ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ

Křížová 25, 225 08 Praha 5

Dodatek č. 3
k
Rámcové smlouvě na Provozní podporu a další rozvoj IKR

(dále jen „Dodatek č. 3")

Smluvní strany

Česká republika - Česká správa sociálního zabezpečení

Sídlo:	Křížová 25, 225 08 Praha 5
Statutární zástupce:	Mgr. František Boháček, ústřední ředitel
Osoba jednající:	Ing. Milan Shrbený, ředitel sekce IKT
IČO:	00006963
Bankovní spojení:	Česká národní banka
Číslo účtu:	10006-127001/710
ID datové schránky:	49kaiq3

(dále jen „**Objednatel**")
na straně jedné

a

Asseco Central Europe, a.s.

Sídlo:	Budějovická 778/3a, 140 00 Praha 4
Zastoupená:	[redacted] prokuristou
Zapsaná v OR:	vedeném Městským soudem v Praze, oddíl B, vložka 8525
Kontaktní osoba:	[redacted]
	tel.: [redacted] e-mail: [redacted]
IČO:	27074358
DIČ:	CZ27074358
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	1657960/0300
ID datové schránky:	qrhcwzg

(dále jen „**Zhotovitel**")
na straně druhé
(Objednatel a Zhotovitel budou v tomto Dodatku č. 3 označováni jednotlivě také jako „Smluvní strana" a společně jako „Smluvní strany")

I.
Předmět Dodatku č. 3

1. Smluvní strany spolu uzavřely dne 8. 9. 2015 Rámcovou smlouvu na Provozní podporu a další rozvoj IKR, ve znění Dodatku č. 1 ze dne 2 .7. 2018 a Dodatku č. 2 ze dne 19.6.2019, jejímž předmětem je závazek Zhotovitele provést a zajišťovat pro Objednatele následující plnění:

   - Poskytování služeb provozní podpory IKR
   - Úpravy stávajících částí a rozvoj nových částí IKR a zajištění jejich servisu
   - Rozšíření provozní podpory IKR

   (dále jen „Smlouva").

2. Smluvní strany se dohodly, že součástí Smlouvy se stává ujednání o zpracování osobních údajů ve smyslu čl. 28 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále též jen „GDPR") a v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, dále též jen „ZoZOÚ"), a o kybernetické bezpečnosti v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů, jehož podmínky se řídí tímto Dodatkem č. 3.

3. Předmětem tohoto Dodatku č. 3 jsou změny Smlouvy uvedené v čl. II. tohoto Dodatku č. 3, na nichž se Smluvní strany dohodly.

II.
Změna ustanovení

1. Do Preambule Smlouvy se doplňují nové odst. 1.4 a 1.5 se zněním:

   „1.4 Informační systém Objednatele, jehož součástí je IKR, je prvkem kritické informační infrastruktury v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti").

   1.5 Vzhledem k významu veřejné zakázky specifikované v odst. 1.3 této Preambule považuje Objednatel Zhotovitele za významného dodavatele a provozovatele části informačního systému Objednatele ve smyslu zákona o kybernetické bezpečnosti."

2. V článku VII. odst. 7.1 Smlouvy se doplňuje nový odst. 7.1.6 se zněním:

   „7.1.6 seznámit Zhotovitele s vnitřními bezpečnostními politikami Objednatele.".

3. V článku VII. odst. 7.1 Smlouvy se doplňuje nový odst. 7.1.7 se zněním:

   „7.1.7 poskytovat Zhotoviteli nezbytnou součinnost k tomu, aby Zhotovitel mohl řádně plnit své povinnosti uložené mu jako Provozovateli dle ZoKB a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB"), zejména se zavazuje
   a. informovat Zhotovitele o opatřeních podle ZoKB a VoKB zavedených u Objednatele;
   b. informovat Zhotovitele o opatřeních, která má zavést Zhotovitel, a stanovit způsob jejich zavedení;

