Smlouva

o poskytování služeb virtuálního WWW serveru (webhostingu) a souvisejících službách

uzavřená 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 **„objednatel“** nebo také **„ČNB“**)

a

T-Mobile Czech Republic a.s.
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 3787
Tomíčkova 2144/1
148 00 Praha 4 – Chodov
zastoupenou: Danielem Štefanem, na základě pověření
IČO: 64949681
DIČ: CZ64949681

(dále jen „**poskytovatel**“ nebo „**T-Mobile**“)

Článek I
Předmět smlouvy a místo plnění

1. Předmětem plnění této smlouvy je povinnost poskytovatele zajistit pro hostování a provozování webových stránek www.cnb.cz technologickou infrastrukturu, a to prostřednictvím zajištění:

   a) výpočetního výkonu v Cloudovém prostředí poskytovatele (služba Virtuálního datového centra (VDC)),
   b) zálohování primárních dat do zálohovací lokality poskytovatele (služba Virtuální záloha),
   c) ochrany proti kybernetickým internetovým útokům (služby DDoS ochrana včetně DDoS Inline a WAF),
   d) propojení poskytovaných služeb a spolehlivé datové komunikace mezi uvedenými službami.

   Popis jednotlivých služeb zajišťujících hostování a provozování webových stránek www.cnb.cz je uveden v přílohách č. 1–4 této smlouvy. Konektivita celého řešení směrem k Internetu z pohledu uvedených služeb poskytovatele (propustnost) činí 1 Gbps.

2. Při zajištění hostování a provozování webových stránek www.cnb.cz je poskytovatel povinen zejména:

   - zajistit garantovanou dostupnost webových stránek www.cnb.cz za každý kalendářní měsíc v rozsahu 99,99 % pro uživatele internetu. Případný výpadek služeb se za splnění podmínek dle čl. III odst. 3 této smlouvy do garantované dostupnosti nezapočítává, resp. v takovém případě se má za účelem výpočtu splnění garantované dostupnosti za to, že služby byly po uvedenou dobu dostupné. Případný výpadek služeb se do garantované

dostupnosti rovněž nezapočítává i za splnění dalších podmínek stanových v této smlouvě, včetně její přílohové části;

- provádět podporu a aktualizaci SW vybavení služeb a aktualizaci a instalaci servisních balíků a související konzultace za podmínek stanovených v rámci čl. III této smlouvy;
- přidělit přístupová práva (vzdálený přístup) určeným zaměstnancům dodavatele SW řešení www.cnb.cz dle smlouvy, ev. č. smlouvy ČNB 92-186-25 (dále jen „dodavatel SW řešení“) do provozního a testovacího prostředí (přístup k UNIX účtu, administrátorskému rozhraní OpenCMS, přístup k logům, restartu Apache, DB serverů atd.), a to v režimu 24/7;
- provádět pravidelné zálohování systému vytvářením záložní kopie obrazu virtuálního serveru. Podrobný popis zálohování je uveden v příloze č. 2 této smlouvy;
- komunikovat, spolupracovat a poskytovat veškerou nezbytnou součinnost dodavateli SW řešení, který je k témuž vázán na základě výše uvedené smlouvy. V případě, že by dodavatel SW řešení s poskytovatelem jakkoli nespolupracoval, resp. by poskytovateli neposkytl součinnost nezbytnou za účelem zajištění dostupnosti webových stránek www.cnb.cz, je pověřená osoba poskytovatele povinna tuto skutečnost pověřené osobě objednatele oznámit, a to do 2 hodin od okamžiku, kdy poskytovatel dodavatele SW řešení k poskytnutí součinnosti vyzval.

3. Místem plnění je sídlo objednatele na adrese Česká národní banka, Na Příkopě 28, 115 03 Praha 1, nestanoví-li dále tato smlouva nebo nedohodnou-li se pověřené osoby smluvních stran jinak. Místem plnění je rovněž místo umístění technologické infrastruktury poskytovatele.
4. Smluvní strany se dohodly, že pokud není v této smlouvě (zejména jejích přílohách č. 1–4) sjednáno jinak, aktuální konfigurace pro plnění služeb dle čl. I odst. 1 této smlouvy byla převzata ve stavu „as is“ podle posledního nastavení služeb poskytovaných dle „Smlouvy o poskytování služeb virtuálního WWW serveru (webhostingu), technické podpoře provozu Redakčního a publikačního systému pro web ČNB - RSWEB a souvisejících službách“ ze dne 30. 8. 2011, ve znění všech jejích dodatků.

Článek II
Ceny a platební podmínky

1. Cena za plnění služeb dle čl. I odst. 1 této smlouvy, vyjma služby DDos Inline, je stanovena paušálně a činí měsíčně 141 986 Kč bez DPH. Podrobný rozpad cen jednotlivých služeb je stanoven v rámci přílohy č. 5 této smlouvy.
2. Cena za plnění služby DDos Inline dle čl. I odst. 1 písm. c) této smlouvy je stanovena paušálně a činí ročně 98 400 Kč bez DPH.
3. V cenách dle odst. 1 a 2 tohoto článku jsou zahrnuty veškeré náklady poskytovatele spojené s plněním této smlouvy, včetně všech konzultací. K cenám plnění bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění.
4. Úhrada cen dle odst. 1 a 2 tohoto článku bude provedena vždy předem, a to na základě daňového dokladu vystaveného poskytovatelem nejdříve v první den období, na které se platí.
5. V případě, že účinnost této smlouvy skončí před koncem účtovacího období, vrátí poskytovatel objednateli alikvotní část předplacené ceny podpory a licencí.
6. Doklad k úhradě bude obsahovat údaje podle § 435 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován

poskytovatelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.

7. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba poskytovatele povinna na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. Uvedenou výzvu zašle objednatel na e-mailovou adresu poskytovatele business@t-mobile.cz. V případě, že je poskytovatel plátcem DPH, musí být účet, na který má být zaplaceno, zveřejněn podle § 98 zákona o dani z přidané hodnoty nebo musí být objednatele výše uvedeným způsobem sděleno číslo jiného účtu, který je tímto způsobem zveřejněn. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle věty první.

