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. Janem Žaloudíkem, CSc., ředitelem
IČO: 00209805, DIČ: CZ00209805
(dále jen „MOÚ")

a

BACH systems s. r. o.
se sídlem Holická 31/N, č. p. 1097, Olomouc, PSČ 772 00
IČO: 60794097, DIČ: CZ607940967
zastoupená Ing. Miroslavem Bayerem, jednatelem společnosti
zapsaná v obchodním rejstříku vedeném Krajským soudem v Ostravě, oddíl C, vložka 7219
(dále jen „společnost")

II.

Předmět smlouvy

1. Dne 25. 5. 2012 smluvní strany uzavřely Smlouvu o poskytování provozní podpory elektronického informačního systému spisové služby WISPI.
2. MOÚ se za účelem plnění povinností vyplývajících z výše uvedené smlouvy zavazuje poskytnout společnosti za níže uvedených podmínek vzdálený přístup k aplikacím a zařízením datové sítě MOÚ, blíže určeným v příloze č. 1 této smlouvy, a to prostřednictvím sítě Internet (dále jen „vzdálený přístup") přes VPN koncentrátor MOÚ.
3. Podmínky této 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 zavazuje poskytnout společnosti, resp. jejím níže uvedeným zaměstnancům:

jméno a příjmení	telefon	e-mail
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

(dále jen „zaměstnanec společnosti"), vzdálený přístup, a společnost se zavazuje využívat vzdálený přístup výhradně v zájmu MOÚ a pouze za účelem uvedeným v čl. II odst. 2 této smlouvy.

2. Smluvní strany se dohodly, že individuální přístupové údaje pro dvoufaktorovou autentizaci budou MOÚ zaměstnanci společnosti zaslány na jeho v předchozím odstavci uvedené kontaktní údaje prostřednictvím e-mailu a SMS.
3. Vzdálený přístup k aplikacím datové sítě MOÚ je poskytován výhradně zaměstnanci společnosti, a to na dobu plnění povinností vyplývajících ze smlouvy/smluv uvedené/uvedených v čl. II. odst. 1 této smlouvy. Vzdálený přístup poskytnutý zaměstnanci společnosti nelze bez výslovného souhlasu MOÚ převádět na jinou osobu.
4. 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.
5. MOÚ má právo kdykoli jednostranně ukončit možnost vzdáleného přístupu.
6. Společnost se zavazuje, že v případě zániku pracovněprávního vztahu zaměstnance společnosti, který má na základě této smlouvy zřízen vzdálený přístup k aplikacím datové sítě MOÚ, oznámí společnost tuto skutečnost MOÚ, a to ve lhůtě do zániku pracovněprávního vztahu zaměstnance společnosti.
7. Společnost se zavazuje neprodleně po uzavření této smlouvy seznámit zaměstnance společnosti s přílohou č. 1 a bezpečnostními pravidly vzdáleného přístupu uvedenými v příloze č. 2 této smlouvy. Porušení těchto bezpečnostních pravidel zaměstnancem společnosti představuje podstatné porušení této smlouvy.

