**SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ**

**č. Klienta S-0047/00067539/2021**

podle čl. 28 Nařízení Evropského parlamentu a Rady (EÚ) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, kterým se zrušuje směrnice 95/46/ES v platném znění (dále jen „Nařízení“) mezi:

|  |  |
| --- | --- |
| **Innovatrics, s.r.o.**Sídlo: Rybná 716/24, Staré Město, 110 00 Praha 1IČO: 283 96 847DIČ: CZ28396847 Zápis: v obchodním rejstříku Městského soudu v Praze, oddíl C, vložka číslo 138595Jednající: Matúš Kapusta, jednatel (dále jen „**Innovatrics**“ nebo „**Zprostředkovatel**“)Kontaktní osoba pro účely ochrany osobních údajů: xxxxxx xxxxxxxxxxx tel.: xxxxxxxxxxxxxxxxxE-mail pro účely této Smlouvy: xxxxxxxxxxxxxx | **Oblastní muzeum Praha - východ, příspěvková organizace**Sídlo: Masarykovo náměstí 97/3, Brandýs nad Labem, 250 01 Brandýs nad Labem-Stará BoleslavIČO: 00067539DIČ: CZ00067539 – neplátce DPHZápis: Pr 895 vedená u Městského soudu v PrazeJednající: Ing. VLASTISLAV JANÍK, ředitel(dále jen “**Klient**” nebo **“Provozovatel“**)Kontaktní osoba pro účely ochrany osobních údajů: tel.: xxxxxxxxxxxxxxxxE-mail pro účely této Smlouvy: xxxxxxxxxxxxxxxxxxxxxxx |

# Preambule

Dne 9. 11. 2021 smluvní strany uzavřely Smlouvu na dodávku a servis docházkového systému FINGERA (dále jen „Smlouva na Systém FINGERA“), na základě které Innovatrics dodal Klientovi docházkový systém FINGERA a zavázal se poskytovat Klientovi servisní služby.

Klient využívá verzi Systému FINGERA, která jako uložiště údajů využívá cloudové

služby vzdálených serverů a datových úložišť (cloudová platforma).

Innovatrics a Klient se v souladu se Článkem 28 Nařízení dohodli na pověření Innovatricsu jako Zprostředkovatele, který bude zpracovávat osobní údaje jménem Klienta jako Provozovatele, a to podle podmínek uvedených v této Smlouvě.

# Předmět, povaha, účel, doba a rozsah zpracovávání

1. Innovatrics poskytne Klientovi cloudový server pro Systém FINGERA, jehož technická specifikace je uvedená v Příloze č. 1 k této Smlouvě.
2. Klient bere na vědomí bezpečnostní opatření, které za účelem ochrany osobních údajů přijal poskytovatel cloudové služby, a které jsou uvedené v Příloze č. 2 této Smlouvy.
3. Provozovatel tímto pověřuje Zprostředkovatele zpracováním osobních údajů zaměstnanců Provozovatele (dále je „dotčené osoby“) za podmínek stanovených dále v této Smlouvě.
4. Vlastníkem osobních údajů dotčených osob je Provozovatel.
5. Zodpovědnosti Provozovatele:
	1. Pro účely ochrany osobních údajů se strany dohodly, že Klient jako provozovatel je zodpovědný zejména za dodržování základních zásad zpracovávání údajů, definování účelu zpracovávání, za zabezpečení zákonnosti a přiměřenosti zpracovávání, minimalizaci zpracovávání údajů, použití případné pseudonymizace, za splnění veškerých povinností vůči dotčeným osobám (informační povinnost, souhlas), přijetí vlastních bezpečnostních opatření, jakož i za splnění případných povinností vyplývajících ze čl. 35 Nařízení.
	2. Klient zodpovídá za všechny úkony a bezpečnosti při uploadovaní osobních údajů do cloudového řešení Systému FINGERA, za jejich změnu, aktualizaci i vymazání v souladu s právními předpisy a vlastními bezpečnostními předpisy a pravidly. Systém FINGERA automaticky zabezpečuje šifrování při uploadu a přenosu osobních údajů do cloudového úložiště.
	3. Klient zodpovídá za to, kterým osobám a v jakém rozsahu udělí přístupová práva k Systému FINGERA, a k jednotlivým modulům případně Klientem objednaných, a též za dodržování vlastních bezpečnostních opatření při přistupovaní k Systému FINGERA (diskrétnost hesel, dodržování stanovených omezení v rámci úrovně příslušného oprávnění apod.).
	4. Klient je zodpovědný za včasnou úhradu příslušných odměn Zprostředkovateli za poskytování služeb k Systému FINGERA podle Smlouvy na Systém FINGERA (tzv. RUP). Klient bere na vědomí oprávnění Zprostředkovatele pozastavit poskytování služeb spojených se Systémem FINGERA, včetně omezení přístupu k němu resp. možnost ukončení Smlouvy na Systém FINGERA v případě prodlení Klienta s úhradou splatných závazků ve smyslu Smlouvy na Systém FINGERA.
6. **Zodpovědnosti Zprostředkovatele**
	1. Innovatrics **zprostředkovává** **pro Klienta cloudové úložiště**, do kterého bude Klient ukládat a v něm uchovávat osobní údaje související s evidováním docházky svých zaměstnanců, resp. osob oprávněných vstupovat do prostorů Klienta (dále společně jen „zaměstnanci“), zejména:
		1. identifikační údaje zaměstnanců Klienta a jejich pracovní pozice
		2. ID zaměstnance Klienta,
		3. čas přístupu k terminálu,
		4. důvod přístupu k terminálu,
		5. číslo RFID karty (při kartových modulech)
		6. číselný vektor získaný matematickým zpracováním otisků prstů resp. tváře (v případě evidence na báze biometrie), obrázek otisku prstu rev. biometrická fotografie tváře se neukládá, je použitá pouze v procesu zpracovávání za účelem získání číselného vektoru a následně je hned automaticky zlikvidovaná;
		7. výsledky zpracování údajů vytvořené systémem FINGERA;
		8. informace o schválení/neschválení docházky resp. absence a jejího důvodu (zejména při schvalovacích modulech Systému FINGERA);
		9. informace o osobách oprávněných používat systém FINGERA a úroveň jejich oprávnění;
		10. další údaje vložené samotným Klientem na uložiště.
		11. další údaje vložené uživatelem mobilní aplikace FINGERA na uložiště.

