohoto dodatku. Tato Pravidla tvoří soubor norem, pravidel a postupů, které vymezují způsob a požadovanou úroveň bezpečnosti, vymezení aktiv a způsob jejich zajištění oprávněnými osobami Dodavatele v rámci vzájemné spolupráce.

6. Dodavatel se zavazuje zajistit seznámení svých pověřených pracovníků a oprávněných osob podílejících se na plnění Rámcové dohody (dále též „zaměstnanci Dodavatele“) s tímto dodatkem, povinnostmi z ní vyplývajícími a provede o tom záznam, který bude na požádání k dispozici zástupci VoZP.
7. Dodavatel je povinen bez odkladu oznámit VoZP změny u oprávněných osob, zejména pak ty, mající dopad na přístupy do systému.
8. Závazek Dodavatele dodržovat veškerá relevantní Pravidla uvedená v Příloze č. 2 tohoto dodatku, jež mají dopad na jeho plnění vzhledem k povaze činností vykonávajících z pozice Dodavatele pro VoZP a platí pro Dodavatele po celou dobu vzájemné spolupráce.
9. V případě, že Dodavatel bude využívat služeb poddodavatele:
  - platí pro něj a pro jeho zaměstnance stejná bezpečnostní pravidla jako pro Dodavatele včetně požadavku mlčenlivosti;
  - úmyslu použít služeb poddodavatele je Dodavatel povinen předem písemně informovat VoZP včetně rozsahu využívaných služeb a je povinen požádat VoZP o povolení takového postupu;
  - Dodavatel nese plnou odpovědnost za činnost svého poddodavatele i v případě porušení povinností vyplývajících z tohoto dodatku;
  - Dodavatel je povinen smluvně zavázat poddodavatele tak, aby pro něj a pro jeho zaměstnance platila stejná bezpečnostní pravidla jako pro Dodavatele, včetně sjednání závazků zachovávat za stejných podmínek mlčenlivost.
10. V případě, že Dodavatel poruší kteroukoliv povinnost dle tohoto dodatku, může VoZP požadovat po Dodavateli zaplacení smluvní pokuty ve výši 50.000,- Kč za každý jednotlivý případ porušení a Dodavatel ji bude v takovém případě povinen zaplatit. Smluvní pokuty dle tohoto dodatku jsou splatné do 30 dnů od doručení oprávněné výzvy k její úhradě spolu s fakturou vystavenou VoZP. Zaplacením jakékoliv smluvní pokuty dle tohoto dodatku není právo VoZP na náhradu škody jakkoliv dotčeno. Oba nároky je VoZP oprávněna uplatňovat samostatně vedle sebe a sjednání smluvní pokuty nemá vliv na odpovědnost za škodu, její uplatňování, výši a právo na její náhradu.
11. Na informace dle odst. 2 a odst. 3 tohoto článku dodatku se neuplatní ustanovení čl. VII a čl. IX odst. 6) Rámcové dohody.

## II. Kontrola a audit

1. Kontrola a audit Dodavatele budou realizovány v souladu s § 16 vyhlášky č. 82/2018 Sb.
2. Dodavatel umožní VoZP v periodě alespoň jednou za 24 měsíců po dobu účinnosti tohoto dodatku provedení zákaznického auditu (kontroly):
  - jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění tohoto dodatku a uloženými či zpracovávanými daty a informacemi VoZP v ICT prostředí Dodavatele; a
  - jehož předmětem bude kontrola stavu plnění bezpečnostních opatření a vyhodnocení rizik dle tohoto dodatku.
3. VoZP má povinnost písemně oznámit Dodavateli provedení auditu, a to nejméně 14 dnů před provedením auditu. Součástí oznámení bude i seznam osob, které jsou pověřeny ze strany VoZP k provedení auditu.
4. VoZP je oprávněna při kontrole bezpečnostních opatření využít třetí stranu. V případě využití třetí strany bude VoZP odpovídat za třetí stranu, jako by kontrolu prováděla sama, včetně odpovědnosti za způsobenou újmu.
5. Dodavatel umožní VoZP kontrolu bezpečnostních opatření provedenou prostředky VoZP nebo třetí

strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky umožňují.

