Smlouva o zřízení a využívání vzdáleného přístupu

uzavřená dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „**občanský zákoník**")

(dále jen „**Smlouva**")

Smluvní strany:

1. Fakultní nemocnice Bulovka

sídlo:	Budínova 67/2, 180 81 Praha 8
IČO:	00064211
DIČ:	CZ00064211
zastoupená:	Mgr. Janem Kvačkem, ředitelem nemocnice
bankovní spojení:	Česká národní banka
číslo účtu:	16231081/0710
datová schránka:	n9hiezm

(dále jen „**FNB**")

a

1. DEYMED Diagnostic s.r.o.

zapsaná:	v OR u Krajského soudu v Hradci Králové, oddíl C, vložka 12882
sídlo:	Kudrnáčova 533, 549 31 Hronov
IČO:	25284584
DIČ:	CZ25284584
zastoupená:	Ing. Kamilem Holubem, jednatelem
bankovní spojení:	Fio banka, a.s., V Celnici 10, 117 21 Praha 1
č. účtu:	2000144679/2010
datová schránka:	R90RTX7K

(dále jen **„přistupovatel"**)

(FNB a přistupovatel společně jako „**smluvní strany**" nebo jednotlivě jako „**smluvní strana**")

Úvodní ustanovení

1. Přistupovatel prohlašuje, že zřízení a provoz vzdáleného přístupu je pro něj nutným předpokladem pro řádné provádění podpory, údržby, aktualizací, upgradů či servisu v této Smlouvě uvedených systémů, aplikací či přístrojů, které jsou v užívání FNB. Přistupovatel dále prohlašuje, že je schopen dodržet veškeré podmínky uvedené v této Smlouvě, zejména pak s ohledem na řádné využívání zřízeného vzdáleného přístupu smluvenými způsoby k provádění činností uvedených v předchozí větě.
2. FNB prohlašuje, že je poskytovatelem zdravotních služeb, zejména dle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů, jež za účelem naplňování svých povinností vyplývajících z právních předpisů, zřídila, provozuje a spravuje vlastní chráněnou datovou síť, do které přistupovateli umožní omezený vzdálený přístup v rozsahu nezbytně nutném (dále jen „**vzdálený přístup**") k výkonu provádění podpory, údržby, aktualizací, upgradů či servisu zařízení, systémů, přístrojů či aplikací spravovaných přistupovatelem (dále jen „**činnosti vzdálené správy**"), za podmínek vymezených touto Smlouvou.

Článek I.
Předmět Smlouvy

1. FNB a přistupovatel touto Smlouvou sjednávají podmínky vzdáleného přístupu přistupovatele za účelem provádění činností vzdálené správy, která je nezbytným předpokladem pro řádné plnění smlouvy, jejímž předmětem je dodávka dodávka 1 ks Elektromyografu vč. magnetického stimulátoru a příslušenství pro

Neurologické oddělení FNB, která byla uzavřena mezi smluvními stranami dne 06.11.2023, (dále jen „**Kupní smlouva**").

2. FNB se zavazuje, že umožní přistupovateli vzdálený přístup do chráněné datové sítě FNB (dále jen „**DS FNB**") k terminálu Evipa prostřednictvím VPN za účelem provádění činností vzdálené správy, a konkrétně instalace, uvedení do provozu a upgrade ke správnému fungování terminálu Evipa, při současném splnění všech podmínek v této Smlouvě uvedených.

3. Technický postup zřízení vzdáleného přístupu do DS FNB, příp. jeho další eventuální technické varianty budou přistupovateli sděleny bez zbytečného odkladu po podpisu této Smlouvy. Na tyto technické postupy, příp. jejich event. varianty se vztahuje povinnost mlčenlivosti a FNB tímto výslovně prohlašuje, že tyto informace považuje za důvěrné a za informace neveřejného charakteru.

4. FNB se zavazuje zřídit vzdálený přístup do DS FNB bez zbytečného odkladu po doručení písemného požadavku přistupovatele, nebude-li mezi smluvními stranami písemně domluveno jinak.

Článek II.
Doba a místo plnění

1. Zřízení a zajištění vzdáleného přístupu do DS FNB pro přistupovatele je ze strany FNB garantováno po dobu provádění činnosti vzdálené správy terminálu Evipa, nejdéle však 48 měsíců od podpisu této Smlouvy, nedojde-li k ukončení této Smlouvy dříve některým z dalších způsobů v ní uvedených.

2. Místem plnění je sídlo přistupovatele, popř. jiné místo, kde je umístěn terminál Evipa, pro který je zřízen a využíván vzdálený přístup do DS FNB dle této Smlouvy a současně jsou přistupovatelem prováděny činnosti vzdálené správy.

Článek III.
Práva a povinnosti smluvních stran

1. Vzdálený přístup do DS FNB je poskytován výhradně přistupovateli nebo jeho zaměstnancům a zástupcům evidovaných FNB, přičemž FNB tímto výslovně přistupovateli zakazuje jej dále převádět na jinou osobu či osoby.

