

SMLOUVA

o poskytování služeb bezpečnostních auditů informačních systémů

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, mezi:

Českou národní bankou

Na Příkopě 28

115 03 Praha 1

zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky

a

Ing. Zdeňkem Viriusem, ředitelem sekce správní

IČO: 48136450

DIČ: CZ48136450

(dále jen „objednatel“)

a

AEC a.s.

Purkyňova 2845/101

612 00 Brno

zastoupenou: Ing. Tomášem Strýčkem, statutárním ředitelem

Společnost je zapsána v Obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 7337

IČO: 26236176

DIČ: CZ26236176

(dále jen „poskytovatel“)

Článek I

Předmět a rozsah plnění

1. Předmětem plnění podle této smlouvy je povinnost poskytovatele poskytovat objednateli služby bezpečnostních auditů informačních systémů a infrastruktury. Tyto audity sestávají zejména z následujících činností:
 - a) Penetrační testy informačních systémů.
 - b) Penetrační testy infrastruktury.
 - c) Audity konfigurace serverů.
 - d) Audity architektury IS/IT.
 - e) Další formy auditů bezpečnosti IS/IT dle konkrétních požadavků objednatele.
2. Výstupem každého bezpečnostního auditu bude „Zpráva s výsledky bezpečnostního auditu“ obsahující zejména Manažerské shrnutí, popis metodiky testování, podrobný popis zjištěných zranitelností a návrhy opatření vedoucí ke zmírnění rizik (dále jen „zpráva“). Zpráva bude objednateli předána nejméně ve dvou tištěných vyhotoveních a dále v elektronickém formátu (docx). Poskytovatel je povinen na žádost objednatele poskytnout konzultace k případně nalezeným zranitelnostem a k návrhům na opatření.
3. Podrobná specifikace předmětu plnění je uvedena v příloze č. 3 smlouvy.

Článek II **Místo a způsob plnění**

1. Místem plnění je sídlo objednatele na adrese Na Příkopě 28, Praha 1, pokud nebude dohodnuto jinak.
2. Plnění podle čl. I této smlouvy bude poskytováno na základě výzvy kontaktní osoby objednatele zaslané e-mailem kontaktní osobě poskytovatele a bude poskytováno v sídle objednatele. Bližší postup je uveden v čl. VI této smlouvy.
3. Plnění bude převzato po předání závěrečné zprávy dle čl. I odst. 2 a to na základě akceptačního protokolu, který podepíší kontaktní osoby smluvních stran.

Článek III **Cena plnění**

1. Smluvní strany se dohodly, že ceny za jednotlivá plnění podle čl. I budou stanoveny dohodou kontaktních osob smluvních stran na základě odsouhlasené nabídky poskytovatele jako cena pevná (tj. bez ohledu na skutečný objem pracnosti). Nabídková cena poskytovatele bude stanovena na základě předpokládaného objemu pracnosti a hodinové sazby dle odst. 2. Konzultace k případně zjištěným zranitelnostem a návrhům na opatření podle čl. I odst. 2 této smlouvy jsou zahrnuty ve sjednané ceně.
2. Hodinová sazba pracovníků poskytovatele:
1325,- Kč/hod.
3. Cena je uvedena bez DPH a jsou v ní zahrnuty veškeré náklady poskytovatele související s plněním dle této smlouvy.
4. Smluvní strany jsou oprávněny navrhnout změnu hodinové sazby uvedených v odst. 2 v návaznosti na vývoj indexu cen tržních služeb, stejné období předchozího roku = 100,1, konkrétně index „Tržní služby celkem“ sloupec „Průměr od počátku roku“, a to průměr za předchozí kalendářní rok, který vyhláší Český statistický úřad. Ceny mohou být sníženy či zvýšeny maximálně o částku odpovídající předmětné roční inflaci. Úprava ceny bude provedena formou dodatku ke smlouvě. První úpravu cen můžou smluvní strany navrhnout nejdříve 1. 1. 2019.

Článek IV **Platební podmínky**

1. Daňový doklad za plnění podle čl. I je poskytovatel oprávněn vystavit nejdříve v den převzetí příslušného plnění kontaktními osobami smluvních stran na základě akceptačního protokolu dle čl. II odst. 3. Akceptační protokol bude přílohou daňového dokladu.
2. Daňový doklad bude vedle náležitostí stanovených zákonem č. 235/2004 Sb, o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 zákona č. 89/2012 Sb. občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) obsahovat i evidenční číslo smlouvy. Objednatel je oprávněn vrátit daňový doklad poskytovateli, nebude-li

obsahovat stanovené náležitosti nebo přílohy nebo bude-li obsahovat chybné údaje. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného daňového dokladu.

