



Řízení letového provozu České republiky

Dodatek č. 15 ke smlouvě o poskytování veřejně dostupných služeb elektronických komunikací (ve znění dodatků č. 1 – 14)

(dále jen „**dodatek**“)

1. Smluvní strany

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

se sídlem: Navigační 787, 252 61 Jeneč

zastoupený: Ing. Janem Klasem, generálním ředitelem

IČO: 497 10 371

DIČ: CZ699004742

bankovní spojení: ČSOB Praha 5, č. účtu 88153/0300

SWIFT kód: CEKOCZPP

zapsaný v obchodním rejstříku vedeném Městským soudem v Praze v oddíle A, vložce 10771,

(dále jen „**uživatel**“)

a

O2 Czech Republic a.s.

se sídlem: Za Brumlovkou 266/2, 140 22 Praha 4

zastoupený: 

IČO: 601 93 336

DIČ: CZ60193336

bankovní spojení: 

zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze v oddíle B, vložce 2322

(dále jen „**poskytovatel**“)

(zákazník a poskytovatel rovněž jako „**smluvní strany**“).

2. Preambule

- 2.1 Smluvní strany uzavřely dne 29.10.2009 smlouvu o poskytování veřejně dostupných služeb elektronických komunikací (číslo smlouvy ŘLP ČR, s.p.: 36/09), ve znění dodatku č. 1 – dodatku č. 14 (dále jen „**smlouva**“).
- 2.2 Vzhledem k tomu, že poskytovatel byl vyhodnocen jako významný dodavatel ve smyslu § 2, písm. n) vyhlášky č. 82/2018 Sb. ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), uzavírají smluvní strany tento dodatek, kterým do smlouvy formou přílohy ke smlouvě implementují požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti).

3. Předmět dodatku

- 3.1 S ohledem na skutečnosti uvedené v odst. 2.2 tohoto dodatku se smluvní strany dohodly, že nedílnou součástí smlouvy se stává příloha č. 1 tohoto dodatku, která obsahuje požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti (tj. informace týkající se bezpečnostních opatření pro smluvní vztahy s významnými dodavateli), přičemž zmíněná příloha č. 1 tohoto dodatku tvoří přílohu č. 8 smlouvy.

- 3.2 Čl. 6 smlouvy, Úrok z prodlení a smluvní pokuta, se doplňuje o následující odstavce:

„6.5 Pokud poskytovatel způsobí škodu porušením povinností uvedených v příloze č. 8 této smlouvy, případně porušením povinností uvedených v bezpečnostních pravidlech zasílaných dle čl. 6 přílohy č. 8 této smlouvy, je povinen ji na vyžádání uživatele bezodkladně nahradit.

6.6. Je-li újma způsobena poddodavatelem, kterým poskytovatel nahradí stávajícího poddodavatele, je poddodavatel povinen k náhradě újmy společně s poskytovatelem, a to společně a nerozdílně.

6.7 Pokud poskytovatel poruší ohlašovací povinnost v oblasti bezpečnostních událostí / incidentů stanovenou v bezpečnostních pravidlech zasílaných dle čl. 8 přílohy č. této smlouvy, je uživatel oprávněn požadovat smluvní pokutu ve výši 100.000,- Kč (slovy: jednostotísíc korun českých) za každý jednotlivý případ porušení.

6.8 Pokud poskytovatel nezajistí v oboustranně odsouhlaseném termínu realizaci oboustranně odsouhlasených nápravných opatření vyplývajících ze zákaznického auditu provedeného dle podmínek popsaných v čl. 15 přílohy č. 8 této smlouvy a dále upřesňované v bezpečnostních pravidlech zasílaných dle čl. 6 přílohy č. 8 této smlouvy, je uživatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení.

