

**Dodatek č. 1  
ke smlouvě o poskytování služby SOC**

uzavřený mezi:

**Českou národní bankou**

Na Příkopě 28

115 03 Praha 1

zastoupenou: Ing. Milanem Zirmsákem, ředitelem sekce informatiky

a

Ing. Zdeňkem Viriusem, ředitelem sekce správní

IČO: 48136450

DIČ: CZ48136450

(dále jen „objednatel“ nebo „ČNB“)

a

**T-Mobile Czech Republic a.s.**

Tomíčková 2144/1

148 00 Praha 4

zastoupenou: Ing. Václavem Molíkem, Manažerem domény cloud a kybernetické bezpečnosti,  
na základě pověření

a

Ing. Petrem Žáčkem, Manažerem prodeje segmentu bankovníctví a financí,  
na základě pověření

č. účtu: 19-2271190247/0100

IČO: 64949681

DIČ: CZ64949681

(dále jen „poskytovatel“)

**Preambule**

Smluvní strany uzavřely dne 3. 10. 2018 Smlouvu o poskytování služby SOC, evidenční číslo smlouvy ČNB: 92-051-18 (dále jen „smlouva“). V souladu s čl. XI odst. 3 smluvní strany uzavírají tento dodatek, jehož předmětem je úprava a doplnění práv a povinností smluvních stran vyplývajících z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB“).

**Článek I  
Změny smlouvy**

1. Poskytovatel bere na vědomí, že objednatel je správcem informačních systémů kritické informační infrastruktury dle ustanovení § 3 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické

Č. zákazníka: 10418553 Č. kontraktu: 40114932984-11, 124010118986-11

DocType: KAS; SubType: PC; Kód dokumentu: 105

CERTIFIKACE - K03-2018-012 - 29-05-2019

bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“) a správcem významných informačních systémů dle ustanovení § 3 písm. e) ZKB, zejména informačních systémů ABO, CERTIS, SKD, KRZR a JERRS.

2. Poskytovatel je při plnění smlouvy v postavení významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VKB.
3. Rozsah zapojení poskytovatele na zajištění bezpečnosti aktiv informačních systémů kritické informační infrastruktury a aktiv významných informačních systémů používaných v prostředí objednatele je určen předmětem smlouvy.
4. Poskytovatel je při poskytování plnění oprávněn užívat data předaná mu objednatelem za účelem plnění předmětu smlouvy či data za tímto účelem získaná pouze v rozsahu nezbytném ke splnění smlouvy a pouze v souladu s touto smlouvou a příslušnými právními předpisy, tj. zejména ZKB a VKB.
5. Poskytovatel se zavazuje zajistit, aby jeho pracovníci či poddodavatelé poskytovatele a jejich pracovníci v plném rozsahu dodržovali „Obecná pravidla pro dodavatele v oblasti bezpečnosti IT“ uvedená v příloze tohoto dodatku (dále jen „pravidla bezpečnosti“). Pravidla bezpečnosti se stávají přílohou č. 9 smlouvy.
6. Poskytovatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy, a zajistit ve spolupráci s objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční a efektivní.
7. Poskytovatel je srozuměn s tím, že objednatel provádí v pravidelných intervalech hodnocení rizik v souvislosti s informačními systémy dle odstavce 1 tohoto článku, kterých se týká poskytování plnění dle smlouvy.
8. Poskytovatel se zavazuje poskytnout objednateli veškerou potřebnou součinnost k zajištění splnění povinností objednatele vyplývajících z § 11 VKB, bude-li takové součinnosti třeba.
9. Poskytovatel se zavazuje informovat objednatele o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním předmětu smlouvy a dále jaká jsou zbytková rizika související s plněním smlouvy.
10. Dojde-li u poskytovatele k výskytu bezpečnostních incidentů vzniklých v souvislosti s plněním smlouvy, zavazuje se poskytovatel o těchto bezpečnostních incidentech bezodkladně informovat objednatele.
11. Poskytovatel se zavazuje informovat objednatele o významné změně ovládání poskytovatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny.
12. Poskytovatel se zavazuje informovat objednatele o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem k plnění smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.