c. zavést a udržovat systém řízení bezpečnosti informací podle § 3 VoKB;
d. zahrnout IS IKR do systému řízení bezpečnosti informací Objednatele;
e. stanovit metodiku pro identifikaci aktiv podle § 4 VoKB a předat ji Zhotoviteli;
f. určit a evidovat garanty aktiv a předat jejich seznam a kontakty na ně Zhotoviteli;
g. stanovit pravidla ochrany nutná pro zabezpečení jednotlivých úrovní aktiv a předat tato pravidla Zhotoviteli;
h. určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 k VoKB a aplikovat je v souladu s body 7.8 až 7.10 tohoto dodatku;
i. stanovit metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik a předat ji Zhotoviteli;
j. provádět hodnocení rizik podle § 5 odst. 2 VoKB nebo pověřit tímto hodnocením Zhotovitele;
k. zpracovávat zprávu o hodnocení rizik a předávat tuto zprávu Zhotoviteli, pokud hodnocení rizik neprovádí Zhotovitel;
l. zpracovávat plán zvládání rizik podle § 5 VoKB nebo pověřit jeho zpracováváním Zhotovitele;
m. zavádět plán zvládání rizik;
n. určit osoby, které budou zastávat bezpečnostní role podle § 6 odst. 3 VoKB, a předat jejich seznam a kontakty na ně Zhotoviteli;
o. zřídit výbor pro řízení kybernetické bezpečnosti podle § 6 odst. 7 VoKB;
p. informovat Zhotovitele o všech doporučeních a rozhodnutích výboru pro řízení kybernetické bezpečnosti týkajících se IS IKR nebo přizvat Zhotovitele do výboru;
q. informovat Zhotovitele o výsledcích kontrol zavedených bezpečnostních opatření prováděných u Zhotovitele podle § 8 odst. 2) písm. c) VoKB;
r. stanovovat plán rozvoje bezpečnostního povědomí a předávat jej Zhotoviteli;
s. hodnotit účinnost plánu rozvoje bezpečnostního povědomí a seznamovat s hodnocením Zhotovitele;
t. určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a předat tato pravidla Zhotoviteli;
u. předávat Zhotoviteli dokumentaci systému řízení bezpečnosti informací obsahující požadavky týkající se řízení provozu a komunikací a schvalovat dokumentaci obsahující pravidla a postupy podle § 10 VoKB vypracovanou Zhotovitelem;
v. řídit změny podle § 11 VoKB, pro každou změnu stanovovat požadavky na činnost Zhotovitele;
w. stanovit politiku řízení přístupu podle § 12 VoKB a předat ji Zhotoviteli;
x. stanovovat bezpečnostní požadavky podle § 13 VoKB a zahrnovat je do projektu akvizice, vývoje a údržby;
y. zavést proces detekce a vyhodnocování kybernetických bezpečnostních událostí a incidentů podle § 14 VoKB a předat jeho dokumentaci Zhotoviteli;
z. stanovit cíle řízení kontinuity činností podle § 15 písm. c) VoKB;
aa. provádět audit kybernetické bezpečnosti podle § 15 VoKB;
bb. zajišťovat fyzickou bezpečnost podle § 17 VoKB;
cc. informovat Zhotovitele o nástroji pro správu a ověření identity uživatelů, administrátorů a aplikací podle § 19, který má Objednatel zaveden, a stanovit požadavky na jeho využití v IS IKR;
dd. informovat Zhotovitele o centralizovaném nástroji pro řízení přístupových oprávnění podle § 20, který má Objednatel zaveden a stanovit požadavky na jeho využití v IS IKR;
ee. stanovit požadavky na ochranu před škodlivým kódem;

[redacted] [redacted]

ff. stanovit požadavky na zaznamenávání událostí IS IKR, jeho uživatelů a administrátorů;
gg. poskytnout nástroj pro uchovávání záznamů po dobu stanovenou § 22 VoKB a umožnit Zhotoviteli přístup k záznamům nebo pověřit Zhotovitele implementací tohoto nástroje;
hh. stanovit požadavky na detekci kybernetických bezpečnostních událostí podle § 23 VoKB;
ii. poskytnout nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí podle § 24 VoKB;
jj. provádět penetrační testy podle § 25 VoKB nebo požadovat jejich provedení po Zhotoviteli;
kk. umožnit Zhotoviteli používat aktuálně odolné kryptografické algoritmy a kryptografické klíče;
ll. umožnit Zhotoviteli používat systém správy klíčů, který splňuje požadavky § 26 písm. b) VoKB;
mm. Stanovit požadavky na opatření na zajišťování úrovně dostupnosti informací podle § 27 VoKB;
nn. předávat Zhotoviteli Bezpečnostní politiku a bezpečnostní dokumentaci podle § 30 VoKB;
oo. kategorizovat kybernetické bezpečnostní incidenty podle § 31 VoKB;
pp. hlásit kybernetické bezpečnostní incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost podle § 32 VoKB;
qq. informovat Zhotovitele o reaktivních opatřeních, požadovat po Zhotoviteli podklady pro posouzení očekávaných dopadů reaktivního opatření na IS IKR, a na zavedená bezpečnostní opatření;
rr. požadovat po Zhotoviteli návrh způsobu rychlého provedení reaktivního opatření a provedení reaktivního opatření podle § 13 ZoKB;
ss. oznamovat Národnímu úřadu pro kybernetickou a informační bezpečnost způsob provedení reaktivního opatření a jeho výsledek podle § 33 VoKB;
tt. požadovat po Zhotoviteli návrh a realizaci opatření v souvislosti s varováním podle § 12 ZoKB;
uu. požadovat po Zhotoviteli návrh a realizaci ochranného opatření nebo opatření obecné povahy podle § 14 a § 15 ZoKB;
vv. hradit Zhotoviteli náklady spojené s přijetím bezpečnostního opatření, na jehož přijetí a způsobu přijetí se Objednatel se Zhotovitelem dohodli."

