Smlouva o vzdáleném přístupu

uzavřená dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

I. Smluvní strany

Masarykův onkologický ústav
se sídlem Žlutý kopec 7, 656 53 Brno
zastoupený prof. MUDr. Markem Svobodou, Ph.D., ředitelem
IČO: 00209805, DIČ: CZ00209805
(dále jen „MOÚ“)

a

AURA Medical s.r.o.
se sídlem K Verneráku 1193/4, 148 00 Praha 4
zastoupená Andreou Krejčí, jednatelkou společnosti
IČO: 65412559, DIČ: CZ65412559
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka 44675
(dále jen „společnost“)

na základě vítězství společnosti v zadávacím řízení k veřejné zakázce **Multidetektorový CT přístroj** (evidenční číslo: Z2022-001156) zadávané MOÚ a v souvislosti s kupní a servisní smlouvou uzavřenou k této veřejné zakázce uzavírají v souladu s § 2079 a násl. a § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), tuto smlouvu o vzdáleném přístupu (dále jen „smlouva“).

II. Předmět smlouvy

1. MOÚ se za účelem plnění povinností vyplývajících z výše uvedené veřejné zakázky a kupní a servisní smlouvy zavazuje poskytnout společnosti za níže uvedených podmínek vzdálený přístup k aplikacím a zařízením datové sítě MOÚ, blíže určeným v příloze č. 1 smlouvy, a to prostřednictvím sítě Internet (dále jen „vzdálený přístup“) přes VPN koncentrátor MOÚ.
2. Podmínky smlouvy se uplatní i na jakékoliv budoucí smluvní vztahy uzavřené mezi týmiž smluvními stranami, pro které je nutné zřídit vzdálený přístup společnosti.

III. Práva a povinnosti

1. MOÚ se za účelem plnění povinností vyplývajících z uvedených smluv zavazuje poskytnout společnosti za níže uvedených podmínek vzdálený přístup k aplikacím a zařízením datové sítě MOÚ, blíže určeným v příloze č. 1 smlouvy (dále jen „vzdálený přístup“) přes VPN koncentrátor MOÚ.
2. Společnost se zavazuje, že nebude připojovat, vzdáleně ovládat či jinak ovlivňovat další stanice, služby či jiné součásti informačních technologií MOÚ, ani se o toto pokoušet.
3. Společnost se zavazuje, že neumožní vzdálené připojení třetí straně, nedohodnou-li se v důvodných případech smluvní strany jinak.
4. Společnost se zavazuje využívat vzdáleného přístupu zřízeného na základě smlouvy k plnění svých zákonných a smluvních povinností vyplývajících z kupní a servisní smlouvy k veřejné zakázce.
5. Jestliže bude mít společnost podezření na možnost narušení bezpečnosti informačních technologií MOÚ v rámci vzdáleného připojení, je povinna o této skutečnosti bez zbytečného odkladu informovat odpovědnou osobu MOÚ.
6. Společnost se zavazuje, že bude udržovat auditní záznam o časech používání vzdáleného přístupu s identifikací osob a obsahu prováděných prací. V případě potřeby auditní záznamy bezodkladně zpřístupní MOÚ.
7. Společnost se zavazuje předcházet vzniku škody na majetku MOÚ a učiní pro to ze své strany všechna nutná opatření. Pokud by přesto měla činnost společnosti negativní důsledek na chod spravovaného systému, je společnost povinna ihned o této skutečnosti informovat odpovědnou osobu MOÚ, aby se přikročilo k nápravným opatřením a minimalizoval se dopad na MOÚ.
8. Společnost se zavazuje neměnit nastavení vzdáleného přístupu, které provedl pověřený zaměstnanec Úseku informačních technologií MOÚ (dále jen „ÚsIT“), a neprovádět jakékoliv jiné neoprávněné zásahy do datové sítě MOÚ. Pokud by v souvislosti s plněním smluvních povinností bylo nutné takovou změnu udělat, je to možné pouze po předchozí dohodě s pověřeným zaměstnancem ÚsIT.
9. O chystaných pracích (např. nasazení nových verzí, změnách nastavení, importu/exportu dat apod.) je společnost povinna informovat zaměstnance odpovědného za provoz instalovaných zdravotnických prostředků MOÚ e-mailem minimálně 24 hodin předem. Bez prokazatelného písemného souhlasu (e-mailem) s termínem provádění prací ze strany MOÚ společnost práce nezahájí. Společnost informuje MOÚ stejným způsobem i o výsledku a ukončení těchto prací.

10. Společnost se zavazuje neprodleně po uzavření smlouvy seznámit zaměstnance společnosti s bezpečnostními pravidly vzdáleného přístupu uvedenými v příloze č. 2 smlouvy. Porušení těchto bezpečnostních pravidel zaměstnancem společnosti představuje podstatné porušení smlouvy.
11. Společnost odpovídá za jakékoli neoprávněné zásahy svých zaměstnanců (i zaměstnanců společností pracujících pomocí VPN přístupu v rámci poskytování podpory/servisu vyplývající z příslušné kupní nebo servisní smlouvy) do vnitřní sítě MOÚ. Odpovědnost společnosti se vztahuje i na bývalé zaměstnance, kteří by zneužili znalosti získané v době trvání zaměstnaneckého poměru ve Společnosti.
12. MOÚ má právo kdykoli jednostranně ukončit možnost vzdáleného přístupu.