2. Veškeré technologie umístěné v FNB potřebné pro vzdálený přístup přistupovatele do DS FNB, nastavení a změny nastavení přístupu přistupovatele, internetová konektivita, licence, a služby spojené s údržbou vzdáleného přístupu do DS FNB zajišťuje FNB i přistupovatel v rámci součinnosti bezplatně.

   Přistupovatel se zavazuje, že vzdálený přístup do DS FNB bude iniciovat pouze ze zařízení, které je dostatečně zabezpečené, tj.:

   a) má instalováno a pravidelně aktualizováno programové vybavení (software) na ochranu proti škodlivému software,
   b) má instalováno pouze takové programové vybavení (software), který bylo instalováno v souladu s licenčními podmínkami autora daného programového vybavení (software),
   c) je chráněno heslem,
   d) má aktivní šifrování datového úložiště a pravidelně aktualizovaný operační systém,
   e) má aktivní funkci automatického uzamknutí v případě nečinnosti.

   FNB je oprávněna splnění výše uvedených požadavků kdykoli zkontrolovat, a to v sídle přistupovatele, či v jakémkoliv jiném místě, ze kterého je realizován vzdálený přístup dle této Smlouvy. Přistupovatel je povinen FNB tuto kontrolu bezodkladně a bezpodmínečně umožnit.

3. Přistupovatel se zavazuje, že vzdálený přístup do DS FNB bude využívat jen za účelem uvedeným v této Smlouvě, případně v Kupní smlouvě. Porušení této povinnosti je považováno za podstatné porušení Smlouvy, jež opravňuje FNB k okamžitému odstoupení od této Smlouvy. Přistupovatel je oprávněn v DS FNB nebo prostřednictvím DS FNB provádět pouze činnosti, které jsou potřebné k řádnému a bezchybnému provádění činností dle čl. 1 odst. 2 Smlouvy k zařízení uvedeným tamtéž. Jiné činnosti má přistupovatel striktně zakázáno provádět.

4. Přistupovatel je povinen po každém vstupu do DS FNB sdělit e-mailem na kontaktní adresu FNB uvedenou v odst. 11 tohoto článku důvod ke vstupu do DS FNB, resp. sdělit, jaké činnosti včetně změn provedl prostřednictvím vzdáleného přístupu (stačí obecný popis). Jakékoliv neoznámení tohoto vstupu přistupovatele ve lhůtě do 3 kalendářních dnů od jeho realizace, je považováno za porušení této Smlouvy. Bude-li se toto porušení povinností ze strany přistupovatele opakovat min. ve třech případech, zakládá to právo FNB od této Smlouvy okamžitě odstoupit.

5. Dále je přistupovatel povinen zajistit, že veškeré technické prostředky jím využité pro vzdálený přístup do datové sítě FNB nebudou přístupné žádné neoprávněné osobě; zjistí-li přistupovatel ztrátu či kompromitování přihlašovacích údajů či certifikátů nebo má-li přistupovatel či jeho zaměstnanci nebo zástupci podezření na pokus o získání přihlašovacích údajů či certifikátů neoprávněnou osobou, nahlásí tuto skutečnost neprodleně na kontaktní adresu FNB uvedenou v odst. 11 tohoto článku.

6. Přistupovatel je povinen zajistit ochranu získaných neveřejných informací i jakýchkoliv dalších informací a dat získaných na základě vzdáleného přístupu dle této Smlouvy takovým způsobem, aby nemohlo dojít k jejich zneužití třetí osobou či samotnými zaměstnanci přistupovatele.

7. Přistupovatel se zavazuje učinit taková opatření, aby jeho zástupci či zaměstnanci zachovávali mlčenlivost o veškerých skutečnostech, osobních údajích a datech, o nichž se dozvěděli při plnění předmětu této Smlouvy, včetně těch, které eviduje pomocí prostředků a zařízení výpočetní techniky. Omezení ve vztahu k mlčenlivosti se nevztahuje na technické informace a data ve vztahu k aplikacím dle čl. 1 odst. 2 Smlouvy, které neobsahují údaje, které svým charakterem jsou nebo mohou být považovány za důvěrné či hodné ochrany dle příslušné právní úpravy a pokud se tyto informace vztahují k prováděné činnosti vzdálené správy zřízené a využívané dle této Smlouvy. Přistupovatel je tedy oprávněn nakládat pouze s informacemi, které jsou nezbytně potřebné k provádění činností uvedených v čl. 1 odst. 2 Smlouvy. Za porušení tohoto závazku mlčenlivosti se považuje i využití těchto údajů a dat pro vlastní prospěch přistupovatele, prospěch třetí osoby nebo pro jiné účely. Přistupovatel bere na vědomí, že závazek mlčenlivosti není časově omezen.

