č. j. MPPH 74734/2023
Ag. SML/2023/03711

Smlouva o zpracování osobních údajů

[...]
Medical Information Technologies s.r.o.

Dne 2023

Obsah

PŘÍLOHY

Tato smlouva („**Smlouva**“) je uzavřena mezi níže uvedenými stranami („**Strany**“) dne 2022

Strany

(1) **Hlavní město Praha**, se sídlem **Mariánské nám. 2, 110 00 Praha 1**, IČO: 00064581, DIČ: CZ00064581

korespondenční a fakturační adresa: *Hlavní město Praha, Městská policie hl. m. Prahy, Korunní 98, 101 00 Praha 10, datová schránka: ktdeucu,* č. ú.: 620023-5157998//6000

(„**Správce**“)

(2) **Medical Information Technologies, s.r.o.**, se sídlem Vachova 43/5, Brno–město, 602 00 Brno, zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně v oddíle C, číslo vložky 86630, IČO: 03759865, DIČ: CZ03759865

(„**Zpracovatel**“)

Preambule

18 -08- 2023

A Strany spolu dne [*****] uzavřeli smlouvu o poskytování služeb – Portál bezpečí („**Smlouva o poskytování služeb**“).

B Vzhledem ke skutečnosti, že v souvislosti se Smlouvou o poskytování služeb bude Správce, jako správce osobních údajů předávat Zpracovatel, jako zpracovateli osobních údajů osobní údaje, uzavírají Strany tuto Smlouvu.

Smluvní podmínky

1 Účel a oblast působnosti

1.1 Účelem této Smlouvy je zajistit soulad s ustanoveními čl. 28 odst. 3 a 4 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 („**GDPR**“).

1.2 Strany se dohodli na této Smlouvě, aby zajistili soulad s čl. 28 odst. 3 a 4 GDPR a/nebo čl. 29 odst. 3 a 4 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů („**EDPS**“).

1.3 Tato Smlouva se uplatňují na zpracování osobních údajů, jak je upřesněno v příloze 1.

1.4 Přílohy 1 až 3 jsou nedílnou součástí této Smlouvy.

1.5 Touto Smlouvou nejsou dotčeny povinnosti, které Správce musí plnit na základě GDPR a/nebo EDPS.

1.6 Tato Smlouva sama o sobě nezajišťuje soulad s povinnostmi týkajícími se mezinárodního předávání podle kapitoly V GDPR a/nebo EDPS.

2 Neměnnost Smlouvy

2.1 Smluvní strany se zavazují, že Smlouvu nebudou měnit, s výjimkou doplňování nebo aktualizace informací v přílohách.

3 Výklad

3.1 V případech, kdy tato Smlouva používá pojmy definované v GDPR nebo EDPS, mají tyto pojmy stejný význam jako v uvedeném nařízení.

4 Popis zpracování

4.1 Zpracovatel zpracovává osobní údaje pouze na základě písemně doložených pokynů Správce, pokud mu takové zpracování neukládá právo Unie nebo členského státu, které se na Správce vztahuje. V tomto případě Zpracovatel Správce informuje o uvedeném právním požadavku před zpracováním, pokud to právní předpisy nezakazují z důvodů důležitého veřejného zájmu. Po celou dobu zpracování osobních údajů může Správce rovněž vydávat další pokyny. Tyto pokyny musí být vždy písemně doloženy.

4.2 Zpracovatel neprodleně informuje Správce v případě, že dle jeho názoru pokyny Správce porušují GDPR / EDPS nebo příslušná ustanovení Unie nebo členského státu o ochraně údajů.

5 Povinnosti stran

Pokyny

5.1 Zpracovatel zpracovává osobní údaje pouze na základě písemně doložených pokynů Správce, pokud mu takové zpracování neukládá právo Unie nebo členského státu, které se na Správce vztahuje. V tomto případě Zpracovatel Správce informuje o uvedeném právním požadavku před zpracováním, pokud to právní předpisy nezakazují z důvodů důležitého veřejného zájmu. Po celou dobu zpracování osobních údajů může Správce rovněž vydávat další pokyny. Tyto pokyny musí být vždy písemně doloženy.