8. Doklad k úhradě (fakturu) zašle poskytovatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:

   Česká národní banka
   sekce rozpočtu a účetnictví
   odbor účetnictví
   Na Příkopě 28
   115 03 Praha 1

9. Splatnost dokladu k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

10. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že je objednatel oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

Článek III
Poskytování podpory

1. Poskytovatel zajišťuje objednateli provozní podporu, v jejímž rámci poskytovatel zajistí fungování všech služeb v souladu s požadavky stanovenými v přílohách č. 1 až 4 této smlouvy, a to při dodržení garantované dostupnosti v rozsahu 99,99 % měsíčně. V rámci provozní podpory je poskytovatel povinen:

   a) odstraňovat jakékoliv provozní problémy (vady, poruchy či bezpečnostní incidenty),

   b) provádět veškeré aktualizace SW vybavení služeb a instalace servisních balíčků,

   c) provádět konzultace provozních problémů a požadavků objednatele nebo požadavků

ohledně provozních problémů vzniklých mezi poskytovatelem a dodavatelem SW řešení webové prezentace www.cnb.cz.

2. Za účelem ohlašování provozních problémů (vad, poruch či bezpečnostních incidentů), jakož i konzultací v souvislosti provozními problémy, zajišťuje poskytovatel nepřetržitě (24 hodin denně, 7 dnů v týdnu, 365 dnů v roce) možnost ohlašování na tel. čísle: 800 737 333 nebo e-mailem: dohled@t-mobile.cz**.** Ohlašování provádí pověřená osoba objednatele dle čl. IV této smlouvy.
3. Pověřené osoby poskytovatele jsou povinny vždy oznámit pověřené osobě objednatele úmysl provádět pravidelnou údržbu min. 2 týdny předem. Konkrétní termín údržby a případného výpadku určuje pověřená osoba objednatele. Dojde-li k výpadku služeb, nesmí nepřístupnost webové prezentace www.cnb.cz přesáhnout 120 minut měsíčně a maximálně 40 minut v jednom kalendářním dni.
4. Pověřené osoby poskytovatele jsou vždy povinny neodkladně nahlásit všechny výpadky služeb. V informaci uvedou důvod výpadku a předpokládaný čas opětovného uvedení služby do provozu. Stejným způsobem je poskytovatel povinen neodkladně od uvedení služeb do provozu nahlásit skutečný důvod a skutečný čas ukončení výpadku služeb.
5. Konzultace dle odst. 1 písm. c) tohoto článku budou poskytovány v termínu dohodnutém smluvními stranami. V případě, že tak stanoví pověřená osoba objednatele, můžou být konzultace poskytovány i ve formě analýz, písemných doporučení či jiných písemných výstupů vyhotovených poskytovatelem. Učinila-li pověřená osoba objednatele dotaz formou e-mailové zprávy, budou konzultace poskytnuty nejpozději do 3 pracovních dnů od přijetí požadavku, a to formou e-mailové zprávy, nedohodnou-li se smluvní strany v konkrétním případě jinak.
6. Poskytovatel je povinen nahlásit případnou změnu kontaktních údajů uvedených v odst. 2 tohoto článku nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob objednatele. Změna je účinná dnem jejího oznámení objednateli, a to bez povinnosti uzavírat dodatek k této smlouvě.

Článek IV
Pověřené osoby smluvních stran

1. Smluvní strany se dohodly, že do 10 pracovních dnů ode dne uzavření této smlouvy si předají seznamy pověřených osob, které jsou oprávněny k činnostem vymezeným touto smlouvou pověřeným osobám, včetně jejich kontaktních údajů, přičemž u každé osoby bude uveden nejméně e-mail a telefonický kontakt.
2. V případě změny pověřené osoby nebo kontaktních údajů se smluvní strany zavazují oznámení změny doručit na e-maily pověřených osob druhé smluvní strany do 3 pracovních dnů, bez povinnosti uzavřít dodatek k této smlouvě. Změna je účinná dnem jejího oznámení druhé smluvní straně.

Článek V
Práva a povinnosti smluvních stran

1. Poskytovatel se zavazuje dodržovat bezpečnostní požadavky objednatele uvedené v přílohách č. 6 a 7 této smlouvy.
2. Poskytovatel potvrzuje, že ke dni nabytí účinnosti této smlouvy on ani jeho poddodavatelé nenaplňují definiční znaky subjektů uvedených v čl. 5k nařízení (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 833/2014“), nebo subjektů

uvedených v čl. 1h rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění jeho změn (dále jen „rozhodnutí 2014/512/SZBP“), kterým je zakázáno zadat či plnit jakoukoli veřejnou zakázku nebo koncesní smlouvu ve smyslu v tomto ustanovení uvedeného nařízení či rozhodnutí. Subjekty naplňující definiční znaky subjektů uvedených v čl. 5k nařízení č. 833/2014 nebo subjektů uvedených v čl. 1h rozhodnutí 2014/512/SZBP budou dále označovány jako „určené subjekty“.

3. Poskytovatel dále potvrzuje, že ke dni účinnosti této smlouvy není osobou uvedenou v příloze I nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „nařízení č. 269/2014“), nebo v příloze I nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, ve znění jeho změn (dále také jako „nařízení č. 208/2014“), nebo v příloze I nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska, ve znění jeho změn (dále také jako „nařízení č. 765/2006“), nebo v příloze rozhodnutí Rady 2014/145/SZBP ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, ve znění jeho změn (dále také jako „rozhodnutí 2014/145/SZBP“). Osoba uvedená v příloze I nařízení č. 269/2014 nebo v příloze I nařízení č. 208/2014 nebo v příloze I nařízení č. 765/2006 nebo v příloze rozhodnutí Rady 2014/145/SZBP bude dále označována jako „určená osoba“.

4. Poskytovatel se současně zavazuje, že určeným osobám dle předchozího odstavce (není-li jí sám) nebo v jejich prospěch nezpřístupní žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo.