8. Přistupovatel je povinen dodržovat při plnění Smlouvy veškerou aktuální bezpečnostní politiku a předpisy Objednatele, které mu byly Objednatelem předány nebo se kterými byl Objednatelem seznámen a které mají dopad na plnění Přistupovatele dle této Smlouvy. Bezpečnostní politikou a předpisy Objednatele, které mají dopad na plnění Přistupovatele dle této Smlouvy, se rozumí bezpečnostní dokumentace, která se vztahuje k plnění Přistupovatele dle této Smlouvy nebo se obvykle vztahuje k povinnostem subjektů, které jsou v dodavatelském vztahu k Objednateli, s přihlédnutím ke skutečnosti, že Objednatel je správcem a provozovatelem informačního systému základní služby. Objednatel je povinen Přistupovateli předat nebo Přistupovatele seznámit s aktuální bezpečnostní politikou a předpisy Objednatele, které mají dopad na plnění Poskytovatele dle této Smlouvy, o čemž bude vždy vyhotoven zápis podepsaný oběma smluvními stranami.

9. Přistupovatel je povinen pravidelně se seznamovat s aktuálními pokyny a doporučeními Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „**NÚKIB**"), přičemž se zavazuje tyto pokyny v co možná nejvyšší míře dodržovat. Bezpečnostní doporučení NÚKIB pro administrátory platná ke dni podpisu této Smlouvy tvoří její přílohu č. 1.

10. Bude-li v souvislosti s plněním této Smlouvy nezbytné zpracovávat osobní údaje fyzických osob, zavazují se smluvní strany bez zbytečného odkladu přistoupit k uzavření smlouvy o zpracování osobnách údajů. která bude uzavřena dle vzoru, který tvoří přílohu č. 2 této Smlouvy, a to tak, aby ke zpracování osobních údajů došlo až po uzavření smlouvy o zpracování osobních údajů.

11. V případě oznamování přístupu do DS FNB dle odstavce 5. tohoto článku, jakýchkoliv změn nebo problematických otázek souvisejících s touto Smlouvou, či v případě důvodného podezření na možnost narušení bezpečnosti, je smluvní strana povinna o tom informovat druhou smluvní stranu, a to bez zbytečného odkladu prostřednictvím dále uvedených kontaktních údajů smluvních stran.

Kontaktní údaje FNB jsou následující:

e-mail:	[redacted]
telefon:	[redacted] (aktivní v časech od 7.00 – 15.30 hod.) (aktivní v časech mezi 15:30 do 7:00 hod.).

Kontaktní osobou přistupovatele:

e-mail:	[redacted]
telefon:	[redacted]

12. FNB je oprávněna kdykoli ukončit přistupovateli vzdálený přístup do DS FNB bez jakýchkoli sankcí vůči FNB, a to zejm. v případě možného ohrožení nebo okamžitého narušení bezpečnosti DS FNB. Sdělení důvodu ukončení vzdáleného přístupu do DS FNB však není podmínkou platnosti ukončení, FNB je oprávněna vzdálený přístup ukončit i bez uvedení důvodu.
13. Porušení smluvních povinností přistupovatele stanovených v tomto článku zakládá právo FNB od Smlouvy kdykoli odstoupit.
14. Odstoupení FNB od této Smlouvy nemá vliv na povinnost přistupovatele uhradit smluvní pokutu dle této Smlouvy, nebo vliv na nárok FNB požadovat po přistupovateli náhradu škody.
15. Odstoupení nebo výpověď musí být učiněny pouze v písemné formě a musí být doručeny druhé smluvní straně osobně, doporučenou poštovní zásilkou nebo datovou schránkou.

Článek IV.
Sankční ujednání

1. V případě porušení povinností přistupovatele uvedených v čl. 3 odst. 3, 4 nebo 9 Smlouvy, je přistupovatel povinen uhradit FNB smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých), a to za každý jednotlivý případ porušení některé z výše uvedených povinností.
2. V případě porušení povinností přistupovatele uvedené v čl. 3 odst. 8 Smlouvy je přistupovatel povinen uhradit FNB smluvní pokutu ve výši 1 000 Kč (slovy: tisíc korun českých) za každý jednotlivý případ porušení této povinnosti.
3. Smluvní pokuty dle tohoto článku jsou splatné ve lhůtě 14 dnů ode dne, kdy oprávněná smluvní strana vyzve povinnou smluvní stranu k příslušné úhradě.
4. Uplatněním smluvní pokuty není dotčeno právo FNB na náhradu škody v plné výši, vzniklé FNB v důsledku porušení povinnosti utvrzené smluvní pokutou, a rovněž tím není dotčena povinnost přistupovatele splnit své povinnosti dle této Smlouvy.