6.9 Zaplacením smluvní pokuty nezaniká uživateli nárok na náhradu újmy. Smluvní strany se dohodly, že maximální souhrnná výše náhrady újmy a smluvních pokut, kterou je uživatel oprávněn uplatnit vůči poskytovateli, činí částku ve výši 20% celkové ceny servisní podpory poskytované podle smlouvy.“

- 3.3 V článku 7 smlouvy, Odstoupení od smlouvy, se mění odst. 7.4 smlouvy, a to tak, že odst. 7.4 smlouvy zní nově následovně:

- „7.4 Uživatel je od této smlouvy oprávněn odstoupit v případě významné změny kontroly nad poskytovatelem nebo změně kontroly nad zásadními aktivy využívanými poskytovatelem k plnění podle smlouvy, přičemž významnou změnou kontroly se rozumí změna ovládající osoby dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.“
- 3.4 Původní odst. 7.4 smlouvy se nově přečíslovává na odst. 7.5, původní odst. 7.5 smlouvy se nově přečíslovává na odst. 7.6, původní odst. 7.6 smlouvy se nově přečíslovává na odst. 7.7.
- 3.5 Odst. 11.3 a 11.4 smlouvy se ruší. Odst. 11.5 smlouvy se nově přečíslovává na odst. 11.3, odst. 11.6 smlouvy se nově přečíslovává na odst. 11.4, odst. 11.7 smlouvy se nově přečíslovává na odst. 11.5, odst. 11.8 smlouvy se nově přečíslovává na odst. 11.6, odst. 11.9 smlouvy se nově přečíslovává na odst. 11.7, odst. 11.10 smlouvy se nově přečíslovává na odst. 11.8.
- 3.6 V článku 10. Ostatní ujednání, se ruší odst. 10.7 smlouvy, který byl do smlouvy začleněn dodatkem č. 7. Zrušený odst. 10.7 smlouvy se nahrazuje novým odst. 10.7, který zní následovně:
- „10.7 Vstup externích subjektů do areálů a objektů uživatele
- Poskytovatel je povinen dodržovat pravidla vstupu externích subjektů do areálů a objektů uživatele. Povinnosti poskytovatele týkající se vstupu externích subjektů do areálů a objektů uživatele jsou uvedeny na následující webové stránce <http://www.rlp.cz/spolecnost/Stranky/Vstupy.aspx>“
- 3.7 Ruší se příloha č. 5 smlouvy – Kontaktní osoby.
- 3.8 Do článku 10. Ostatní ujednání, se přidává nový odst. 10.8 smlouvy, který zní následovně:
- „10.8 Kontaktními osobami pro účely této smlouvy jsou:
- 10.8.1 Za uživatele: [REDAKCE]
- 10.8.2 Za poskytovatele: [REDAKCE]
- 3.9 Do článku 10. Ostatní ujednání, se dále přidává nový odst. 10.9 smlouvy, který zní následovně:
- 3.10 „10.9 Kontaktní údaje manažerů kybernetické bezpečnosti a další kontaktní údaje nezbytné pro plnění této smlouvy budou druhé smluvní straně předány prostřednictvím kontaktních osob uvedených v odst. 10.8.1 a 10.8.2 této smlouvy. Tyto kontaktní údaje/osoby mohou být čas od času měněny, nicméně každá taková změna musí být druhé smluvní straně neprodleně oznámena prostřednictvím kontaktních osob uvedených v článku 10.8.1 a 10.8.2 této smlouvy. Komunikace ohledně kontaktních údajů manažera kybernetické bezpečnosti a dalších kontaktních údajů bude mezi uvedenými kontaktními osobami probíhat formou dopisu zaslaného prostřednictvím poskytovatele poštovní licence, prostřednictvím datové schránky nebo elektronicky podepsaným emailem.“
- 3.11 Do článku 10. Ostatní ujednání, se dále přidává nový odst. 10.10 smlouvy, který zní následovně:
- „10.10 Kontakty H24 smluvních stran jsou následující:
- 10.10.1 Kontakt H24 za uživatele: tel. 220 374 081
- 10.10.2 Kontakt H24 za poskytovatele: tel. 800 333 777
- 10.10.3 Poskytovatel bere na vědomí, že telefonní linka H24 uživatele uvedená v odst. 10.10.1 této smlouvy je nahrávána z důvodu zajištění všech potřebných podkladů pro případná šetření incidentů v leteckém provozu. Výstupy z těchto šetření jsou následně využity pro zvýšení bezpečnosti leteckého provozu.“