4. V článku VII. Smlouvy se znění odst. 7.3.3 ruší a nahrazuje se zněním:

„7.3.3 poskytnout další relevantní součinnost za účelem splnění této Smlouvy, zejména při předávání řešení do produkčního prostředí, odstraňování výpadků řešení v produkci a provádění školení obsluhy včetně poskytnutí součinnosti při aktivaci řízení kontinuity činností; detailní požadavky na součinnost jsou uvedeny v Příloze č. 1 této Smlouvy;".

5. V článku VII. odst. 7.3 Smlouvy se doplňují nové odst. 7.3.6, 7.3.7, 7.3.8 a 7.3.9 se zněním:

„7.3.6 poskytnout Objednateli i kontrolním orgánům nezbytnou součinnost při provádění auditu bezpečnostních opatření kybernetické bezpečnosti;

7.3.7 dodržovat vnitřní bezpečnostní politiky Objednatele;

7.3.8 informovat uvedené kontaktní osoby Objednatele pro účely jednání ve věcech kybernetických bezpečnostních událostí a incidentů o kybernetických bezpečnostních incidentech souvisejících s plněním předmětu této Smlouvy nejpozději následující pracovní den po detekci;

7.3.9 informovat Objednatele o způsobu řízení rizik na straně Zhotovitele souvisejících s předmětem plnění této Smlouvy.".

6. Do čl. VII. Smlouvy se doplňují nové odst. 7.4, 7.5, 7.6, 7.7, 7.8 a 7.9 se zněním:

7.4 Objednatel tímto pověřuje Zhotovitele zpracováním dat obsažených v IKR v rámci plnění této Smlouvy. Zhotovitel je povinen zpracovávat data obsažená v IKR pro Objednatele na základě jeho pokynů a v rozsahu nezbytném k řádnému plnění povinností Zhotovitele vyplývajících z této Smlouvy.

7.5 Zhotovitel zpracovává data automatizovanými prostředky.

7.6 Ochrana dat je zabezpečena v souladu s požadavky kybernetické bezpečnosti.

Likvidace osobních údajů a dat

7.7 Technické nosiče dat obsahující data, osobní údaje nebo zvláštní kategorie osobních údajů, musí být při jejich vyřazení z používání likvidovány pouze takovým způsobem, který zajistí, že před jejich likvidací nebo opakovaným použitím budou veškerá uložená data odstraněna nebo bezpečně přepsána.

7.8 Zhotovitel je povinen předat nefunkční a vyřazené technické nosiče těchto dat, které jsou majetkem Objednatele, k fyzické likvidaci Objednateli.

7.9 Fyzickou likvidaci technických nosičů dat obsahující data, osobní údaje nebo zvláštní kategorie osobních údajů zajišťuje v souladu s požadavky kybernetické bezpečnosti Objednatel.".

6. V článku VIII. Smlouvy se znění odst. 8.3 ruší a nahrazuje se zněním:

„8.3 Zhotovitel je oprávněn poskytovat potřebné informace subdodavatelům a je povinen subdodavatele zavázat k mlčenlivosti v rozsahu daném tímto článkem a k dodržování ujednání mezi Objednatelem a Zhotovitelem v plném rozsahu této Smlouvy."

7. Článek IX. Smlouvy se ruší a nahrazuje se zněním:

„IX. Ochrana osobních údajů

9.1 S ohledem na předmět této Smlouvy smluvní strany předpokládají, že Zhotovitel bude zpracovávat osobní údaje nebo zvláštní kategorie osobních údajů, (dále společně jen „osobní údaje") obsažené v IKR. Nedílnou součástí Smlouvy je tak i ujednání o zpracování osobních údajů mezi Objednatelem jako správcem a Zhotovitelem jako zpracovatelem, uvedené níže v tomto čl. IX. Smlouvy.

9.2 Objednatel tímto pověřuje Zhotovitele zpracováním osobních údajů subjektů údajů poskytovaných Objednatelem v rámci plnění Smlouvy. Zhotovitel je povinen zpracovávat osobní údaje pro Objednatele na základě jeho pokynů a v rozsahu nezbytném k řádnému plnění povinností Zhotovitele vyplývajících ze Smlouvy.