3. Daňový doklad bude posílán elektronicky na adresu faktury@cnb.cz, přičemž daňový doklad musí být vložen jako příloha mailové zprávy ve formátu PDF. V jedné mailové zprávě smí být pouze jedna faktura (další faktury je třeba posílat jako další mailovou zprávu). Mimo vlastní fakturu může být přílohou mailu jedna až tři přílohy k faktuře ve formátech PDF, DOC, DOCX, XLS, XLSX. Nebude-li možné faktury zasílat elektronicky, zašle poskytovatel fakturu v analogové formě na adresu objednatele:

Česká národní banka
sekce rozpočtu a účetnictví
odbor centrální účtárna
Na Příkopě 28
115 03 Praha I.

4. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.
5. Smluvní strany se dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele.

Článek V

Osoby poskytovatele poskytující plnění

1. Poskytovatel se zavazuje, že plnění dle čl. I bude poskytováno pouze osobami uvedenými v příloze č. 2 smlouvy. Změna v těchto osobách může být provedena pouze se souhlasem objednatele, a to po splnění kvalifikačních požadavků objednatele ve stejném rozsahu, jaký byl stanoven v poptávce na výběr dodavatele pro poskytování služeb uvedených v této smlouvě, nebude-li dohodnuto jinak. Odsouhlasení změny v osobách uvedených v příloze č. 2 bude provedeno e-mailem alespoň jednou kontaktní osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě.

Článek VI

Uplatnění požadavků na poskytnutí služeb

Postup při uplatnění požadavku na poskytnutí služeb dle čl. I odst. 1 této smlouvy je následující:

- a) objednatel výzvu na poskytnutí služeb uvedených v čl. I odst. 1 této smlouvy zašle e-mailem kontaktní osobě poskytovatele;
- b) poskytovatel ve lhůtě 5 pracovních dnů od doručení výzvy zašle e-mailem kontaktním osobám objednatele nabídku, která obsahuje nabídkovou cenu (dle počtu očekávaných hodin potřebných na poskytnutí poptávaných služeb a příslušné sazby pracovníků poskytovatele) a harmonogram prací,
- c) po vzájemném odsouhlasení nabídky včetně harmonogramu je poskytovatel povinen práce realizovat dle harmonogramu uvedeného v nabídce,

Článek VII

Součinnost, odpovědnost, kontaktní osoby

1. Objednatel se zavazuje poskytnout poskytovateli všechny informace, podklady a písemnosti, které má k dispozici a které jsou nezbytné pro činnost poskytovatele podle této smlouvy.
2. Kontaktní osoby:
 - a. za poskytovatele: Lukáš Bláha
tel. +420 774 470 860 email: lukas.blaha@aec.cz
 - b. za objednatele: Ing. Tomáš Klíma, Ph.D.
tel.: +420 733 783 797 e-mail: tomas.klima@cnb.cz
3. V případě změny v kontaktních osobách či údajích uvedených v odst. 2 se smluvní strany zavazují neprodleně oznámit změnu druhé smluvní straně, a to písemným oznámením zaslaným do sídla druhé smluvní strany. Změna osob je účinná dnem jejího oznámení druhé smluvní straně, a to bez povinnosti uzavírat dodatek k této smlouvě.
4. Poskytovatel se zavazuje v případě zjištění závažnějšího nedostatku v systému objednatele, jehož další testování by mohlo vést k snížení dostupnosti či poškození systémového prostředí, kontaktovat pověřenou osobu objednatele uvedenou v čl. VII odst. 2 písm. b) a v testování pokračovat až po jejím souhlasu.

Článek VIII

Mlčenlivost a bezpečnostní požadavky objednatele

1. Poskytovatel se zavazuje zajistit, že osoby podílející se na plnění dle této smlouvy zachovají mlčenlivost o všech skutečnostech, se kterými se seznámí v průběhu plnění této smlouvy a které nejsou veřejně dostupné. Povinnost mlčenlivosti trvá i po skončení platnosti smlouvy.
2. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele uvedené v příloze č. 1 této smlouvy.

Článek IX

Uveřejnění smlouvy

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu (celé znění) včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“) uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele je v době uzavření této smlouvy <https://ezak.cnb.cz/>.
3. Povinnost uveřejnění této smlouvy včetně jejích změn a dodatků je objednateli uložena § 219 odst. 1 ZZVZ. Povinnost objednatele k uveřejnění skutečně uhrazené ceny vyplývá z ust. § 219 odst. 3 ZZVZ.
4. Uveřejnění bude provedeno dle ZZVZ a příslušného prováděcího předpisu.