5. Poskytovatel dále potvrzuje, že plnění jím poskytované dle této smlouvy neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie [tj. zejména zákazy dovozu výrobků ze železa a oceli ve smyslu nařízení Rady (EU) č. 2022/428 ze dne 15. března 2022, kterým se mění „základní“ nařízení (EU) č. 833/2014, nebo nařízení Rady (EU) č. 2022/355 ze dne 2. března 2022, kterým se mění „základní“ nařízení (ES) č. 765/2006 o omezujících opatřeních vzhledem k situaci v Bělorusku apod.]. Objednatel je oprávněn při porušení této povinnosti poskytovatele plnění nepřevzít v jakékoliv jeho části.

6. V případě, že by v průběhu účinnosti této smlouvy poskytovatel nebo jeho jakýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo se poskytovatel stal určenou osobou, je poskytovatel povinen o takové skutečnosti objednatele bez zbytečného odkladu, nejpozději do 2 pracovních dnů od nastání takové skutečnosti, písemně informovat.

7. Dojde-li za dobu účinnosti této smlouvy ke změnám v kterémkoliv z výše uvedených nařízení Rady (EU) či rozhodnutí Rady nebo k přijetí jakékoliv jiné nové legislativy tak, že bude nezbytné dát tuto smlouvu s nařízením Rady (EU), rozhodnutím Rady nebo jinou novou legislativou do souladu, zavazují se smluvní strany uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava či doplnění práv a povinností smluvních stran v rámci této smlouvy (sankční mechanismy či nové možnosti ukončení smlouvy z toho nevyjímaje), a to bez zbytečného odkladu, nejpozději do 15 pracovních dnů poté, co změny nařízení Rady (EU), rozhodnutí Rady či jiná nová legislativa nabudou platnosti, nedohodnou-li se smluvní strany jinak.

8. Vznikne-li objednateli v souvislosti s nepravdivým prohlášením nebo porušením povinností poskytovatele dle tohoto článku smlouvy jakákoliv škoda, je poskytovatel tuto škodu objednateli povinen v plné výši nahradit.

9. Smluvní strany se dohodly, že ujednání odst. 5.4, čl. 9, odst. 13.3 a 13.4. Obchodních podmínek pro změnu poskytovatele služby zpracování dat společnosti T-Mobile Czech Republic, a.s. se na smluvní vztah založený touto smlouvou neaplikují.

Článek VI
Smluvní pokuty a úrok z prodlení

1. V případě nedodržení garantované dostupnosti webových stránek www.cnb.cz ze strany poskytovatele v příslušném kalendářním měsíci v rozsahu 99,99 % v důsledku jeho zavinění je objednatel oprávněn požadovat po poskytovateli smluvní sankci ve výši 100 % ze sjednané pravidelné ceny uvedené v článku čl. II odst.1 této smlouvy. Tato smluvní sankce je objednateli poskytována formou slevy z vyúčtované pravidelné ceny.
2. V případě prodlení poskytovatele v kterékoliv lhůtě dle čl. V odst. 6 a 7 této smlouvy je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
3. V případě, že se ukáže tvrzení poskytovatele uvedené v čl. V odst. 2, 3 a 5 této smlouvy jako nepravdivé nebo poruší-li poskytovatel závazek stanovený v čl. V odst. 4 této smlouvy, vzniká objednateli nárok na smluvní pokutu ve výši 100 000 Kč za každé jednotlivé nepravdivé tvrzení poskytovatele či za každé jednotlivé porušení závazku poskytovatele.
4. V případě prodlení objednatele v úhradě daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle příslušných ustanovení předpisů občanského práva.
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.

Článek VII
Výpověď, odstoupení od a trvání smlouvy

1. Smlouva se uzavírá na dobu určitou, a to do zahájení plnohodnotného provozu nového webu ČNB, na jehož realizaci se v současné době pracuje. Plánované zahájení tohoto provozu objednatel předpokládá za cca 3 roky od uzavření této smlouvy. Objednatel je povinen o zahájení tohoto provozu dle předchozí věty písemně informovat poskytovatele minimálně 3 měsíce předem.
2. Smlouvu lze ukončit odstoupením v případě podstatného porušení smlouvy jednou ze smluvních stran.
3. Za podstatné porušení smlouvy je považováno zejména:
   - ze strany poskytovatele nepřetržitá nedostupnost webových stránek www.cnb.cz po dobu delší než 24 hodin,
   - ze strany objednatele prodlení s úhradou daňového dokladu, a to po dobu delší než 30 dnů.
4. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele odstoupit od smlouvy.
5. Objednatel je oprávněn odstoupit od této smlouvy, a to i v její jakékoliv části, dále v případě, kdy na základě písemné informace od poskytovatele či z vlastní iniciativy shledá, že poskytovatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo poskytovatel se stane určenou osobou nebo poskytovatel neuzavře dodatek ke smlouvě

ve smyslu čl. V odst. 7 této smlouvy nebo poskytovatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie.

6. Objednatel je oprávněn vypovědět tuto smlouvu, a to i v její jakékoliv části, bez výpovědní doby v případě, kdy na základě písemné informace od poskytovatele či z vlastní iniciativy shledá, že poskytovatel nebo jeho kterýkoliv poddodavatel naplnili definiční znaky určeného subjektu nebo poskytovatel se stane určenou osobou nebo poskytovatel neuzavře dodatek ke smlouvě ve smyslu čl. V odst. 7 této smlouvy nebo poskytovatel poruší povinnost nezpřístupnit jakékoliv určené osobě (není-li jí sám) nebo v její prospěch žádné finanční prostředky ani hospodářské zdroje získané v souvislosti s plněním dle této smlouvy, a to přímo ani nepřímo, nebo povinnost dodat či poskytnout plnění, které neporušuje žádným způsobem jakékoliv platné právní předpisy vydané zejména orgány Evropské unie.
7. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení druhé smluvní straně.