4. Závěrečná ustanovení dodatku

4.1 Ostatní ustanovení smlouvy zůstávají v platnosti beze změn.

4.2 **Tento dodatek se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**

4.3 Tento dodatek nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv.

Uveřejnění. Poskytovatel bere na vědomí, že uživatel je povinen uveřejnit tento dodatek v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv (zákon o registru smluv) ve znění pozdějších předpisů.

Při uveřejnění tohoto dodatku (tj. dodatku č. 15) v registru smluv budou znečitelněny tyto údaje: bankovní spojení poskytovatele v čl. 1 dodatku č. 15, jméno osoby zastupující poskytovatele v čl. 1 a u podpisu a dále podpisy na dodatku č.15.

4.4 Nedílnou součástí tohoto dodatku je následující příloha:

Příloha č. 1 dodatku tvořící novou přílohu č. 8 smlouvy – „Bezpečností opatření pro smluvní vztahy s významnými dodavateli dle přílohy č. 7 vyhlášky č. 82/2018 Sb. bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“

.....

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

Key Account Manager O2 Czech Republic a.s.

O2 Czech Republic a.s.

Příloha č. 1 - Zajištění opatření v oblasti informační a kybernetické bezpečnosti

„Smluvní zajištění opatření v oblasti informační a kybernetické bezpečnosti ve smyslu § 8, odst. 2 vyhlášky č 82/2018 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“

1. Preambule

- 1.1 Smluvní partner bere na vědomí, že je významným dodavatelem dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti pro objednatele Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.), který je správcem informačních a komunikačních systémů kritické informační infrastruktury. Dodavatelem se pro účely této přílohy smlouvy rozumí společnost O2 Czech Republic, a.s., která je ve smlouvě označena jako „poskytovatel“. Objednatelem se pro účely této přílohy dodatku smlouvy rozumí ŘLP ČR, s.p., který je ve smlouvě veden jako „uživatel“.
- 1.2 Systémy, k nimž se vztahuje role významného dodavatele, jsou uvedeny v Příloze č. 2 smlouvy.
- 1.3 Dodavatel se zavazuje dodržovat požadavky systému řízení bezpečnosti informací uvedené v této příloze dodatku smlouvy, smlouvě a bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.
- 1.4 Plnění dále uvedených bezpečnostních pravidel vyžaduje objednatel ve vztahu ke všem systémům uvedeným v čl. 1.2 této přílohy dodatku smlouvy. U ostatních systémů je dodržování bezpečnostních pravidel vyžadováno přiměřeným způsobem v souladu s nejlepší praxí informační bezpečnosti.
- 1.5 Pokud je některé z ustanovení smlouvy a jejích příloh v konfliktu s ustanoveními této přílohy dodatku smlouvy nebo bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy, postupuje dodavatel v souladu s ustanoveními později uzavřeného ujednání.

2. Definice pojmů

- 2.1 „Aktivem“ se rozumí souhrn informací a služeb, které jsou nezbytné pro provozování systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.
- 2.2 „Bezpečnostním incidentem“ se rozumí narušení bezpečnosti informací systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.
- 2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti informací systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy, jeho dostupnosti a spolehlivosti v kybernetickém prostoru.
- 2.4 „Bezpečnostní politikou“ je soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
- 2.5 „Bezpečnostní událostí“ taková událost, která může způsobit narušení bezpečnosti informací systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.
- 2.6 „Dodavatelem“ významný dodavatel dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti.
- 2.7 „Kritickou informační infrastrukturou“ prvek nebo systém prvků nezbytných pro provozování informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

- 2.8 „Poddodavatelem“ – dodavatel, který poskytuje služby nebo výrobky dodavateli. Přitom musí jít o produkty nezbytné pro zajištění bezpečnosti systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy. Nejedná se o dodavatele typizovaného hardware a / nebo softwarového řešení (COTS).