Článek X **Smluvní pokuta, úrok z prodlení, náhrada škody**

1. V případě prodlení poskytovatele ve lhůtách plnění stanovených v odsouhlaseném harmonogramu dle čl. VI písm. c) této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý den prodlení.
2. V případě prodlení poskytovatele ve lhůtě dle čl. VI písm. b) k zaslání nabídky je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý den prodlení
3. V případě porušení povinnosti poskytovatele dle čl. VIII odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 50 000 Kč za každé jednotlivé porušení mlčenlivosti.
4. V případě prodlení kupujícího s úhradou daňového dokladu je prodávající oprávněn požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
5. Smluvní pokuta i úrok z prodlení jsou splatné do 14 dnů od doručení příslušného dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
6. Smluvní pokutou není dotčeno právo na náhradu škody.
7. Poskytovatel se zavazuje postupovat tak, aby jeho činností nedošlo ke vzniku škody na zařízeních nebo datech objednatele. Toto ustanovení se nevztahuje na škody, jejichž skutečnou příčinou je vada systému, která se projevila na základě provádění šetření v rámci plnění předmětu smlouvy.

Článek XI **Ochrana osobních údajů**

1. Smluvní strany se dále zavazují dodržovat ujednání o zpracování osobních údajů, které tvoří přílohu č. 4 této smlouvy.

Článek XII **Trvání smlouvy, výpověď smlouvy**

1. Tato smlouva se uzavírá na dobu neurčitou.
2. Každá ze smluvních stran může smlouvu jednostranně písemně vypovědět bez udání důvodu s 2 měsíční výpovědní lhůtou, která začne plynout prvního dne měsíce následujícího po doručení výpovědi druhé smluvní straně.

Článek XIII **Závěrečná ustanovení**

1. Tuto smlouvu lze měnit pouze dohodou smluvních stran písemným dodatkem podepsaným oprávněnými zástupci smluvních stran, není-li ve smlouvě stanoveno jinak.
2. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
3. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém jazyce, nebude-li smluvními stranami

v konkrétním případě dohodnuto jinak.

4. Smluvní strany se dohodly, že tato smlouva a právní vztahy s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník a dále rovněž příslušnými ustanoveními zákona č. 121/2000 Sb., o právu autorském o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, a ostatními souvisejícími platnými právními předpisy.
5. Tato smlouva je vyhotovena ve čtyřech stejnopisech, z nichž objednatel obdrží tři a poskytovatel jedno vyhotovení.
6. Smlouva nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.

Přílohy:

- Příloha č. 1 - Bezpečnostní požadavky objednatele
- Příloha č. 2 - Seznam pracovníků poskytovatele
- Příloha č. 3 - Podrobná specifikace předmětu plnění
- Příloha č. 4 – Ujednání o zpracování osobních údajů

V Praze dne 23.3.2018

Za objednatele:

Ing. Zdeněk Vírnius
ředitel sekce správy

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

V Praze dne 20.3.2018

Za poskytovatele:

Ing. Tomáš Strýček
statutární ředitel

Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni na seznamu pracovníků schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Poskytovatel předloží seznam ČNB nejpozději v den podpisu smlouvy.
2. Seznam bude obsahovat tyto položky: název poskytovatele, adresu sídla poskytovatele, telefonní a emailový kontakt na poskytovatele, tituly, jména a příjmení pracovníků poskytovatele, čísla průkazů totožnosti pracovníků poskytovatele a pro vozidla bude uveden typ vozidla a registrační značka. Součástí seznamu je „Prohlášení o získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů“ a ve smyslu obecného nařízení o ochraně osobních údajů – 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 (dále je „GDPR“). Poskytovatel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu byli poučeni:
 - a) o tom, že poskytovatel předá jejich osobní údaje v rozsahu: titul, jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1, v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do objektu ČNB z důvodu ochrany majetku a osob a správy přístupového systému kontrol vstupů ČNB;
 - b) o veškerých právech subjektů údajů, která mohou uplatnit vůči poskytovateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovány, právo na námitku proti zpracování osobních údajů, požadovat nápravu situace, která je v rozporu s právními předpisy, zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním či právem podat stížnost k Úřadu pro ochranu osobních údajů.
3. Poskytovatel si je vědom povinností vyplývajících pro správce osobních údajů z GDPR, které nabývá účinnosti 25. května 2018, a obsah poučení upraví tak, aby požadavky tohoto nařízení ode dne jeho účinnosti splňoval.
4. Požadavky na případné doplňky a změny schváleného seznamu pracovníků poskytovatele je nutno neprodleně oznámit ČNB. Případné doplňky a změny podléhají schválení ČNB. Pracovníci neschválení ze strany ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Poskytovatel uvede pracovníky, pro které požaduje vystavení vstupních karet ke vstupu do objektu objednatele. Vystavení vstupních karet podléhá schválení objednatele. První vstupní karty budou vystaveny na náklady objednatele. Každé další vystavení vstupní karty bude zpoplatněno částkou 240,- Kč (vč. DPH) s tím, že tato částka bude poskytovateli vyfakturována. Vstupní karta se nebude platit v případech, kdy:
 - prestane fungovat bez viditelného mechanického poškození,
 - dojde-li ke změně příjmení,
 - byla-li karta odcizena a událost je doložitelná protokolem od Policie ČR.
6. Poskytovatel bude při zahájení činnosti vybaven základním počtem vstupních karet pro jednotlivé pracovníky podle schváleného seznamu. Vstupní karta umožní pracovníkovi