Článek VIII
Závěrečná ustanovení

1. Smlouva nabývá platnosti dnem podpisu obou smluvních stran a účinnosti dne 1. 10. 2025.
2. Smlouva může být měněna a doplňována pouze formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě stanoveno jinak. Dodatek v elektronické podobě se považuje za řádně podepsaný objednatelem, je-li podepsán kvalifikovanými elektronickými podpisy.
3. Tato smlouva a právní vztahy s ní související se řídí občanským zákoníkem a ostatními souvisejícími platnými právními předpisy České republiky.
4. Spory vyplývající z této smlouvy budou řešeny především dohodou smluvních stran. Nebude-li možné dosáhnout dohody, bude spor řešen před místně a věcně příslušným soudem, popř. příslušným správním úřadem České republiky, a to výlučně podle českého práva.
5. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami/pověřenými osobami smluvních stran v konkrétním případě dohodnuto jinak.
6. Smluvní strany vylučují uplatnění ustanovení § 1765 a § 1766 a § 2620 občanského zákoníku na svůj smluvní vztah založený touto smlouvou, čímž se ruší nárok poskytovatele na jednání podle § 1765 odst. 1 občanského zákoníku. Poskytovatel tímto přebírá nebezpečí změny okolností dle § 1765 odst. 2 občanského zákoníku.
7. Práva a povinnosti vzniklé z této smlouvy mohou být postoupeny pouze po předchozím písemném souhlasu druhé smluvní strany.
8. Ukončením smlouvy nejsou dotčena ustanovení smlouvy týkající se nároků z odpovědnosti za vady, nároků z odpovědnosti za škodu a nároků ze smluvních pokut, závazku mlčenlivosti ani další ustanovení, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti smlouvy.
9. Smlouva je vyhotovena v elektronické podobě, přičemž každá ze smluvních stran obdrží vyhotovení smlouvy opatřené elektronickými podpisy.
10. Součástí této smlouvy jsou následující přílohy:

Příloha č. 1 Popis služby T-Cloud VDC

Příloha č. 2 Popis služby Virtuální záloha
Příloha č. 3 Popis služby DDoS ochrana a DDoS ochrana inline
Příloha č. 4 Popis služby WAF
Příloha č. 5 Specifikace cen služeb
Příloha č. 6 Bezpečnostní požadavky objednatele
Příloha č. 7 Obecná pravidla pro dodavatele v oblasti bezpečnosti IT
Příloha č. 8 Obchodní podmínky pro změnu poskytovatele služby zpracování dat společnosti T-Mobile Czech Republic, a.s.

V Praze

Za objednatele:

…….
Ing. Milan Zirnsák
ředitel sekce informatiky
podepsáno elektronicky

……
Ing. Zdeněk Virius
ředitel sekce správní
podepsáno elektronicky

V Praze

Za poskytovatele:

……..
Daniel Štefan
na základě pověření
podepsáno elektronicky

Příloha č. 1: Popis služby T-Cloud Virtuální datová centra (VDC)

Služba T-Cloud VDC pro ČNB je poskytována v datovém centru T-Mobile na území České republiky, konkrétně v lokalitě DC THP, Vinohradská 190, Praha 3

Na službě T-Cloud VDC pro ČNB zajišťuje T-Mobile provoz a správu virtuálních serverů produkčního a testovacího prostředí webových stránek CNB.CZ

- Názvy virtuálních serverů produkčního prostředí: nd1, nd2, DB1, , micro
- Názvy virtuálních serverů testovacího prostředí: nd1-test, nd2-test, DB1-test, , micro-test,
- Pro aplikaci webových služeb je využit server micro, kde jsou alokovány i výpočetní zdroje pro aplikaci WS, stejně tak i v testovacím prostředí. Výpočetní zdroje databázového serveru DB2 v provozním prostředí jsou alokovány na aktivním serveru DB1.

Přidělený výpočetní výkon pro jednotlivé servery:

Produkce

Název virtuálního serveru	Počet jader (CPU)	Velikost RAM (GB)	HDD (GB)
nd1	16	36	550
nd2	16	36	550
DB1	8	16	230
micro	8	8	25

Test

Název virtuálního serveru	Počet jader (CPU)	Velikost RAM (GB)	HDD (GB)
nd1-test	8	20	350
nd2-test	8	20	350
DB1-test	4	8	330
micro-test	8	8	25

Služba T-Cloud VDC pro ČNB je poskytována a spravována výhradně společností T-Mobile. Objednatel nemá přístup pro správu.

Parametry služby – Výkonové zdroje celkem

Organizační VDC identifikovaná VS kódem	Výkonový zdroj	Jednotka	Zdroje v „Rezervované“ části	Zdroje v části „Dle využití“	Celková kvóta (Rezervovaná + Dle využití)	Paušálem zpoplatněna kvóta
Platební model Kombinovaný	**CPU**	[GHz-vCPU]	140 GHz	0	140	**0**
	RAM	[GB]	152	0	152	0
	Storage Policy STANDARD	[GB]	2500	0	2500	0

Parametry služby – Profesionální služby

Správa VDC: ANO	Správa OS: Ano	Správa aplikací: Ne	Počet spravovaných virtuálních strojů: 10

Parametry služby – Licence

Operační systémy	Druh (jednotka)	Počet
☐ Linux free Edition nebo Linux OS licence vlastněná zákazníkem	VM	10

Základním rozhraním pro správu virtuálních serverů IT administrátorem je webový portál **Cloud Director,** který je chráněný na perimetru ochranou proti DDoS útokům technologií **Arbor** společnosti NetScout, dále Web Application FW technologií společnosti **F5**.

Virtualizace je prováděná hypervizorem společnosti **Broadcom** (bývalý VMware**)**.

Clustery serverů výrobce **HPE** jsou navrženy a provozovány s ohledem na nutnost dodržení nejvyšší možné dostupnosti služby, datová úložiště výrobce **NetApp** jsou stejným principem navržena tak, aby byla chráněna proti současnému výpadku několika fyzických disků a redundantním osazením komponent jsou chráněna i proti jiným typům selhání HW.

Zálohování virtuálních serverů zabezpečuje software společnosti **VEEAM** na datová úložiště výrobce **Dell EMC**.
Síťová infrastruktura je provozována na technologiích společnosti **Cisco**.
V celé platformě minimalizujeme pravděpodobnost tzv. Single-Point-of-Failure.

Služba je provozována v souladu s těmito standardy: ISO 20000, ISO 27001, ISO 27017, ISO 27018.

Výhradním správcem infrastrukturních systémů s plným fyzickým přístupem je Poskytovatel.