6. Dodavatel se zavazuje poskytnout VoZP bezplatnou součinnost maximálně v rozsahu 2 MD (MD = člověkoden v rozsahu 8 pracovních hodin) při provádění každého zákaznického auditu ze strany VoZP a pro tuto činnost zajistit účast kvalifikovaných pracovníků. V případě požadavku na součinnost ve větším rozsahu, bude tato účtována dle Ceny služeb za 1 člověkoden uvedené v Rámcové dohodě. Dále se Dodavatel zavazuje nedostatky zjištěné:

- a) na základě provedení hodnocení rizik dle tohoto dodatku a/nebo;
- b) v rámci zákaznického auditu dle tohoto dodatku

odstranit ve lhůtě určené oběma smluvními stranami v auditní zprávě.

7. Dodavatel se dále zavazuje:

- a) poskytnout na vyžádání VoZP dokumenty a obdobné vstupy, které budou prokazovat naplnění následných bezpečnostních opatření;
- b) na požádání s VoZP konzultovat kdykoli v průběhu realizace plnění dle Rámcové dohody detailní nastavení bezpečnostních opatření a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;
- c) neprodleně informovat VoZP o všech významných změnách v naplnění bezpečnostních opatření, které nastanou kdykoli v průběhu trvání Rámcové dohody;
- d) bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění bezpečnostních opatření, pokud stávající řešení přestalo být funkční a efektivní;
- e) při výkonu své činnosti včas a prokazatelně upozornit VoZP na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k bezpečnostním opatřením, jejichž následkem může vzniknout újma nebo nesoulad s legislativou.

8. Výstupem v provedeného auditu bude auditní zpráva; s jejími výsledky bude Dodavatel seznámen a může se k nim vyjádřit.

### III. Řízení změn

1. Řízení změn bude realizováno v souladu s ustanovením § 11 vyhlášky č. 82/2018 Sb.

2. VoZP stanovuje následující významné změny

- zásadní změnu technologie HW, SW i infrastruktury;
- zásadní změnu v komunikačním rozhraní;
- zásadní změnu funkčnosti systému;
- upgrade systému;
- implementace nového (části) systému;
- změna vyvolaná změnou organizační struktury mající vliv na změny funkčnosti a změny přístupových oprávnění;
- změnu Dodavatele;
- zpřístupnění systému mimo interní síť organizace (pro Dodavatele nebo jiné externí subjekty);
- změnu v autentizaci uživatelů;
- změnu v řízení přístupu uživatelů;
- změnu rozsahu skupin oprávnění.

3. V případě, že Dodavatel při svém plnění Rámcové dohody identifikuje významnou změnu, je povinen o této skutečnosti bezodkladně informovat VoZP.

### IV. Specifikace podmínek pro řízení kontinuity činností

1. Dodavatel je povinen se s VoZP podílet na aktualizování relevantní dokumentace vztahující se ke specifikaci podmínek pro řízení kontinuity činností (zpracování havarijního plánu, disaster recovery plánů).
2. Dodavatel se zavazuje průběžně konzultovat práce na zhotovení dokumentace s VoZP.

#### **V. Likvidace dat**

1. Likvidace dat bude realizována v souladu se zákonem č. 181/2014 Sb., vyhláškou č. 82/2018 Sb. a dalšími relevantními právními předpisy.

### **1. Obecné povinnosti**

- a) Zaměstnanci Dodavatele jsou povinni chránit aktiva VoZP, která používají ke své práci pro VoZP anebo k nim mají přístup, a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití nebo odcizení. Tato aktiva jsou definována v Seznamu podpůrných aktiv, se kterým se smluvní strany seznámily před uzavřením dodatku.
- b) Povinnosti zaměstnanců Dodavatele při ochraně informací a aktiv VoZP:
  - dodržovat platnou obecně závaznou legislativu, včetně zákona č. 181/2014 Sb.,
  - využívat uživatelské systémy tak, jak bylo stanoveno vlastníkem informací (oprávněný zaměstnanec VoZP),
  - 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 vlastní přístup k informacím VoZP, provedený prostřednictvím přidělených autentizačních údajů,
  - respektovat všechna bezpečnostní opatření a procedury určené vlastníkem informací (oprávněný zaměstnanec VoZP),
  - nerozšiřovat data bez souhlasu VoZP.