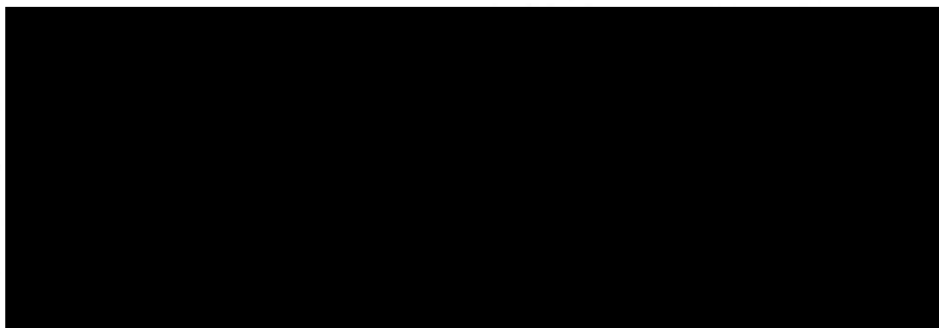
poskytovatele samostatný vstup do vyhrazených prostor objektu objednatele a samostatný pohyb v nich. Vstupní karta bude nepřenosná a bude vydávána odborem bankovní bezpečnosti a krizového řízení.

7. Vstupní karty budou vydávány objednatelem každému pracovníkovi poskytovatele jednotlivě proti podpisu, po předložení výpisu z rejstříku trestů, který nebude starší než tři měsíce. Výpis z rejstříku trestů bude vrácen pracovníkovi poskytovatele. Při převzetí vstupní karty bude pracovník poskytovatele poučen o způsobu používání vstupní karty a o režimu vstupu osob a vjezdu vozidel do objektu objednatele a o pohybu v něm.
8. Pracovník poskytovatele, kterému byla vydána vstupní karta, je povinen okamžitě po zjištění ztráty, odcizení, zneužití, zničení nebo poškození vstupní karty, které brání jejímu řádnému užívání, toto oznámit odboru bankovní bezpečnosti a krizového řízení.
9. Při ukončení pracovního poměru pracovníka poskytovatele uvedeného v seznamu nebo při ukončení plnění podle smlouvy je poskytovatel povinen neprodleně vrátit vstupní karty odboru bankovní bezpečnosti a krizového řízení.
10. Objednatel si vyhrazuje právo nevydat vstupní kartu pracovníkům poskytovatele bez udání důvodu.
11. Objednatel si vyhrazuje právo vstupní kartu pracovníku poskytovatele odebrat z důvodu porušení režimu vstupu osob a vjezdu vozidel do objektu objednatele nebo porušení režimu pohybu v něm.
12. Objednatel si vyhrazuje právo odvolat schválené pracovníky poskytovatele ze seznamu bez udání důvodů. Schválení pracovníci musí dodržovat směrnice ČNB a pokyny ostrahy pro vstup do vyhrazených prostor a pro pobyt v nich.
13. Pracovníci poskytovatele jsou povinni podrobit se při každém vstupu do objektu ČNB bezpečnostní kontrole prováděné bankovními policisty.
14. Objednatel si vyhrazuje právo nepustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
15. Vstup do objektů ČNB se zvířaty je zakázán.
16. Vstup soukromých návštěv do vnitřních prostor objektů ČNB je zakázán. Pro tyto účely je možné využít určené návštěvní místnosti.
17. Poskytovatel a jeho pracovníci budou věnovat při plnění díla v oblasti požární ochrany zvýšenou pozornost:
 - dodržování právních předpisů o požární ochraně,
 - předpisům objednatele při provádění požárně nebezpečných prací se zvýšeným požárním nebezpečím (svařování, řezání plamenem, pájení, broušení, rozbrušování apod.),
 - průrazům a průchodům u rozvodů instalací a technologií hranicemi požárních úseků, včetně zachování, obnovení nebo nového vyhotovení jejich protipožárních ucpávek.
18. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorců zaměstnance ČNB a dále instrukcemi vyhlášenými vnitřním rozhlasem.
19. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny, hořlavé kapaliny, tlakové lahve apod. O tom, co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
20. Fotografování a pořizování videozáznamů je ve všech prostorech objektů ČNB zakázáno.