9.3 Zhotovitel se, za podmínek dále uvedených v tomto dodatku, zavazuje k tomu, že bude po celou dobu trvání Smlouvy disponovat nezbytnými úředními

povoleními, odbornými znalostmi a zdroji potřebnými k tomu, aby mohl řádně plnit své závazky založené touto Smlouvou a že zavede (nebo má zavedena) a bude udržovat technická a organizační opatření, která splňují požadavky GDPR a ZoZOÚ, včetně požadavků na bezpečnost zpracování osobních údajů a zavazuje se, že bude po celou dobu trvání této Smlouvy tento stav udržovat.

9.4 Správce se, za podmínek dále uvedených v tomto dodatku, zavazuje k tomu, že bude po celou dobu trvání Smlouvy disponovat nezbytnými zdroji potřebnými k tomu, aby mohl řádně plnit své závazky založené touto Smlouvou a že bude znát, řádně vykonávat a plnit všechna svá oprávnění a povinnosti podle této Smlouvy a aplikovatelných právních předpisů, zejména GDPR a ZoZOÚ.

9.5 Smluvní strany se zavazují si vzájemně při plnění závazků založených touto Smlouvu poskytnout sjednanou, vždy však alespoň nezbytnou, součinnost.

Účel zpracování

9.6 Účelem zpracování osobních údajů Zhotovitelem pro Objednatele, resp. za Objednatele, je v souladu se Smlouvou a s obecně závaznými právními předpisy poskytovat provozní podporu a další rozvoj IKR, poskytování služeb provozní podpory IKR, úpravy stávajících částí a rozvoj nových částí IKR a zajištění jejich servisu a rozšíření provozní podpory IKR.

Povaha zpracování

9.7 Zpracování osobních údajů bude mít povahu shromažďování, zaznamenávání, uspořádávání, (re)strukturování, třídění, seřazení či zkombinování, ukládání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení;

a to s využitím manuálních a automatizovaných prostředků v rozsahu nezbytném pro zajištění řádného poskytování služeb.

9.8 Osobní údaje budou zpracovány z titulu plnění právní povinnosti, která se na Objednatele vztahuje, z titulu splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen Objednatel a z titulu oprávněných zájmů Objednatele, a to těchto typů osobních údajů a kategorií subjektů:

- osobních údajů klientů a kurately, zejména identifikační údaje, adresní údaje, údaje pro provádění nemocenského pojištění, údaje pro provádění důchodového pojištění, údaje pro provádění lékařské posudkové služby, údaje o výběru pojistného a údaje, evidované na základě požadavků práva Evropských společenství a z mezinárodních smluv o sociálním zabezpečení.

9.9 Předmětem zpracování osobních údajů na základě této Smlouvy jsou i zvláštní kategorie osobních údajů ve smyslu GDPR a ZoZOÚ – údaje o zdravotním stavu klientů.

Doba trvání zpracování a jeho ukončení

9.10 Zpracování osobních údajů bude ze strany Zhotovitele probíhat po dobu účinnosti této Smlouvy. Povinnosti Zhotovitele týkající se ochrany osobních údajů se Zhotovitel zavazuje plnit po celou dobu účinnosti této Smlouvy, pokud z ustanovení této Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti.

9.11 V případě ukončení této Smlouvy je Zhotovitel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Zhotovitel od Objednatele písemně jiné pokyny nebo pokud právo EU nebo členského státu nepožaduje uložení daných osobních údajů.

Kategorie příjemců

9.12 V rámci zpracování bude jediným příjemcem osobních údajů Objednatel. Předávání osobních údajů třetím osobám je možné pouze na základě písemného pokynu Objednatele v souladu s čl. 30 GDPR a dalšími aplikovatelnými právními předpisy.

Povinnosti Smluvních stran

Smluvní strany jsou při plnění této Smlouvy povinny:

9.13 Zavést a udržovat technická, organizační, personální a jiná vhodná opatření ve smyslu čl. 32 GDPR a ZoZOÚ, aby zajistily a byly schopny kdykoliv doložit, že zpracování osobních údajů je prováděno v souladu s uvedenými a dalšími aplikovatelnými právními předpisy tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům a k datovým nosičům, které tyto údaje obsahují, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití, a tato opatření podle potřeby průběžné revidovat a aktualizovat. V oblasti zpracování vykonávaného plně či částečně prostředky výpočetní a přenosové techniky budou za nezbytná opatření považována vždy alespoň opatření:

i. zajišťující to, že příslušné systémy a zařízení pro automatizovaná zpracování osobních údajů budou používat pouze oprávněné osoby,

ii. zajišťující to, že fyzické osoby oprávněné k používání systémů a zařízení pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

iii. zabraňující neoprávněnému přístupu k datovým nosičům osobních údajů.

