Smlouva č. CTU/2024_0055
na dodávku loadbalanceru a aplikačního firewallu

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku,
ve znění pozdějších předpisů (dále jen „smlouva“)

mezi těmito smluvními stranami:

1. Česká republika – Český telekomunikační úřad

se sídlem:	Sokolovská 58/219, Praha 9
adresa pro doručování	pošt. přihrádka 02, 225 02 Praha 025
bankovní spojení:	Česká národní banka, pobočka Praha
Číslo účtu:	725001/0710
IČO:	70106975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
jejímž jménem jedná:	Ing. Marek Ebert, předseda Rady Českého telekomunikačního úřadu

(dále jen „Objednatel“ nebo „ČTÚ“) na straně jedné

a

2. ICZ a.s.

se sídlem:	Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
zastoupen:	[redacted], na základě plné moci
IČO:	251 45 444
DIČ:	CZ699000372
bankovní spojení:	UniCredit Bank Czech Republic and Slovakia, a.s.
číslo účtu:	2109164825/2700

zapsaná v obchodním rejstříku vedeným Městským soudem v Praze, oddíl B, vložka 4840

(dále jen „Dodavatel“) na straně druhé,

společně označované také jako „strany“ nebo jednotlivě též jako „strana“.

Článek I.
Účel a předmět smlouvy

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě proběhne dodávka a instalace loadbalanceru a aplikačního firewallu, to vše v návaznosti na výsledky zadávacího řízení na veřejnou zakázku s názvem „Dodávka loadbalanceru a aplikačního firewallu“.
2. Objednatel má v plánu rozšířit stávající infrastrukturu o zařízení typu ADC (Application delivery controller), který zajistí vysokou dostupnost aplikací prostřednictvím loadbalancingu a zároveň zvýší jejich úroveň ochrany pomocí aplikačního firewallu (WAF).
3. Předmětem smlouvy je na straně jedné závazek Dodavatele dodat Objednateli 2 kusy appliance (webový aplikační firewall [WAF] a loadbalancer) zapojených ve vysoké dostupnosti (tzv. HA), a to včetně dodávky veškerých potřebných provozních licencí, instalace, konfigurace, integrace a zajištění záručního servisu a podpory plnění po dobu 60 měsíců ode dne akceptace dodávky. Podrobná specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy. Na straně druhé je předmětem smlouvy závazek Objednatele za řádně a včas poskytnuté plnění zaplatit Dodavateli sjednanou cenu.

Článek II.
Místo a čas plnění

1. Místem plnění je sídlo Objednatele.
2. Dodání zařízení včetně instalace, konfigurace a školení nejpozději do 46 pracovních dnů ode dne účinnosti smlouvy. Podpora dodaného zařízení po dobu 60 měsíců ode dne akceptace plnění podle první věty.

Článek III.
Cena a platební podmínky

1. Celková cena za plnění dle čl. I odst. 3 této smlouvy a dle cenové kalkulace uvedené v příloze č. 2 této smlouvy, činí 7.929.536 Kč bez DPH. Celková cena bude hrazena postupně takto:
   a) cena za plnění dle bodu 1 a 3 přílohy č. 2 této smlouvy (Cenová kalkulace) za dodávku, implementaci a zaškolení činí 2.531.232 Kč bez DPH,
   b) cena za servisní podporu po dobu 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD (man-day) dle bodu 4 přílohy č. 2 této smlouvy (Cenová kalkulace) činí 2.550.000 Kč bez DPH, tj. 17.000 Kč bez DPH/1 MD (man-day),
   c) cena za SW moduly zajišťující všechny funkce, SW pro centrální management včetně příslušných licencí dle bodu 2 přílohy č. 2 této smlouvy (Cenová kalkulace) činí 1.230.344 Kč bez DPH,
   d) cena za 5 let RMA podpory 10x5xNBD pro 2 kusy appliance zapojených ve vysoké dostupnosti dle bodu 5 přílohy č. 2 této smlouvy (Cenová kalkulace) činí 1.617.960 Kč bez DPH.
2. Ceny jsou stanoveny v měně CZK jako pevné a lze je měnit pouze při změně sazby DPH. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni zdanitelného plnění. Ceny zahrnují veškeré náklady Dodavatele nezbytné pro plnění smlouvy.
3. Cena za plnění bude hrazena následujícím způsobem:
   a) cena dle odstavce 1 písm. a), c) a d) tohoto článku bude uhrazena po převzetí řádného plnění Objednatelem na základě podepsání příslušného akceptačního protokolu, který bude přílohou příslušné faktury vystavené Dodavatele,
   b) cena dle odstavce 1 písm. b) tohoto článku bude hrazena jako součin skutečného rozsahu poskytnutých služeb (MD) a jednotkové ceny dle odstavce 1 písm. b) tohoto článku. Podkladem pro stanovení skutečné hodnoty poskytnuté služby je podepsaný výkaz práce (viz odstavec 5 tohoto článku), jehož kopie bude přílohou daňového dokladu – faktury (dále jen „faktura“).
4. Splatnost faktury je sjednána na 21 dnů ode dne doručení Objednateli. V případě faktury doručené Objednateli mezi 20. prosincem a 10. lednem je taková faktura splatná nejdříve následujícího 1. února. Platební povinnosti Objednatele plynoucí z této smlouvy jsou splněny dnem odepsání příslušné částky ve prospěch účtu Dodavatele. Úhrada bude provedena bezhotovostním převodem z účtu Objednatele ve prospěch účtu Dodavatele.
5. Všechny faktury musí mít náležitosti podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 OZ, a musí obsahovat číslo této smlouvy. Přílohou faktury musí být příslušný akceptační protokol (pro plnění dle odstavce 1 písm. a), c) a/nebo d) tohoto článku smlouvy), potažmo podepsaného výkazu práce servisní podpory (pro plnění dle odstavce 1 písm. b) tohoto článku smlouvy) potvrzující poskytnutí služeb v daném období či rozsahu. Objednatel je oprávněn fakturu Dodavateli vrátit bez zbytečného odkladu po zjištění, že obsahuje údaje nesprávné nebo chybí-li některá ze zákonem či touto smlouvou požadovaných náležitostí, a to před uplynutím

doby splatnosti, aniž by došlo k prodlení s jeho úhradou. Nová doba splatnosti počíná běžet ode dne vystavení bezvadné faktury.

