



DODATEK Č. 10

KE SMLOUVĚ O DÍLO

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) **Slovenská technická univerzita v Bratislavě**

Sídlo: Vazovova 5, 812 43 Bratislava, Slovenská republika

IČO: 003 97 687

DIČ SK: 20 20 84 52 55

IČ DPH SK 20 20 84 52 55

Statutární orgán: prof. Ing. Robert Redhammer, PhD., rektor

Kontaktní osoba: Ing. Marian Ďurkovič, riaditeľ CVT STU

Bankovní spojení: Štátna pokladnica, Radlinského 32, Bratislava 15 Slovenská republika

SWIFT: SPSRSKBAXXX

IBAN: SK79 8180 0000 0070 0024 0727

Právní forma: verejnoprávna inštitúcia zriadená zákonom č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov ako verejná vysoká škola

(„Objednatel“)

a

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

Sídlo: U Vodárny 2a, 616 00 Brno, Česká republika

IČO: 292 05 336

DIČ: CZ 292 05 336

Bankovní spojení: Raiffeisenbank a.s.

Číslo účtu: 5128744001/5500

IBAN: CZ90 5500 0000 0051 2874 4001

SWIFT: RZBCCZPP

Právní forma: Společnost je vedena u rejstříkového soudu v Brně pod spisovou značkou C 65487

Kontaktní osoba: Ing. Tomáš Majer, jednatel

(„Zhotovitel“)(Objednatel a Zhotovitel společně „Strany“ nebo „Smluvní strany“, a každý z nich samostatně „Strana“ nebo „Smluvní strana“)

PREAMBULE

- (A) Strany, resp. Objednatel a právní předchůdce Zhotovitele, Mendelova zemědělská a lesnická univerzita v Brně, která svá práva a povinnosti dne 1. 1. 2011 převedla na Zhotovitele, uzavřely dne 1. 6. 2007 smlouvu o dílo, na základě které Zhotovitel poskytuje Objednateli servisní služby pro podporu provozu Univerzitního informačního systému („AIS“), ve znění pozdějších dodatků („Smlouva“).
- (B) Vzhledem k tomu, že činnosti Zhotovitele v systému AIS 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.

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 Zhotovitelem jakožto zpracovatelem osobních údajů při zpracování osobních údajů v AIS.
- 2.2 Na základě tohoto Dodatku Objednatel pověřuje Zhotovitele zpracováním osobních údajů ve vymezeném rozsahu a pro vymezené účely a pouze v mezích plnění povinností Zhotovitele podle Smlouvy a Zhotovitel pověření ke zpracování osobních údajů v plném rozsahu a za podmínek vymezených v tomto Dodatku přijímá.

3. VYMEZENÍ ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

- 3.1 Zhotovitel 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 AIS	osobní údaje obsažené v AIS	ne	uchazeči o studium studenti absolventi

Účel zpracování	Rozsah osobních údajů	Zvláštní kategorie osobních údajů	Kategorie subjektů údajů
			zaměstnanci bývalí zaměstnanci externí pracovníci
uložení dat v aplikaci	osobní údaje obsažené v AIS	ne	uchazeči o studium studenti absolventi zaměstnanci bývalí zaměstnanci externí pracovníci

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

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

3.4 Zhotovitel 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 Zhotovitel 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 právními předpisy vykonat.

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

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

6. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

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

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

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

6.4 Zhotovitel 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 narušení 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 („Narušení 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 Zhotovitele pro dílčí zpracování osobních údajů podle Smlouvy. Další zpracovatelé musí být vázáni veškerými povinnostmi při zpracování osobních údajů podle této Smlouvy (resp. tohoto Dodatku).

8. PROHLÁŠENÍ

- 8.1 Zhotovitel 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, 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 Zhotoviteli 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 Narušení 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 Zhotovitele podle čl. 9.1 písm. c) a d) jsou placenými službami, které je třeba u Zhotovitele objednat.

- 9.3 Zhotovitel se zavazuje na výzvu Objednatele poskytnout ve stanovené lhůtě, která nesmí být

kratší než tři (3) pracovní dny nezbytné informace potřebné k doložení, že zpracování osobních údajů podle Smlouvy je prováděno v souladu s platnými právními předpisy.