13. Poskytovatel je povinen zajistit, aby byly v případě ukončení smlouvy veškerá data a informace získané či vzniklé v souvislosti s plněním této smlouvy likvidovány bezpečným způsobem, který zaručí, že nebude možné zrekonstruovat jednotlivé datové struktury, části dat a informací do podoby, jež by umožnily identifikovat obsah a zpracování nebo použití dat a/nebo informací na konkrétním nosiči dat. Poskytovatel je přitom povinen zajistit soulad postupu při likvidaci dat s přílohou č. 4 VKB.
14. Dojde-li za dobu účinnosti smlouvy ke změnám ZKB a/nebo VKB takového charakteru a rozsahu, že s nimi nebude smlouva v souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran, a to bez zbytečného odkladu poté, co legislativní změny ZKB a/nebo VKB nabydou platnosti.
15. Objednatel je oprávněn odstoupit od smlouvy, pokud dojde k významné změně kontroly nad poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými poskytovatelem k plnění smlouvy a tato změna bude objednatelům vyhodnocena jako bezpečnostní riziko ve smyslu ZKB a/nebo VKB.
16. V souladu s čl. VIII odst. 4 smlouvy je objednatel oprávněn požadovat smluvní pokutu v případě porušení jakékoliv povinnosti poskytovatele dle tohoto článku, a to ve výši 20 000 Kč za každé jednotlivé porušení.

## **Článek II**

### **Závěrečná ustanovení**

1. Ostatní ustanovení smlouvy nedotčená tímto dodatkem zůstávají v platnosti beze změn.
2. Tento dodatek nabývá platnosti a účinnosti dnem podpisu oběma smluvními stranami.
3. Dodatek se vyhotovuje ve čtyřech stejnopisech, přičemž objednatel obdrží tři stejnopisy a poskytovatel obdrží jeden stejnopis.

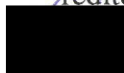
**Přílohy:** nová příloha č. 9 smlouvy „Obecná pravidla pro dodavatele v oblasti bezpečnosti IT“

V Praze dne: 4. 6. 2019

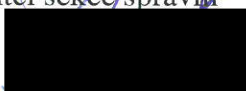
Za objednatele:



Ing. Milan Zírnsák  
ředitel sekce informatiky



Ing. Zdeněk Virius  
ředitel sekce správy



**ČNB** ČESKÁ NÁRODNÍ BANKA  
Na Příkopě 28, 115 03 Praha 1  
48

V Praze dne: 03-06-2019 2019

Za poskytovatele:



Ing. Václav Mólík  
Manažer domény cloud a  
kybernetické bezpečnosti  
na základě pověření



Ing. Petr Žáček  
Manažer prodeje segmentu  
bankovníctví a financí  
na základě pověření



T-Mobile Czech Republic a.s.  
Tomášková 2144/1  
148 00 Praha 4  
IČ: 649 49 681, DIČ: CZ64949681

435



## **Příloha č. 9**

### **Obecná pravidla pro dodavatele v oblasti bezpečnosti IT**

- 1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu smlouvy nebo zadávací dokumentace nebo její jiná příloha.
- 2) Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovávají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
- 3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
- 4) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
- 5) Dodavatel a jeho pracovníci nejsou oprávněni:
  - a) obcházet bezpečnostní mechanismy prostředků výpočetní techniky;
  - b) sdělovat své přístupové údaje k systémům ČNB;
  - c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelským oprávněním);
  - d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
- 6) Dodavatel a jeho pracovníci jsou povinni:
  - a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejít bezpečnostních mechanismů prostředků výpočetní techniky. To neplatí pro dodavatele a uživatele, jejichž předmět smlouvy nebo pracovní náplň obsahuje tuto činnost.
- 7) Pracovníci dodavatele nesmí:
  - a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);
  - b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).
- 8) Pracovníci dodavatele nejsou oprávněni:
  - a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;
  - b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

- c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB (případně pod správou dodavatele nebo smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).
- 9) Dodavatel a jeho pracovníci nejsou oprávněni:
- a) nepovoleně používat, kopírovat a šířit software;
  - b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;
  - c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

#### **Archivace elektronické pošty**

- 1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.
- 2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

#### **Kontrola přístupu na Internet**

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů ze sítě ČNB na Internet automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).