5.2 Zpracovatel neprodleně informuje Správce v případě, že dle jeho názoru pokyny Správce porušují GDPR / EDPS nebo příslušná ustanovení Unie nebo členského státu o ochraně údajů.

Omezení účelu

5.3 Zpracovatel zpracovává osobní údaje pouze pro konkrétní účel nebo účely zpracování, jak je stanoveno v příloze 1, pokud od Správce neobdrží další pokyny.

Doba trvání zpracování osobních údajů

5.4 Zpracování Zpracovatelem probíhá pouze po dobu stanovenou v příloze 1.

Zabezpečení zpracování

5.5 Za účelem zajištění bezpečnosti osobních údajů musí Zpracovatel zavést přinejmenším technická a organizační opatření uvedená v příloze 2. Součástí těchto opatření musí být ochrana údajů před narušením bezpečnosti, které by vedlo k jejich náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k nim (porušení zabezpečení osobních údajů). Při posuzování vhodné úrovně zabezpečení vezmou strany v úvahu aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování a rizika pro subjekty údajů.

5.6 Zpracovatel poskytne svým zaměstnancům přístup ke zpracovávaným osobním údajům pouze v rozsahu nezbytně nutném pro provádění, správu a kontrolu Smlouvy. Zpracovatel zajistí, aby se osoby oprávněné zpracovávat obdržené osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

Citlivé údaje

5.7 Pokud zpracování zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu nebo o sexuálním životě či sexuální orientaci dané osoby nebo údaje týkající se odsouzení v trestních věcech a trestných činů (dále jen „citlivé údaje"), uplatní Zpracovatel zvláštní omezení nebo další záruky.

Dokumentace a soulad

5.8 Strany musí být schopny prokázat dodržování této Smlouvy.

5.9 Zpracovatel neprodleně a odpovídajícím způsobem vyřídí dotazy Správce, které se týkají zpracovávání podle této Smlouvy.

5.10 Zpracovatel poskytne Správci na žádost informace potřebné k prokázání souladu s povinnostmi stanovenými v této Smlouvě. Zpracovatel též v souladu s GDPR na žádost Správce umožní audity činností zpracování.

5.11 Strany na požádání zpřístupní informace uvedené v bodě 5 Smlouvy, včetně výsledků případných auditů, příslušnému dozorovému úřadu, respektive příslušným dozorovým úřadům.

Využívání dílčích zpracovatelů údajů

5.12 Pokud Zpracovatel zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem Správce), učiní tak prostřednictvím smlouvy, která ukládá dílčímu zpracovateli v podstatě stejné povinnosti v oblasti ochrany údajů, jaké jsou v souladu s touto Smlouvou uloženy Zpracovateli údajů. Zpracovatel zajistí, aby dílčí Zpracovatel plnil povinnosti, které se na Zpracovatele vztahují podle této Smlouvy a GDPR a/nebo EDPS.

Mezinárodní předávání údajů

5.13 Správce souhlasí s tím, že pokud Zpracovatel zapojí dílčího zpracovatele do provádění konkrétních činností zpracováním (jménem Správce) a uvedené činnosti zahrnují předání osobních údajů do třetí země nebo mezinárodní organizaci, mohou Zpracovatel a dílčí zpracovatel zajistit soulad s GDPR použitím standardních smluvních doložek přijatých Komisí v souladu s čl. 46 odst. 2 GDPR.

6 Pomoc poskytovaná Správci

6.1 Zpracovatel neprodleně informuje Správce o každé žádosti, kterou obdržel od subjektu údajů. Na tuto žádost neodpovídá sám, pokud k tomu není Správcem zmocněn.

7 Ohlašování případů porušení zabezpečení osobních údajů

7.1 V případě porušení zabezpečení osobních údajů Zpracovatel spolupracuje se Správcem a pomáhá mu při plnění jeho povinností podle článků 33 a 34 GDPR nebo případně podle článků 34 a 35 EDPS, přičemž zohlední povahu zpracování a informace, které má Zpracovatel k dispozici.

