Evidenční číslo smlouvy ČNB: 92-099-18
Evidenční číslo dodatku č. 1 ČNB: 92-215-19

Dodatek č. 1
smlouvy o poskytování datových služeb

uzavřený mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „uživatel")

a

O2 Czech Republic a.s.
Za Brumlovkou 266/2
140 22 Praha 4
zastoupenou: Martin Zach, Manažer, TOP CS - Finance
IČO: 60193336
DIČ: CZ60193336

(dále jen „provozovatel")

Preambule

Smluvní strany uzavřely dne 27. 17. 2018 smlouvu o poskytování datových služeb, evidenční číslo smlouvy ČNB: 92-099-18 (dále jen „smlouva"). V souladu s čl. X odst. 7 smlouvy 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. Provozovatel bere na vědomí, že uživatel 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 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. Provozovatel je při plnění smlouvy v postavení významného dodavatele ve smyslu § 2 písm. n) VKB.

[redacted]

3. Provozovatel prohlašuje, že v okamžiku uzavření tohoto dodatku má platnou certifikaci dle ISO 27001, zahrnující předmět smlouvy, a zavazuje se tuto certifikaci udržovat po dobu platnosti a účinnosti smlouvy.
4. Rozsah zapojení provozovatele na zajištění bezpečnosti aktiv informačních systémů kritické informační infrastruktury a aktiv významných informačních systémů používaných v prostředí uživatele je určen předmětem smlouvy.
5. Provozovatel je při poskytování plnění oprávněn užívat data předaná mu uživatelem 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.
6. Provozovatel se zavazuje dodržovat „Obecná pravidla pro dodavatele v oblasti bezpečnosti IT" uvedené v příloze č. 8 tohoto dodatku. Dále se provozovatel zavazuje zajistit, aby též jeho pracovníci či poddodavatelé a jejich pracovníci dodržovali uvedené požadavky v plném rozsahu. Obecná pravidla pro dodavatele v oblasti bezpečnosti IT se stávají přílohou č. 8 smlouvy.
7. Provozovatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit uživatele 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 uživatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční a efektivní.
8. Provozovatel je srozuměn s tím, že uživatel provádí v pravidelných intervalech hodnocení rizik v souvislosti s informačními systémy dle odstavce 1 tohoto článku, kterých se týká poskytování plnění dle smlouvy.
9. Dojde-li u provozovatele nebo jeho poddodavatelů k výskytu bezpečnostních incidentů vzniklých v souvislosti s plněním smlouvy, zavazuje se provozovatel o těchto bezpečnostních incidentech bezodkladně informovat uživatele.
10. Provozovatel se zavazuje informovat uživatele o významné změně ovládání provozovatele. 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.
11. Provozovatel se zavazuje informovat uživatele o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými provozovatelem k plnění smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.
12. Uživatel je oprávněn odstoupit od smlouvy, pokud dojde k významné změně kontroly nad provozovatelem, 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 provozovatelem k plnění smlouvy a tato změna bude uživatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZKB a/nebo VKB.
13. V případě porušení jakékoliv povinnosti provozovatele dle tohoto článku, je uživatel oprávněn požadovat smluvní pokutu ve výši 50 000 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 uživatel obdrží tři stejnopisy a provozovatel obdrží jeden stejnopis.

Přílohy: nová příloha č. 8 smlouvy „Obecná pravidla pro dodavatele v oblasti bezpečnosti IT"

V Praze dne: 17 -03- 2020
Za uživatele:

[redacted]

Ing. Milan Zirnsák
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

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

V Praze dne: 11. 3. 2020
Za provozovatele:

[redacted]

Martin Zach
Manažer, TOP CS - Finance

Příloha č. 8

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, zachovají 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) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) 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.
6) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Dodavatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit, a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.

8) 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).
9) 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 nebo dodavatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).
10) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) nepovoleně používat, kopírovat a šířit software, jako např.:
      i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);
      ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy obsahuje tuto činnost;
      iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí
         (1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a
         (2) v případech, kdy předmět smlouvy obsahuje tuto činnost;
   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 na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).