3. Bezpečnost informací

- 3.1 Dodavatel je povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy a vést o nich bezpečnostní dokumentaci.
- 3.2 Výchoziskem pro nastavení bezpečnostních opatření jsou požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhlášky o kybernetické bezpečnosti, případně normy ČSN ISO/IEC 27001.
- 3.3 Provádění bezpečnostních opatření u dodavatele ověřuje objednatel postupem dle čl. 15 této přílohy dodatku smlouvy nebo platným certifikátem ISO/IEC 27001, případně jiným zavedeným a platným mezinárodně uznávaným systémem řízení bezpečnosti informací u dodavatele.
- 3.4 Dodavatel provádí opatření k zajištění důvěrnosti dat souvisejících s poskytováním služeb v souladu s čl. 10 smlouvy.
- 3.5 Dodavatel provádí opatření k zajištění integrity dat souvisejících s poskytováním služeb v souladu s bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy.
- 3.6 Dodavatel provádí opatření k zajištění dostupnosti služeb v souladu s požadavky přílohy č. 2 a přílohy č. 3 smlouvy.

4. Oprávnění užívat data, pravidla přístupu

- 4.1 Dodavatel odpovídá za dodržování pravidel přístupu definovaných v čl. 5 smlouvy, případně bezpečnostních pravidel distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.
- 4.2 Dodavatel zejména odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů a k informačním / komunikačním systémům objednatele. Při ukončení pracovní-právního vztahu nebo převedení na jinou funkci pracovníka oprávněného k přístupu je dodavatel o této skutečnosti povinen neprodleně informovat objednatele (tato komunikace bude probíhat prostřednictvím kontaktních osob uvedených v odst. 10.8 smlouvy).
- 4.3 Veškerá komunikace dle tohoto článku bude probíhat elektronicky podepsanými e-mailovými zprávami.

5. Autorská a licenční práva

- 5.1 Dodavatel odpovídá za ochranu autorských a licenčních práv v souladu s čl. 11.6 smlouvy.

6. Dodržování bezpečnostní politiky objednatele

- 6.1 Dodavatel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy dodatku resp. smlouvy, prokazatelné seznámení s bezpečnostními pravidly objednatele, která budou distribuována elektronicky podepsanými e-mailovými zprávami

manažerem kybernetické bezpečnosti objednatele kontaktní osobě dodavatele uvedené v odst. 10.8 smlouvy.

7. Soulad s obecně závaznými právními předpisy

7.1 Dodavatel se zavazuje poskytovat servisní podporu dle smlouvy řádným způsobem a v souladu s platnými normami a obecně závaznými právními předpisy, které se na tento druh činnosti vztahují. Veškeré škody, které vzniknou porušením těchto norem a předpisů ze strany dodavatele, jdou k tíži dodavatele.

8. Řízení změn

8.1 Dodavatel je povinen řídit rizika související s plněním dle smlouvy, včetně zbytkových rizik. Na vyžádání manažera kybernetické bezpečnosti objednatele nebo osob provádějících kontrolní činnost dle čl. 15 této přílohy dodatku smlouvy je povinen způsob řízení těchto rizik doložit.

8.2 Dodavatel bere na vědomí, že objednatel při provádění změn postupuje v souladu s § 11 vyhlášky o kybernetické bezpečnosti.

8.3 U významných změn provádí objednatel analýzu rizik v souladu s metodikou CRAMM, nástrojem RAMSES.

8.4 Dodavatel a všichni subdodavatelé poskytnou objednateli nezbytnou součinnost a budou nápomocni při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatel.