IV.
Ochrana osobních údajů

1. Společnost v souvislosti s plněním této smlouvy předává MOÚ předem dohodnutým způsobem osobní údaje zaměstnance společnosti v rozsahu uvedeném v čl. III odst. 1 této smlouvy. Společnost prohlašuje, že poskytnuté osobní údaje zaměstnance společnosti jsou přesné a úplné a zavazuje se MOÚ neprodleně informovat o veškerých jejich změnách (tj. opravách, omezeních či výmazech). MOÚ po přijetí těchto osobních údajů s nimi dále nakládá v postavení správce zpracovávajícího osobní údaje na základě jeho oprávněného zájmu, a to za účelem řízení a kontroly přístupů externích uživatelů k aplikacím a zařízením datové sítě MOÚ a za účelem zajištění integrity zpracovávaných dat. MOÚ se zavazuje osobní údaje zaměstnance společnosti zpracovávat po dobu, po kterou mu bude poskytován vzdálený přístup dle této smlouvy.
2. 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.
3. 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.
4. 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 této 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 této 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 zaměstnance společnosti, osoby jednající na základě pověření společnosti či na základě smluvního vztahu se společností) poruší povinnost vyplývající z čl. III. až V. této smlouvy, zejména:
   - povinnost nepřevádět vzdálený přístup na jiné osoby bez souhlasu MOÚ,
   - 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 uvedenými v příloze č. 2 této smlouvy a s podmínkami zpracování jejich osobních údajů dle čl. IV. odst. 4 této smlouvy,
   - oznamovací povinnost dle čl. III. odst. 6, IV. odst. 1 a 3, V. odst. 3 a 4 této smlouvy, 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. V případě, že společnost nesplní povinnost dle čl. III. odst. 6 této smlouvy, odpovídá za jakoukoliv škodu, kterou MOÚ bývalý zaměstnanec společnosti v souvislosti se vzdáleným přístupem k vnitřní síti MOÚ způsobí.
3. MOÚ neodpovídá za nepřetržitou dostupnost vzdáleného přístupu.

VII.

Závěrečná ustanovení

1. Tato smlouva se uzavírá 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. Tato smlouva automaticky zaniká dnem ukončení poslední platné smlouvy uzavřené mezi MOÚ a společností, pro kterou MOÚ poskytuje vzdálený přístup společnosti dle čl. II. této smlouvy.
4. Ustanovení čl. V. této smlouvy o ochraně důvěrných informací zůstávají v platnosti a účinnosti i po ukončení této smlouvy, nedohodnou-li se smluvní strany výslovně jinak.
5. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž jeden obdrží MOÚ a jeden společnost.
6. Dnem uzavření této smlouvy zaniká smlouva o vzdáleném přístupu uzavřená mezi shodnými smluvními stranami před uzavřením této smlouvy.
7. Nedílnou součást této smlouvy tvoří příloha č. 1 - Aktiva, pro která je vzdálený přístup zřízen a příloha č. 2- Bezpečnostní pravidla přístupu do datové sítě MOÚ.
8. Veškerá další ujednání mohou být učiněna jen formou číslovaných písemných dodatků, podepsaných oběma smluvními stranami.
9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena podle jejich pravé a svobodné vůle, vážně, určitě a srozumitelně. Na důkaz výše uvedeného připojují své podpisy.

V Brně dne 05. 11. 2018

[redacted]

prof. MUDr. Jan Žaloudík, CSc.
ředitel

V Olomouci dne 30. 10. 2018

[redacted]

Ing. Miroslav Bayer
jednatel

Příloha č. 1

Aktiva, pro která je vzdálený přístup zřízen

název zařízení/aplikace	určený zaměstnanec společnosti
WISPI spisová služba	[redacted]

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 mu byla udělena přístupová oprávnění.
3. Zaměstnanec společnosti je povinen chránit obdržené individuální přístupové údaje před jejich ztrátou, zneužitím, odcizením nebo neoprávněným přístupem jiné osoby. Případnou ztrátu, zneužití, odcizení anebo neoprávněný přístup jiné osoby k individuálním přístupovým údajům je zaměstnanec společnosti povinen bez zbytečného odkladu oznámit 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 do datové sítě MOÚ musí zaměstnanec společnosti dodržovat tyto základní zásady:
   - neumožnit přístup do spravovaných systémů žádné třetí osobě,
   - po ukončení práce v IS MOÚ provést neprodleně odhlášení tak, aby se zamezilo zneužití jeho přístupových práv.
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 zaměstnancem společnosti zasílána Vedoucí Oddělení informatiky MOÚ, na e-mail: [redacted] a současně Vedoucímu Úseku informačních technologií MOÚ, na e-mail: [redacted]