Článek V.
Závěrečná ustanovení

1. Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední smluvní stranou.
2. Smluvní strana je oprávněna ukončit tuto Smlouvu kdykoliv písemnou výpovědí z jakéhokoliv důvodu anebo bez uvedení důvodu, s výpovědní lhůtou dvou měsíců, která započne prvním dnem kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně.
3. V případě odstoupení od Smlouvy ze strany FNB účinky odstoupení nastávající dnem doručení tohoto písemného oznámení přistupovateli. Odstoupením od Smlouvy není dotčena platnost kteréhokoliv ustanovení Smlouvy, jež má výslovně či ve svých důsledcích zůstat v platnosti i po skončení platnosti Smlouvy, zejména závazku mlčenlivosti a ochrany informací, zajištění a utvrzení závazků.
4. Tato Smlouva automaticky zaniká dnem ukončení činností vzdálené správy ze strany Přistupovatele, nejpozději však uplynutím doby uvedené v čl. 2 odst. 1 Smlouvy. Smluvní strany jsou si následně povinny poskytnout veškerou nezbytnou součinnost k ukončení vzdáleného přístupu přistupovatele do DS FNB. Ustanovení věty druhé odst. 3 tohoto článku Smlouvy se použije přiměřeně.
5. Smluvní strany sjednávají, že měnit nebo doplňovat text Smlouvy je možné, s výjimkami ve Smlouvě výslovně uvedenými, pouze formou písemných dodatků podepsaných oběma smluvními stranami. Možnost měnit Smlouvu jinou formou smluvní strany vylučují. Uzavření písemného smluvního dodatku není třeba pouze

v případě změny kontaktních osob nebo kontaktních údajů smluvních stran uvedených v článku 3 odst. 11 Smlouvy, kdy stačí písemné oznámení zaslané druhé smluvní straně.

6. Tato Smlouva a vztahy z této Smlouvy vyplývající se řídí právním řádem České republiky, zejména příslušnými ustanoveními občanského zákoníku.
7. Pokud některé z ustanovení této Smlouvy je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost Smlouvy jako celku ani jiných ustanovení této Smlouvy, pokud je takovéto ustanovení oddělitelné od zbytku této Smlouvy. Smluvní strany se zavazují takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejvěrněji odpovídat podstatě a smyslu původního ustanovení.
8. Smluvní strany se dohodly, že případné spory z této Smlouvy, nedojde-li k dohodě smluvních stran smírnou cestou, budou na návrh kterékoliv smluvní strany dány k rozhodnutí věcně a místně příslušnému soudu FNB.
9. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu. Každá ze smluvních stran obdrží po jednom stejnopisu této Smlouvy, jež má platnost originálu, nejedná-li se o případ, kdy je Smlouva vyhotovena v jediném elektronickém originálu, ke kterému zástupci smluvních stran připojí své elektronické podpisy.
10. Smluvní strany si před podpisem tuto Smlouvu řádně přečetly a svůj souhlas s obsahem jejích jednotlivých ustanovení stvrzují svým podpisem.
11. Nedílnou součástí této Smlouvy je:
    - Příloha č. 1 - Bezpečnostní doporučení NÚKIB pro administrátory 4.0
    - Příloha č. 2 - Smlouva o zpracování osobních údajů

V Praze: 08.12.2023

Elektronicky podepsáno

.....

Mgr. Jan Kvaček
ředitel
Fakultní nemocnice Bulovka
FNB

V Praze: 29.11.2023

Elektronicky podepsáno

.....

Ing. Kamil Holub
jednatel
DEYMED Diagnostic s.r.o.
přistupovatel

Příloha č. 1 - Bezpečnostní doporučení NÚKIB pro administrátory 4.0

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

NASAĎTE ANTI-DDoS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE A SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE,
pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,
které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE
a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY
– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),
tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

NASTAVTE HESLO UEFI / BIOS
unikátní pro každou stanici s centrální správou hesel.

VYNUCUJTE SECURE BOOT
a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA
u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA.
Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použít pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

Příloha č. 2 - Smlouva o zpracování osobních údajů

Smlouva o zpracování osobních údajů

Tuto smlouvu o zpracování osobních údajů (dále jen „**Smlouva**“) uzavírají níže uvedeného dne, měsíce a roku v souladu s čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; dále jen „**GDPR**“) následující smluvní strany:

1. Fakultní nemocnice Bulovka

sídlo: Budínova 67/2, 180 81 Praha 8
IČO: 00064211
DIČ: CZ00064211
zastoupená: Mgr. Janem Kvačkem, ředitelem nemocnice
bankovní spojení: Česká národní banka
číslo účtu: 16231081/0710
datová schránka: n9hiezm

(dále jen „**Správce**“)

a

2. DEYMED Diagnostic s.r.o.

zapsaná: v OR u Krajského soudu v Hradci Králové, oddíl C, vložka 12882
sídlo: Kudrnáčova 533, 549 31 Hronov
IČO: 25284584
DIČ: CZ25284584
zastoupená: Ing. Kamilem Holubem, jednatelem
bankovní spojení: Fio banka, a.s., V Celnici 10, 117 21 Praha 1
č. účtu: 2000144679/2010
datová schránka: R90RTX7K

(dále jen **„Zpracovatel“**)

Správce a Zpracovatel jsou dále označování také jako „**Smluvní strana**“ nebo společně jako „**Smluvní strany**“.