Výjimku tvoří pořizování dokumentace technických havárií a poruch. Konkrétní případ musí předem písemně povolit ředitel odboru bankovní bezpečnosti a krizového řízení nebo ředitel příslušné pobočky ČNB.

21. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení k provedení požárně nebezpečné práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou dozorujícího zaměstnance ČNB, a to vždy nejpozději jeden pracovní den před zahájením prací.
22. Pracovníci poskytovatele se musí zdržet poškozování či zcizení majetku ČNB, a dále nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
23. Pracovníci poskytovatele uvedení na seznamu se musí před započítím výkonu práce v objektech objednatele prokazatelně seznámit s „Pravidly pro smluvní partnery ČNB k zajištění bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí v ČNB“ (dále jen „pravidla“). Pravidla budou v listinné formě předána zástupci poskytovatele požárním a bezpečnostním technikem ČNB. Zástupce poskytovatele s pravidly seznámí všechny dotčené pracovníky poskytovatele.
24. Objednatel je oprávněn v objektu ČNB kdykoliv podrobit kontrole kteréhokoliv pracovníka poskytovatele uvedeného na seznamu z dodržování požární ochrany, bezpečnosti práce a výše uvedených ustanovení.

Seznam pracovníků poskytovatele



Podrobná specifikace předmětu plnění

1. Činnosti uvedené v bodě 1, čl. I této smlouvy budou probíhat na systémovém prostředí sestávajícím z následujících technologií/produktů (uvedeny pouze vybrané položky):
 - a) Operační systém: Windows server 2008 R2, Windows server 2016, Windows 7, Windows 10, Red Hat Enterprise Linux 5/6/7
 - b) Databáze: Oracle DB 11/12, MSSQL
 - c) Aplikační servery: Oracle Application Server, WebLogic
 - d) Webové servery: Apache, Tomcat, Oracle HTTP Server, Microsoft IIS
 - e) Virtualizace: VMWare, OracleVM, Citrix XenApp
2. Pracovník dodavatele při plnění využívá své vlastní zařízení (notebook), které bude připojeno do vnitřní sítě ČNB, pokud nebude dohodnuto jinak. Pracovník dodavatele je povinen zajistit důvěrnost dat uložených na tomto zařízení pomocí šifrování pevného disku.
3. Pokud je to pro daný audit nutné, bude pracovník dodavatele vybaven přístupovým oprávněním pro testované prvky/IS a dodatečnými informacemi o testovaných prvcích/IS.
4. Pro každý audit bude pracovník dodavatele vybaven přesným vymezením testovaných prvků/IS buď ve formě IP adres, doménových jmen, nebo jiným vymezením rozsahu (části) aplikace/infrastruktury.
5. Během auditu bude pracovník dodavatele průběžně informovat kontaktní osobu objednatele o plánovaných dílčích testech a jejich výsledcích. Pokud dojde k nalezení vysoce rizikové zranitelnosti, pracovník dodavatele informuje kontaktní osobu objednatele neprodleně.
6. Před provedením testů, které by mohly mít dopad na dostupnost či integritu testovaných prvků/IS, je pracovník dodavatele povinen další postup konzultovat s kontaktní osobou objednatele a pokračovat pouze po získání jejího souhlasu.
7. Po skončení auditu a vytvoření závěrečné zprávy pracovník dodavatele buď veškerá data získaná během auditu smaže, nebo uloží do bezpečného úložiště s řízeným přístupem. Zejména tato data nesmí zůstat na zařízení, které bylo využíváno po dobu auditu.
8. Pokud bude zařízení pracovníka dodavatele odnášeno během auditu mimo prostory ČNB, je nezbytné vždy konzultovat rozsah a obsah dat, která se nachází na tomto zařízení, s kontaktní osobou objednatele.
9. Celý proces auditu bude pracovníkem dodavatele dokumentován. Zaznamenány budou jednotlivé kroky v dostatečné podrobnosti a s časovými značkami. Také budou vytvořeny logy z využitých nástrojů (těch, které toto podporují). Tato dokumentace bude předána objednateli společně se závěrečnou zprávou.
10. Na vyžádání dodavatel poskytne závěrečnou formální prezentaci výsledků auditu v sídle objednatele.

Ujednání o zpracování osobních údajů
v souvislosti s **poskytováním služeb bezpečnostního auditu informačních systémů**
(dále také jen „**ujednání**“)

Objednatel a poskytovatel se dohodli na tomto ujednání, které splňuje požadavky na smlouvu o zpracování osobních údajů podle ustanovení § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ZOOÚ“).