Článek IV.
Ostatní podmínky plnění smlouvy, práva a povinnosti smluvních stran

1. Dodavatel zajistí provedení následujících činností v rozsahu minimálně:
   a) zpracování projektové dokumentace, plány a harmonogram postupu projektu,
   b) přípravné práce a příprava HW včetně validace umístění technologií do cílového místa – místo v racku, napájení, konektivita atd.,
   c) fyzická instalace zařízení na dohodnuté místo za předem dohodnutých podmínek,
   d) základní konfigurace interface, routingu a návazných síťových služeb,
   e) instalace SW včetně potřebných licencí,
   f) rozšířená konfigurace jednotlivých komponent a nasazení příslušných politik web aplikačního firewallu ve spolupráci se Objednatelem,
   g) v případě potřeby implementace příslušných HW/SW update od výrobce,
   h) dokumentace skutečného provedení,
   i) provedení akceptačních testů,
   j) plnění dle této smlouvy bude Dodavatel Objednateli poskytovat nejpozději v termínech uvedených v příloze č. 4 této smlouvy. Ve stanovených termínech musí být plnění Dodavatele poskytnuto řádně, tj. musí být poskytnuto v takové kvalitě, která již nebude vyžadovat jakékoliv následné odstraňování vad či nedostatků. Dodavatel se zavazuje nejméně 1 pracovní den předem písemně uvědomit kontaktní osobu objednatele uvedenou v čl. XI odst. 5 písm. a) této smlouvy o předpokládaném termínu předání, instalace či konfigurace plnění nebo jeho části. Objednatel do 3 pracovních dnů ode dne předání plnění Dodavatelem potvrdí převzetí řádného plnění podepsáním příslušného akceptačního protokolu nebo ve stejné lhůtě v rámci akceptačního protokolu vytkne Dodavateli zjištěné vady. Způsob a termín jejich odstranění bude navržen Dodavatelem s tím, že určení termínu pro odstranění vad a nedostatků nemá vliv na povinnost Dodavatele dodat řádné plnění nejpozději do termínu ve smyslu čl. II odst. 2 této smlouvy; odstranění zjištěných vad a nedostatků bude opětovně ověřeno a výsledek bude zaznamenán formou samostatného zápisu v akceptačním protokolu).
2. Další podmínky plnění smlouvy:
   a) veškeré nabízené plnění musí být plně kompatibilní se současnou infrastrukturou Objednatele,
   b) součástí veškerého nabízeného plnění musí být i všechny potřebné licence (HW/SW), jež budou zahrnuty ve sjednané ceně,
   c) veškerý dodaný HW musí být nový, nepoužitý a určený výrobcem pro český trh,
   d) SW licence musí být bez jakýchkoli právních vad, Objednatel nepřipouští produkty třetích stran (tzv. OEM kompatibilní),
   e) Dodavatel musí být certifikovaný partner výrobce pro Českou republiku.
3. Dodavatel je dále po celou dobu trvání této smlouvy zajistit:
   a) plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak předpisů pracovněprávních, předpisů v oblasti zaměstnanosti, a dále

oblasti bezpečnosti a ochrany zdraví při práci, a to vůči všem osobám, které se budou podílet na plnění této smlouvy,

b) dodržování zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů,

c) řádné a včasné plnění finančních závazků vůči svým případným poddodavatelům.

Plnění uvedených povinností zajistí poskytovatel i u svých případných poddodavatelů.

4. Objednatel je povinen zajistit:

   a) aby zařízení a software byly užívány v souladu se specifikacemi a návody výrobce,

   b) poskytnou Dodavateli v přiměřené lhůtě nezbytně nutnou součinnost při provádění činností servisu a údržby.

5. V případě úmyslu Dodavatele či jeho poddodavatele zahájit podnikání ve smyslu § 8 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, v poštovních službách ve smyslu § 17 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, v oblasti služeb dodávání balíků ve smyslu čl. 2 bodu 3) nařízení Evropského parlamentu a Rady (EU) 2018/644 o službách přeshraničního dodávání balíků, ani nejsou provozovatelé rozhlasového a/nebo televizního vysílání podle § 3 odst. 1 a § 2 odst. 1 písm. c), e) a f) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů, je Dodavatel povinen předem písemně informovat Objednatele.

Článek V.
Vyšší moc a okolnosti vylučující odpovědnost

1. Smluvní strany nebudou odpovědné za částečné nebo úplné neplnění smluvních závazků následkem okolností vylučujících odpovědnost v případech tzv. vyšší moci.

2. Výraz vyšší moc znamená a zahrnuje zejména: přírodní katastrofu, požár, záplavy, zemětřesení a dále povstání, stávky, pracovní boje jakéhokoliv druhu nebo terorismus, které mají přímou souvislost a brání plnění povinností ze smlouvy a plnění povinností nelze zajistit jinak nebo je nahradit, nehody, pád letadla včetně nehod, kterým se nedalo vyhnout v souvislosti s plněním této smlouvy včetně přijetí zákona nebo mimořádného rozhodnutí přísl. úřadu v souvislosti se zásahem vyšší moci, pokud příčiny a události mají vliv na plnění povinností stran ze smlouvy a plnění povinností vyplývajících ze smlouvy nelze zajistit jinak.

3. Vyskytne-li se působení překážky, s níž jsou spojeny účinky vylučující odpovědnost, lhůty ke splnění smluvních závazků se prodlouží o dobu trvání takové překážky. Smluvní strana, která je postižena takovou překážkou, je však povinna okamžitě, písemně, uvědomit druhou smluvní stranu o této skutečnosti, o začátku trvání této překážky a předpokládané době jejího trvání.

Článek VI.
Ochrana informací

1. Objednatel a Dodavatel se zavazují, že obchodní, technické, jakož i netechnické informace, které mají nebo by mohly mít potenciální hodnotu, a které jim byly svěřeny smluvním partnerem, nezpřístupní třetím osobám bez předchozího písemného souhlasu druhé smluvní strany a nepoužijí tyto informace ani pro jiné účely než pro plnění svých závazků podle podmínek této smlouvy. Za důvěrnou informaci se pokládá vždy taková informace, která je takto kteroukoliv smluvní stranou kdykoliv označena. To však neplatí

v případě, že by se stala tato informace, k níž se zavazují k povinnosti mlčenlivosti či k povinnosti zachovat důvěrnost informace, podle tohoto ustanovení smlouvy, obecně známou či dostupnou. To se nevztahuje na výstupy z plnění podle této smlouvy. Toto ustanovení platí i po dobu 5 let od ukončení účinnosti této smlouvy, nemá však vliv na případné povinnosti Objednatele vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

2. Dodavatel se výslovně zavazuje, že informace získané v souvislosti s plněním předmětu smlouvy nezneužije k jinému účelu než výlučně k plnění této smlouvy.