Článek I.
Úvodní ustanovení

Smluvní strany vzájemně prohlašují a potvrzují, že mezi sebou uzavírají tuto Smlouvu vycházejíce z toho, že: Datum smlouvy

1. Zpracovatel uzavřel se Správcem Smlouvu o zřízení a využívání vzdáleného přístupu (dále jen „**Smlouva o vzdáleném přístupu**“). Na základě **Smlouvy o vzdáleném přístupu** je Zpracovatel povinen vést (a to jak v papírové, tak i v elektronické podobě za pomoci softwarové aplikace (Microsoft Excel), evidenci přístupů (dále jen „**evidence**“).
2. Zpracovatel v rámci vedení evidencí dle **Smlouvy o vzdáleném přístupu** zpracovává pro Správce osobní údaje (dále jen „**osobní údaje**“), a to za podmínek stanovených v této Smlouvě a ve Smlouvě o vzdáleném přístupu.

Článek II.
Předmět smlouvy

1. Předmětem této Smlouvy je stanovení vzájemných práv a povinností Smluvních stran v souvislosti se zpracováváním osobních údajů Zpracovatelem pro Správce v rámci plnění Smlouvy o vzdáleném přístupu.

Článek III.
Zpracování osobních údajů

1. Zpracovatel je na základě Smlouvy o poskytování služeb povinen zpracovávat pro Správce osobní údaje pro účely poskytnutí vzdáleného přístupu k Elektromyografu vč. magnetického stimulátoru a příslušenství v rozsahu sjednaném ve Smlouvě o koupy (dále jen „Účely"), a to vždy po dobu nezbytnou pro naplnění daného Účelu, nejdéle však po dobu trvání této Smlouvy (dále jen „**Doba zpracování**").
2. Pro realizaci Účelů jsou Zpracovatelem zpracovávány osobní údaje, které se týkají kategorie subjektů údajů: pacienta, jejichž osobní údaje bude nezbytné zpracovávat při vedení evidence v rámci poskytování služeb (dále jen „**Kategorie subjektů**").
3. Předmětem zpracování dle této Smlouvy jsou osobní údaje Kategorie subjektů spojených s plněním povinností Správce, zejména **následující typ osobních údajů:** identifikační údaje a údaje o zdravotním stavu (dále jen „**Údaje**").
4. Zpracovatel se zavazuje zpracovávat Údaje vždy pouze v rozsahu nezbytném pro plnění příslušné povinnosti dle Smlouvy o dodávce 1 ks Elektromyografu vč. magnetického stimulátoru a příslušenství Zpracovatel není oprávněn zpracovávat Údaje pro jiné účely než pro Účely dle této Smlouvy.
5. Zpracovatel je povinen Údaje zpracovávat v souladu s právními předpisy, zejména GDPR, touto Smlouvou a pokyny Správce, které vyplývají přímo z této Smlouvy a/nebo ze Smlouvy o poskytování služeb. V případě, že je pro zpracování Údajů dle této Smlouvy potřebné a/nebo vhodné, aby Správce udělil Zpracovateli dodatečné pokyny, je Zpracovatel povinen si takové pokyny od Správce písemně vyžádat.

Článek IV.
Technické a organizační zabezpečení zpracování

1. Zpracovatel prohlašuje, že před uzavřením této Smlouvy provedl veškerá vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající možným rizikům zpracování Údajů dle této Smlouvy, a zavazuje se, že bude tuto ochranu zabezpečovat, tj. že bude plnit povinnosti k zabezpečení a ochraně Údajů v rozsahu dle této Smlouvy, a to až do výmazu veškerých Údajů dle čl. V, odst. 7 této Smlouvy.
2. Zpracovatel se zejména zavazuje, že:
   a) příjme taková opatření a zabezpečí, že nedojde k neoprávněnému nebo nahodilému přístupu k Údajům, jejich změně, zničení, ztrátě či neoprávněným přenosům, neoprávněnému zpracování či jinému zneužití;
   b) zabezpečí neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
   c) zajistí schopnost obnovit dostupnost Údajů a přístup k nim včas v případě fyzických či technických incidentů;
   d) zajistí proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
   e) tam, kde to bude možné, zabezpečí zpracování Údajů pomocí anonymizace, pseudonymizace a/nebo šifrování;
   f) servery Zpracovatele s Údaji budou uzamčeny;
   g) zajistí, aby k Údajům měly přístup pouze osoby, které tímto Zpracovatel výslovně pověří, a jejichž přístup je pro plnění povinností Zpracovatele dle této Smlouvy nebo Smlouvy o poskytování služeb nezbytně nutný, a Zpracovatel bude vhodným způsobem monitorovat jednotlivé přístupy těchto osob k Údajům (např. přístup pod jednoznačným identifikátorem apod.), přičemž zároveň bude kontrolovat neoprávněné přístupy a účinně jim bránit, včetně dokumentování všech incidentů.
3. Zpracovatel se zavazuje, že umožní přístup k Údajům pouze těm svým pracovníkům (ať už zaměstnancům, nebo jiným smluvním partnerům), kteří budou náležitě a pravidelně proškolováni v oblasti ochrany osobních údajů,

