DODATEK Č. 7

K RÁMCOVÉ SMLOUVĚ O ÚDRŽBĚ A VÝVOJI SOFTWARU

uzavřený podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů („**občanský zákoník**"), a podle 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) („**GDPR**")
(„**Dodatek**")

SMLUVNÍ STRANY

(1) **Mendelova univerzita v Brně**

sídlo Zemědělská 1665/1, 613 00 Brno, IČO: 62156489, zastoupená prof. Ing. Danuší Nerudovou, Ph.D., rektorkou

(„**Objednatel**)

a

(2) **IS4U, s.r.o.**

společnost založená a existující podle právního řádu České republiky, sídlo U vodárny 3032/2a, Královo Pole, 616 00 Brno, IČO: 29205336, zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 65487

(„**Poskytovatel**")

(Objednatel a Poskytovatel společně „**Strany**" nebo „**Smluvní strany**", a každý z nich samostatně „**Strana**" nebo „**Smluvní strana**")

PREAMBULE

(A) Strany uzavřely dne 11. 4. 2011 rámcovou smlouvu o údržbě a vývoji softwaru, na základě které Poskytovatel poskytuje Objednateli servisní služby pro podporu provozu Univerzitního informačního systému („**UIS**"), ve znění pozdějších dodatků („**Smlouva**").

(B) Vzhledem k tomu, že činnosti Zhotovitele v systému UIS vykonávané podle Smlouvy mohou zahrnovat operace zpracování osobních údajů, mají Strany zájem na základě tohoto Dodatku vymezit podmínky zpracování osobních údajů ve smyslu čl. 28 odst. 3 GDPR.

(C) Objednatel a Poskytovatel se zavazují, v souvislosti s tímto dodatkem k rámcové smlouvě, postupovat v souladu se Směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. K vyloučení všech pochybností smluvní strany prohlašují, že jsou jim známy účinky platného Obecného nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 (dále jen „Nařízení").

(D) Poskytovatel bere na vědomí, že se ve smyslu všech výše uvedených právních předpisů považuje a bude považovat za Zpracovatele osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi. Objednatel je a bude nadále považován za Správce osobních údajů, se všemi pro něj vyplývajícími důsledky a povinnostmi.

(E) Ustanovení o vzájemných povinnostech Objednatele jako Správce a Poskytovatele jako Zpracovatele při zpracování osobních údajů má za cíl zajistit, aby nedošlo k nezákonnému použití osobních údajů týkajících se Subjektů údajů ani k jejich předání do rukou neoprávněné třetí strany. Smluvní strany se dohodly na podmínkách zajištění odpovídajících opatření k zabezpečení

ochrany osobních údajů a základních práv a svobod Subjektů údajů při zpracování osobních údajů Zpracovatelem.

1. VÝKLAD DODATKU

1.1 Na základě tohoto Dodatku dochází k doplnění Smlouvy výhradně o smluvní ustanovení obsažená v tomto Dodatku týkající se zpracování osobních údajů. V ostatním zůstávají ustanovení Smlouvy nedotčena.

1.2 Tento Dodatek bude vykládán podle následujících pravidel:

(a) Odkazy na „**články**“ a „**přílohy**“ se vykládají jako odkazy na příslušné články a přílohy tohoto Dodatku.

(b) Odkazy na „**osobu**“ nebo „**strany**“ zahrnují jakoukoli fyzickou osobu, právnickou osobu, svěřenský fond, tiché společenství, vládu, stát, úřad veřejné správy, společný podnik, závod, sdružení nebo společenství (bez ohledu na to, zda má právní osobnost či nikoli).

(c) Odkazy na „**pracovní dny**“ se vykládají jako odkazy na jakýkoli den jiný než sobota, neděle a státní svátek v souladu s platnými právními předpisy České republiky.

(d) Pojmy vymezené v tomto Dodatku v množném čísle odkazují i na pojmy v jednotném čísle a naopak.

(e) Vedle právních ustanovení, jejichž uplatnění se tímto Dodatkem výslovně vylučuje, se pro účely tohoto Dodatku nepoužijí ani další ustanovení právních předpisů v rozsahu, v jakém jsou nahrazena jinými závazky Smluvních stran dle Smlouvy a tohoto Dodatku.