O obsahu a rozsahu uložených údajů rozhoduje výlučně Klient; v cloudovém uložišti se však automaticky z bezpečnostních důvodů ukládající údaje o činnosti v systému (tzv. logy).

* 1. Z titulu zprostředkování cloudového prostoru může mít Zprostředkovatel pasivní přístup k údajům uloženým v tomto úložišti, nevykonává však s nimi žádné operace bez zvláštního pokynu Klienta.
	2. Innovatrics k osobním údajům Klienta nepřistupuje, jelikož přístup do systému je chráněný heslem nebo jiným zabezpečením zvoleným samotným Klientem a údaje v něm uložené jsou šifrované.
	3. S výjimkou případů, pokud to vyžaduje právo EÚ nebo české právní předpisy, k osobním údajům může Zprostředkovatel přistupovat **pouze na pokyn Klienta a za jeho součinnosti**, a to pro účely poskytovaní servisních služeb podle Smlouvy na Systém Fingera, zejména pokud bude potřebné provést v systému servisní zásah. Povolenými operacemi v takovémto případě jsou:
		1. prohlížení
		2. uspořádávání
		3. přeskupování
		4. změna pouze na zvláštní pokyn Klienta
		5. vymazání pouze na zvláštní pokyn Klienta (s výhradou podle čl. II bod 8 této Smlouvy).

# Povinnosti zprostředkovatele

1. Zprostředkovatel se zavazuje v souvislosti s plněním svých povinností vyplývajících z této Smlouvy

a) dodržovat platné právní předpisy na ochranu osobních údajů - zejména Nařízení, platný zákon o ochraně osobních údajů a písemné pokyny Provozovatele;

b) plnit předmět této Smlouvy jen prostřednictvím řádných a prokazatelně poučených nebo vyškolených oprávněných osob pro účel plnění předmětu této Smlouvy;

c) přistupovat k osobním údajům výlučně za účelem plnění této Smlouvy nebo Smlouvy na Systém Fingera a jen v rozsahu nezbytném na jejich plnění,

d) pokud všeobecné závazné právní předpisy nebo tato Smlouva neustanovuje jinak, osobní údaje, se kterými se dostal do styku v souvislosti s realizací této Smlouvy nezveřejňovat, neposkytovat a nezpřístupňovat třetím stranám;

e) zachovávat mlčenlivost a zabezpečit důvěrnost při přístupu k údajům, a to i po skončení této Smlouvy resp. po skončení poskytovaní služeb;

f) nevyhotovovat kopie jakýchkoliv osobních údajů, nedělat z nich odpisy;

