PŘÍLOHA 1
BANKOVNÍ OUTSOURCING

1. Dodavatel bere na vědomí, že poskytování služeb pro objednatele může být považováno za bankovní outsourcing podle vyhlášky č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry („Vyhláška“).

2. Pro tento případ se dodavatel zavazuje akceptovat pravidla stanovená ve Vyhlášce, která mohou být detailněji rozpracována v této příloze nebo v kterékoliv smlouvě splňující předpoklady poskytování outsourcingu uzavřené mezi dodavatelem a objednatelem.

3. Osoba provádějící prověrku, kontrolu nebo audit je povinna dodržovat veškerá bezpečnostní opatření dodavatele, se kterými bude prokazatelně seznámena.

4. Dodavatel se pro účely splnění požadavků Vyhlášky zavazuje spolupracovat s objednatelem a umožnit objednateli (eventuálně České národní bance [“ČNB”]) zejména následující:

a) Prověrku dodavatele před a v průběhu poskytování Plnění – zahrnující zejména prověrku důvěryhodnosti, oprávnění podnikat nebo jiné oprávnění k výkonu dané činnosti, odborné způsobilosti a zkušeností, finanční stability a způsobilosti zajišťovat Plnění.

b) Pravidelné kontroly dodavatele - zahrnující zejména:

- ověření, zda je Plnění trvale poskytováno v souladu se všemi příslušnými právními předpisy, s obchodními podmínkami a Smlouvou,
- ověření, zda je dodavatel nadále důvěryhodný a právně, finančně, odborně i technicky způsobilý k poskytování Plnění,
- ověření, zda dodavatel pravidelně prověřuje funkčnost a dostatečnost svých mechanismů vnitřní kontroly a řízení rizik včetně řízení rizika výskytu mimořádných událostí, které by mohly mít významný negativní vliv na řádný výkon Plnění. Objednatel se zavazuje vzít v přiměřeném rozsahu v úvahu písemné doporučení dodavatele týkající se rizik spojených s Plněním, a přijmout doporučená opatření k jejich minimalizaci, za předpokladu, že tím není v neodůvodněné míře přenášena povinnost dodavatele předcházet riziku na objednatele,
- ověření, zda ochrana bankovního tajemství a osobních údajů klientů objednatele je zajištěna trvale a dostatečně,
- ověření, zda při Plnění nedochází k porušování vnitřních zásad a postupů objednatele,
- ověření, zda vnitřní kontrolní mechanismy dodavatele zajišťují včasné zjištění případných nedostatků Plnění a přijetí opatření k nápravě, celkovou funkčnost a efektivnost Plnění,
- vyhodnocení souladu Plnění s Vyhláškou,
- ověření, zda dodavatel zavedl a udržuje alespoň takové vnitřní řídicí a kontrolní zásady a postupy, které zajišťují v porovnání s obdobnými pravidly objednatele alespoň srovnatelnou úroveň kvality a spolehlivosti.

Dodavatel se zavazuje objednateli v rámci pravidelné kontroly umožnit součinnost a přístup k datům a dalším informacím týkajícím se Plnění, včetně přístupu k primárním informacím a výsledným datům, ověřovat správnost zpracování primárních informací, je-li takové zpracování součástí Plnění.

c) Kontroly z hlediska IT bezpečnosti, zahrnující zejména závazek dodavatele:

- poskytnout objednateli (v podobě umožňující jejich trvalé uchování) dokumenty obsahující popis:
  - bezpečnostní strategie (včetně hlavních zásad pro zajištění důvěrnosti, integrity, klasifikace a dostupnosti dat),
  - příslušných interních předpisů, např. bezpečnostní politiku, popis organizace bezpečnosti včetně rozdělení pravomocí, odpovědností,
  - řešení bezpečnostních incidentů, vč. povinnosti objasňovat bezpečnostní incidenty bez zbytečného odkladu, a navazující dokumenty z oblastí IS bezpečnosti, zálohování, verzování příslušných předpisů (bezpečnostní politiky), doklady o vyhlášení změn, auditování a archivace záznamů o bezpečnostních incidentech nejméně 5 let po vyřešení bezpečnostního incidentu,
  - personální politiky včetně způsobu prověřování zaměstnanců a zajištění mlčenlivosti, správy uživatelů, proškolování zaměstnanců, způsobu prováděných prověřování a vyhodnocování bezpečnosti IS
  - etc. nákupu, výměny, rušení HW/SW včetně bezpečné likvidace dat a podobně,
- poskytnout objednateli popis architektury konkrétního řešení poskytovaného Plnění včetně nastavení bezpečnostních parametrů v jednotlivých komponentech a celcích.
- stanovit reporting včetně komunikačních kanálů, komunikační matice, termínů atd. o bezpečnostních incidentech, plánovaných změnách v architektuře, komunikaci.

d) Kontroly z hlediska Fyzické bezpečnosti, zahrnující závazek dodavatele:

- poskytnout Plnění v souladu s obecně uznávanými normami : ISO ……., EN ……,, PCI ……,, DSS ……,
- poskytnout objednateli seznam svých aktiv (objektů, systémů a zařízení) relevantních pro poskytování Plnění a udržovat tento seznam aktuální. Pokud aktiva (objekty, systémy a zařízení) nevyhovují výše dohodnutým normám nebo požadavkům objednatele, musí dodavatel identifikovat neshody a obě strany se musí dohodnout na jejich vyřešení,
- umožnit a podpořit objednatele při nezávislém ověření bezpečnosti poskytovaného Plnění, včetně pravidelného i mimořádného přezkoumání bezpečnosti aktiv (objektů, systémů a zařízení) relevantních pro poskytované Plnění,
- informovat objednatele předem o každé plánované změně bezpečnostní úrovně poskytovaného Plnění. Pokud je změna neplánovaná, informuje dodavatel o změně objednatele neprodleně po identifikaci takové změny,
- vést záznamy o bezpečnostně relevantních skutečnostech / událostech, které mohou mít dopad na bezpečnost Plnění poskytovaného objednateli. Ze záznamů musí vyplývat co, kde a kdy se stalo, jaký byl dopad události a jaká opatření byla v návaznosti na tento incident přijata. V případě že událost bude ohrožovat bezpečnost Plnění, musí dodavatel neprodleně o události objednatele informovat. Záznamy musí být vedeny způsobem vylučujícím jejich pozdější pozměňování. Záznamy musí být udržovány po celou dobu trvání smluvního vztahu a dalších nejméně 5 let po ukončení smluvního vztahu,
- umožnit objednateli přezkoumání záznamů týkajících se bezpečnosti Plnění poskytovaného objednateli,
- předat objednateli kompletní výčet subdodavatelů využívaných při outsourcingu poskytovaného Plnění (HW, SW vybavení či podpora mající přístup k datům). Při změně uvedeného seznamu musí dodavatel objednateli poskytnout aktuální výčet subdodavatelů,
- pro případ řetězení outsourcingu umožnit objednateli přezkoumání údajů a informací týkajících se subdodavatelů (obdobně zástupců za něj jednajících) a skutečnosti, zda spolupráce s nimi není pro objednatele v rozporu s obezřetnostními požadavky (právními předpisy, přímo použitelnými předpisy Evropské unie atd.). Dodavatel se zavazuje sjednat ve smlouvách se subdodavateli možnost okamžitého ukončení spolupráce se subdodavatelem, budou-li to vyžadovat obezřetnostní požadavky objednatele,
- doložit, že jeho subdodavatelé aplikují přinejmenším stejné požadavky na bezpečnost jako dodavatel a že jejich soulad s těmito požadavky je průběžně kontrolován a dodržován.

e) Audit objednatele a ČNB a kontrola ČNB – zahrnující:

1. audit účetní závěrky
2. audit řídícího a kontrolního systému včetně zpráv o provedených kontrolách
3. případně zpřístupnění zpráv o provedených kontrolách dle bodu a) a b).

Dodavatel předá jednou ročně objednateli svůj roční výkaz (sestavený v souladu s Českými účetními standardy) ověřený objednatelem předem odsouhlaseným auditorem spolu s příslušným výrokem auditora za uplynulé účetní období, a to jakmile je bude mít k dispozici, nejpozději však 180 dnů po skončení příslušného účetního období. Nesplnění této povinnosti dodavatele je podstatným porušením jeho smluvních povinností a objednateli tak vzniká právo odstoupit od smluvního vztahu s dodavatelem.

5. Dodavatel se zavazuje umožnit prověrky, kontroly či audity prováděné za účelem naplnění požadavků Vyhlášky, (včetně sledování věcné správnosti provádění outsourcovaných činností) zaměstnanci objednatele, ČNB nebo třetí osobou pověřenou nebo zmocněnou objednatelem, a to i v sídle dodavatele anebo v dalších místech poskytování Plnění (i pokud jsou v zahraničí).

6. Dodavatel se zavazuje hlásit objednateli s dostatečným předstihem jakékoliv změny, které negativně ovlivňují nebo by mohly negativně ovlivnit poskytování Plnění (např. vlastnická, organizační, majetková struktura, finanční závazky, rizika, změna legislativy) a veškerá relevantní data a další informace související s činnostmi vykonávanými na základě smlouvy.