9.14 vést a průběžné revidovat a aktualizovat záznamy o zpracování osobních údajů ve smyslu GDPR;

9.15 navzájem se informovat o všech okolnostech významných pro plnění předmětu této Smlouvy;

9.16 zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení této Smlouvy;

9.17 postupovat v souladu s dalšími požadavky GDPR a ZoZOÚ, zejména dodržovat obecné zásady zpracování osobních údajů, plnit své informační povinnosti, nepředávat osobní údaje třetím osobám bez potřebného oprávnění, respektovat práva subjektů údajů a poskytovat v této souvislosti nezbytnou součinnost;

9.18 Smluvní strany shodně konstatují, že, jestliže Zhotovitel poruší GDPR tím, že určí účely a prostředky zpracování osobních údajů, považuje se ve vztahu k takovému zpracování, ve smyslu GDPR, za správce dotčených osobních údajů.

Povinnosti Objednatele

Objednatel je povinen:

9.19 zajistit, že osobní údaje budou zpracovány vždy v souladu s GDPR a ZoZOÚ, a dalšími aplikovatelnými předpisy, a že tyto údaje budou aktuální, přesné a pravdivé, jakož i to, že tyto údaje budou odpovídat stanovenému účelu zpracování;

9.20 přijmout vhodná opatření, aby poskytl subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace a učinil veškerá sdělení požadovaná GDPR a ZoZOÚ.

Povinnosti Zhotovitele

Zhotovitel je povinen:

9.21 dodržovat všechny povinnosti, které mu jako zpracovateli vyplývají z právních předpisů o ochraně osobních údajů, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu;

9.22 v případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Zhotovitelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Zhotovitelem, oznámit tuto skutečnost okamžitě Objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení;

9.23 zpracovávat osobní údaje pouze na základě doložených pokynů Objednatele, včetně pokynů v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci. Pokud Zhotoviteli určité zpracování ukládá právo Evropské unie nebo členského státu, které se vztahuje na zpracovatele, je Zhotovitel povinen Objednatele o tomto právním požadavku písemně informovat před zahájením předmětného zpracování, ledaže by uvedené právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu; zároveň je však Zhotovitel povinen neprodleně informovat o tom, že podle názoru Zhotovitele

porušuje určitý pokyn Objednatele předpisy Evropské unie anebo členského státu EU, jehož předpisy jsou na zpracování aplikovatelné, zejména právních předpisů České republiky; Postupuje-li Zhotovitel při zpracování osobních údajů podle pravidla výslovně uvedeného v této Smlouvě (včetně popisu zpracování), má se za to, že jedná na základě pokynu Objednatele, ledaže obdrží podle tohoto odstavce od Objednatele doložený pokyn k odlišnému postupu;

9.24 v případě, že je podle právních předpisů o ochraně osobních údajů vyžadováno jakékoli oznámení nebo jiný úkon vůči správnímu orgánu, upozornit na tuto skutečnost Objednatele v dostatečném předstihu a v případě, že tím Objednatel Zhotovitele pověří a zmocní, zajistit provedení těchto úkonů;

9.25 nezapojit do zpracování osobních údajů žádného dalšího (pod)zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele. Pokud Zhotovitel zapojí dalšího zpracovatele, aby provedl či prováděl určité činnosti zpracování osobních údajů, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny v této Smlouvě, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky právních předpisů, zejména GDPR. Přitom platí, že neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany osobních údajů, odpovídá Objednateli za plnění povinností dotčeného dalšího zpracovatele i nadále plně Zhotovitel.

9.26 zachovávat mlčenlivost o osobních údajích a zajišťovat, aby osoby, které se zpracování osobních údajů účastní nebo mají k osobním údajům při jejich zpracování Zhotovitelem přístup (včetně případného automatizovaného zpracování), byly zavázány k mlčenlivosti nebo šlo o osoby, na které se vztahuje zákonná povinnost mlčenlivosti;

9.27 zajistit a kontrolovat plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům;

9.28 zabránit neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování;

9.29 zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje;

9.30 zavést opatření, která umožní určit a ověřit, komu byly osobní údaje předány;

9.31 bez zbytečného odkladu ohlašovat na Formuláři pro ohlášení incidentu správci, který je přílohou tohoto dodatku, případná porušení nebo podezření na porušení zabezpečení osobních údajů Objednateli nejpozději však do 48 hodin od jejich zjištění a poskytnout mu veškerou součinnost a veškeré informace, které může Objednatel potřebovat ke splnění svých zákonných povinností, zejména, nikoliv však výlučně, v rozsahu podle čl. 33 odst. 3 GDPR;