Článek I
Úvodní ustanovení

1. Objednatel v souladu se smlouvou o poskytování služeb bezpečnostních auditů informačních systémů, evidenční číslo: 92-442-17 (dále také jako „smlouva“), určuje účel a prostředky zpracování osobních údajů subjektů údajů, kterými jsou uživatelé informačních systémů v systémovém prostředí objednatele a zaměstnanci objednatele (společně dále také „subjekty údajů“), kdy objednatel je v postavení správce osobních údajů ve smyslu § 4 písm. j) ZOOÚ.
2. Poskytovatel bude na základě smlouvy zpracovávat osobní údaje subjektů údajů a bude v postavení zpracovatele osobních údajů ve smyslu § 4 písm. k) ZOOÚ.

Článek II
Účel ujednání

3. Účelem tohoto ujednání je úprava práv a povinností smluvních stran při zpracování a v souvislosti se zpracováním osobních údajů zpracovatelem při plnění povinností ze smlouvy tak, aby zpracování probíhalo v souladu s právními předpisy o ochraně osobních údajů.

Článek III
Předmět ujednání

1. Toto ujednání upravuje vztahy mezi správcem a zpracovatelem osobních údajů, zejména pak vymezuje rozsah osobních údajů, které bude zpracovatel zpracovávat, prostředky a účel, pro který bude osobní údaje zpracovávat, dobu zpracování osobních údajů a podmínky a záruky zpracovatele osobních údajů z hlediska technického a organizačního zabezpečení ochrany osobních údajů.

Článek IV
Účel a rozsah zpracování osobních údajů

1. Zpracovatel bude zpracovávat veškeré osobní údaje subjektů údajů pouze v rozsahu nezbytném pro zajištění realizace smlouvy, ve znění pozdějších dodatků. Za osobní údaje jsou podle tohoto ujednání považovány veškeré informace v níže uvedených výčtech (dále také jako „osobní údaje“).
2. Zpracovatel je oprávněn zpracovávat osobní údaje předané ze strany správce pro účely řádného plnění povinností podle smlouvy, tj. zejména zajištění řádného provedení bezpečnostních auditů pouze v následujícím rozsahu nezbytném pro výkon práv a povinností podle smlouvy:
 - adresní a identifikační údaje (např. jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, telefonní spojení domů, do zaměstnání apod.)

- popisné údaje (např. vzdělání, znalost cizích jazyků, odborné znalosti a dovednosti, počet dětí, obrazový záznam z kamerového systému, vojenská služba, předchozí zaměstnání, zdravotní pojišťovna, mzda, číslo cestovního dokladu, bankovní spojení apod.)
 - údaje o jiné osobě (např. adresní a identifikační údaje člena rodiny, manžel/manželka, dítě apod.)
3. Zpracovatel bude osobní údaje zpracovávat pouze ve formě možného nahlédnutí zpracovatele do osobních údajů ve smyslu § 4 písm. e) ZOOÚ. Toto nahlédnutí přitom není cílem plnění smlouvy, ale může k němu v rámci spolupráce správce se zpracovatelem docházet.
 4. Zpracovatel je ve všech případech při zpracování osobních údajů subjektů údajů vázán prokazatelnými pokyny správce. Zpracovatel nesmí bez předchozího prokazatelného výslovného souhlasu anebo pokynu správce zpracovávané osobní údaje nijak upravit nebo pozměnit, třídít nebo kombinovat, zpřístupnit ani předat třetí osobě, šířit ani zveřejňovat, ani jakýmkoli způsobem použít pro vlastní potřebu.

Článek V Doba zpracování

1. Zpracovatel bude všechny osobní údaje zpracovávat pouze způsobem podle čl. IV odst. 3 po dobu nezbytně nutnou pro účel bezprostředního plnění smlouvy ve vztahu ke konkrétnímu informačnímu systému obsahujícímu osobní údaje.

Článek VI Práva a povinnosti smluvních stran

1. Správce pověřuje zpracovatele zpracováním osobních údajů výhradně za účelem zajištění služeb bezpečnostního auditu informačních systémů a infrastruktury a za účelem splnění povinností stanovených platnými právními předpisy.
2. Zpracovatel se zavazuje, že osobní údaje nebudou zpracovatelem použity, zpřístupněny, zpracovávány či poskytnuty třetím osobám, nebudou předávány mimo území EU či s nimi nebude nakládáno jinak, než pouze za účelem, pro který byly osobní údaje zpřístupněny a v souladu s pokyny správce.
3. Zpracovatel je povinen zabezpečit osobní údaje a zachovávat mlčenlivost o osobních údajích a řídit se pokyny správce ve všech případech, kdy se jedná o zpracování či zabezpečení osobních údajů. Zpracovatel přijme technická, organizační a personální opatření adekvátní způsobu zpracování a v souladu s pokyny správce – přičemž toto zabezpečení bude odpovídat příslušným aktuálním používaným bezpečnostním standardům (podrobněji v odst. 5 a násl. tohoto článku VI. ujednání).
4. Správce stanoví opatření, která považuje za dostatečná pro technické a personální zabezpečení osobních údajů následovně:
 - a) Technické zabezpečení osobních údajů se zajistí pomocí prostředků:
 - (i) počítačové bezpečnosti; zpracovatel se zavazuje ke zpracování používat výhradně takové technické a programové prostředky, jejichž používání při vyloučení nepředvídatelných okolností eliminuje možnost narušení, neoprávněného přístupu k osobním údajům či neoprávněného nakládání s osobními údaji;
 - (ii) komunikační bezpečnosti; zpracovatel se zavazuje dodržovat taková opatření k zabezpečení ochrany osobních údajů při jejich přenosu telekomunikačními kanály, jejichž povaha eliminuje při vyloučení nepředvídatelných okolností možnost narušení (šifrování);
 - (iii) fyzické bezpečnosti; v tomto ohledu zpracovatel prohlašuje, že místo, ve kterém budou osobní