- 9.4 Zhotovitel 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 bezpečnostních 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 Zhotovitel 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 Zhotovitel 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) 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:
- (i) svých poradců vázaných povinností mlčenlivosti ve stejném rozsahu jako Strany, nebo
 - (ii) příslušných státních a jiných správních úřadů a soudů, pokud jsou strany povinny podle obecně závazných předpisů jim tyto informace poskytnout, nebo
 - (iii) informací, které jsou nebo se stanou veřejně dostupnými jinak než porušením této Smlouvy.
- 11.2 Zhotovitel se zavazuje k povinnosti mlčenlivosti v rozsahu tohoto článku Dodatku zavázat své zaměstnance a jiné spolupracovníky ve smluvním vztahu se Zhotovitelem, 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 USTANOVENÍ

- 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 jednom stejnopise.
- 12.3 Tento Dodatek nabývá platnosti a účinnosti podpisem oběma Stranami.
- 12.4 Nedílnou součástí tohoto Dodatku tvoří:
- Příloha č. 1 Seznam přijatých technických a organizačních opatření k ochraně osobních údajů

Slovenská technická univerzita v Bratislavě

IS4U, s.r.o.

Místo: Bratislava

Místo: Brno

Datum:

Datum: 17. 5. 2018

Jméno: prof. Ing. Robert Redhammer, PhD.

Jméno: Ing. Tomáš Majer

Funkce: rektor

Funkce: jednatel

Faint, illegible text, possibly a stamp or signature.

PŘÍLOHA 1

SEZNAM PŘIJATÝCH TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K OCHRANĚ OSOBNÍCH ÚDAJŮ

TECHNICKÁ BEZPEČNOSTNÍ OPATŘENÍ

a. fyzická bezpečnost:

Opatření	ANO/NE	Popis
mechanické zábranné prostředky	ANO	Dveře kanceláří na klíče, serveroven na čipovou kartu, klíčové servery v DC s autentizací na OP vybraných osob
zařízení elektrické zabezpečovací signalizace	ANO	V rámci budovy
prostředky omezující působení požárů	ANO	V rámci budovy
prostředky omezující působení projevů živelních událostí	ANO	V rámci budovy
systémy pro kontrolu vstupu	ANO	Čipový systém na budově
kamerové systémy	ANO	Chodby, serverovna
zařízení pro zajištění ochrany před selháním dodávky elektrického napájení	ANO	Velká UPS pro serverovnu
zařízení pro zajištění optimálních provozních podmínek	ANO	Klimatizace

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 uživatele:

požadavky na heslo:	15 znaků, složitost stupně 4 ZXCVCBN
doba platnosti hesla:	2 roky
deaktivace po stanovené době nečinnosti:	Ihned s odchodem zaměstnance, ihned s pominutím požadavku využívání daného systému
důsledky zadání nesprávného hesla:	Po 3 pokusech blokování přístupu s exponenciálně narůstající dobou

d. nástroje pro řízení přístupových oprávnění:

- přístup
- čtení
- zápis
- změna
- výmaz
- export dat

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

e. nástroje pro ochranu před škodlivým kódem:

Ověření a kontrola:

Na stanicích povinně antivirus, centrální zálohování, na e-mailu antispam

Vlastní nástroje pro detekci a korekci škodlivého kódu při vývoji.

- komunikace mezi vnitřní sítí a vnější sítí: ANO/NE ANO, omezená
- serverů a sdílených datových úložišť: ANO/NE NE, pouze zprostředkovaně
- pracovních stanic: ANO/NE ANO, po schválení konkrétnímu pracovníkovi

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

- 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/NE

ANO u systémů zpracovávajících osobní údaje

- ochrana získaných informací před neoprávněným čtením nebo změnou: ANO/NE

ANO, omezení okruhu osob s přístupem k datům, omezení možnosti přenášet tyto údaje mimo prostor firmy, vše u systémů zpracovávajících osobní údaje

- logování:

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

g. nástroje pro detekci bezpečnostních událostí:

Allerting:

AIS bugsystém na aplikační úrovni

Monitorovací systém nagios, ganglia na servery a komunikační prvky

h. aplikační bezpečnost:

- bezpečnostní testy zranitelnosti aplikací: ANO/NE

ANO, pravidelné testy rootkity

- ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou: ANO/NE

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/NE

ANO, ochranná vrstva triggerů v databázi AIS, business logika oddělena od vývojářů

i. kryptografické prostředky: ANO/NE

Pokud ANO, využití

ANO, šifrované diskové kapacity, šifrované komunikační protokoly

j. nástroje pro zajišťování úrovně dostupnosti informací:

Zálohování:

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

k. nástroje k auditingu:

Syslog, AIS wlog, AIS auditní vrstva