Porušení zabezpečení údajů zpracovávaných Správcem

7.2 V případě porušení zabezpečení osobních údajů zpracovávaných Správcem Zpracovatel napomáhá Správci:

(a) při ohlašování případů porušení zabezpečení osobních údajů příslušnému dozorovému úřadu, respektive příslušným dozorovým úřadům, a to bez zbytečného odkladu poté, co se o něm Správce dozvěděl, je-li to relevantní / (pokud je nepravděpodobné, že by porušení zabezpečení osobních údajů vedlo k ohrožení práv a svobod fyzických osob);

(b) při získávání následujících informací, které musí být podle čl. 33 odst. 3 GDPR uvedeny v oznámení Správce, a to musí přinejmenším zahrnovat:

(i) povahu daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

(ii) pravděpodobné důsledky porušení zabezpečení osobních údajů;

(iii) opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

(c) při plnění povinnosti v souladu s článkem 34 GDPR oznámit bez zbytečného odkladu subjektu údajů porušení zabezpečení osobních údajů, pokud je pravděpodobné, že dané porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

Porušení zabezpečení údajů zpracovávaných Zpracovatelem

7.3 V případě porušení zabezpečení osobních údajů zpracovávaných Zpracovatelem o tom Zpracovatel informuje Správce bez zbytečného odkladu poté, co se o tomto porušení dozvěděl. Takové oznámení obsahuje alespoň:

(a) popis povahy daného případu porušení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a záznamů údajů);

(b) údaje o kontaktním místě, kde lze získat více informací o daném porušení zabezpečení osobních údajů;

(c) pravděpodobné důsledky a opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení, a to včetně opatření ke zmírnění možných nepříznivých dopadů.

7.4 Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

8 Závěrečná ustanovení

8.1 Aniž jsou dotčena jakákoli ustanovení GDPR a/nebo EDPS, pokud Zpracovatel poruší své povinnosti podle této Smlouvy, může mu Správce nařídit, aby pozastavil zpracovávání

osobních údajů, dokud Zpracovatel nebude plnit povinnosti podle této Smlouvy, nebo dokud nebude Smlouva vypovězena. Zpracovatel neprodleně informuje Správce v případě, že z jakéhokoli důvodu není schopen plnit ustanovení této Smlouvy.

8.2 Správce je oprávněn vypovědět Smlouvu v rozsahu, v němž se týká zpracování osobních údajů v souladu s touto Smlouvou, pokud:

(a) Správce pozastavil podle bodu 8.1 zpracovávání osobních údajů Zpracovatelem a plnění povinností podle této Smlouvy není obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;

(b) Zpracovatel závažně nebo trvale porušuje tuto Smlouvu nebo povinnosti, které pro něj vyplývají z GDPR a/nebo EDPS;

(c) Zpracovatel neplní závazné rozhodnutí příslušného soudu nebo příslušného dozorového úřadu, respektive příslušných dozorových úřadů týkající se jeho povinností vyplývající z této Smlouvy nebo z GDPR a/nebo EDPS.

8.3 Zpracovatel je oprávněn vypovědět Smlouvu, pokud poté, co informoval Správce o tom, že pokyny Správce porušují platné právní požadavky podle bodu 5.2, Správce na splnění těchto pokynů trvá.

8.4 Po ukončení Smlouvy Zpracovatel podle volby Správce vymaže veškeré osobní údaje zpracovávané jménem Správce a potvrdí Správci, že tak učinil, nebo vrátí veškeré osobní údaje Správci a vymaže stávající kopie, pokud právo Unie nebo členského státu nepožaduje uchovávání osobních údajů. Dokud nejsou osobní údaje vymazány nebo vráceny, Zpracovatel nadále zajišťuje dodržování souladu s touto Smlouvou.