9.32 zohledňovat při své činnosti povahu zpracování osobních údajů a být Objednateli nápomocen (zejména prostřednictvím vhodných technických a organizačních

opatření, pokud je to možné a ve spravedlivě požadovatelném rozsahu) při zajišťování souladu zpracování v oblastech:

i. zabezpečení zpracování,

ii. ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu anebo subjektům osobních údajů,

iii. plnění povinnosti Objednatele reagovat na žádosti o výkon práv subjektu osobních údajů, V případě, že subjekt osobních údajů uplatňuje některé své právo u Zhotovitele, ač jej má uplatnit výhradně u Objednatele, zavazuje se Zhotovitel takový požadavek bez zbytečného odkladu předat oprávněné osobě Objednatele, nejpozději však do 24 hodin od jejího převzetí.

iv. poskytne Objednateli součinnost při komunikaci s dozorovým orgánem a dle pokynů Objednatele bude spolupracovat při přípravě odpovědí dozorovému úřadu ohledně činností prováděných Zhotovitelem;

v. posuzování vlivu zpracování na ochranu osobních údajů (výstupem tohoto posouzení bude poskytnutí podkladových materiálů a vlastních odborných vyjádření);

vi. při (tzv. předchozích) konzultacích před zpracováním s dozorovým úřadem, to při zohlednění povahy zpracování a informací, jež má Zhotovitel k dispozici;

vii. jakož i pro splnění dalších povinností správce ve smyslu GDPR;

9.33 Zhotovitel není oprávněn osobní údaje jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy;

9.34 poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti Objednatele anebo Zhotovitele stanovené v GDPR pro zpracování osobních údajů, a umožnit audity, včetně inspekcí, prováděné Objednatelem nebo jiným auditorem, kterého Objednatel pověřil, a k těmto auditům přispět. Objednatel nebo jím pověřený auditor je při výkonu auditu povinen dbát oprávněných zájmů Zhotovitele, zejména nesmí být ohrožena bezpečnost dat zpracovávaných Zhotovitelem ani nesmí dojít k neoprávněnému zásahu do práv třetích osob. Zhotovitel je oprávněn podmínit umožnění auditů uzavřením zvláštní dohody o ochraně důvěrnosti informací;

9.35 umožnit Objednateli na vyžádání kontrolu dodržování povinností dle této Smlouvy, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložit seznam osob s přístupem k osobním údajům či doložit, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby, jak je tato definována níže;

9.36 umožnit Objednateli přístup do informačního systému užívaného pro zpracování a k probíhajícím operacím zpracování;

9.37 v součinnosti s Objednatelem vést, průběžné revidovat a aktualizovat písemné záznamy o všech kategoriích činností zpracování prováděných pro Objednatele, jež obsahují alespoň náležitosti podle článku 30 GDPR a poskytovat tyto záznamy na žádost a podle žádosti dozorového úřadu. Tyto záznamy mohou mít, při zachování písemnosti, elektronickou formu a obsahují zejména:

- jméno a kontaktní údaje Zhotovitele, Objednatele a případného zástupce Objednatele nebo Zhotovitele a pověřence pro ochranu osobních údajů;
- kategorie zpracování prováděného pro Objednatele;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci; a
- popis technických a organizačních bezpečnostních opatření;

9.38 na základě písemné výzvy Objednatele Objednateli vedené záznamy zpřístupnit.

Cena a platební podmínky

9.39 Smluvní strany se dohodly, že zpracování osobních údajů na základě této Smlouvy je zahrnuto v ceně plnění podle této smlouvy, přičemž Zhotovitel nemá nárok na náhradu nákladů spojených s plněním povinností uvedených v čl. IX této Smlouvy. To neplatí pro náklady na (a) posuzování vlivu zpracování na ochranu osobních údajů a (b) součinnost při (tzv. předchozích) konzultacích před zpracováním s dozorovým úřadem, které Zhotovitel poskytne za předem sjednanou úhradu.

Náhrada vzniklé újmy

9.40 Vznikne-li Objednateli v důsledku nesplnění povinnosti Zhotovitele dle právních předpisů o ochraně osobních údajů újma (škoda i nemajetková újma), zavazuje se Zhotovitel Objednateli tuto újmu v plném rozsahu nahradit. Újmou vzniklou Objednateli se pro účely tohoto ustanovení rozumí zejména (i) náhrada újmy (škody i nemajetkové újmy) subjektům údajů ve smyslu právních předpisů o ochraně osobních údajů a (ii) pokuty uložené Úřadem pro ochranu osobních údajů či jiným správním úřadem.