3. Dodavatel se zavazuje, že neposkytne bez souhlasu Objednatele žádné informace třetím stranám ohledně plnění této smlouvy, včetně informací o konfiguraci SW a HW komponentech datového centra a systému dohledu, které mohl Dodavatel zjistit při implementaci a konfiguraci, nebo jiných prvků, které nejsou součástí plnění této smlouvy. Zároveň se Dodavatel zavazuje, že bude uchovávat citlivé informace ohledně plnění této smlouvy, jako jsou logy, konfigurace a topologie jen po nezbytně nutnou dobu, potřebnou pro řádné a efektivní plnění této smlouvy. Veškeré takové informace je také Dodavatel povinen chránit proti odcizení, či zneužití.

4. Dodavatel se zavazuje, že všechny povinnosti stanovené mu v tomto článku ve stejné podobě uplatní vůči svým zaměstnancům, resp. tyto povinnosti přenese v rámci svých smluvních vztahů na případné poddodavatele.

Článek VII.
Kybernetická bezpečnost

1. Ve vztahu k předmětu plnění Smluvní strany prohlašují, že:

   a) plnění smlouvy bude probíhat na aktivech představujících soubor technických a programových prostředků, jež jsou významnou a nedílnou součástí více informačních systémů naplňujících definici významného informačního systému (VIS) dle § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“);

   b) Objednatel je v pozici správce těchto významných informačních systémů dle § 3 písm. e) ZoKB;

   c) Dodavatel vystupuje jako významný Dodavatel ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 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 jen „VoKB“).

2. Dodavatel je povinen v rozsahu plnění dle této smlouvy naplnit všechny kybernetické požadavky a dodržovat tyto po celou dobu trvání této smlouvy (pokud příloha č. 3 této smlouvy nestanoví jinou dobu dodržování kybernetického požadavku).

3. Dodavatel se současně zavazuje poskytovat plnění dle této smlouvy v souladu se ZoKB, VoKB a přílohou č. 3 této smlouvy a s opatřeními, která na jeho základě přijmou k tomu oprávněné orgány veřejné moci, a to včetně opatření, která mají pouze doporučující charakter.

4. Objednatel spadá pod dikci ZoKB a dodané řešení tedy nesmí být v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů a informačních systémů základních služeb.

5. Dodané řešení musí proto splňovat všechny související požadavky a nařízení a musí umožňovat Objednateli řádné plnění povinností podle ZoKB. V souladu s výše uvedeným je Objednatel povinen podle § 5 VoKB, provádět analýzu rizik a identifikovaná rizika řídit.

Současně je Objednatel povinen se zabývat všemi hrozbami, které prostřednictvím varování vydává NÚKIB, těmito hrozbami se dále zabývat a zohlednit je v analýze rizik.

6. Dodavatel je povinen po celou dobu plnění zajistit dostatečnou bezpečnost jím provozovaných aktiv a souvisejících dat v souladu s platnými obecně závaznými právními předpisy, zejména ZoKB, VoKB a dalšími závaznými akty vydanými ze strany orgánů veřejné moci (NÚKIB či jiného správního orgánu).
7. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZoKB a VoKB. Jestliže Dodavatel při plnění této smlouvy zjistí rozpor postupů Objednatele se ZoKB nebo VoKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.
8. Smluvní strany v průběhu plnění smlouvy spolu vzájemně komunikují za účelem dosažení požadované úrovně bezpečnosti. V případě ohrožení anebo porušení kybernetické bezpečnosti, zejména v případě výskytu kybernetické bezpečností události anebo incidentu, jsou smluvní strany povinny ihned po zjištění takových skutečností hlásit jejich výskyt druhé smluvní straně a společně podnikat potřebné kroky k zajištění obnovení požadované úrovně bezpečnosti.
9. Dle požadavků Objednatele poskytne Dodavatel potřebnou součinnost pro účely testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

Článek VIII.
Salvátorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

Článek IX.
Trvání a ukončení smlouvy

1. Tato smlouva může být ukončena písemnou dohodou obou smluvních stran.
2. Smluvní strany jsou dále oprávněny od této smlouvy odstoupit v případech stanovených občanským zákoníkem nebo touto smlouvou.
3. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným nebo neodstranitelným způsobem své povinnosti vyplývající z této smlouvy.
4. Za podstatné porušení smluvních povinností Objednatelem se podle této smlouvy považuje prodlení Objednatele s uhrazením ceny plnění o více než 30 dnů.
5. Za podstatné porušení smlouvy Dodavatelem se považuje:
   a) nedodržení povinnosti Dodavatele podle čl. VI nebo VII této smlouvy,
   b) neprovádění plnění podle smlouvy řádně a včas v souladu s pokyny Objednatele nebo v souladu s příslušnými právními předpisy, a to ani v dodatečně stanovené lhůtě 10 pracovních dnů,
   c) neodstranění vad ve sjednané lhůtě, a to ani v dodatečně stanovené lhůtě 10 pracovních dnů,

d) dodatečně zjištěný fakt, že údaje uvedené Dodavatelem v rámci předchozího zadávacího řízení nebyly pravdivé.

6. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají okamžikem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně, není-li stanoveno jinak.

7. Objednatel je dále oprávněn odstoupit od smlouvy, pokud:

   a) bylo vydáno pravomocné rozhodnutí o úpadku Dodavatele nebo bylo zahájeno insolvenční řízení proti Dodavateli na jeho návrh, nebo v případě, že soud pravomocně rozhodl o zrušení Dodavatele a nařídil jeho likvidaci, nebo Dodavatel přijme rozhodnutí o vstupu do likvidace; nebo

   b) dojde k významné změně kontroly nad Dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění smlouvy a tato změna bude Objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZoKB.

8. V případě, že tato smlouva zanikne odstoupením, má poskytovatel právo na poměrnou úhradu za část díla již provedeného podle této smlouvy. Toto ustanovení neplatí v případě, že dojde k odstoupení od smlouvy z důvodů na straně Dodavatele.

9. Smluvní strany se dohodly, že v případě ukončení této smlouvy z důvodu uplynutí doby jejího trvání nebo z důvodu jejího ukončení některou ze smluvních stran, a v případě zájmu Objednatele o přechod poskytování všech či některých služeb na třetí osobu, a současně jestliže Objednatel předloží Dodavateli detailní plán přechodu služeb na nového Dodavatele je Dodavatel povinen poskytnout Objednateli a novému Dodavateli součinnost, a to v nezbytně nutném rozsahu a podle plánu přechodu služeb. Dodavatel se zavazuje Objednateli poskytnout rovněž nezbytnou součinnost pro účely vytvoření relevantního plánu přechodu služeb.