2. PŘEDMĚT DODATKU

2.1 Tento Dodatek upravuje vztahy mezi Objednatelem jakožto správcem osobních údajů a Poskytovatelem jakožto zpracovatelem osobních údajů při zpracování osobních údajů v UIS.

2.2 Na základě tohoto Dodatku Objednatel pověřuje Poskytovatele zpracováním osobních údajů ve vymezeném rozsahu a pro vymezené účely a pouze v mezích plnění povinností Poskytovatele podle Smlouvy a Poskytovatel pověření ke zpracování osobních údajů v plném rozsahu a za podmínek vymezených v tomto Dodatku přijímá.

3. VYMEZENÍ ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

3.1 Poskytovatel pro Objednatele na základě Smlouvy zpracovává osobní údaje v uvedeném rozsahu („**Osobní údaje**“):

Účel zpracování	**Rozsah osobních údajů**	**Zvláštní kategorie osobních údajů**	**Kategorie subjektů údajů**
poskytování servisních služeb pro podporu provozu UIS	osobní údaje obsažené v UIS	ne	studenti absolventi zaměstnanci bývalí zaměstnanci externí pracovníci uchazeči o studium
uložení dat v aplikaci	osobní údaje obsažené v UIS	ne	studenti absolventi

Účel zpracování	Rozsah osobních údajů	Zvláštní kategorie osobních údajů	Kategorie subjektů údajů
			zaměstnanci bývalí zaměstnanci externí pracovníci uchazeči o studium

3.2 Poskytovatel bude osobní údaje podle Smlouvy zpracovávat manuálně i automatizovaně.

3.3 Poskytovatel bude osobní údaje podle Smlouvy zpracovávat v elektronické podobě.

3.4 Poskytovatel se zavazuje osobní údaje zpracovávat s odbornou péčí.

4. ODMĚNA

4.1 Zpracování osobních údajů podle tohoto Dodatku je bezúplatné.

5. SAMOSTATNOST ZPRACOVATELE A POKYNY SPRÁVCE

5.1 Poskytovatel bude osobní údaje zpracovávat samostatně pro dosažení stanoveného účelu zpracování ve smyslu článku 3.1. a s vynaložením odborné péče samostatně rozhodovat o provedení jednotlivých úkonů v rámci zpracování osobních údajů, které je třeba v souladu s platnými právní předpisy vykonat.

5.2 V případě, že Poskytovatel od Objednatele obdrží v souvislosti s plněním Smlouvy instrukci, je ji vázán, ledaže je taková instrukce v rozporu s platnými právními předpisy.

5.3 Pokud nastane jakýkoliv případ, kdy Poskytovatel není pokynem Objednatele vázán, je o takové skutečnosti povinen Objednatele bez zbytečného odkladu informovat.

6. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

6.1 Poskytovatel se zavazuje, že bude Osobní údaje zpracovávat bezpečně a bude používat veškeré přiměřené bezpečností systémy a postupy obvyklé pro zpracování Osobních údajů.

6.2 Strany si mohou Osobní údaje předávat pouze v rámci UIS.

6.3 Poskytovatel se zavazuje bránit, případně podniknout veškeré možné kroky k zamezení neoprávněnému přístupu, kopírování, úpravě, ukládání, reprodukci, zveřejnění nebo distribuci Osobních údajů.

6.4 Poskytovatel prohlašuje, že přijal a dodržuje technická a organizační opatření ochrany osobních údajů vymezená v **příloze č. 1** Smlouvy.

6.5 V případě, že kterákoliv ze Stran zjistí, že:

(a) došlo k neoprávněnému či nezákonnému zpracování Osobních údajů;

(b) došlo ke ztrátě, poškození nebo zničení či jinému způsobu znehodnocení Osobních údajů;

(c) nastal případ jakéhokoliv porušení zabezpečení Osobních údajů, které s odbornou péčí vyhodnotí Strana jako dostatečně závažné a odůvodňující ohlášení u Úřadu pro ochranu osobních údajů ve smyslu článku 33 GDPR („**Porušení zabezpečení**“);

je povinna toto bez zbytečného odkladu druhé Straně a poskytnout maximální součinnost k nápravě.