### **2. Pracovní stanice, mobilní prostředky**

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

- a) Použití počítače VoZP je povoleno pouze oprávněné osobě Dodavatele.
- b) Zaměstnancům Dodavatele je zakázáno připojovat vlastní počítače a mobilní prostředky včetně mobilních telefonů do vnitřní sítě VoZP bez vědomí bezpečnostního správce za oblast IT VoZP.
- 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 Dodavatele, který má být připojen do vnitřní sítě VoZP, musí mít instalován a spuštěn antivirový program v nejnovější verzi programu i virové databáze.
- e) Zaměstnanec Dodavatele je povinen chránit vybavení VoZP a udržovat bezpečné pracovní prostředí.
- f) V případě ukončení práce se zařízením je zaměstnanec Dodavatele povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

### **3. Využívání internetu**

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



- b) Zaměstnanci Dodavatele mají dovoleno používat internetové připojení do a z vnitřní sítě VoZP pouze za účelem naplnění předmětu Rámcové dohody. Způsob připojení do vnitřní sítě VoZP a jejich autentizace musí být předem dohodnuta s útvarem pro správu systémů ICT. Není-li smluvně dohodnuto jinak, jsou zaměstnanci Dodavatele povinni písemně předem oznámit oprávněnému zaměstnanci VoZP datum a čas přihlášení k vnitřní síti VoZP a následně ukončení práce.

#### **4. Bezpečnost systémů IT**

U vyvíjených nebo dodávaných informačních systémů musí Dodavatel 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 18 měsících.
- V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je nutné, aby aplikace umožnila vynutit změnu inicializačního hesla.
- Heslo (pokud se neautorizuje v AD nebo na úrovni UNIXových serverů), musí být kontrolováno aplikací, zda má alespoň 12 znaků, administrátorská hesla 17 znaků.
- V případě požadavku VoZP 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 VoZP po dodání všech jím požadovaných údajů do evidence technických účtů VoZP. Změny v rozsahu oprávnění podléhají rovněž schválení a povolení manažerem kybernetické bezpečnosti VoZP.
- 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 Core systému

- 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 Core systému.
- Integrita dat musí být zajištěna transakčním zpracováním.
- Data vstupující do Core systému musí být kontrolována (neplatné znaky, rozsah, přetečení, formát, kompletnost, souvislost...), zjištěná chyba musí být srozumitelně popsána.

Pokud VoZP 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 Dodavateli

- Předáváním dat Dodavateli se rozumí předávání informací z VoZP smluvnímu Dodavateli na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty VoZP, CD, DVD, pevné disky počítačů a jiné nebo zasílané e-mailem, datovou schránkou, na datové úložiště Dodavatele nebo jiným elektronickým způsobem. Dodavatel je povinen nakládat s předanými daty v souladu s vyhláškou 82/2018 Sb..
- Předávání dat musí probíhat bezpečným způsobem a musí být v rámci předání proveden popis struktury dat v rámci předávacího protokolu.
- Uchovávání a případné zpracování dat u Dodavatele 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 Dodavatel
- Dodavatel je povinen dbát na bezpečnost likvidace již nepotřebných dat, případně médií s daty. Pro likvidaci médií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možné běžně dostupnými prostředky obnovit (skartovačka, SW skartovačka).
- Dodavatel si nesmí sám stahovat žádná data z Core systému VoZP; vytváření souborů musí provést oprávněný zaměstnanec VoZP a teprve takto vytvořená data smí být (na smluvním základě) předána Dodavateli. Toto opatření neplatí pro soubory vytvářené na žádost oprávněných zaměstnanců VoZP z Core systému, které Dodavatel 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 Dodavateli

- Vývoj software musí probíhat na vývojovém prostředí u Dodavatele, který je povinen je udržovat po celou dobu trvání smluvního vztahu souvisejícího s vývojem software. Poté musí být software otestován v testovacím prostředí VoZP, které je oddělené od produkčního prostředí. Vývoj musí probíhat:
  - legálním software,
  - na testovacích datech, která nejsou převzata z provozní databáze,
  - tak, že instalace SW do provozního prostředí může být provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení.
- Dodavatel 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.
- Přístup Dodavatele do Core systému VoZP (testovacího i provozního prostředí) může být použit pouze pro činnosti směřující k naplnění předmětu Rámcové dohody.
- Pro realizaci údržby systémů platí tytéž bezpečnostní požadavky, jako v případě jejich vývoje.