10. Smluvní strany se dohodly, že součinnost podle odstavce 10 tohoto článku smlouvy bude Dodavatelem poskytována tak, aby byla minimalizována rizika s přechodem poskytování služeb, a aby byla zajištěna kontinuita poskytování služeb.

Článek X.
Smluvní pokuty, odpovědnost za škody

1. V případě prodlení Objednatele s uhrazením řádně fakturovaných částek podle podmínek stanovených touto smlouvou má Dodavatel nárok na úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení, nejvýše však v součtu do výše 5 % z fakturované částky.

2. V případě prodlení Dodavatele s plněním této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení.

3. V případě porušení své povinnosti ve věci ochrany informací stanovené podle čl. VI této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 50.000 Kč za každý jednotlivý případ porušení takové povinnosti.

4. V případě porušení své povinnosti ve věci ochrany kybernetické bezpečnosti stanovené podle čl. VII této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 50.000 Kč za každý jednotlivý případ porušení takové povinnosti.

5. Úrok z prodlení a smluvní pokuta jsou splatné ve lhůtě 10 dnů ode dne doručení písemné výzvy k jejich úhradě.

6. Objednatel nemá právo uplatnit smluvní pokutu, jestliže Dodavatel prokáže, že Objednatel neposkytl Dodavateli spolupůsobení nutné k tomu, aby Dodavatel mohl splnit svůj závazek.
7. Objednatel je oprávněn započítat případné smluvní pokuty oproti ceně za plnění této smlouvy.
8. Zaplacením smluvní pokuty podle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci.

Článek XI.
Závěrečná ustanovení

1. Právní vztahy touto smlouvou výslovně neupravené nebo z ní vyplývající se řídí příslušnými ustanoveními občanského zákoníku, příp. zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
2. Smluvní strany bezvýhradně souhlasí s uveřejněním této smlouvy, případných dodatků k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv, ve znění pozdějších předpisů. Uveřejnění zajistí Objednatel.
3. Změny a doplnění této smlouvy (s výjimkou změny kontaktních osob dle odstavce 5 tohoto článku smlouvy) lze činit pouze se souhlasem obou smluvních stran písemnou formou, a to prostřednictvím vzestupně číslovaných dodatků, jinak jsou neplatné.
4. Jakékoli oznámení ve smyslu této smlouvy od druhé smluvní strany musí být učiněno písemně.
5. Veškerá komunikace mezi smluvními stranami ve věcech této smlouvy bude probíhat prostřednictvím kontaktních (pověřených) osob, jimiž v dané věci jsou:

   a) na straně Objednatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			
[redacted]			

   b) na straně poskytovatele:

Jméno	E-mail	Telefon	Mobil
[redacted] – ve věcech obchodních	[redacted]		
[redacted] – ve věcech technických	[redacted]		

6. Smlouva vzniká dnem podpisu oprávněnými zástupci smluvních stran a nabývá účinnosti dnem zveřejnění smlouvy podle zákona o registru smluv.
7. Tato smlouva se vztahuje na právní nástupce smluvních stran.
8. Nedílnou součástí této smlouvy jsou:

   Příloha č. 1 – Specifikace předmětu plnění

   Příloha č. 2 – Cenová kalkulace

   Příloha č. 3 – Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Příloha č. 4 – Harmonogram dílčích etap.

9. Tato smlouva je vyhotovena v elektronické podobě, kdy bude příslušný dokument opatřen elektronickými podpisy zástupců obou smluvních stran.
10. Obě smluvní strany prohlašují, že se s textem této smlouvy seznámily, obsahu porozuměly, souhlasí s ním a na důkaz toho připojují své podpisy.

V Praze dne dle el. podpisu

Objednatel:

Ing. Marek Ebert

Digitálně podepsal Ing. Marek Ebert
Datum: 2024.10.14 11:05:18 +02'00'

.....

Ing. Marek Ebert
předseda Rady
Českého telekomunikačního úřadu

V Praze dne dle el. podpisu

Dodavatel:

[redacted]

Digitálně podepsal [redacted]
Datum: 2024.10.01 14:08:42 +02'00'

.....

[redacted]
na základě plné moci
ICZ a.s.

Specifikace předmětu plnění

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje požadavek (dodavatel doplní ANO/NE)
Platforma	
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.	ANO
Každé zařízení podporuje připojení 4 x 10/1 Gbps metalické RJ45 porty a alespoň 4x 25/10 Gbps optické SFP+ porty.	ANO
Datová propustnost zařízení alespoň 23 Gbps či více na L4 a 15 Gbps či více na L7	ANO, 25Gbps na L4 a 17Gbps na L7
Minimální propustnost HTTP požadavků: 1,5 mil. za sekundu	ANO, 1,8 mil. za sekundu
Minimální propustnost L7 požadavků: 800 tis. za sekundu	ANO, 875 tis. za sekundu
Počet současných L4 spojení: min. 17 mil.	ANO, 19 mil.
Offload – HW komprese – propustnost min. 10 Gbps	ANO, 15 Gbps
SSL akcelerace v HW	ANO
Počet SSL transakcí za sekundu min. 10 tis. (při použití 2K klíče)	ANO, 15 tis.
Počet SSL transakcí za sekundu min. 8 tis. (při použití ECDSA P-256 klíče)	ANO, 10 tis.
Celkový šifrovací výkon min. 8 Gbps	ANO, 10 Gbps
Nezávislé rozhraní pro management	ANO
Redundantní napájení	ANO
K dispozici jako autonomní box nebo ve formě šasi	ANO
Management: sériový port, GUI, příkazový řádek, iLO	ANO
Operační systém	
Full-Proxy architektura (plné oddělení klientského a serverového spojení)	ANO
Podpora IPv4	ANO
Plná podpora IPv6, IPv4/IPv6 gateway	ANO
Podpora externích šifrovacích karet pro SSL (HSM)	ANO
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)	ANO
Podpora Spanning Tree Protokolu (STP)	ANO
Možnost přidat vlastní funkce pomocí skriptování	ANO
Podpora HTTP/2	ANO
Podpora IPSec IKEv2	ANO
Podpora konfigurace a správu zařízení přes REST API	ANO
Podpora SNMP (v1/v2c/v3)	ANO
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall	ANO