Podpisová strana

V Praze dne 18. 8. 2023

Hlavní město Praha

Podpis

Jméno: Ing. Eduard Šuster

Funkce: ředitel Městské po **ny**

Medical Information Technol **s.r.o.**

Podpis

Jméno

Funkce: JEDNATEL

Příloha 1 – Popis zpracování

Kategorie subjektů údajů, jejichž osobní údaje jsou zpracovávány

- fyzické osoby nahlašující události spadající do kompetence obecní policie;

Kategorie zpracovávaných osobních údajů

- polohové údaje o volajícím telefonním čísle;
- chatová komunikace s osobou;
- fotodokumentace z místa hlášené události;
- videozáznam z místa hlášené události.

Zpracovávané citlivé údaje (v relevantních případech) a použitá omezení nebo záruky, které plně zohledňují povahu těchto údajů a související rizika, jako je například přísné omezení účelu, omezení přístupu (včetně přístupu pouze pro pracovníky, kteří absolvovali specializovanou odbornou přípravu), vedení záznamů o přístupu k údajům, omezení dalšího předávání nebo další opatření k zajištění zabezpečení.

NEJSOU

Účel/účely, pro který/které jsou osobní údaje zpracovávány jménem Správce

- plnění zákonných povinností Správce vyplývajících z jeho postavení obecní policie

Doba trvání zpracování

- polohové údaje, chatová komunikace, fotodokumentace – jeden rok
- videozáznam – po dobu kontaktu s osobou nahlašující událost a maximálně následujících 24 hodin po ukončení videozáznamu

U zpracování (dílčím) Zpracovatelem rovněž upřesněte předmět, povahu a dobu trvání zpracování.

NEPOUŽIJE SE

Příloha 2 – Technická a organizační opatření včetně technických a organizačních opatření k zajištění zabezpečení údajů

BEZPEČNOSTNÍ OBLAST	BEZPEČNOSTNÍ OPATŘENÍ NA OCHRANU OSOBNÍCH ÚDAJŮ
	Produkční (reálná) data by měla být povolena jen v produkčních prostředích. V případě výjimky, a se všemi nutnými souhlasy, mohou prostředí QA zpracovávat (reálné) osobní údaje pouze, pokud jsou chráněny jako produkční prostředí.
BEZPEČNOST OSOBNÍCH ÚDAJŮ	Doba, po kterou se udržují osobní údaje, musí být omezena na dobu nezbytnou pro každou jednotlivou zpracovatelskou činnost a musí být v souladu se zákonnými a/nebo regulatorními povinnostmi týkajícími se doby udržování.
	Musí se realizovat bezpečnostní protokoly, aby bylo možné ochránit osobní údaje během předávání prostřednictvím otevřené, veřejné nebo nedůvěryhodné sítě.
	Kódování databází/úložiště dat by mělo být založeno na řádné klasifikaci aktiv podle úrovně kritičnosti. Například: databáze/úložiště dat sloužící hlavním obchodním procesům/službám banky nebo skladování velkého množství osobních údajů mohou být chráněny silným kódováním. Každá právnická osoba se musí rozhodnout o realizaci kódování a o rozčlenění kódování, které se má vymáhat (např. na úrovni úložiště nebo tabulky).
	Média obsahující osobní údaje musí být chráněna pře neoprávněným přístupem prostřednictvím přiměřených fyzických (např. zámek) a logických (např. kódování, přístupová kontrola, atd.) bezpečnostních opatření.
	Při návratu a/nebo zamítnutí aktiv a zdroje ICT by měly být zavedeny bezpečnostní postupy (např. vymazání), aby bylo možné odstranit všechny osobní údaje a/nebo je bezpečně přepsat před likvidací nebo opětovným použitím.
	Zaměstnanci musí být přiměřeně vzděláváni a školeni o správných pravidlech chování, které si musí osvojit k ochraně osobních údajů obsažených v papírových dokumentech (např. v případě vzdálení se od pracovní stanice je třeba se přesvědčit, že nikdo nemůže mít přístup k důvěrným informacím, chránit původní dokumenty a fotokopie před krádeží nebo neoprávněným použitím, udržovat dokumentaci v zamykatelných skříních a zásuvkách na konci pracovní doby)
DOSTUPNOST DAT	Měly by být zavedeny řádné postupy, aby bylo možné včas obnovit dostupnost osobních údajů (jako právo subjektu údajů). Záložní postupy by měly zajišťovat kopie osobních údajů aspoň v týdenních intervalech.
SPRÁVA TOTOŽNOSTI A PŘÍSTUPU	Přístupové oprávnění do produkčních prostředí obsahujících osobní údaje by mělo být poskytnuto podle principů „musí vědět“ a „nejmenší privilegium“.
	K zajištění řádné identifikace uživatelů a administrátorů, kteří mají přístup do systémových komponentů řídících osobní údaje, se musí přijmout vhodné metody a postupy. Všem uživatelům by mělo být přiděleno unikátní