Uložení zákaznických dat:
Uložením dat Smluvního partnera do Služby ani jejich změnou nedochází ke změně vlastnictví dat a Poskytovatel se tak nestává jejich vlastníkem ani za ně a jejich obsah Poskytovatel nepřebírá žádnou odpovědnost.

Data Smluvního partnera ve stavu aktivních i neaktivních jsou ukládána výhradně na území České republiky, v datových centrech DC 7 a DC THP, a jsou zpracovávána na území ČR.

Většina specifických provozních údajů je ukládána a zpracovávána na území ČR (konfigurace, logy, monitoring apod.). Některé specifické provozní údaje Služby ve stavu aktivních i neaktivních dat mohou být uložena a zpracovávána na území Spolkové republiky Německo. Jedná se zejména o data spojená se skenováním zranitelností systémů.

Výkon správy a dohledu:
Správa a dohled Služby je prováděna pouze z území České republiky interními zaměstnanci společnosti T-Mobile Česká republika.

Informace o jurisdikci, které podléhá infrastruktura informačních a komunikačních technologií použitá pro zpracování dat jejich jednotlivých služeb:

P.č.	Služba zpracování dat	Země, kde jsou umístněna IKT aktiva služby
1	T-Cloud Virtuální datové centrum	Česká republika
2	T-Cloud Virtuální záloha	Česká republika

Informace o standardních poplatcích za změnu poskytovatele:

Smluvní strany se dohodly, že všechny poplatky za přenos služby zpracování dat jsou již zahrnuty v ceně plnění dle této smlouvy.

V ostatním se na službu uplatní Popis služby Virtuální datová centra, přičemž pokud se v popisu služby hovoří o Smluvním partnerovi, rozumí se jím ČNB, a pokud se v něm odkazuje na Specifikaci služby, rozumí se jí tato smlouva.

Příloha č. 2: Popis služby Virtuální záloha

Služba spočívá:

- v pronájmu sady zdrojů sdílené virtuální infrastruktury Poskytovatele Smluvnímu partnerovi sestávajícího
  - z předem definovaného množství úložní kapacity pro zálohování
  - ze SW licencí pro zálohování virtuálních serverů
- v připojení virtuální infrastruktury do zálohovací sítě
- a v údržbě a servisu zálohovací infrastruktury do úrovně „Infrastructure as a Service“ Poskytovatelem, s garancí SLA.

Služba umožňuje vytváření záložních kopií do zálohovací lokality v DC THP a umožní jejich následnou obnovu po ztrátě nebo poškození primárních dat těchto kategorií:

- celých virtuálních serverů,
- zvolených adresářů, nebo souborů
- podporovaných databází a aplikací.

Specifikace služby

Služba virtuální zálohy je dodavatelem poskytována varianta Managed

Základní garantovaná SLA na dostupnost Služby je 99,9 % a je zahrnuta v ceně Služby.

Vlastnosti varianty Managed

Varianta Managed zahrnuje správu zálohovacích úloh specialisty Poskytovatele.

Smluvní partner přístup do nástroje pro správu zálohovacích úloh **neobdrží**. Konfigurační změny jsou ze strany Poskytovatele prováděny na základě změnových požadavků Smluvního partnera. Poskytovatel může iniciovat změnu nastavení spravovaných systémů, v takovémto případě ji provádí až po vzájemné dohodě se Smluvním partnerem.

V rámci **Premium managementu**:
- se definují nastavení zálohovacích úloh a provádí se obnova dat ze záloh
- rámcové množství časového fondu potřebného pro správu vychází z analýzy potřeb daného případu,
- pravidelný měsíční poplatek zahrnující Premium Management opravňuje objednatele k provedení určitému počtu předem domluvených požadavků za kalendářní měsíc.

Prováděné úkony popisuje následující tabulka:

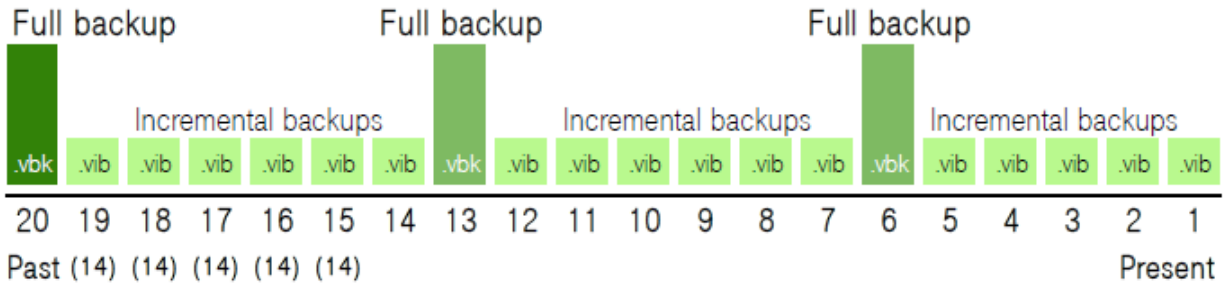
Úkon	**Rozsah**	**Zahrnuto ve službě Premium Management**
Konfigurace zálohovacích úloh	Konfigurace / rekonfigurace úloh	Ano
Konfigurace zálohovacího agenta	Instalace / smazání / rekonfigurace 1 agenta	Ano
Obnovení virtuálního serveru	Obnovení virtuálních serverů na místo určené zákazníkem	Ano

Obnovení souboru	Obnovení 1 souboru na místo určené zákazníkem	Ano
Obnovení dat aplikace	Obnovení zákaznických dat na místo určené zákazníkem	Ne (na bázi hodinové sazby)

Principy fungování

Zálohovací řetězec se skládá z .vbk a .vib souborů. Plné a přírůstkové zálohy korespondují s body obnovy (Restore Points), což jsou snapshoty dat virtuálního stroje v daném čase. Toto umožňuje obnovu virtuálního serveru do daného časového bodu obnovy.

Jak standardní zálohovací schéma pracuje, vysvětluje následující obrázek (14denní retence):



Doba retence dat v zálohách je dána nastavenou **retenční politikou v zálohovací úloze.**
Jedenkrát týdně, o víkendu, je vytvořena tzv. Syntetická plná záloha (**Synthetic full backup**), ostatní dny se vytváří přírůstková záloha (**Incremental backup**).