IV. Ochrana osobních údajů

1. Smluvní strany se zavazují nakládat s osobními údaji zaměstnanců společnosti v souladu s právními předpisy, zejména podle nařízení Evropského parlamentu a Rady (EU) 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení o ochraně osobních údajů"), a poskytovat si součinnost při plnění povinností vyplývajících z těchto právních předpisů v rámci zpracování osobních údajů zaměstnanců společnosti.
2. MOÚ se zavazuje zajistit vhodným způsobem bezpečnostní, technická a organizační opatření dle článku 32 obecného nařízení o ochraně osobních údajů tak, aby v souvislosti se shora uvedenou činností nemohlo na jeho straně dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Smluvní strany se zavazují, že si bez zbytečného odkladu sdělí jakékoliv podezření z nedostatečného zabezpečení osobních údajů zaměstnance společnosti nebo z porušení tohoto zabezpečení.
3. Smluvní strany se dohodly, že informační povinnost MOÚ podle čl. 14 obecného nařízení o ochraně osobních údajů bude splněna prostřednictvím společnosti. Společnost tímto potvrzuje, že nejpozději v okamžiku poskytnutí osobních údajů MOÚ předala zaměstnanci společnosti informace dle čl. 14 obecného nařízení o ochraně osobních údajů (tj. informace o kategorii dotčených osobních údajů, rozsahu, účelu, právním důvodu a době zpracování, právech zaměstnance společnosti, totožnosti MOÚ a kontaktech na MOÚ jmenovaného pověřence pro ochranu osobních údajů atd.), které jsou dostupné na webových stránkách MOÚ v sekci Ochrana osobních údajů a především pak na webové stránce Zpracování osobních údajů – Oddělení informatiky a informovala jej, že bližší informace o podmínkách zpracování jeho osobních údajů lze nalézt na webových stránkách MOÚ.

V. Ochrana důvěrných informací

1. Společnost se zavazuje zachovávat mlčenlivost o veškerých informacích, se kterými se seznámí nebo je získá v informačních systémech MOÚ (dále jen „důvěrné informace").
2. Společnost je oprávněna šířit jakékoliv informace o předmětu plnění smlouvy či o spolupráci s MOÚ (web, publikace, tisk apod.) pouze s předchozím písemným souhlasem MOÚ.
3. Společnost je povinna zajistit, aby nedošlo k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí či zpřístupnění přenášených, uložených nebo jinak zpracovávaných důvěrných informací jakékoliv třetí osobě bez výslovného souhlasu MOÚ. Za tímto účelem je společnost povinna přijmout příslušná bezpečnostně technická opatření. Přijetí bezpečnostně technických opatření se společnost zavazuje na žádost MOÚ doložit, a to ve lhůtě 3 pracovních dní od doručení žádosti MOÚ, nedohodnou-li se smluvní strany jinak.
4. Společnost je povinna bez zbytečného odkladu (po zjištění náhodného nebo protiprávního zničení, ztráty, změny nebo neoprávněného poskytnutí či zpřístupnění přenášených, uložených nebo jinak zpracovávaných důvěrných informací), tuto skutečnost oznámit MOÚ na kontaktní údaje uvedené v odst. 9 přílohy č. 2 smlouvy. Společnost je povinna neprodleně přijmout vhodná bezpečnostně technická opatření, aby pokračování závadného stavu zabránila nebo zmírnila případné následky. Případné přijetí těchto bezpečnostně technických opatření se společnost zavazuje doložit za podmínek uvedených výše.
5. Společnost se zavazuje poučit o povinnosti zachovávat mlčenlivost o důvěrných informacích své zaměstnance, zástupce, jakož i spolupracující třetí strany.

VI. Odpovědnost

1. Pokud společnost (včetně zaměstnanců společnosti, osoby jednající na základě pověření společnosti či na základě smluvního vztahu se společností) poruší povinnost vyplývající z čl. III. až V. smlouvy, zejména:
    - povinnost neprovádět zásahy do nastavení vzdáleného přístupu,
    - povinnost zachovávat mlčenlivost o důvěrných informacích,
    - povinnost přijmout a doložit bezpečnostně technická opatření,
    - povinnost seznámit zaměstnance s bezpečnostními pravidly
    - oznamovací povinnosti uvedené ve smlouvě,

je povinna zaplatit MOÚ smluvní pokutu ve výši 50 000 Kč za každé jednotlivé porušení smluvní povinnosti. Ujednáním o smluvní pokutě není nijak dotčeno právo MOÚ na náhradu škody v plné výši.