#### **b) Dodávka software**

- 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) Dodávka hardware**

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

#### **d) Dodávka služeb**

- Dodávka služeb musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Způsob předání závisí na konkrétní službě a na Rámcové dohodě (smlouvě) s Dodavatelem (Dodavatelem).
- Součástí dodávky služeb musí být jednoznačná deklarace požadované služby a musí být nastaveny její kvalitativní parametry.
- Je-li součástí dodávky služeb údržba Core systému nebo aplikací VoZP a je-li tato údržba prováděna zaměstnanci Dodavatele, nelze ji zahájit bez souhlasu oprávněného zaměstnance VO rozvoje a podpory provozního systému – kontaktní osoba dle Rámcové dohody.

#### **e) Servis hardware a software**

Dodavatelé, zajišťující servis hardware nebo software, jsou oprávněni pohybovat se na neveřejných místech ve VoZP pouze s vědomím vedoucího oddělení rozvoje a podpory provozního systému.

#### f) Ostatní služby

Dodavatelé zajišťující ostatní služby (např. úklid, ostrahu atd.) jsou oprávněni pohybovat se na neveřejných místech ve VoZP. Při svém pohybu musí dbát bezpečnostních pravidel a pokynů útvaru pro provoz.

#### g) 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 Rámcové dohody z důvodu jejího nenaplnění ze strany Dodavatele.

#### h) 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 vedoucím oddělení rozvoje a podpory provozního systému.
- O provedení akceptačních testů provede Dodavatel záznam a v podobě akceptačního protokolu jej předloží VoZP ke schválení.

#### i) Externí zpracování dat

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

### 7. Fyzická bezpečnost

- a) Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva VoZP, zabránit náhodnému i cílenému neautorizovanému přístupu, poškození nebo narušení aktiv v prostorách VoZP.
- b) Ve VoZP jsou všechny prostory rozděleny na prostory pro veřejnost a prostory neveřejné. V neveřejných prostorách není dovolen pohyb cizích osob bez doprovodu zaměstnance VoZP a cizí osoba nesmí být také zanechána bez dozoru v neveřejném prostoru, pokud tyto případy nejsou zajištěny Rámcovou dohodou.
- c) Zaměstnanci Dodavatele mají povinnost pohybovat se jen v prostorách určených mu oprávněným zaměstnancem VoZP a nesmí vstupovat do jiných neveřejných prostor VoZP.

### 8. Poskytování informací třetím stranám

Zaměstnanci Dodavatele jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při své práci ve VoZP.

Každé veřejné použití neveřejných informací VoZP (např. na veřejných vystoupeních, do publikací) musí být schváleno oprávněným zaměstnancem VoZP (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 VoZP.
- b) Dodavatel musí informovat vedoucího oddělení systémové podpory VoZP neprodleně poté, jakmile zjistí, že ke kybernetickému bezpečnostnímu incidentu došlo.

- c) Každý kybernetický bezpečnostní incident musí být na straně VoZP zaevidován a vyšetřen, aby mohlo být zabráněno stejným situacím v budoucnu.
- d) Zaměstnanci Dodavatele jsou povinni v rámci svých možností poskytnout součinnost při vyšetřování a odstraňování následků kybernetického bezpečnostního incidentu.
- e) Ohlašovací povinnost Dodavatele vůči VoZP platí také v případě kybernetických bezpečnostních událostí (nestandardní bezpečnostní situace, při které mohlo dojít, ale nedošlo k ohrožení bezpečnosti neveřejných dat VoZP).