údaje zpracovávají a ve kterém budou uchovávány spisy a dokumenty, bude mít charakter prostoru zabezpečeného před možností narušení.

Zpracovatel bude plnit povinnosti stanovené v tomto odstavci, písm. a) po bodech (i) až (iii) využíváním prostředků odpovídajících dosaženému stupni technického pokroku a možnostem zpracovatele.

b) Personální zabezpečení:

- (i) osobní údaje budou zpřístupněny pouze určeným osobám z oprávněného personálu zpracovatele a případně oprávněným osobám, které odpovídají za zajištění bezpečnosti systémů, kde jsou osobní údaje uloženy, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;
- (ii) zpracovatel je povinen zabezpečit poučení všech osob, které mají v rámci zpracování osobních údajů přístup k těmto údajům, aby tyto osoby byly řádně poučeny o svých povinnostech při zpracovávání osobních údajů, zejména pak o povinnosti mlčenlivosti ve vztahu k těmto osobním údajům.

c) Dále je zpracovatel povinen zajistit následující:

- (i) zpracovatel je povinen zabránit neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování a dále zabránit neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje.
5. Zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s právními předpisy, zejména se ZOOÚ a dalšími předpisy regulujícími ochranu osobních údajů, jakož i provádět nejméně jednou ročně hodnocení efektivnosti přijatých opatření, a to včetně vedení a zpřístupnění následující dokumentace:
- seznamu osob, které jsou oprávněny přistupovat k osobním údajům (včetně rozsahu oprávnění);
 - elektronického přehledu informací o veškerých přístupech jednotlivých osob k osobním údajům;
 - elektronického přehledu informací o nakládání s osobními údaji.
6. Zpracovatel bude neprodleně písemně informovat správce v případě jakýchkoliv potíží při plnění povinností z tohoto ujednání a o všech okolnostech týkajících se porušení povinností při zpracování a ochraně osobních údajů, zejména pokud dojde k neoprávněnému přístupu k osobním údajům, či k jejich ztrátě nebo zničení. V takovém případě zpracovatel přijme v nejkratším možném termínu veškerá nezbytná opatření k zajištění ochrany osobních údajů, notifikuje správce o těchto skutečnostech prostřednictvím kontaktní osoby/osob uvedených ve smlouvě a následně postupuje v souladu se ZOOÚ a pokyny správce, budou-li mu sděleny.
7. Zpracovatel plní informační povinnost vůči subjektům údajů v souladu se ZOOÚ a dle požadavků správce. V případě, že v souvislosti se zpracováním osobních údajů zpracovatelem bude zahájeno řízení ze strany orgánu veřejné správy, zpracovatel poskytne správci v těchto řízeních veškerou potřebnou součinnost.
8. Zpracovatel je správci na jeho žádost nápomocen při posuzování vlivu zpracovávání osobních údajů na ochranu osobních údajů a při konzultacích správce s dozorovým orgánem, při zohlednění povahy zpracovávání a informací, jež má zpracovatel k dispozici.
9. Zpracovatel je správci na jeho žádost nápomocen při výkonu práv subjektů osobních údajů, a to zejména při výkonu práva na přístup k osobním údajům, práva na opravu, výmaz a omezení zpracovávání osobních údajů, práva na přenositelnost údajů a práva vznést námitku vůči zpracovávání osobních údajů.
10. Zpracovatel nezapojí do zpracovávání osobních údajů dalšího zpracovatele bez předchozího písemného povolení správce. V případě, že jakákoliv část zpracovávání osobních údajů bude vykonávána dalším zpracovatelem po předchozím písemném povolení správce, zůstává

zpracovatel plně odpovědný vůči správci za zpracovávání osobních údajů. Správce si vyhrazuje právo uzavřít s dalším potencionálním zpracovatelem zvláštní smlouvu o zpracovávání osobních údajů.