8.5 Vzhledem k tomu, že dodavatel v rámci svého řešení nezbytného pro poskytování služeb dle smlouvy využívá technických nebo programových prostředků společností Huawei Technologies Co., Ltd. nebo ZTE Corporation, včetně jejich dceřiných společností, je povinen předložit manažerovi kybernetické bezpečnosti objednatele nejpozději ke dni podpisu dodatku, kterým se do smlouvy začleňuje tato příloha, anonymizovanou analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost.

9. Informační povinnost

9.1 Dodavatel bezodkladně informuje objednatele prostřednictvím kontaktních údajů předaných v souladu s odst. 10.9 smlouvy, pokud zjistí narušení bezpečnosti informací v důsledku kybernetické bezpečnostní události a poskytne objednateli dostatečné informace, které umožní splnění všech povinností odstranit následky takové události, vyšetřit ji a ohlásit ji Národnímu úřadu pro kybernetickou bezpečnost v souladu s požadavky vyhlášky o kybernetické bezpečnosti. Dodavatel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.

9.2 Dodavatel prostřednictvím kontaktních údajů předaných v souladu s odst. 10.9 smlouvy průběžně a bezodkladně informuje objednatele o všech jemu známých hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatel.

9.3 Dodavatel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládnutí dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy s objednatel.

9.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

10. Řízení kontinuity

10.1 Dodavatel postupuje při zajišťování kontinuity v souladu s pokyny předávanými oprávněnými osobami, jejichž kontaktní údaje jsou uvedeny v odst. 10.8 smlouvy.

11. Podmínky předávání dat

11.1 Veškeré provozní údaje, databáze, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s předmětem plnění smlouvy jsou ve výhradním vlastnictví objednatele, s výjimkou případů týkajících se povinností daných poskytovateli zákonem č. 127/2005 Sb., o elektronických komunikacích, v platném znění.

11.2 Předávání dat musí probíhat tak, aby nemohly neoprávněné osoby údaje číst, kopírovat, měnit ani mazat.

11.3 Uchovávání předávaných dat na datových nosičích (mobilní, ftp server) musí být zabezpečené proti přístupu neoprávněných osob.

12. Poddodavatelé

12.1 Ve vztahu ke každému novému poddodavateli, kterým dodavatel nahradí svého stávajícího poddodavatele, dodavatel zajistí, aby při řetězení poddodavatelů byla vzájemná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti upravena takovým způsobem, který zajistí alespoň stejnou úroveň ochrany jako ty, které jsou uvedeny ve smlouvě a splňují požadavky příslušných právních předpisů vztahujících se ke smluvnímu plnění.

13. Bezpečnostní podmínky při ukončení smlouvy

13.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

14. Pravidla pro likvidaci dat

14.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

15. Kontrola

15.1 Dodavatel a všichni subdodavatelé zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou dodatku smlouvy a umožní a budou nápomocni při auditech a inspekcích, jakýmkoli auditorem pověřeným objednatelem.

15.2 S přiměřeným předstihem před zahájením kontroly informuje objednatel dodavatele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrného narušení prostor, zařízení, personálu a činnosti dodavatele. Dodavatel není povinen při provádění umožnit přístup do svých prostor pouze v případě, že:

- a) osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;
- b) je kontrola prováděna mimo běžnou pracovní dobu, leda že kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil dodavateli, že se jedná o takový případ.

15.3 Dodavatel bere na vědomí, že objednatel provádí periodické hodnocení dodavatelů v souladu s požadavky normy ČSN ISO/IEC 9001.

16. Smluvní pokuty a sankční ujednání

16.1 Sankční ustanovení pro oblast informační a kybernetické bezpečnosti jsou uvedeny v čl. 6 smlouvy.

17. Kontaktní údaje osob odpovědných za informační a/nebo kybernetickou bezpečnost

17.1 Kontaktní údaje osob odpovědných za informační / kybernetickou bezpečnost budou mezi smluvními stranami vzájemně sděleny způsobem popsaným v odst. 10.9 smlouvy.