Zabezpečení osobních údajů

9.41 Zhotovitel přijal a udržuje taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

9.42 Zhotovitel je povinen zajistit, že přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Zhotoviteli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se

zpřístupněním osobních údajů a jejich zpracováním (dále jen „**pověřené osoby**"). Splnění této povinnosti zajistí Zhotovitel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou.

9.43 Zhotovitel dále vhodným způsobem zajistí, že pověřené osoby budou zpracovávat osobní údaje na základě smlouvy se Zhotovitelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Zhotovitelem stanoveném a odpovídajícím této Smlouvě uzavírané mezi Zhotovitelem a Objednatelem a právními předpisy, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.

9.44 Zhotovitel přijal a udržuje zejména následující opatření k zajištění úrovně zabezpečení:

9.44.1 zajištění toho, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby;
9.44.2 zajištění toho, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;
9.44.3 pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;
9.44.4 zabránění neoprávněnému přístupu k datovým nosičům
9.44.5 provádění šifrování osobních údajů;
9.44.6 schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;
9.44.7 schopnost obnovit dostupnost osobních údajů a přístup k nim včas a v případě fyzických či technických incidentů; a
9.44.8 proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
9.44.9 víceúrovňový firewall;
9.44.10 antivirovou ochranu a kontrolu neoprávněných přístupů;
9.44.11 provádění šifrovaného přenosu dat prostřednictvím IT technologií mimo perimetr IIS (Integrovaný informační systém) ČSSZ pouze po předchozím souhlasu Objednatele;
9.44.12 přístup k osobním údajům mají pouze pověřené osoby Zhotovitele;
9.44.13 servery s osobními údaji jsou uzamčené místnosti se zvláštním režimem vstupu; a
9.44.14 zálohy dat se provádějí do oddělené části IIS ČSSZ šifrovaným přenosem a přístup k nim mají pouze pověřené osoby Zhotovitele.

9.45 Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě.

9.46 Při zpracování osobních údajů v jiné než elektronické podobě budou osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby.

9.47 Zhotovitel se zavazuje na písemnou žádost Objednatele přijmout v přiměřené lhůtě stanovené Objednatelem další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.

9.48 V případě zjištění porušení záruk dle odst. 9.44 čl. IX. této Smlouvy je Zhotovitel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do 3 pracovních dnů poté, co je k tomu Objednatelem vyzván.

8. Do článku XI. Smlouvy se doplňuje nový odst. 11.2 se zněním:

„11.2 Pro účely jednání ve věcech kybernetických bezpečnostních událostí a incidentů souvisejících s touto Smlouvou jsou odpovědnými osobami:

11.2.1 na straně Objednatele:

[redacted]
e-mail: [redacted]
tel: [redacted]

11.2.2 na straně Zhotovitele:

[redacted]
e-mail: [redacted]
tel.: [redacted]

9. Dosavadní odstavce 11.2 až 11.5 čl. XI. Smlouvy se přečíslovávají a nově se jedná o odstavce 11.3 až 11.6 čl. XI. Smlouvy.

10. Do článku XII. Smlouvy se vkládá nový odst. 12.10, který zní:

„12.10 V případě, že se Zhotovitel dostane do prodlení s nahlášením kybernetického bezpečnostního bezpečnostních událostí nebo incidentů oproti termínu uvedenému v čl. VII. odst. 7.3.8 této Smlouvy uvedené kontaktní osobě Objednatele pro účely jednání ve věcech kybernetických bezpečnostních událostí a incidentů, je Objednatel oprávněn požadovat na Zhotoviteli zaplacení smluvní pokuty ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý započatý den prodlení s nahlášením incidentu Objednateli. Uplatněním smluvní pokuty nezaniká právo Objednatele na náhradu škody.".

11. V čl. XII. Smlouvy se dosavadní odst. 12.10 nově označuje jako odst. 12.11.

ČSSZ

III.
Závěrečná ujednání

1. Tento Dodatek č. 3 nabývá platnosti dnem jeho podpisu oběma Smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) ve znění pozdějších předpisů, Objednatelem. Zhotovitel souhlasí s tím, aby tento Dodatek č. 3 byl zveřejněn v registru smluv v souladu se zákonem o registru smluv.