11. Správce je oprávněn kontrolovat dodržování pravidel stanovených pro zpracování ZOOÚ či tímto ujednáním u zpracovatele, resp. na jiném místě, kde dochází ke zpracování údajů. Zpracovatel za tímto účelem zajistí zástupcům správce, kteří budou k provedení kontroly pověřeni, přístup ke všem relevantním informacím a na příslušná místa tak, aby mohlo dojít k hodnocení oprávněnosti zpracování. Zpracovatel poskytne správci na jeho vyžádání veškeré podklady o přijatých a provedených technicko-organizačních opatřeních k zajištění ochrany osobních údajů.
12. Po ukončení poskytování služeb dle smlouvy zpracovatel vrátí veškeré osobní údaje správci, s výjimkou těch údajů, které je zpracovatel povinen uchovávat na základě platných právních předpisů.

Článek VII

Odpovědnost za škodu a smluvní pokuty

1. Tento článek upravuje odpovědnost za škodu a smluvní pokuty pro případ porušení tohoto ujednání. Znění tohoto článku VII. se nevztahuje na smluvní pokuty a úrok z prodlení podle smlouvy, který zůstává zachován.
2. Zpracovatel se zavazuje odškodnit správce za jakékoliv nároky, a to zejména zadostiučinění, peněžité náhrady nebo pokuty, úspěšně uplatněné v soudním popř. správním řízení třetími osobami, a to zejména subjekty údajů nebo Úřadem na ochranu osobních údajů, které vznikly v příčinné souvislosti s porušením povinností stanovených ZOOÚ nebo tímto ujednáním ze strany zpracovatele.
3. Pokud dojde k prokazatelnému porušení ZOOÚ pouze v důsledku jednání té smluvní strany, které je uložena pokuta podle § 45 ZOOÚ, hradí náklady na uhrazení pokuty plně ta strana, která ZOOÚ porušila a již současně byla uložena pokuta.
4. V případě, že zpracovatel správci neumožní kontrolu ohlášenou v souladu s čl. VI. odst. 12 tohoto ujednání, anebo během ní správci neposkytne pro předmět kontroly potřebnou součinnost, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1.000,- Kč za každý započatý pracovní den takto trvajících prodlení na straně zpracovatele.
5. Zpracovatel je povinen odstranit kontrolou zjištěné nedostatky neprodleně, nejpozději ve lhůtě 5 dnů, nedohodnou-li se smluvní strany jinak. V případě, že zpracovatel neodstraní kontrolou zjištěné nedostatky ve lhůtě stanovené dle předchozí věty, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1.000,- Kč za každý započatý den prodlení na straně zpracovatele.
6. V případě, že zpracovatel poruší kteroukoli z povinností sjednaných v čl. VI. (vyjma čl. VI. odst. 12) tohoto ujednání, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 5.000,- Kč za každý jednotlivý případ takového porušení.
7. Ujednáním o smluvní pokutě podle tohoto článku VII. není dotčeno právo správce na náhradu škody vzniklé z porušení povinností v plné výši.

Článek VIII

Trvání závazků

1. Povinnost zpracování osobních údajů se sjednává pouze na dobu existence závazkového vztahu vzniklého ze smlouvy, nejpozději do dne likvidace posledního zpracovávaného osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOÚ.

Článek IX Další ujednání

1. Zpracovatel se zavazuje plnit veškeré povinnosti vyplývající z obecného nařízení o ochraně osobních údajů (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), a to ode dne jeho účinnosti (25. května 2018).
2. Smluvní strany se zavazují vstoupit v jednání o doplnění tohoto ujednání, jehož potřeba případně vzejde z účinnosti obecného nařízení podle odst. 1 tohoto čl. IX., a poskytnout si veškerou potřebnou součinnost ke sjednání dodatku smlouvy, pokud bude pro potřeby plnění požadavků tohoto obecného nařízení potřebný.
3. Za písemnou formu se pro účely tohoto ujednání nepovažuje e-mailová či jiná elektronická forma. Výjimkou je situace, v níž zpracovatel informuje správce ve smyslu čl. VI. odst. 7 tohoto ujednání (potíže při plnění povinností z tohoto ujednání a okolnosti týkající se porušení povinností při zpracování a ochraně osobních údajů) a oznámení kontroly ve smyslu čl. VI. odst. 12 ujednání, které lze provést i elektronickým oznámením prokazatelně doručeným druhé smluvní straně. V případě oznámení kontroly postačuje prokazatelné odeslání oznámení správcem na e-mailovou adresu uvedenou pro tento účel zpracovatelem. V případě oznámení kontroly postačuje prokazatelné odeslání oznámení správcem na e-mailovou adresu zpracovatele uvedenou ve smlouvě.