7. ŘETĚZENÍ ZPRACOVATELŮ

7.1 Objednatel souhlasí s využitím dalších zpracovatelů podle volby Poskytovatele pro dílčí zpracování osobních údajů podle Smlouvy. Další zpracovatelé musí být smluvně vázáni

veškerými povinnostmi při zpracování osobních údajů podle této Smlouvy (resp. tohoto Dodatku).

7.2 Poskytovatel je povinen na žádost Objednatele neprodleně předložit kompletní seznam zpracovatelů.

8. PROHLÁŠENÍ

8.1 Poskytovatel prohlašuje a Objednateli zaručuje, že

(a) splňuje veškeré zákonné povinnosti, které pro něho z GDPR a jiných právních předpisů vyplývají;

(b) bude po celou dobu trvání Smlouvy zpracovávat osobní údaje pro Objednatele v souladu s českým právním řádem a zejména v souladu s GDPR;

(c) bude po celou dobu trvání Smlouvy vést řádné záznamy o činnostech zpracování Osobních údajů ve smyslu čl.30 odst. 2 GDPR;

(d) bude podle Smlouvy zpracovávat pouze osobní údaje v rozsahu a pro účel stanoveným Smlouvou.

8.2 Objednatel prohlašuje a Poskytovateli zaručuje, že:

(a) v době předání Osobních údajů jsou Osobní údaje aktuální a existuje platný zákonný titul pro jejich zpracování;

(b) splňuje veškeré zákonné povinnosti, které pro něho jako správce osobních údajů z GDPR a jiných právních předpisů vyplývají, zejména, nikoliv však výlučně, plní ve vztahu k subjektům údajů informační povinnost a vede záznamy o činnostech zpracování;

(c) není si vědom žádného rizika porušení platných právních předpisů v souvislosti s dosavadním zpracování Osobních údajů.

8.3 Pokud kterékoliv Straně vznikne v souvislosti s porušením povinností druhé Strany týkající se zpracování osobních údajů podle Smlouvy a platných právních předpisů škoda, Strana se zavazuje uhradit druhé Straně škodu v plném rozsahu.

9. SOUČINNOST

9.1 Smluvní strany se zavazují poskytnout si vzájemně potřebnou součinnost, kterou po nich lze spravedlivě požadovat, zejména při:

(a) zavádění a udržování vhodných technických a organizačních opatření k zabezpečení osobních údajů;

(b) ohlašování případů Porušení zabezpečení;

(c) posuzování vlivu zpracování na ochranu osobních údajů, pokud Objednatel rozhodne, že je posouzení vlivu zpracování ve smyslu čl. 35 GDPR nezbytné provést;

(d) plnění povinností předchozí konzultace s Úřadem na ochranu osobních údajů ve smyslu čl. 36 GDPR, pokud k tomu nastanou zákonné podmínky.

9.2 Objednatel bere na vědomí, že služby Poskytovatele podle odst. 9.1 písm. c) a d) jsou placenými službami, které je třeba u Poskytovatele objednat.

9.3 Poskytovatel se zavazuje na výzvu Objednatele poskytnout ve stanovené lhůtě, která nesmí být kratší než tři (3) a delší než deset (10) pracovních dnů, nezbytné informace potřebné k doložení, že zpracování osobních údajů podle Smlouvy je prováděno v souladu s platnými právními předpisy.

9.4 Poskytovatel se zavazuje umožnit Objednateli a jeho zástupcům na jeho výzvu v přiměřené lhůtě, která nesmí být kratší než tři (3) pracovní dny:

(a) přístup k záznamům o činnostech zpracování Osobních údajů ve smyslu čl. 30 odst. 2 GDPR;

(b) provést kontrolu technických a organizačních opatření Osobních údajů za předpokladu, že se kontroly osobně zúčastní statutární zástupce Objednatele;

(c) provést osobní kontrolu jednotlivých operací zpracování Osobních údajů za předpokladu, že se kontroly osobně zúčastní statutární zástupce Objednatele.

10. DOBA TRVÁNÍ ZPRACOVÁNÍ

10.1 Strany se dohodly, že Poskytovatel bude zpracovávat osobní údaje podle Smlouvy a tohoto Dodatku po dobu trvání Smlouvy.