včetně povinností dle této Smlouvy, a zároveň kteří budou zavázáni zachovávat mlčenlivost dle čl. 7, odst. 3 této Smlouvy. Zpracovatel je povinen Správci bez zbytečného odkladu na jeho žádost prokázat písemnými doklady absolvovaná školení a uzavřené závazky k mlčenlivosti dle předchozí věty. Zpracovatel se zavazuje, že tento odstavec se použije obdobně i na další zpracovatele, které Zpracovatel zapojí do zpracování dle této Smlouvy.

4. Zpracovatel je povinen vést záznamy o zpracování Údajů prováděném pro Správce dle této Smlouvy, přičemž v nich uvede všechny informace stanovené čl. 30 odst. 2 GDPR. Záznamy dle předchozí věty je Zpracovatel povinen vést písemně (a to v listinné nebo elektronické formě). Zpracovatel se zavazuje kopie těchto záznamů předat Správci bez zbytečného odkladu na jeho žádost.
5. Zpracovatel se zavazuje, že Údaje nepředá do třetí země a/nebo mezinárodní organizaci a že Údaje nebudou do třetí země a/nebo mezinárodní organizaci předány ani dalším zpracovatelem, zapojeným do zpracování dle této Smlouvy.

Článek V.
Informování Správce, součinnost, výmaz Údajů

1. Zpracovatel se zavazuje, že bude Správce informovat o veškerých skutečnostech, které budou nebo by mohly mít vliv na plnění povinností Zpracovatele dle této Smlouvy, zejména pokud jde o zabezpečení a ochranu Údajů.
2. V případě, že dojde k porušení zabezpečení při zpracování Údajů Zpracovatelem, zavazuje se Zpracovatel bez zbytečného odkladu (nejpozději však do 24 hodin) poté, co k porušení zabezpečení došlo, porušení písemně oznámit Správci, konkrétně osobě uvedené v čl. 11.1. Smlouvy. Oznámení Zpracovatele musí obsahovat všechny informace stanovené čl. 33 odst. 3 GDPR, tj. (i) popis povahy daného případu porušení zabezpečení Údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů Údajů, dále (ii) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace, (iii) popis pravděpodobných důsledků porušení zabezpečení Údajů a (iv) popis opatření, která Zpracovatel přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení Údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
3. V případě, že Zpracovatel po oznámení dle čl. V, odst. 2 této Smlouvy zjistí jakoukoli další skutečnost související s daným porušením, zavazuje se bez zbytečného odkladu (nejpozději však do 24 hodin) poté, co danou skutečnost zjistí, o ní písemně informovat Správce.
4. V případě, že subjekt údajů u Správce uplatní některé z práv, které subjektu údajů dle GDPR náleží, zavazuje se Zpracovatel poskytnout Správci veškerou součinnost potřebnou pro splnění povinnosti Správce reagovat na požadavek subjektu údajů, tj. zejména se zavazuje na požádání Správce:
   a) pozastavit zpracování Údajů;
   b) opravit neaktuální či jinak chybné či nepřesné Údaje;
   c) vymazat Údaje týkající daného subjektu údajů;
   d) sdělit Správci veškeré příjemce Údajů; a/nebo
   e) omezit zpracování Údajů;

   a to vše bez zbytečného odkladu (nejpozději však bezprostředně následující pracovní den) poté, co o to Správce požádá, přičemž provedení požadovaného opatření je Zpracovatel povinen Správci písemně potvrdit.
5. Zpracovatel se zavazuje poskytovat Správci veškerou součinnost potřebnou pro zajišťování souladu s povinnostmi Správce dle GDPR, zejména dle čl. 32 až 36, přičemž se zavazuje Správci na jeho žádost poskytovat veškeré informace potřebné k doložení toho, že byly splněny všechny požadavky právních předpisů upravujících nakládání s osobními údaji. Ve všech případech, kdy má Zpracovatel dle této Smlouvy a/nebo právního předpisu poskytnout Správci určité informace, zavazuje se Zpracovatel tam, kde to bude technicky možné, poskytnout Správci příslušné informace ve strukturovaném, běžně používaném a strojově čitelném formátu.
6. Správce se zavazuje poskytovat Zpracovateli veškerou součinnost nezbytnou pro plnění jeho povinností dle této Smlouvy.
7. Zpracovatel se zavazuje, že neprodleně po uplynutí Doby zpracování vymaže veškeré Údaje. V případě, že Zpracovatel do zpracování dle této Smlouvy zapojí dalšího zpracovatele, zavazuje se zajistit a odpovídá za to, že výmaz dle předchozí věty provede i takový další zpracovatel. Zpracovatel se současně zavazuje, že bez

zbytečného odkladu po uplynutí Doby zpracování písemně Správci potvrdí, že příslušný výmaz provedl a rovněž že příslušný výmaz provedli všichni další zpracovatelé, zapojení do zpracování dle této Smlouvy.