Doba potřebná pro obnovu dat ze zálohy (tzv. **Recovery Time Objective)** je závislá na množství obnovovaných dat, tento fakt je potřebné brát do úvahy při definování parametrů plánu obnovy.

Příloha č. 3: Popis služby DDoS ochrana a DDoS ochrana inline

DDoS Ochrana je tvořena kombinací:

- operátorské ochrany
- a inline ochrany

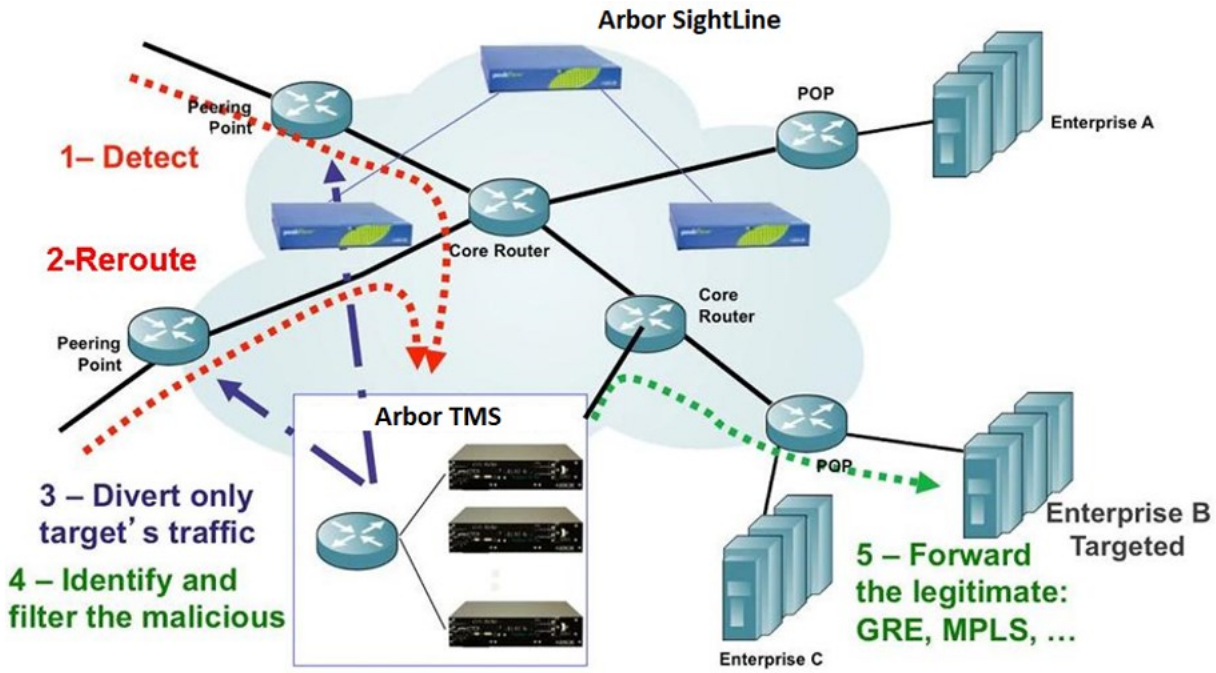
Doplňková služba **DDoS Ochrana** je komplexní doplňková komponenta ke službě Webhosting.

Smyslem doplňkové služby **DDoS Ochrana** je poskytnutí centrálně spravované ochrany proti DDoS (Distributed Denial of Service – útok distribuovaným odepřením služby) a zmírnění následků DDoS útoků.

Vlastnosti doplňkové služby DDoS Ochrana

Doplňková služba **DDoS Ochrana** zajišťuje síťově orientovanou ochranu telekomunikačních systémů proti DDoS útokům. Tato Služba je založena na technologii ARBOR od společnosti NetScout Systems, Inc. (dále jen „Platforma“) a na znalostech a zkušenostech specialistů Poskytovatele.

Služba čistí datový tok směřovaný na IP adresy definované jako chráněné cíle objednatele (dále také jako „Smluvní partner“), a to již na úrovni páteřní sítě a snižuje tak dopady útoku díky rychlé detekci a nasazení předdefinovaných pravidel.



Během útoku je čistý legitimní provoz standardně potlačen obrovským počtem požadavků, který generují útočící zařízení. Hlavním smyslem obrany je tak ochránit legitimní provoz Smluvního partnera směřující na chráněné cíle a zajistit jeho doručení k chráněnému cíli, a přitom odstranit datový tok útočníků, kteří přetěžují linky a cílové počítače (servery) Smluvního partnera.

Služba nabízená Poskytovatelem kombinuje síťovou technologii a znalosti a zkušenosti specialistů síťové bezpečnosti. Služba poskytuje nepřetržitou ochranu prostřednictvím automatické i manuální mitigace, která se v případě automatizované varianty Služby opírá o optimální přednastavení Služby, i v případě manuálně řízených variant Služby je navíc díky nepřetržité podpoře specialistů Poskytovatele schopna se pružně přizpůsobovat i dynamicky se měnícím okolnostem útoku.

Pro aktivaci služby není nutné měnit BGP routing nebo provádět DNS manipulaci. Služba je postavena na následujících komponentách.

Základní součásti Služby

Operátorská vrstva DDoS ochrany v rámci Služby sestává ze dvou nedílných částí: Monitoringu a vlastní Ochrany (Mitigace).

DDoS Monitoring

Monitoring (Flow-based Monitoring), který běží na úrovni páteřní sítě Poskytovatele, spočívá v analýze vzorků datových toků shromážděných od okrajových směrovačů sítě TMCZ prostřednictvím Platformy. Systém Poskytovatele analyzuje příchozí provoz (provoz na chráněné cíle), který je přesměrován na koncový bod přípojky Smluvního partnera.

Současně v rámci Služby Platforma v páteřní síti Poskytovatele používá tři metody pro detekci DDoS útoku:

- analýzu zneužití vybraných síťových protokolů
- analýzu vzorků metadat provozu (netflow) směrovaného na chráněné cíle Smluvního partnera
- obecné signatury útoků ukládané v databázi Platformy.