10.2 Každá ze Stran je oprávněna odstoupit od Smlouvy nad rámec ustanovení Smlouvy také v případě, že:

(a) Strana neposkytuje součinnost druhé Straně ani na základě písemného oznámení druhé Strany v dodatečné lhůtě, která nesmí být kratší než deset (10) dní;

(b) jakékoliv prohlášení Stran učiněné v článku 8 se ukáže jako nepravdivé nebo neúplné a závadný stav neodstraní ani na základě písemného oznámení druhé Strany v dodatečné lhůtě, která nesmí být kratší než deset (10) dní.

10.3 Odstoupením se Smlouva ruší s účinky *ex nunc*, tj. do budoucna, a Strany si nejsou povinny vracet plnění poskytnutá před účinností odstoupení.

10.4 Při ukončení zpracování osobních údajů podle Smlouvy se Poskytovatel zavazuje:

(a) poskytnout Objednateli veškeré dokumenty vztahující se ke zpracování Osobních údajů podle jeho instrukcí, zejména záznamy o činnostech zpracování vedené podle čl. 30 odst. 2 GDPR;

(b) nevratně vymazat veškeré existující kopie Osobních údajů, ledaže to nedovolují platné právní předpisy.

11. MLČENLIVOST

11.1 Smluvní strany prohlašují, že všechny údaje, informace a skutečnosti související se zpracováním Osobních údajů podle Smlouvy, jsou důvěrnými informacemi („**Důvěrné informace**“). Strany se zavazují, že Důvěrné informace neposkytnou třetí straně a nepoužijí je k jinému účelu než pro plnění Smlouvy, s výjimkou:

(a) svých poradců vázaných povinností mlčenlivosti ve stejném rozsahu jako Strany, nebo

(b) příslušných státních a jiných správních úřadů a soudů, pokud jsou strany povinny podle obecně závazných předpisů jim tyto informace poskytnout, nebo

(c) informací, které jsou nebo se stanou veřejně dostupnými jinak než porušením této Smlouvy.

11.2 Poskytovatel se zavazuje k povinnosti mlčenlivosti v rozsahu tohoto článku Dodatku zavázat své zaměstnance a jiné spolupracovníky ve smluvním vztahu se Poskytovatelem, kteří vykonávají činnosti související se Smlouvou a jejím plněním a poskytováním služeb na základě Smlouvy.

11.3 Povinnost mlčenlivosti trvá i po zániku Smlouvy. Strany nejsou oprávněny po skončení Smlouvy důvěrné informace ve smyslu této Smlouvy jakýmkoliv způsobem rozšiřovat či využít či umožnit jejich šíření či využití.

12. ZÁVĚREČNÁ UJEDNÁNÍ

12.1 Ostatní ujednání Smlouvy zůstávají tímto Dodatkem nedotčena.

12.2 Tento Dodatek je vyhotoven ve čtyřech stejnopisech v českém jazyce. Každá Strana obdrží po dvou stejnopisech.

12.3 Tento Dodatek nabývá platnosti a účinnosti dnem uveřejnění v Registru smluv

12.4 Nedílnou součást tohoto Dodatku tvoří:

Příloha č. 1 Seznam přijatých technických a organizačních opatření k ochraně osobních údajů

Mendelova univerzita v Brně	**IS4U, s.r.o.**
Místo:	Místo: Brno
Datum:	Datum: 24. 5. 2018
_____	_____
Jméno: prof. Ing. Danuše Nerudová, Ph.D.	Jméno: Ing. Tomáš Majer
Funkce: rektorka	Funkce: jednatel

PŘÍLOHA 1

SEZNAM PŘIJATÝCH TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K OCHRANĚ OSOBNÍCH ÚDAJŮ

a. fyzická bezpečnost:

Opatření	**ANO/NE**
mechanické zábranné prostředky	ANO
zařízení elektrické zabezpečovací signalizace	ANO
prostředky omezující působení požárů	ANO
prostředky omezující působení projevů živelních událostí	ANO
systémy pro kontrolu vstupu	ANO
kamerové systémy	ANO
zařízení pro zajištění ochrany před selháním dodávky elektrického napájení	ANO
zařízení pro zajištění optimálních provozních podmínek	ANO

b. nástroje pro ochranu integrity komunikačních sítí:

Opatření	**ANO/NE**	**Popis**
řízení bezpečného přístupu mezi vnější a vnitřní sítí	ANO	Firewall firemní, dílčí firewally serverů
zařízení elektrické zabezpečovací signalizace	ANO	V rámci budovy
segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí	ANO	Segment zákaznických serverů, segment firemních serverů, segment zaměstnanců, segment návštěvníků, striktně odděleno
vzdálený přístup, vzdálená správa nebo pro přístup pomocí bezdrátových technologií	ANO	Individuální povolení pro stanice vývojářů, kontrolní vstupní bod pro vzdálený vývoj, WiFi přístup jen návštěvnická oblast, jinak WiFi přístup vyžaduje firemní zařízení
opatření pro odstranění nebo blokování přenášených dat	ANO	Není možné jednoduše přenášet soubory z interních serverů pryč, několikastupňová ochrana

c. nástroje pro ověřování identity uživatelů:

Opatření	Popis
požadavky na heslo:	ANO
doba platnosti hesla:	omezená
deaktivace po stanovené době nečinnosti:	ANO
důsledky zadání nesprávného hesla:	Blokace po neúspěšných pokusech

d. nástroje pro řízení přístupových oprávnění:

Nástroje pro řízení přístupových oprávnění	ANO/NE
ActiveDirectory	ANO
Radius	ANO
Interní systém oprávnění HD	ANO
Interní systém oprávnění UIS	ANO

e. nástroje pro ochranu před škodlivým kódem:

Opatření	Popis
Ověření a kontrola:	Na stanicích povinně antivirus, centrální zálohování, na e-mailu antispam Vlastní nástroje pro detekci a korekci škodlivého kódu při vývoji
Ověření a kontrola komunikace mezi vnitřní sítí a vnější sítí:	ANO, omezená
Ověření a kontrola serverů a sdílených datových úložišť:	NE, pouze zprostředkovaně
Ověření a kontrola pracovních stanic	ANO, po schválení konkrétnímu pracovníkovi

f. nástroje pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů:

Opatření	Popis
Sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti	ANO
Původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti	ANO u systémů zpracovávajících osobní údaje
Ochrana získaných informací před neoprávněným čtením nebo změnou:	ANO, omezení okruhu osob s přístupu k datům, omezení možnosti přenášet tyto údaje mimo prostor firmy, vše u systémů zpracovávajících osobní údaje

Ověření a kontrola pracovních stanic	ANO, po schválení konkrétnímu pracovníkovi

Logování:

	ANO / NE	Systém:
přihlášení a odhlášení uživatelů a administrátorů	ANO	Syslog, UIS
činnosti provedené administrátory	ANO	Syslog, UIS
činnosti vedoucí ke změně přístupových oprávnění	ANO	AD, Radius, HD, UIS wlog
neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů	ANO	Bezpečnostní vrstva UIS
zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému	ANO	Evidence v dokumentaci serverů, zásadní informace UIS
automatická varovná nebo chybová hlášení technických aktiv	ANO	UIS bugsystém
přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností	ANO	Syslog, UIS bugsystém, UIS wlog
použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení	ANO	UIS modul „bezpečnostní politiky“

g. nástroje pro detekci bezpečnostních událostí:

Allerting	ANO	UIS bugsystém na aplikační úrovni Monitorovací systém nagios, ganglia na servery a komunikační prvky

h. aplikační bezpečnost:

Bezpečnostní testy zranitelnosti aplikací	ANO	pravidelné testy rootkity
Ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou	ANO	pravidelné penetrační testy interními zdroji, v minulém roce 1x testováno CESNET FLAB (forenzní laboratoř)
Ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním	ANO	ochranná vrstva triggerů v databázi UIS, business logika oddělena od vývojářů

i. kryptografické prostředky:

šifrované diskové kapacity, šifrované komunikační protokoly	ANO	x

j. nástroje pro zajišťování úrovně dostupnosti informací:
Zálohování:

Zálohování	ANO	Trvalé zálohování serverů rsync, periodické zálohování pracovních stanic na centrální zálohovací server, distaster recovery plán, periodické prověřování obnovitelnosti záloh serverů automaticky 1x týdně u všech zákazníků, monitoring Nagios a Ganglia

k. nástroje k auditingu:

Syslog, UIS wlog, UIS auditní vrstva