Článek VI.
Další zpracovatelé

1. Zpracovatel není oprávněn předat Údaje žádné třetí straně bez předchozího písemného pokynu Správce. Dalšího zpracovatele je Zpracovatel oprávněn zapojit do zpracování dle této Smlouvy pouze s předchozím písemným souhlasem Správce.
2. Aniž by tím byl dotčen čl. 6, odst. 1 této Smlouvy, je Zpracovatel oprávněn zapojit do zpracování pouze takového dalšího zpracovatele, s nímž bude mít uzavřenou písemnou smlouvou ve smyslu čl. 28 odst. 4 GDPR, na základě které bude další zpracovatel zavázán k plnění povinností alespoň ve stejném rozsahu, k jakému je zavázán Zpracovatel dle této Smlouvy, a to zejména v oblasti technického zabezpečení a ochrany Údajů a poskytování součinnosti Správci. Zpracovatel je zároveň oprávněn zapojit pouze takového dalšího zpracovatele, který bude poskytovat dostatečné záruky, pokud jde o vhodná technická a organizační opatření tak, aby zpracování naplňovalo požadavky GDPR.

Článek VII.
Mlčenlivost

1. Smluvní strany se zavazují zachovávat mlčenlivost o veškerých informacích, které jsou uvedeny v této Smlouvě (tj. o obsahu této Smlouvy), a dále o veškerých informacích týkajících se plnění této Smlouvy (dále jen „**Důvěrné informace**"). Za Důvěrné informace se považují také informace, které jsou takového charakteru, že mohou v případě uveřejnění přivodit druhé Smluvní straně újmu, bez ohledu na to, zda mají povahu osobních, obchodních či jiných informací. Smluvní strany nesmí jakékoli Důvěrné informace bez předchozího písemného souhlasu druhé Smluvní strany poskytnout jakékoli třetí osobě a zavazují se zajistit, aby tyto Důvěrné informace nebyly bez souhlasu druhé Smluvní strany sděleny třetím osobám a aby ani jinak nebylo umožněno třetím osobám zjistit obsah Důvěrných informací, s výjimkou (i) svých poradců vázaných zákonnou povinností mlčenlivosti (ii) příslušných státních a jiných správních orgánů a soudů, pokud je Smluvní strana podle právních předpisů povinna jim tyto informace poskytnout, a to pouze v nezbytně nutném rozsahu, nebo (iii) informací, které jsou nebo se stanou veřejně dostupnými jinak než porušením této Smlouvy. Správce je oprávněn poskytovat Důvěrné informace osobám v rámci holdingu, do kterého patří, a/nebo osobám, které Správce ovládají, a/nebo osobám, které ovládá Správce, a dále v souvislosti s plněním této Smlouvy také svým smluvním partnerům.
2. Povinnost mlčenlivost dle čl. 7, odst. 1 této Smlouvy se Smluvní strany zavazují zachovávat po celou dobu trvání této Smlouvy i po jejím skončení. V případech, kdy je Smluvní strana povinna zavázat třetí osobu k mlčenlivosti dle této Smlouvy, je povinna tuto třetí osobu zavázat tak, aby zachovávala mlčenlivost v rozsahu dle této Smlouvy i po skončení této Smlouvy.
3. Zpracovatel se zavazuje, že veškeré své zaměstnance a jiné pracovníky (smluvní partnery), kterým umožní přístup k Údajům, zaváže zachovávat mlčenlivost o veškerých Údajích, a to po celou dobu trvání právního vztahu ke Zpracovateli i po jeho skončení.

Článek VIII.
Odměna

1. Smluvní strany se dohodly, že odměna za zpracování dle této Smlouvy je zahrnuta a zcela vypořádána v odměně dle Smlouvy o poskytování služeb.

Článek IX.
Trvání Smlouvy

1. Tato Smlouva se uzavírá na dobu trvání Smlouvy **o zřízení a využívání vzdáleného přístupu**.
2. Smluvní strany se dohodly, že tato Smlouva a Smlouva o poskytování jsou na sobě závislé ve smyslu § 1727 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**"). Zánik některé z těchto Smluv automaticky působí zánik druhé.