V případě detekce chybové události nebo výrazného překročení obvyklé hranice datového toku Služba automaticky pošle oznámení o podezření na útok v rozsahu uvedeném v Zadání (konfigurační formulář Služby sjednaný před zahájením poskytování služby a dále písemně upravovaný pověřenou osobou objednatele) a zahájí proces analýzy a klasifikace, který podle sjednané varianty Služby (DDoS ochrana L) buď následně dokončují pracovníci Security dohledového operačního centra Poskytovatele (dále jen „SOC“) nebo Platforma Poskytovatele sama automaticky. Monitoring dokáže odhalit útoky na druhé až čtvrté vrstvě (L2-L4 dle ISO 7498 a jeho aktualizace) OSI modelu a částečně i na vrstvě aplikační (L7).

DDoS Mitigace

DDoS Mitigace je součást Služby, která zajišťuje aktivní ochranu a zahájení nasazení protiopatření, která čistí provoz a zmírní dopady útoku na chráněné cíle. Díky vysokokapacitní síti a specializované DDoS technologii, může Poskytovatel poskytnout vysokou účinnost čištění, filtrování a potlačení nežádoucích datových toků.

Tato část Služby je spuštěna automaticky nebo v souladu se Zadáním dohodnutým se Smluvním partnerem, které definuje mj. rozsah vlastních činností a postupů, které mají být použity při identifikaci nežádoucího provozu.

V případě hrozby útoku je veškerý příchozí provoz přímo z páteřní sítě Poskytovatele přesměrován na Platformu, která analyzuje a identifikuje legitimní provoz a odstraní (zlikviduje) provoz nežádoucí. Nežádoucím provozem je provoz, který byl Platformou vyhodnocen jako neobvyklý či nenaučený nebo

provoz vykazující škodlivé signatury. Ostatní provoz, který byl Platformou vyhodnocen jako legitimní komunikace, je pak směrován dále na určený chráněný cíl.

Samostatné profily ochrany – Chráněné cíle/Managed object

Služba **DDoS Ochrana** umožňuje více samostatných profilů pro ochranu částí infrastruktury s typickými druhy provozu, resp. s typických chováním:

- veřejný web
- mailový provoz
- eshop atd.

Provoz je možné rozdělit mezi profily na základě koncové IP adresace (nikoliv na úrovni hostname). Jednotlivé profily jsou vzájemně nezávislé a umožňují granulárně nastavit politiky ochran pro subnety. To umožňuje mít pro služby s různou úrovní kritičnosti různé úrovně ochrany a detekce útoků.

Služba je poskytována v následujícím rozsahu:

- Nabízí komplexní ochranu s možností individuálního nastavení a plnou součinnost SOC během útoku
- Předpokládá dostupnost znalých pracovníků na straně Smluvního partnera, kteří jsou během útoku připraveni efektivně spolupracovat se SOC na mitigaci útoku.
- Umožňuje zajistit detekci a mitigaci volumetrických DDoS útoků na úrovni jednotlivých chráněných aplikací, individuální přístup a maximální flexibilitu mitigace s cílem minimalizovat dobu nedostupnosti chráněných cílů Smluvního partnera
- 24×7 on-line monitoring na páteřní síti (Flow based) s automatickou notifikací detekovaných událostí
- Součinnost týmu SOC v režimu 24×7
  - Proaktivní monitoring výskytu bezpečnostních událostí a dle potřeby nasazení protiopatření ve spolupráci se Smluvním partnerem
- Plán ochrany je tvořen individuálně dle potřeb Smluvního partnera
  - Způsob ochrany lze nastavit individuálně pro jednotlivé chráněné skupiny aplikací (web, dns, vpn…) či jednotlivé servery.
  - Mitigace probíhá za plné asistence SOC a umožňuje flexibilní ladění / modifikaci mitigačních pravidel v průběhu útoku pro jejich maximální účinnost
- Počet přístupových účtů do Portálu dle potřeb Smluvního partnera
- Počet notifikačních cílů dle potřeb Smluvního partnera (email, sms)
- Kapacita chráněné linky – dle požadavků Smluvního partnera
- Pravidelný měsíční reporting
- Čas bezpečnostních konzultantů SOC (technická podpora) v ceně Služby
- rozšíření Služby o In-line ochranu a vzájemnou integraci obou služeb

Eskalační matice

Pokud není Smluvní partner spokojen se standardní procedurou řešení události, může použít následující eskalační matici:

Úroveň	1	2
Jméno	[redacted]	[redacted]
Pozice	Head of SOC/CERT	Head of Protect Domain and Security Cross Border Services
Mobilní telefon	+420 737 087 888	+420 603 413 533
E-mail	[redacted]	[redacted]
Dostupnost	8×5	8×5

8×5 – znamená dostupnost v pracovní dny od 9:00 do 17:00.

1) Specifikace služby DDoS Ochrana - operátorská vrstva

Služba je poskytována nepřetržitě všechny dny v roce 24 hodin denně. Služba je poskytována nepřetržitě všechny dny v roce 24 hodin denně.

2) Specifikace služby DDoS Ochrana – inline vrstva

Inline zařízení chrání vnitřní síť před DDoS útoky ze strany botnetů, pomocí aktualizovaných seznamů (threat intel feedy): Active Attacers, Known Attack Bots/Tools, Search Crawlers, Malware IoCs, Search Crawlers. Inline ochrana disponuje schopností naučit se běžné hodnoty provozu a navrhuje vhodné prahové hodnoty ochrany pro každý chráněný cíl, dále poskytuje analýzu hrozeb s možností vyhledávat a filtrovat informace pomocí: countries, threat classification, MITRE Attack Techniques and Tactics, traffic direction, protocol and port a zahrnuje dedikované inline DNS řešení ochrany proti DNS Water Torture útokům, pomocí kontinuálního učení legitimních doménových jmen, a jejich automatickým blokováním bez ručního vstupu během útoku. Kombinuje několik stupňů detekce narušení od rozpoznání útoků na základě signatur přes pravidla chování, anomálií provozu, rozpoznání aplikací a „Zero Day Attack" ochran. Poskytuje snadný přechod z detekce na prevenci, precizně a rychle blokuje hrozby bez zastavení legitimního provozu, a tím šetří celkové náklady na provoz, ochranu a obnovu systémů.