Možnost dodatečně aktivovat další funkcionalitu zakoupením licencí: - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall - IP reputační databáze	
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu	ANO
Podpora Active-Active a Active-Pasive módu	ANO
Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou	ANO
Web aplikační Firewall	
Integrace s nástrojem na detekci zranitelností webových aplikací	ANO
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	ANO
Možnost doprogramovat si filtrovaci pravidla pro aplikace	ANO
Automatická korelace zranitelností do jednoho bezpečnostního incidentu	ANO
Ochrana AJAX a JSON aplikací	ANO
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	ANO
Podpora Captcha metody	ANO
Automatické odlišení skutečných uživatelů od robotů	ANO
Integrovaný XML firewall	ANO
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…	ANO
Automatické nahrávání a aplikování nových signatur	ANO
Podpora pozitivního a negativního bezpečnostního modelu	ANO
Blokování útočníků na základě geolokace	ANO
Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP	ANO
Ochrana SMTP a FTP na aplikační úrovni	ANO
Podpora SSL (šifrování a dešifrování)	ANO
Podpora různých typů reportů – PCI, geolokační reporty	ANO
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	ANO
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications, Wordpress a Microsoft SharePoint	ANO
Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)	ANO
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: • Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning	ANO
Podpora aplikačního firewallu ve virtuálních kontextech	ANO
Podpora aplikačního firewallu v cloudu	ANO

Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	ANO
Ochrana proti Session Highjacking pomocí Browser Fingerprintingu	ANO
Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávací URL apod.)	ANO
Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace	ANO
Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI	ANO
Podpora a filtrování WebSocket provozu	ANO
Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice	ANO
Možnost ochrany proti Credential Stuffing útokům	ANO
Možnost doplnění modulu pro přístup k online databázi nejnovějších útoků	ANO
Možnost rozšířit DoS ochranu proti přetížení napojením na čističku provozu přes cloud.	ANO
Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování	ANO
Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů	ANO
Možnost napojení na CDN	ANO
Schopnost detekovat probíhající útok konkrétní útočné skupiny s cílem zneužít známé zranitelnosti CVE, aktualizace definicí těchto útoků a vytvoření signatur ve WAF v reálném čase.	ANO
Řízení provozu	
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	ANO
Podpora REST API	ANO
Autentizace klientů přes LDAP/Radius	ANO
Povolení/zakázání ICMP a ARP pro VIP	ANO
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení	ANO
Podpora rozvažování zátěže alespoň pro následující metody: - Round Robin - Least Connections - Ratio - Ration Least Connections - Weighted Least Connections	ANO
Podpora filtrace paketů	ANO
Podpora ToS, QoS (marking/preservation/mimic)	ANO
Podpora SNMP (v1/v2c/v3)	ANO
Podpora rozvažování zátěže založené na poměrech (ratio) s perzistencí	ANO
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	ANO
Podpora práce s 4096-bit klíči	ANO
Současná podpora ECC a RSA certifikátu	ANO
Podpora Camellia šifer SSL	ANO

Podpora pro TLS 1.2 a TLS 1.3	ANO
Podpora ECC a DH šifer v HW	ANO
Podpora SSL Forward proxy	ANO
Stavové filtrované paketů (ACL)	ANO
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb	ANO
Podpora monitorování služeb na základě výkonu konkrétních hostů	ANO
TCP optimalizace síťových toků	ANO
Komprese a cachování specifických služeb	ANO
Podpora zrcadlení SSL relací a SSL spojení v HA clusteru	ANO
Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)	ANO
Řízení přístupu k aplikacím	
Podpora autentizace: - HTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SerurID - OAM - Tacacs+ - Local DB	ANO
Import uživatelských identit IF-MAP	ANO
Podpora externích přihlašovacích stránek aplikací	ANO
Podpora vysoké dostupnosti AAA serverů	ANO
OTP (generování a ověření)	ANO
Podpora CAPTCHA	ANO
SAML: - SP role - IdP role	ANO
Modifikace SAML atributů	ANO
Podpora SAML 2.0	ANO
Podpora pro vytvoření Single Sign-On (SSO): - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML	ANO
Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy)	ANO
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)	ANO

Podpora Kerberos ticketing	ANO
PCoIP proxy	ANO
RDP proxy	ANO
Patching (maskování) webových portálů: - HTML - JavaScript - CSS - Java	ANO
Podpora uživatelského portálu při publikaci služeb v režimu jednoho URL	ANO
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv	ANO
Podpora L7 ACL	ANO
Podpora importu dynamických ACL z AAA	ANO
Podpora dynamického řízení přístupu	ANO
Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele	ANO
Síťová SSL VPN DTLS	ANO
Podpora publikace aplikací formou portálu	ANO
Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta	ANO
Podpora OS: - Windows - MAC - Linux - iOS - Android	ANO
Nativní podpora MDM	ANO
Podpora Oauth 2.0	ANO
Kontrola nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů aj. parametrů na straně klienta	ANO
Filtrování URL	ANO
URL kategorizační databáze	ANO
Podpora pro vytváření flexibilní a granulární přístupové politky	ANO
GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace	ANO
Podpora Microsoft ActiveSync a Outlook Anywhere s klientskou NTLM autentizací	ANO
Zjednodušené řízení přístupové politiky pro VDI technologie Citrix XenApp a XenDesktop	ANO
Podpora „Step-up“ autentizace	ANO

Příloha č. 2 smlouvy

CENOVÁ KALKULACE

	Požadované plnění	Obchodní označení produktu	Cena celkem v Kč bez DPH	Cena celkem v Kč vč. DPH
1.	Dodání 2 kusů appliance zapojených ve vysoké dostupnosti	F5-BIG-AWF-R2800 F5-ADD-BIG-APMR28XXB F5-UPG-AC-I2XXX F5-UPG-SFP+-R	2 242 232,00	2 713 100,72
2.	SW moduly zajišťující požadované funkce, SW pro centrální management včetně příslušných licencí s platbou za 5 let provozu	F5-SBS-BIG-TC-1-3YR F5-SBS-BIG-IPI-3-3YR F5-SBS-BIG-TC-1-1YR F5-SBS-BIG-IPI-3-1YR	1 230 344,00	1 488 716,24
3.	Instalace, konfigurace, zaškolení	Instalace, konfigurace, zaškolení	289 000,00	349 690,00
4.	Servisní podpora na 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD	Servisní podpora na 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD (man-day)	2 550 000,00	3 085 500,00
5.	5 let RMA podpory 10x5xNBD pro 2 kusy appliance zapojených ve vysoké dostupnosti	F5-SVC-BIG-STD-L1-3 F5-SVC-BIG-RMA-2 F5-SVC-BIG-STD-L1-3	1 617 960,00	1 957 731,60
Celkem			**7 929 536,00**	**9 594 738,56**

Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Vymezení pojmů

Pro potřeby této přílohy smlouvy jsou použity následující zkratky a pojmy:

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

VoKB – vyhláška 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) v platném znění

Kybernetické požadavky – kybernetickými požadavky se rozumí všechny bezpečnostní požadavky ve smyslu ZoKB a VoKB,

Produkční prostředí – produkčním prostředím se rozumí prostředí běžně přístupné uživatelům IS ČTÚ v ostrém provozu,

Testovací prostředí – prostředí určené k provádění testů, vzdělávání uživatelů apod, a to v podobě, nastavení a rozsahu umožňujícím účinně zkoumat funkcionality testovacích verzí IS ČTÚ,

Prostředí objednatele – fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku objednatele anebo logický perimetr definovaný hraničními síťovými prvky ve správě nebo majetku objednatele,

Osoba na straně dodavatele – fyzická osoba podílející se na poskytování předmětu plnění a mající pracovněprávní či obdobný smluvní vztah s dodavatelem nebo jeho poddodavateli,

Osobní údaje – každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat,

Zpracování osobních údajů – jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

1. ÚVODNÍ USTANOVENÍ

1.1 Z důvodu nutnosti plnění povinností stanovených objednateli jakožto povinné osobě ve smyslu VoKB je dodavatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této přílohy č. 9 smlouvy. Účelem této přílohy č. 9 smlouvy tak je dodržet povinnost objednatele dle § 4 odst. 4 ZoKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s dodavatelem.

2. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

2.1 Dodavatel je povinen se v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění dle smlouvy.

b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy objednateli zpřístupnit.

d) Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

2.2 Dodavatel je dále povinen dodržovat bezpečnostní politiku objednatele, byl-li s ní prokazatelně seznámen.

3. ŘÍZENÍ AKTIV

3.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, hardware prvky – infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení apod.), a tato aktiva strukturovaně popsat a objednateli předložit následně na vyžádání, a to po celou dobu trvání smlouvy.

4. ŘÍZENÍ RIZIK

4.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle smlouvy.

b) V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro objednatele nebo změn spravovaných aktiv) vytvořit a bude-li to objednatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:

   i) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;

   ii) Identifikaci a hodnocení rizik s vazbou na předmět plnění;

   iii) Realizovaná bezpečnostní opatření;

   iv) Nepokrytá bezpečnostní rizika a návrh opatření;

   v) Vyhodnocení bezpečnostních událostí a incidentů;

   vi) Aktuální stav souladu dodavatele s kybernetickými požadavky včetně přehledu kybernetických požadavků, které:

   - nebyly aplikovány, včetně odůvodnění, a
   - byly aplikovány, včetně způsobu plnění.

5. ORGANIZAČNÍ BEZPEČNOST

5.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Jmenovat nejpozději do 30 dnů po uzavření smlouvy odpovědnou kontaktní osobu/y pro potřeby zajištění plnění kybernetických požadavků a související komunikace mezi smluvními stranami (dále jen „kontaktní osoba pro kybernetickou bezpečnost“). Kontaktní osobu/y pro kybernetickou bezpečnost sdělí dodavatel písemně objednateli v téže lhůtě.

b) Využívat pro poskytování předmětu plnění dle smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních předpisů objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle smlouvy a stanovit bezpečnostní role těchto oprávněných osob s jasně definovanými odpovědnostmi a pravomocemi.

6. ŘÍZENÍ DODAVATELŮ

6.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Využívá-li při poskytování předmětu plnění dle smlouvy subdodavatele, zajistit v obdobném rozsahu dodržování kybernetických požadavků rovněž ve smluvních vztazích se svými subdodavateli.

b) Dodržovat podmínky při zpracování osobních údajů pro zapojení každého dalšího dodavatele.

7. BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 9 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit, aby kontaktní osoba pro kybernetickou bezpečnost nejpozději do 60 dnů od uzavření smlouvy potvrdila písemně objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle smlouvy za dodavatele byly prokazatelně seznámeny s těmito kybernetickými požadavky a příslušnými ustanoveními interních předpisů objednatele.

b) Dodržovat příslušná ustanovení interních předpisů objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje:

i) školení pracovníků dodavatele zajištěné objednatelem

ii) protokolární či elektronické předání příslušných předpisů nebo

iii) objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy, jejichž konkrétní jmenovitý seznam bude dodavateli – současně s poskytnutím přístupu – protokolárně předán.

c) Při provádění dohledu nad předmětem plnění dle smlouvy, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění dle smlouvy.

d) Zajistit, aby osoby podílející se na poskytování plnění objednateli v prostředí/nebo s prostředky objednatele:

i) pro uložení a sdíleni dat a informací objednatele využívaly pouze k tomu schválené prostředky (aktiva);

ii) neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující dobré jméno objednatele;

iii) nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;

iv) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

v) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani ke zdrojům jiných subjektů;

vi) nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků objednatele, a to ani v případě, kdy jim byl prostředek objednatele svěřen do správy;

vii) nepodílely se s prostředky objednatele na šíření spamu ani škodlivého softwaru,

a to i tehdy, pokud jsou prostředky objednatele používány mimo jeho prostředí.

7.2 Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům objednatele je na straně objednatele zpracování osobních údajů pověřených osob dodavatele, které se podílejí na poskytování plnění dle smlouvy. Pokud nebude objednateli umožněno osobní údaje pověřených osob dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům objednatele.

7.3 Dodavatel je dále povinen:

a) Prohlubovat znalostí osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

b) Stanovit práva a povinnosti osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

8. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 10 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění dle smlouvy.

b) Na vyžádání ve lhůtě, která nebude kratší než 10 pracovních dnů, poskytnout objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

c) Zajistit, že pro poskytování předmětu plnění dle smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou legislativou, a to především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů).

8.2 Dodavatel je dále povinen provést a zabezpečit dodržování následujících opatření:

a) Implementaci procesů pro řízení ICT (tj. řízení incidentů, řízení změn, řízení životního cyklu systémů apod.).

b) Zavedení postupů pro ochranu proti škodlivému kódu včetně řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle smlouvy.

c) Zavedení pravidel a postupů pro ochranu informací a dat.

d) Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv a pracovní postupy pro řešení mimořádných stavů.

e) Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění dle smlouvy.

9. ŘÍZENÍ ZMĚN

9.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 11 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Přiměřeně reagovat na změny v oblasti kybernetické bezpečnosti na straně objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

b) Aktivně spolupracovat při testování významné změny v oblasti kybernetické bezpečnosti na straně objednatele.