g) poučit zaměstnance nebo jiné osoby, které přijdou nebo můžou přijít do styku s osobními údaji, o povinnosti zachovávat mlčenlivost a důvěrnost osobních údajů jako i o jiných povinnostech souvisejících s přístupem k osobním údajům, o zodpovědnosti za jejich porušení, a to všechno před pověřením těchto osob na uskutečnění operace s osobními údaji;

h) informovat Provozovatele o skutečnostech zabraňujících plnění povinností Zprostředkovatele podle této Smlouvy, jako i o jakémkoliv porušení ochrany osobních údajů, o kterém se dozví;

i) bezodkladně informovat Provozovatele, pokud se podle jeho názoru pokynem Provozovatele porušuje Nařízení nebo zákon o ochraně osobních údajů;

j) na základě písemné žádosti Provozovatele pomáhat Provozovateli při posouzení vlivu na ochranu osobních údajů a při předcházející konzultaci s příslušným úřadem na ochranu osobních údajů, pokud se toto posouzení vlivu bude uplatňovat, a pokud se bude týkat zpracovatelských operací zabezpečovaných Zprostředkovatelem podle této Smlouvy.

2. Zprostředkovatel s přihlédnutím na charakter služby, kterou Provozovateli poskytuje, pomáhá Provozovateli vhodnými technickými a organizačnými opatřeními při plnění jeho povinností reagovat na žádosti o výkon práv dotčené osoby. V případě, že přímo Zprostředkovatel obdrží žádost dotčené osoby, která si uplatňuje vůči Provozovateli svá práva podle článku 15 až 22 Nařízení (např. právo na přístup k údajům, právo na vymazání nebo opravu osobních údajů), Zprostředkovatel bezodkladně, nejpozději však do 3 pracovních dní od jejího přijetí, takovou to žádost zašle Provozovateli na emailovou adresu uvedenou v záhlaví této Smlouvy. Zprostředkovatel není oprávněný vyřizovat žádost dotčené osoby.

3. Zprostředkovatel na základě písemné žádosti (včetně e-mailové) pomáhá Provozovateli zabezpečit plnění povinností podle článku 32 až 36. Nařízení s přihlédnutím na povahu zpracování, které Zprostředkovatel zabezpečuje a informace dostupné Zprostředkovateli.

4. Zprostředkovatel poskytne Provozovateli všechny informace potřebné na prokázání splnění povinností mu stanovených v této Smlouvě a umožní kontrolovat plnění jeho povinností Provozovatelem nebo auditorem, kterého pověřil Provozovatel, a při těchto kontrolách spolupracuje. Provozovatel a auditoři Provozovatele jsou povinni při výkonu auditu postupovat tak, aby nedošlo k ohrožení nebo přerušení provozu Zprostředkovatele nebo jeho informačního systému, k úniku, poškození nebo ztrátě dat nebo k jiné škodě. Zprostředkovatel je oprávněný prokázat dodržování svých povinností resp. účinnost bezpečnostních opatření i audity, ověření či vyhlášení třetí odborné osoby, kterou může on nebo jeho subdodavatel disponovat.

5. Zprostředkovatel je povinný s přihlédnutím na charakter činnosti, kterou pro Klienta vykonává a operace, kterými je pověřený, přijmout vhodné a přiměřené technické, organizační a personální opatření na zabezpečení ochrany osobních údajů před jejich poškozením, náhodným zničením, ztrátou, změnou, neoprávněným přístupem a zpřístupněním, poskytnutím nebo zveřejněním apod., jako i před jakýmkoliv nepřípustnými způsoby zpracování. Zprostředkovatel na tento účel přijal zejména následující opatření:

(i) poučení vlastních oprávněných osob o manipulaci s osobními údaji a informování těchto osob o přesném popisu jednotlivých operací s osobními údaji, aby se zabránilo náhodnému nebo neoprávněnému zničení, ztrátě, záměně, zpřístupnění osobních údajů nebo jakýmkoli neoprávněným formám zpracovaní osobních údajů; na požádání Provozovatele Zprostředkovatel tyto poučení předloží Provozovateli;

(ii) poučení vlastních oprávněných osob o povinnosti mlčenlivosti, aby se zabezpečila důvěrnost osobních údajů; na požádání Provozovatele Zprostředkovatel tyto poučení předloží Provozovateli;

(iii) pravidelné přeškolováni oprávněných osob a aktualizace vlastních bezpečnostních opatření;

(iv) disciplinární opatření pro případ porušení povinností na úseku ochrany osobních údajů;

(v) organizační procesy pro zpracování žádostí dotčených osob o uplatnění jejich práv podle Nařízení a oznamování bezpečnostních incidentů;

(vi) umístnění prostředků zpracovávání na území Evropské unie.