	uživatelské jméno ještě předtím, než jim bude povolen přístup k systémovým komponentům nebo osobním údajům.
	Na uživatelské účty, které jsou přiřazeny unikátním uživatelům, musí být přiděleny systémové zdroje a přístupová práva.
	Veškeré přístupy do databází obsahujících osobní údaje by měly být chráněny/kontrolovány takto: - Přihlašovací údaje do aplikace pro přístup do databází nemohou používat jednotliví uživatelé nebo jiné neaplikační procesy, - Přihlašovací údaje uživatele do aplikace/systému musí být přiměřeně chráněno před možným zneužitím. - Přístup musí být udělen pouze osobě, která ho skutečně potřebuje pro výkon své práce/úkolů (princip „musím vědět") - Měl by se realizovat proces formální registrace a zrušení registrace uživatelů, aby bylo možné přiřadit přístupová práva ke správě osobních údajů.
	Počet úložišť osobních údajů (databáze, soubory, kopie, archívy) by měl být udržován na absolutním minimu, aby nedošlo ke zbytečné duplicitě. Místo duplicity by se měla dát přednost pseudonymizované databázi, která vyhledává v hlavních úložištích specifické osobní údaje, pokud a když je to nutné.
	Viditelnost osobních údajů musí být omezena na pouhý soubor informací, které jsou nutné pro jednotlivé zpracovatelské činnosti. Uživatelům by neměla být k dispozici žádná osobní data, která nepotřebují.
ZAREGISTROVÁNÍ A MONITOROVÁNÍ	Přístup do produkčních prostředí obsahujících osobní údaje, a pokud je technicky možný přístup k osobním údajům, by měl být monitorován a zaregistrován, aby mohlo být přesně zaznamenáno spojení mezi přístupem a jednotlivým uživatelem, který se dostal do osobních údajů
	V případě nutnosti a/nebo na žádost regulátora má Správce osobních údajů právo získat protokoly od Zpracovatele dat třetí strany nebo poskytovatele cloudu zpracovávajících osobní údaje jeho jménem.
	Měly by být jasně stanoveny odpovědnosti a povinnosti zaměstnanců ohledně důvěrnosti osobních údajů, které budou platit i po ukončení nebo změně zaměstnaneckého poměru.
	Osobní údaje se nesmí kopírovat na výměnné nosiče s výjimkou těch médií, které jsou Zpracovatelem výslovně schváleny pro specifické úkoly.
ZÁMĚRNÁ OCHRANA DAT	Procesy a nástroje pro Secure Software Development Lifecycle (SDLC) musí být integrovány s řádnou bezpečnostní kontrolou a požadavky, aby se zajistilo, že nové ICT softwarové aplikace jsou navrženy a vyvíjeny tak, že berou v úvahu požadavky na bezpečnost.

	Procesy změnového řízení ICT musí být integrovány s příslušnou bezpečnostní kontrolou a požadavky, aby se zajistila trvalá ochrana existujícího softwaru/aplikací ICT v případě změny.
OZNÁMENÍ O PORUŠENÍ OSOBNÍCH ÚDAJŮ	Zpracovatel je povinen vytvořit a vést evidence porušení ochrany osobních údajů.