10. ŘÍZENÍ PŘÍSTUPU

10.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele.

b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu dodavatele. V opačném případě musí dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit objednateli kdykoli v průběhu trvání účinnosti této smlouvy a tři měsíce po jejím ukončení, ve lhůtě, která nebude kratší než 6 pracovních dnů.

c) Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou, 1 rok, 1 měsíc apod).

d) Zajistit, aby osoby podílející se na poskytování předmětu plnění dle smlouvy a mající přístup k informačním aktivům objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

e) Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně dodavatele, které přistupují do prostředí objednatele.

10.2 Dodavatel bere na vědomí, že oprávnění přístupu k systémům ICT objednatele je možné povolit pouze fyzické identitě zaměstnance dodavatele/subdodavatele, a to na základě příslušného požadavku dodavatele.

10.3 Dodavatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.

10.4 Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet objednatelem zablokován a řešen jako bezpečnostní incident a dále mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům objednatele).

11. AKVIZICE, VÝVOJ A ÚDRŽBA

11.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, pokud jsou předmětem plnění dle smlouvy či jeho součástí.

b) Není-li smlouvou stanoveno jinak, předat při ukončení smlouvy objednateli kompletní provozní a bezpečnostní dokumentaci předmětu plnění dle smlouvy. Ta musí být předána minimálně v následujícím rozsahu:

i) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

ii) dokumentaci obsahující popis autorizačního konceptu a oprávnění;

iii) dokumentaci obsahující instalační a konfigurační postupy;

Výše uvedenou dokumentaci dodavatel předá objednateli v přiměřené lhůtě, nejpozději pak dle předchozí dohody smluvních stran.

11.2 V případě, že předmět plnění dle smlouvy zahrnuje částečně i vývoj softwaru, je dodavatel povinen:

a) Dodržovat a implementovat obecně uznávané „nejlepší praktiky“ pro bezpečný vývoj softwaru. Základním pravidlem zde je myslet na bezpečnost softwaru ve všech jeho vývojových fázích.

b) Na vyžádání alespoň 6 pracovních dnů předem umožnit objednateli audit prováděného nebo provedeného plnění a na písemnou žádost objednatele předložit ve stanovené lhůtě vyvíjený zdrojový kód na provedení tzv. codereview, a to především za účelem ověření skutečnosti, zda dodavatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito bezpečnostními požadavky.

c) Poskytovat objednateli v termínech stanovených objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru (nejdříve však od zahájení testovacího provozu) či kdykoli po jeho předání.

d) Pokud je součástí plnění dle smlouvy i instalace operačního systému, případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v testovacím prostředí či produkčním prostředí objednatele.

e) Zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat objednatelem.

f) Zajistit, že v rámci poskytovaného plnění bude dodávaný software

i) v souladu s bezpečnostními politikami a standardy objednatele;

ii) otestován na soulad s bezpečnostními politikami objednatele, pokud byl s takovými bezpečnostními politikami prokazatelně seznámen.

g) Instalovat software pouze na základě předem schválených migračních postupů objednatelem.

h) Předat zdrojový kód objednateli bezpečnou formou zajišťující jeho integritu.

i) Zajistit řízení verzí zdrojového kódu, jeho zálohování a jeho uložení mimo produkční prostředí.

12. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

12.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 14 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy:

a) Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.

b) Bez zbytečného odkladu hlásit objednateli všechny kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím kontaktní osoby pro kybernetickou bezpečnost.

c) Vyhodnocovat informace o kybernetických bezpečnostních incidentech a uchovávat je pro budoucí použití, a to s ohledem na požadavky použitelné platné a účinné legislativy.

d) V případě vzniku kybernetické bezpečnostní události a následného zvládání a vyhodnocování možného kybernetického bezpečnostního incidentu a/nebo v případě podezření na možný kybernetický bezpečnostní incident poskytnout objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či podezřelém jednání osob na straně dodavatele.

e) Spolupracovat při analýze příčin kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Zhotovitel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

f) Po dohodě s objednatelem realizovat bez zbytečného odkladu opatření požadovaná objednatelem ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení pokračování kybernetického bezpečnostního incidentu, nejpozději pak v termínech prokazatelně stanovených objednatelem.

12.2 Dodavatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků, jehož příčina je na straně dodavatele, nebude posuzován jako okolnost vylučující odpovědnost dodavatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy dodavateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti dodavatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

13. ŘÍZENÍ KONTINUITY ČINNOSTÍ

13.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění dle smlouvy.

b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu těchto aktiv zajistit dle sjednané SLA.

14. KONTROLA A AUDIT

14.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy poskytnout adekvátní součinnost při výkonu kontroly objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZoKB.

14.2 Dodavatel umožní objednateli alespoň jednou ročně po dobu účinnosti smlouvy provedení auditu kybernetické bezpečnosti (dále jen audit) u dodavatele a jeho případných subdodavatelů:

a) jehož rozsah bude ohraničen v rámci ICT prostředků dodavatele používaných pro potřeby plnění smlouvy a uloženými či zpracovávanými daty a informacemi objednatele v ICT prostředí dodavatele a

b) jehož předmětem bude naplnění kybernetických požadavků a vyhodnocení rizik dle bodu 4 této přílohy smlouvy.

14.3 Objednatel je oprávněn při provedení auditu využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za případnou způsobenou újmu.

14.4 Dodavatel umožní objednateli audit provedený prostředky objednatele nebo třetí strany, a to v lokalitě dodavatele i vzdáleně, pokud to technické prostředky dodavatele umožňují.

14.5 Dodavatel je povinen nedostatky zjištěné:

a) na základě provedení hodnocení rizik dle bodu 4 této přílohy smlouvy, nebo

b) v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této přílohy smlouvy

odstranit ve lhůtě určené v písemném oznámení objednatele, která nebude kratší než 20 pracovních dnů. Nestanoví-li objednatel lhůtu v písemném oznámení, zavazují se smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 60 dnů.

14.6 Dodavatel je dále povinen:

a) Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění kybernetických požadavků.

b) Na požádání s objednatelem konzultovat kdykoli v průběhu realizace plnění dle smlouvy detailní nastavení bezpečnostních opatření k naplnění kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

c) Neprodleně informovat objednatele o všech významných změnách v naplnění kybernetických požadavků, které nastanou kdykoli v průběhu trvání smlouvy.

d) Bezodkladně a s vyvinutím maximálního úsilí zajistit náhradní způsob naplnění kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.

e) Při výkonu své činnosti včas a prokazatelně upozornit objednatele na případnou zřejmou nevhodnost jeho příkazů či doporučení, vztahujících se ke kybernetickým požadavkům, jejichž následkem může vzniknout případná újma anebo nesoulad s příslušnými zákony nebo jinými obecně závaznými právními předpisy.