7. Dodavatel je povinen zavést alespoň takové postupy řízení rizik a kontrolní mechanismy, jaké by použil objednatel v souladu se svými zásadami pro řídící a kontrolní systém, pokud by Plnění zajišťoval sám. Objednatel na vyžádání dodavateli zpřístupní dokumenty, obsahují požadované postupy a kontrolní mechanismy. Dodavatel je zejména povinen zajistit hlášení objednateli všech událostí operačního rizika souvisejících s

dodáváním Plnění, u kterého potenciální ztráta přesahuje limit 1000 EUR, a to na email oprisk@csas.cz. Hlášení musí obsahovat zejména následující:

- místo a datum vzniku události
- stručný popis události
- kontaktní osobu, která má o události informace
- výši škody (není-li známa v okamžiku hlášení, pak její kvalifikovaný odhad)

8. Dodavatel je povinen s roční periodou provádět posouzení rizik, obsahující popis rizik v činnostech, které jsou poskytovány pro objednatele včetně vyčíslení jejich potenciálního dopadu. Objednatel má právo vyžádat si výstupní informace z risk assessmentu, případně se ho účastnit. V případě, že dodavatel nemá zaveden standardní systém hodnocení rizik, může objednatele požádat o spolupráci na vyhodnocení rizik pro činnosti, které souvisí se zajišťováním Plnění pro objednatele. Objednatel poskytne součinnost a doporučí své standardy, které budou bez zbytečného odkladu dodavatelem implementovány. Dodavatel se dále zavazuje poskytnout objednateli zpracovanou analýzu rizik (v závislosti na nabízených dodávkách Plnění).

9. Dodavatel se zavazuje zpracovat business continuity plán, tj. dokumentaci pro případ ohrožení dostupnosti dodávek Plnění z důvodu mimořádné události a tuto dokumentaci, popř. její výtah v souladu s interními předpisy a závazky mlčenlivosti dodavatele, tyto dokumenty poskytne k dispozici objednateli nejpozději do 3 měsíců od uzavření Smlouvy. Objednatel se zavazuje, že poskytnuté informace využije výhradně pro interní potřebu a pro zpracování mimořádných postupů v souvislosti s předmětem Smlouvy. Objednatel si sjedná s dodavatelem minimální rozsah obnovené dodávky Plnění, který lze ze strany objednatele akceptovat jakožto obnovení dodávky Plnění v částečném rozsahu.

10. Dodavatel prohlašuje, že bude průběžně vytvářet a zkvalitňovat opatření, která zajistí minimalizaci rizika přerušení dodávek Plnění a že disponuje dostatečnými záložními kapacitami pro obnovu dodávek Plnění. Dodavatel souhlasí s přítomností zástupce objednatele při testování business continuity plánu a další dokumentace zpracované dodavatelem pro zajištění kontinuity předmětu Smlouvy.

11. Dodavatel se zavazuje, že oznámí objednateli předem nezbytnost zajišťování poskytování Plnění, ať zcela nebo zčásti prostřednictvím další osoby (dále také „řetězový outsourcing“) a vyžádá si předchozí souhlas objednatele s využitím takové osoby. Smlouva uzavřená mezi dodavatelem a takovou další osobou bude odpovídat zásadám a pravidlům uvedeným v této příloze. Dodavatel zajistí a poskytne veškerou nezbytnou a nutnou součinnost a součinnost další osoby v případě, že objednatel nebo ČNB bude oprávněn provádět výše uvedené kontrolní činnosti také u této další osoby.

12. Pokud je důsledkem prokazatelného porušení povinností ze strany dodavatele, případně další osoby v řetězovém outsourcingu, uložení sankce ze strany ČNB objednateli, je objednatel oprávněn požadovat úhradu této sankce po dodavateli v poměrné výši dle jeho zavinění (a to i z nedbalosti). Kompenzací sankce uložené ze strany ČNB objednateli není dotčen nárok objednatele na úhradu veškeré prokazatelné škody vzniklé porušením povinnosti, na niž se sankce ČNB vztahovala.

13. Pokud není v Smlouvě uvedeno jinak, je objednatel oprávněn odstoupit od Smlouvy v případě, že dojde k závažnému porušení povinností uvedených v ustanoveních této přílohy. Objednatel je sám oprávněn posoudit závažnost porušení a buď poskytnout dodavateli přiměřenou lhůtu k nápravě, nebo odstoupit od předmětné Smlouvy s účinností k okamžiku doručení odstoupení. Objednatel je oprávněn od Smlouvy odstoupit též v případě, že to vyžaduje nápravné opatření ČNB.

14. Dodavatel je povinen vzít v úvahu písemné doporučení objednatele, týkající se rizik spojených s dodávaným Plněním, a přijímat opatření k jejich minimalizaci, objednatel se zavazuje využít informace a nálezy auditu výhradně pro vnitřní potřebu a vzájemnou komunikaci mezi objednatelem a dodavatelem.

15. V případě ukončení poskytování Plnění je dodavatel povinen poskytnout objednateli veškerou součinnost pro převedení Plnění zpět na objednatele nebo třetí osobu určenou objednatelem tak, aby byla zajištěna kontinuita činností i po ukončení Smlouvy. Tato součinnost zahrnuje i předání veškerých dat a informací, spojených s Plněním objednateli ve formátu určeném objednatelem, předání veškerých relevantních dokumentů a další kroky vedoucí k převzetí výkonu Plnění objednatelem (nebo třetí osobou).