3. Zpracovatel se zavazuje, že jakoukoli smlouvu, kterou uzavře s dalším zpracovatelem, a na základě které bude tento další zpracovatel zpracovávat Údaje, učiní závislou na této Smlouvě, a to tak, že v případě zániku této Smlouvy automaticky zanikne také smlouva s dalším zpracovatelem, a to minimálně v rozsahu zpracování Údajů dle této Smlouvy.
4. Správce je bez dalšího oprávněn odstoupit od této Smlouvy, poruší-li Zpracovatel tuto Smlouvu podstatným způsobem. Správce je dále oprávněn odstoupit od této Smlouvy, poruší-li Zpracovatel tuto Smlouvu (ať už podstatným, nebo nepodstatným způsobem) a nezjedná-li nápravu, a to ani v dodatečné přiměřené lhůtě stanovené výzvou Správce. Odstoupením se tato Smlouva zrušuje s účinky do budoucna (tzv. ex nunc), a to ode dne doručení odstoupení Zpracovateli. Tento odstavec nevylučuje použití § 2005 Občanského zákoníku ani jiná ustanovení Občanského zákoníku, jejichž předmět úpravy tento odstavec neupravuje.
5. Zpracovatel není oprávněn od této Smlouvy odstoupit.

Článek X.
Sankce

1. Za každý případ porušení této Smlouvy podstatným způsobem ze strany Zpracovatele se Zpracovatel zavazuje zaplatit Správci smluvní pokutu ve výši 5.000,- Kč.
2. Za každý případ jakéhokoli porušení povinnosti Zpracovatele dle čl. 4, 5, 6, 7 a/nebo 8 této Smlouvy se Zpracovatel zavazuje zaplatit Správci smluvní pokutu ve výši 10.000,- Kč.
3. V případě podstatného porušení povinnosti Zpracovatele dle čl. IV., V., VI. a VII. této Smlouvy bude Zpracovatel povinen k zaplacení smluvní pokuty pouze dle čl. 10, odst. 1 této Smlouvy.
4. Uplatněním kterékoli smluvní pokuty dle této Smlouvy není dotčeno právo Správce na náhradu škody v plné výši. Smluvní strany se přitom dohodly, že náhrada škody, na kterou vznikne Správci právo vůči Zpracovateli, bude též zahrnovat: (i) peněžitou náhradu (ať už majetkové, nebo nemajetkové újmy), k jejímuž zaplacení subjektu údajů bude Správce povinen, a/nebo (ii) pokuty uložené Správci ze strany dozorového úřadu.

Článek XI.
Kontakty smluvních stran

1. Kontaktní osobou ve věcech zpracování osobních údajů za:

Za Správce:	jméno: zástupce oddělení využívajícího specialista UIKT pro poskytování vzdáleného přístupu, tel.: [redacted], e-mail: [redacted]
Za Zpracovatele:	jméno: [redacted], tel.: [redacted], e-mail: [redacted]

Článek XII.
Závěrečná ustanovení

1. Tato Smlouva, jakož i práva a povinnosti vzniklé na základě této Smlouvy nebo v souvislosti s ní se řídí právním řádem České republiky.
2. V případě, že se ke kterémukoli ustanovení této Smlouvy či k jeho části podle zákona jako ke zdánlivému právnímu jednání nepřihlíží, nebo že kterékoli ustanovení této Smlouvy či jeho část je nebo se stane neplatným, neúčinným a/nebo nevymahatelným, oddělí se v příslušném rozsahu od ostatních ujednání této Smlouvy a nebude mít žádný vliv na platnost, účinnost a vymahatelnost ostatních ujednání této Smlouvy. Smluvní strany se zavazují nahradit takové zdánlivé, nebo neplatné, neúčinné a/nebo nevymahatelné ustanovení či jeho část novým ujednáním, které bude platné, účinné a vymahatelné a jehož věcný obsah a ekonomický význam bude shodný nebo co nejvíce podobný nahrazovanému ujednání tak, aby účel a smysl této Smlouvy zůstal zachován. Smluvní strany pro vyloučení všech pochybností výslovně sjednávají, že tento odstavec v celém rozsahu nahrazuje § 576 Občanského zákoníku.
3. Jakékoli změny této Smlouvy mohou být učiněny pouze písemnými dodatky k této Smlouvě podepsanými oběma Smluvními stranami, vyjma změny kontaktních osob Smluvních stran uvedench v čl. XI. Smlouvy, kdy postačí zaslaní písemné informace o změně těchto údajů druhé Smluvní straně.

4. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží po jednom, nejedná-li se o případ, kdy je tato Smlouva vyhotovena v jediném elektronickém stejnopisu, ke kterému zástupci Smluvních stran připojí své elektronické podpisy.
5. Smluvní strany souhlasně prohlašují, že obsah této Smlouvy vyjadřuje jejich pravou a svobodně projevenou vůli, prostou omylu a že tato Smlouva nebyla uzavřena v tísni ani za nápadně nevýhodných podmínek, což stvrzují svými podpisy.

V Praze: 08.12.2023

Elektronicky podepsáno

.....

Mgr. Jan Kvaček
ředitel nemocnice
Fakultní nemocnice Bulovka
Správce

V Praze: 29.11.2023

Elektronicky podepsáno

.....

Ing. Kamil Holub
jednatel
DEYMED Diagnostic s.r.o.
Zpracovatel