15. TECHNICKÁ OPATŘENÍ

15.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Dodržovat příslušné interní předpisy objednatele, s nimiž byl prokazatelně seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěna aktiva systémů ICT, anebo datové nosiče.

b) V rozsahu předmětu plnění dle smlouvy zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv objednatele, pokud s ní byl dodavatel seznámen.

c) Realizovat bezpečnostní opatření pro odstranění nebo blokování komunikačních spojení, která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.

d) Realizovat přístupy z mobilních zařízení k aktivům v produkčním i testovacím prostředí objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).

e) Připojovat do produkčního prostředí objednatele pouze ta síťová zařízení (switch, wifi router apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně objednatele.

f) Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pakliže tento je součástí sjednaného rozsahu předmětu plnění dle smlouvy a je současně ve správě dodavatele.

g) Na aktiva objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí objednatele následující typy nástrojů, pokud vysloveně nejsou součástí předmětu plnění dle smlouvy:

   i) Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

   ii) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

   iii) Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

   iv) Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do počítačového systému.

   v) Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje stávající bezpečnostní opatření v prostředí Objednatele.

h) Připojovat do prostředí objednatele pouze zařízení ICT, která splňují následující požadavky:

   i) jsou příslušným způsobem zabezpečena a chráněna proti malware a jinému škodlivému softwaru – minimálně instalovaný a aktivní antivir s aktuální definiční sadou, pokud možno instalované veškeré doporučené bezpečnostní záplaty pro OS a používaný SW, správně nakonfigurovaný a aktivní firewall;

   ii) způsob jejich připojení je definován v příslušné provozní nebo projektové dokumentaci nebo je v souladu s příslušnými interními předpisy objednatele.

i) Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

j) Na vyžádání poskytnout objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění dle smlouvy, a to po celou dobu trvání smlouvy a pak po dobu 2 let po jejím ukončení.

k) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

l) Pro veškeré on-line transakce realizované prostřednictvím webových technologií implementovat doporučené a schválené TLS/SSL certifikáty s cílem zajistit důvěrnost a integritu komunikace protistran.

m) Veškeré neveřejné informace poskytnuté objednatelem a ukládané na mobilní zařízení anebo přenosná paměťová média, která jsou ve správě dodavatele, chránit vhodným šifrováním a proti neautorizovanému přístupu.

15.2 Dodavatel bere na vědomí, že v případě, kdy technické spojení ze strany dodavatele narušuje bezpečný chod ostatních služeb objednatele, může být toto spojení ze strany objednatele bez předchozího upozornění ihned ukončeno.

15.3 Dodavatel bere na vědomí, že veškeré jeho aktivity a jeho plnění realizované v prostředí objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění smlouvy a v souladu s příslušnými interními dokumenty objednatele.

Harmonogram dílčích etap

Pořadí aktivit	Název aktivity	Nejzazší termín plnění
1	Nabytí účinnosti smlouvy	T0
2	Zpracování projektové dokumentace	T0 + 23 PD
3	Přípravné práce a příprava HW, fyzická instalace zařízení	T0 + 35 PD
4	Základní konfigurace včetně instalace SW a potřebných licencí, v případě potřeby implementace příslušných HW/SW update od výrobce	T0 + 35 PD
5	Rozšířená konfigurace jednotlivých komponent a nasazení příslušných politik web aplikačního firewallu ve spolupráci s Objednatelem	T0 + 38 PD
6	Dokumentace skutečného provedení, zaškolení obsluhy	T0 + 42 PD
7	Ukončení akceptačního řízení	T0 + 46 PD

PD – pracovní den

PLNÁ MOC

ICZ a.s., IČ: 25145444, se sídlem Na hřebenech II 1718/10, Nusle, 140 00 Praha 4, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 4840 (dále jen „**Zmocnitel**“)

tímto uděluje plnou moc

[redacted] dat. nar. [redacted], trvale bytem [redacted], [redacted] (dále jen „**Zmocněnec**“),

aby za Zmocnitele činil veškerá právní jednání a jiné úkony **v obchodních vztazích** (včetně vztahů týkajících se veřejných zakázek ve smyslu ustanovení zákona č. 134/2016 Sb., zákon o zadávání veřejných zakázek, ve znění pozdějších předpisů), v nichž cena předmětu plnění vyjádřená peněžní částkou nepřesáhne částku **13.000.000,-Kč** (slovy třináct miliónů korun českých) s tím, že půjde-li o opakující se plnění, je základem pro výpočet tohoto limitu součet ceny všech opakujících se plnění bez DPH.

Tato plná moc nezahrnuje oprávnění Zmocněnce nakupovat a zcizovat cenné papíry, obchodní podíly, uzavírat smlouvy o prodeji části nebo celého podniku, zprostředkovatelské smlouvy, smlouvy o sdružení, smlouvy příkazní či mandátní, smlouvy nájemní, podnájemní či leasingové, přijímat a poskytovat úvěry, sjednávat odstupné, podepisovat směnky, zcizovat nemovitosti a zatěžovat je právními závazky. Zmocněnec dále není na základě této plné moci oprávněn zavazovat Zmocnitele jakýmikoli ručitelskými závazky.

Tato plná moc nahrazuje jakoukoli plnou moc dříve udělenou Zmocněnci Zmocnitelem ohledně výše uvedeného předmětu plné moci.

Tato plná moc se uděluje na dobu neurčitou.

V Praze dne 4 / 12 /2023

[redacted]

Mgr. Dan Rosendorf
předseda představenstva
ICZ a.s.

[redacted]

Zmocnění přijímám v plném rozsahu.

[redacted]

[redacted]

Doložka z konverze dokumentu do elektronické podoby – na žádost

Dokument [redacted] vznikl převedením listinného dokumentu do elektronického dokumentu pod pořadovým číslem [redacted] Vzniklý dokument obsahem odpovídá vstupnímu dokumentu. Počet stran dokumentu: **1**

Vstup neobsahoval viditelný prvek, který nelze plně přenést na výstup.

Konverzi provedl subjekt: [redacted]

Pracoviště: [redacted]

Datum vyhotovení: **04.12.2023**

Jméno a příjmení osoby, která konverzi provedla: [redacted]

Poznámka:

Konverzí dokumentu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy. Kontrolu doložky lze provést v centrální evidenci doložek na adrese https://www.czechpoint.cz/overovacidolozky .

[redacted]