Software602 a.s.
IČ: 630 78 236
DIČ: CZ63078236
sídlem Praha 4, Hornokrčská 15, PSČ: 140 21
zastoupená
na základě plné moci XXXXXXXXX, výkonným ředitelem,
XXXXXXXXX, ředitelem divize Public
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 3044
(dále jen „**Zhotovitel**“)

a

ČR - Rada pro rozhlasové a televizní vysílání
IČ: 452 51 002
sídlem Škrétova 44/6, 120 00 Praha 2
zastoupená XXXXXXXXXX, vedoucím Úřadu Rady pro rozhlasové a televizní vysílání
(dále jen „**Objednatel**“)

uzavřely níže uvedeného dne, měsíce a roku zejména ve smyslu §§ 2358 a 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**Občanský zákoník**“)

tento

Dodatek č. 1

ke Smlouvě o dílo a licenční smlouvě uzavřené mezi smluvními stranami dne 29. 3. 2016
(dále jen „Dodatek“)

1. Do smlouvy se tímto dodatkem přidává nová Příloha č. 4 ve znění:

Příloha č. 4 – Bezpečnostní požadavky

Zhotovitel poskytuje na základě Smlouvy o dílo a licenční smlouvy Objednateli licenci k Software602 Elektronické spisové službě, která je instalována na serverech Objednatele (dále jen „*ESSL*“). ESSL je **Významným informačním systémem (VIS)** Objednatele ve smyslu vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

1. Za účelem naplnění bezpečnostních požadavků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti vč. jeho prováděcích předpisů se Zhotovitel zavazuje:

   a) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele, pokud byl s takovými dokumenty nebo jejich částmi seznámen a to bez ohledu na způsob, jakým byl s takovou dokumentací seznámen, pokud je toto seznámení se ze strany Objednatele prokazatelně doloženo.

   b) předkládat Objednateli na vyžádání a bez zbytečného odkladu záznamy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do informačního nebo komunikačního systému a záznamy o správě uživatelů prováděná na straně Zhotovitele a to po celou dobu trvání smlouvy i po jejím ukončení.

c) neprodleně informovat Objednatele o všech bezpečnostních incidentech na straně Zhotovitele, které mohou mít vliv na funkčnost VIS, a které by mohly mít za následek především, ale nikoliv výlučně:

- porušení zabezpečení osobních údajů ve smyslu Nařízení EU č. 2016/679 (GDPR)
- únik, ztrátu, změnu a zneužití dat
- neautorizovanou změnu zdrojového kódu

a to na kontaktní údaje uvedené v článku 9.1. Smlouvy či kontaktní údaje níže uvedené a zároveň poskytnout Objednateli veškerou možnou součinnost při jejich zvládání a vyhodnocování (např. poskytnutí logů nebo identifikačních údajů) a to vč. uchování záznamů o těchto incidentech pro jejich budoucí použití s ohledem na aktuálně platné požadavky legislativy České republiky.

Kontaktní osobou ve věcech technických na straně Objednatele: XXXXX
Kontaktní osobou ve věcech technických na straně Zhotovitele: XXXXX

2. Přístup k informačním a komunikačním systémům Objednatele:

a) Zhotovitel bere na vědomí, že:

- veškerá jeho aktivita a plnění realizované v systémovém prostředí Objednatele budou Objednatelem průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů Objednatele, se kterými byl Zhotovitel seznámen.
- přístup k informačnímu nebo komunikačnímu systému je možné povolit pouze osobě Zhotovitele uvedené v registru Objednatele, a to na základě požadavku Zhotovitele na přístup. Požadavek Zhotovitele musí obsahovat údaje minimálně o těchto skutečnostech: rozsah dat/informací, služby, účelu, pro které je přístup k technologickému nebo komunikačnímu systému Objednatele požadován a časový údaj o délce platnosti přístupu. Přidělení oprávnění zaměstnanci Zhotovitele musí být řízeno principem nezbytného minima a není nárokové. Udělený přístup nesmí být sdílen více osobami.
- v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Zhotovitele, pokud byl s takovou řídící dokumentací Objednatele seznámen).
- postup zvládání bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost Zhotovitele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy Zhotoviteli či jiné osobě ze strany Objednatele.

b) Zhotovitel se zavazuje, že:

- bude chránit autentizační prostředky a údaje k informačnímu nebo komunikačnímu systému Objednatele.,
- nebude instalovat a používat síťové infrastruktuře Objednatele a na prostředcích, které jsou využívány pro přístup do sítě Objednatele malware ani jiný škodlivý kód. A zároveň všechny jeho systémy, které se připojují do síťové infrastruktury Objednatele, jsou a budou po celou dobu připojení proti malware a jinému škodlivému kódu chráněny,
- všechna jeho zařízení, které se připojují do síťové infrastruktury Objednatele, jsou a budou po celou dobu připojení mít nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu a aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a Javy),
- zajistí, aby osoby uvedené v registru Objednatele nevyužívali přístup k informačnímu nebo komunikačnímu systému Objednatele k:
  - návštěvě internetových stránek s eticky nevhodným obsahem a to vč. ukládání či sdílení eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
  - stahování, sdílení, ukládání, archivaci či instalaci datových a spustitelných souborů v rozporu s licenčními podmínkami nebo autorským zákonem;
  - ukládání a sdílení dat a informací Objednatele na nepovolených datových úložištích nebo médiích;
  - zasílání řetězových emailů.

- bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku,
- nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací.

2. Smluvní strany jsou si plně vědomy zákonné povinnosti od 1. 7. 2016 uveřejnit dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) tento dodatek včetně všech případných smluv, kterými se tento dodatek doplňuje, mění, nahrazuje nebo ruší, a to prostřednictvím registru smluv. Smluvní strany se dále dohodly, že tento dodatek vč. původní smlouvy zašle správci registru smluv k uveřejnění prostřednictvím registru smluv Objednatel.
3. Ostatní ustanovení smlouvy se tímto dodatkem nemění.
4. Tento dodatek je sepsán a podepsán ve dvou vyhotoveních, z nichž každá ze smluvních stran obdrží po jednom.
5. Tento dodatek nabývá účinnosti zveřejnění v registru smluv.
6. Smluvní strany prohlašují, že si dodatek řádně přečetly, porozuměly jeho obsahu, s nímž souhlasí a nemají vůči němu žádné námitky a tento dodatek podepisují jako projev svobodné, vážné, nijak nepředstírané vůle.

v Praze dne	v Praze dne
---	---
XXX	XXX

4