2. Ostatní ujednání Smlouvy tímto Dodatkem č. 3 nedotčena zůstávají v platnosti a účinnosti beze změn.

3. Tento Dodatek č. 3 je vyhotoven v 5 stejnopisech, z nichž 3 stejnopisy obdrží Objednatel a 2 stejnopisy Zhotovitel.

4. Smluvní strany prohlašují, že si tento Dodatek č. 3 přečetly, jeho obsahu porozuměly, a že je projevem jejich pravé a svobodné vůle prosté jakéhokoliv omylu, na důkaz čehož tento Dodatek č. 3 vlastnoručně podepisují.

Příloha: Formulář pro ohlášení incidentu správci

V Praze dne: 30 -07- 2019

Za Českou republiku – Českou správu sociálního zabezpečení:

[redacted]

Jméno: Ing. M[redacted]
Funkce: ředitel

ČESKÁ SPRÁVA SO
ČSSZ OSTREDI
Křížová
26 225 08

V Praze dne: [redacted]

Za Asseco Central Europe, a.s.:

[redacted]

Jméno: [redacted]
Funkce: prokurista

asseco
CENTRAL EUROPE
Budějovická 778/3a, 140 00 Praha 4

[redacted]

Příloha

Formulář pro ohlášení incidentu správci

Kontaktní údaje	
Název:	*uveďte název zpracovatele*
Sídlo:	*uveďte sídlo zpracovatele*
IČO:	*uveďte IČO zpracovatele*
Kontaktní osoba:	*uveďte pozici [útvaru odpovědného za řešení incidentů / pověřence / odpovědného pracovníka / jiné osoby], jméno, email, telefon, adresa*
Splnění lhůty pro ohlášení incidentu	
Čas, kdy se zpracovatel dozvěděl o incidentu	*uveďte čas dle čl. 33 odst. 2 Nařízení*
Odůvodnění zpoždění ohlášení	*uveďte důvody, pro které zpracovatel neohlásil incident v stanovené lhůtě 48 hodin od času, kdy se o incidentu dozvěděl (důvodem může být časová náročnost posouzení veškerých detailů a důsledků incidentů, apod.)*
Detaily incidentu	
Základní popis incidentu:	*popište základní detaily incidentu*
Čas vzniku incidentu:	*uveďte čas vzniku, který jste určili na základě vnitřní analýzy incidentu*
Čas zániku incidentu:	*uveďte čas zániku incidentu, který jste určili na základě vnitřní analýzy incidentu; v případě trvajícího incidentu popište aktuální stav a odhad trvání*
Druh incidentu	*popište, o jaký druh incidentu se jedná: incident v oblasti důvěrnosti (např. neoprávněný přístup k údajům), dostupnosti (např.: ztráta přístupu nebo zničení údajů) nebo integrity (např.: neoprávněná změna) údajů*
Důvod vzniku incidentu	*popište, co bylo příčinou vzniku incidentu: útok (malware, ransomware, apod.), technická nebo lidská chyba, nedbalost, apod.*

Kategorie dotčených osob	*např.: klienti, zaměstnanci, děti, příp. jiné ohrožené skupiny, apod.*
Státy, ze kterých pochází dotčené osoby	*uveďte státy, ve kterých se nachází dotčené osoby, jejichž osobní údaje byly zasaženy incidentem*
Počet dotčených osob	*uveďte (odhadovaný) počet dotčených osob*
Vědomost dotčených osob	*uveďte, zda dotčené osoby vědí o tomto incidentu*
Kategorie osobních údajů	*např.: údaje o zdravotním stavu, o finanční situaci, apod.*
Množství osobních údajů	*uveďte (odhadované) množství osobních údajů zasažených incidentem*
Opatření implementované před vznikem incidentu	*uveďte, jaká opatření zpracovatel implementoval za účelem prevence výskytu a snížení rizika tohoto typu incidentu*
Důsledky incidentu	
Rizika incidentu	*popište pravděpodobná rizika, která jsou důsledkem incidentu, zejména rizika vyplývající z konkrétní kategorie údajů nebo kategorie dotčených osob (např.: zveřejnění údajů, krádež identity, finanční škoda, podvod, apod.)*
Další důsledky	*popište další důsledky tohoto incidentu*
Opatření pro odstranění nebo snížení rizika	
Seznam opatření, která zpracovatel implementoval po vzniku incidentu	*u každého opatření, které zpracovatel implementoval, uveďte odůvodnění pro jeho využití a popis toho, jakým způsobem snižuje nebo odstraňuje riziko pro dotčené osoby*
Obnova údajů	*uveďte, zda a jak došlo k náhradě nebo obnovení osobních údajů, které byly dotčeny incidentem*
Seznam opatření, která zpracovatel navrhuje pro implementaci	*u každého opatření, které má zpracovatel v plánu implementovat, uveďte odůvodnění pro jeho využití a popis toho, jakým způsobem snižuje nebo odstraňuje riziko pro dotčené osoby*