2. MOÚ neodpovídá za nepřetržitou dostupnost vzdáleného přístupu.

VII. Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami a uzavírá se na dobu neurčitou.
2. Obě strany mohou smlouvu vypovědět bez uvedení důvodu. Smlouva v takovém případě zanikne následujícího dne po doručení písemné výpovědi druhé straně.
3. Ustanovení čl. V. smlouvy o ochraně důvěrných informací zůstávají v platnosti a účinnosti i po ukončení smlouvy, nedohodnou-li se smluvní strany výslovně jinak.
4. Smlouva je vyhotovena ve dvou stejnopisech, z nichž jeden obdrží MOÚ a jeden společnost.
5. Nedílnou součást smlouvy tvoří příloha č. 1 – Seznam aktiv, pro která je vzdálený přístup zřízen a příloha č. 2 – Bezpečnostní pravidla přístupu do datové sítě MOÚ.
6. Veškerá další ujednání mohou být učiněna jen formou číslovaných písemných dodatků, podepsaných oběma smluvními stranami.
7. Smluvní strany prohlašují, že si smlouvu před jejím podpisem přečetly a že s jejím obsahem souhlasí, na důkaz výše uvedeného připojují své podpisy.

V Brně dne

prof. MUDr. Marek Svoboda, Ph.D.
Digitálně podepsal prof. MUDr. Marek Svoboda, Ph.D.
Datum: 2022.03.24 18:03:32 +01'00'

prof. MUDr. Marek Svoboda, Ph.D.
ředitel Masarykova onkologického ústavu

V Praze dne

Andrea Krejčí
Digitálně podepsal Andrea Krejčí
Datum: 2022.03.24 14:34:43 +01'00'

Andrea Krejčí
jednatelka společnosti AURA Medical s.r.o.

Příloha č. 1

Seznam aktiv, pro která je vzdálený přístup zřízen

zařízení, přístroj
CT Aquilion PRIME SP
Multimodalitní serverový portál VITREA Enterprise Single Server

Příloha č. 2

Bezpečnostní pravidla přístupu do datové sítě MOÚ

1. Zaměstnanec společnosti je oprávněn se připojovat do datové sítě MOÚ za účelem poskytování servisu nebo technické podpory zařízení nebo aplikace, pro která byl vzdálený přístup zřízen.
2. Zaměstnanec společnosti je oprávněn přistupovat pouze do těch částí informačních systémů MOÚ (dále jen „IS MOÚ"), pro které byla udělena přístupová oprávnění.
3. Zaměstnanec společnosti je povinen chránit přístupové údaje před jejich ztrátou, zneužitím, odcizením nebo neoprávněným přístupem jiné osoby. Případnou ztrátu, zneužití, odcizení anebo neoprávněný přístup jiné osoby k přístupovým údajům je zaměstnanec společnosti povinen bez zbytečného odkladu oznámit společnosti, která zajistí informovanost odpovědné osoby MOÚ.
4. Zaměstnanec společnosti bere na vědomí, že je povinen zachovávat mlčenlivost o veškerých informacích, se kterými se seznámí nebo je získá v IS MOÚ (dále jen „důvěrné informace"), jakož i o všech přijatých bezpečnostně technických a organizačních opatřeních, jejichž zveřejnění by mohlo ohrozit zabezpečení důvěrných informací.
5. Při práci na zařízení připojeném v datové síti MOÚ nesmí zaměstnanec společnosti umožnit přístup do spravovaných systémů žádné třetí osobě.
6. Při práci v prostorách MOÚ musí zaměstnanec společnosti rovněž dodržovat tyto zásady:
   - v předstihu informovat zaměstnance Oddělení informatiky MOÚ o účelu a termínu práce,
   - nepřipojovat do datové sítě MOÚ vlastní zařízení.
7. Zaměstnanec společnosti je povinen chránit aktiva MOÚ a dle svých nejlepších odborných znalostí a schopností bránit porušení jejich zabezpečení, které by mohlo způsobit jejich poškození, zneužití, neoprávněné zpřístupnění, změnu nebo odcizení. Aktivem se rozumí jakákoliv komponenta nebo část celkového systému, která má pro MOÚ určitou hodnotu, kterou je nutné chránit, zejména se jedná o informační aktiva (datové a databázové soubory) a softwarová aktiva. V případě zjištění nebo nabytí podezření na porušení zabezpečení aktiv MOÚ (např. jejich odcizení, kopírování, změna, zneužití, ztráta anebo neoprávněný přístup) je zaměstnanec společnosti povinen oznámit tuto skutečnost bez zbytečného odkladu MOÚ.
8. Zaměstnanec společnosti je povinen vyvinout maximální úsilí pro odvrácení vzniku bezpečnostního incidentu. Bezpečnostním incidentem se rozumí nežádoucí bezpečnostní událost, která může způsobit narušení bezpečnosti informací v IS MOÚ nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítě MOÚ. Případná podezření nebo potvrzení vzniku bezpečnostního incidentu je zaměstnanec společnosti povinen bez zbytečného odkladu oznámit MOÚ. Zaměstnanec společnosti je povinen poskytnout maximální součinnost při analýze bezpečnostního incidentu a implementovat případná nápravná opatření stanovená MOÚ.
9. Veškerá výše uvedená oznámení určená MOÚ budou Společností zasílána na e-mail vedouci-IT@mou.cz.