6. Zprostředkovatel je oprávněný začít zpracovávat osobní údaje podle této Smlouvy dnem nabytí platnosti a účinnosti této Smlouvy. Oprávnění Zprostředkovatele zpracovávat osobní údaje podle této Smlouvy trvá do ukončení Smlouvy na Systém FINGERA.

7. Zálohovaní údajů uložených v Systému FINGERA je řešené samostatným zálohovacím cloudovým serverem, přičemž komunikace cloudového serveru pro Systém FINGERA a zálohovacího uložiště je šifrovaná; zálohy jsou vytvářené denně a jsou udržování po dobu 30 dní, následně budou vymazané. Přístup k zálohovaným údajům mají jen řádně poučené oprávněné osoby Zprostředkovatele.

8. Po skončení Smlouvy na Systém FINGERA bude Zprostředkovatel udržovat zálohu údajů uložených v cloudu Provozovatele pro Systém FINGERA po dobu 30 dní ode dne skončení platnosti a účinnosti Smlouvy na Systém FINGERA. Po uplynutí 30 dní od skončení Smlouvy na Systém FINGERA Zprostředkovatel zruší cloudový server pro Systém FINGERA Provozovatele, čímž dojde k vymazání veškerých údajů uložených Provozovatelem na cloudovém serveru pro Systém FINGERA. Provozovatel ve výše uvedené lhůtě 30 dní na vlastní náklady a zodpovědnost zabezpečí přesun údajů uložených v cloudovém serveru pro Systém FINGERA do vlastních resp. jiných systémů.

# zvláštní ustanovení

* + - 1. Provozovatel a Zprostředkovatel se ve Smlouvě na Systém FINGERA dohodli na použití cloudového řešení systému FINGERA s tím, že provozovatel cloudu je **subdodavatelem** podle Nařízení. Identifikace provozovatele cloudu a jím poskytované záruky a bezpečnostní opatření jsou uvedené v  **Příloze č. 2** této Smlouvy. Prostředky zpracovávání (datové uložiště) se nacházejí v Evropské unii. Provozovatel souhlasí s využitím subdodavatele tak, jak je uvedené v bodě 1 tohoto článku a v Příloze č. 1. a 2. Zprostředkovatel je povinný informovat Provozovatele o jakýchkoli zamýšlených změnách v osobě subdodavatele. Provozovateli se tudíž umožní namítat vůči takovým to změnám. Provozovatel při výběru Zprostředkovatele a odsouhlasení subdodavatele má za to, že Zprostředkovatel a subdodavatel poskytují dostatečné záruky na to, že jsou přijaté přiměřené technické a organizační opatření tak, aby zpracování splnilo požadavky Nařízení, a aby se zabezpečila ochrana práv dotčených osob.
			2. Pokud si Klient objednal nebo v buducnosti objedná **Mobilní aplikaci FINGERA**, Klient bere na vědomí, že tato aplikace představuje komunikační nástroj se Systémem FINGERA a aplikace jako taková neuchovává žádné z osobních údajů uvedených v čl. I bod 6 této Smlouvy, pouze k nim zabezpečuje přístup ze strany uživatelů oprávněných ze strany Klienta používat mobilní aplikaci FINGERA. Mobilní aplikace FINEGRA není určená pro osoby mladší než 16 let. Za správnost a aktuálnost údajů uploadovaných do Systému FINGERA zodpovídá uživatel mobilní aplikace FINGERA. V mobilní aplikaci FINGERA jsou uchovávané informace o uživatelském menu a hesle k aplikaci, které zadává konkrétnímu uživateli sám Klient, aplikaci též zpracovává IP adresu zařízení, z kterého se uživatel do aplikace připojuje, UUID číslo, typ používaného mobilního zařízení, typ operačního systému, typ a verze mobilního prohlížeče, jako také čas stáhnutí/použití aplikace. Mobilní aplikace FINGERA nesleduje automaticky GPS polohu zařízení, tuto funkcionalitu si však uživatel zařízení může zapnout ve svém zařízení, v takovémto případě aplikace FINGERA zaznamená přibližnou GPS polohu zařízení v čase, kdy se aplikace používá (např. při zadaní příchodu do práce). Účelem zpracovávaní výše uvedených údajů je, zabezpečení splnění Smlouvy na Systém FINGERA, a zpracovávané údaje jsou nevyhnutelné na to, aby Innovatrics mohl službu mobilní aplikace FINGERA, kterou si Klient objednal, Klientovi poskytnout. Klient bere na vědomí, že další podmínky použití mobilní aplikace FINGERA včetně příslušné Privacy Policy můžou být uvedené přímo při downloadu či aktualizaci aplikace. Klient se zavazuje splnit informační povinnost vůči vlastním zaměstnancům resp. uživatelům mobilní aplikace FINGERA o podmínkách zpracovávání osobních údajů v mobilní aplikaci FINGERA a v Systému FINGERA.

# závěrečné ustanovení

* + - 1. Tato Smlouva a Smlouva na Systém FINGERA obsahují úplné pokyny Provozovatele Zprostředkovateli týkající se zpracovávání osobních údajů. Pokud Provozovatel vydá další pokyny, Zprostředkovatel ve smyslu čl. 28 odst. 3 písm. a) Nařízení požaduje, aby mu Provozovatel zaslal (minimálně e-mailem) tyto písemné pokyny ke zpracovávání osobních údajů na adresu uvedenou v záhlaví této Smlouvy.
			2. Smluvní strany se zavazují vzájemně se informovat o případné změně identifikačních/kontaktních údajů smluvních stran a kontaktních osob, a to minimálně formou e-mailu. Změna se bude považovat za účinnou doručením příslušného oznámení druhé straně.
			3. Neoddělitelnou součástí této Smlouvy jsou následující přílohy:

**Příloha č. 1** – Specifikace cloudového serveru pro Systém FINGERA;

**Příloha č. 2** – Identifikace provozovatele cloudu a jím poskytované záruky a bezpečnostní opatření.

* + - 1. Tato Smlouva nabývá platnost a účinnost dnem jejího podepsání oběma smluvními stranami.
			2. Smlouva je vyhotovená ve dvou originálech, jeden pro každou smluvní stranu.
			3. Smluvní strany prohlašují, že se s obsahem této Smlouvy a jejich příloh obeznámily, porozuměly jim a svůj souhlas s jejím obsahem vyjadřují vlastnoručními podpisy.

|  |  |  |
| --- | --- | --- |
| **Obchodní jméno** | **Oprávněná osoba** | **Město, datum a podpis** |
| **ZaInnovatrics, s.r.o.** | Matúš Kapusta | V Brně dne: Podpis:  |
| **Za** **Klienta** | Ing. Vlastislav Janík | V dne:Podpis:  |

**Příloha č. 1 – Specifikace Cloud Serveru**

Innovatrics poskytne Klientovi cloudový server pro systém FINGERA, jehož technická specifikace je následující:

* Amazon AWS t2.small (1CPU, 2GB RAM)

**Příloha č. 2**

Systém FINGERA je provozovaný na **cloudové platformě** společnosti Amazon Web Services, Inc., se sídlem Seattle, Washington, USA („AWS“), která je jedna z nejznámějších a nejstabilnějších globálně dostupných cloudových platforem.

Pro systém FINGERA jsou využívané služby Amazon EC2, S3 a RDS.

Bezpečnostní procesy přijaté AWS ke dni podpisu této smlouvy je možné najít na této stránce: <https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf>

Z hlediska GDPR poskytuje uvedená platforma hlavně garance, jejichž popis je možné najít na této stránce: <https://aws.amazon.com/compliance/gdpr-center/>.

Mezi základní garance patří zejména:

1. **Lokalizace dat v Evropské unii**

Vaše data budou uložená na serverech v Evropské unii a nebudou odtud přenášená na jiné místo.

1. **Dostupnost**

AWS se zavazuje, že použije komerčně přiměřené úsilí na to, aby zařazené produkty a služby byly k dispozici s měsíčním procentním uptime ve výši minimálně 99,99 % v každém měsíčním fakturačním cyklu. Více info na ([https:/aws.amazon.com/compute/sla/](https://aws.amazon.com/compute/sla/))

1. **Šifrování dat při přenosu a ukládání**

Při podpisu této smlouvy: šifrování uložených dát s AES256 (EBS/S3/Glacier/RDS)

Možnost volby vlastního šifrovacího klíče

1. **Monitoring a logging**

Umožňuje kontrolu toho, co se děje s uloženými daty, včetně toku dat.

1. **Kontrola přístupu včetně možnosti vícefaktorové autentifikace**
2. **Bezpečnost „by design“**
3. **Důvěrnost**
4. **Bezpečnost a Certifikace**

<https://aws.amazon.com/compliance/programs/>

Platforma AWS splňuje požadavky technických norem **ISO 27001, 27017 a taktéž 27018**, které jsou první mezinárodní normou zaměřenou na ochranu osobních údajů v cloudu. <https://aws.amazon.com/compliance/iso-27018-faqs/>.

1. V případě požadavků deklaruje AWS **připravenost umožnit klientům přístup ke zprávám nezávislých auditorů.**