Inline zařízení bude nasazeno v ČNB v režimu L2 Bridge a bude použito mimo jiné na zamezení „nežádoucích" robotických přístupů na kurzovní lístek www.cnb.cz.

Inline zařízení bude dedikováno výhradně pouze pro ČNB, tzn. nebude sdíleno s jinými uživateli, zákazníky poskytovatele.

Důvodem nutnosti nasazení inline ochrany pro tyto účely jsou permanentně detekované problémy s elektronickými systémy (roboty) přistupujícími na stránky www.cnb.cz, konkrétně na kurzovní lístek, vyčítající informace o aktuálním kurzovém lístku ve 100-kách tisíc přístupů denně, i když je kurzovní lístek aktualizován pouze 1x denně.

Byť je tento provoz legitimní, z pohledu ČNB je nežádoucí z důvodu zatěžování celého dedikovaného výpočetního prostředí, redakčního systému, síťové infrastruktury a zdrojů zajišťujících provoz www.cnb.cz. V některých situacích dochází i k přetížení systému a v takovém případě je www.cnb.cz nedostupný nebo s omezenou dostupností.

Obsah DDoS Ochrana - inline

DDoS Ochrana - inline spočívá v dodávce, implementaci, konfiguraci a správě bezpečnostního zařízení společnosti Netscout (Arbor Edge Defence). Design řešení a jeho implementace je v souladu se Zákonem o kybernetické bezpečnosti, Směrnicí o ochraně osobních údajů (GDPR) a normami řady ISO 27000 pro zabezpečení platformy pro provoz webu www.cnb.cz.

Základní princip služby spočívá v dodávce a implementaci bezpečnostního řešení na rozhraní internetové přípojky a platformy provozující servery a infrastrukturu web serverů a DB serverů www.cnb.cz a redakčního systému pro správu obsahu www.cnb.cz. Veškerá komunikace směřující na web server www.cnb.cz prochází inline vrstvou, který zajišťuje ochranu systému a dodržování definovaných bezpečnostních politik. Zařízení a software jsou ve vlastnictví poskytovatele. Správu a konfiguraci v dohodnutém rozsahu zajišťuje poskytovatel formou služby. Veškeré aktualizace operačního systému a modulů zařízení, bezpečnostní patche (záplaty) vydané výrobcem a další služby jsou prováděny prostřednictvím specialistů poskytovatele, kteří mají v oblasti bezpečnosti dlouholeté zkušenosti.

DDoS Ochrana - inline

Navrhované řešení využívá pro dosažení vysoké míry bezpečnosti bez negativního dopadu na datovou propustnost skutečnost, že funguje jako transparentní filtr na úrovni L2 (bridge). Toto zařízení je schopno zmírnit DDoS útoky na L3 až L7 (ISO OSI modelu). Pro další detekční schopnosti disponuje rozšířením AIF Advanced, které v sobě zahrnuje neustále aktualizované reputační databáze.

Adaptive DDoS Protection

Adaptivní DDoS ochrana v NETSCOUT Arbor Edge Defense (AED) je technologie založená na strojovém učení (ML) speciálně navržená tak, aby se přizpůsobila jakýmkoli změnám ve strategii nebo metodologii útočníka, aby byla zajištěna trvalá dostupnost vašich nejdůležitějších podnikových služeb a aplikací.

Účinná obrana vyžaduje technologii řízenou ML, která se dokáže přizpůsobit neustále se měnícím výzvám útočníků, a globální zpravodajství o hrozbách, které poskytuje operativní a přesné znalosti o protivníkovi.

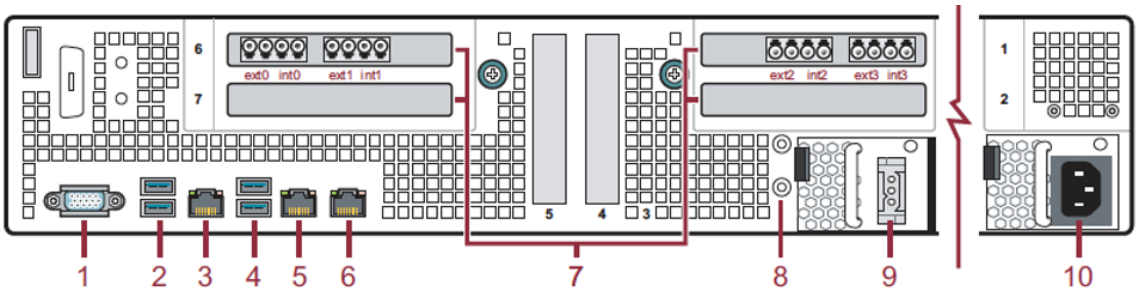
V rámci AED využívá proces Adaptive DDoS Protection ML k průběžné kontrole nového útočného provozu proti stávajícím protiopatřením, aby bylo zajištěno ověření nového útoku. Jakmile jsou identifikována, vytvoří se doporučení ochrany, včetně aktivace stávajících protiopatření, a předloží se proti stávajícím protiopatřením, aby byla zajištěna úplná viditelnost změn. Poté se proces opakuje, aby bylo zajištěno, že ochrana drží krok s vývojem útočného provozu. Dále pak budou aplikována bezpečnostní pravidla na zařízení z důvodu permanentně detekovaných problémů s elektronickými systémy (roboty) přistupujícími na stránky www.cnb.cz, konkrétně na kurzovní lístek, kteří generují nadměrný nežádoucí provoz, který má charakter DDoS provozu, avšak legitimní. Na základě těchto opatření budou nastavena pravidla na omezení počtu přístupů ze zdrojových adres těchto nežádoucích provozů, byť legitimních, v reálném čase s definovanými pravidly pro zamezení přístupu na definované URL (nikoliv celý web cnb.cz), obnovu přístupu, zařazení do režimu karantény, apod.

Tato opatření nebudou mít vliv na propustnost zařízení, resp. nebudou omezovat standardní provoz na servery webu www.cnb.cz. V kombinaci s již nasazeným bezpečnostním řešením DDoS nemůže dojít ani k omezení provozu na základě rozsáhlého DDoS útoku, který by inline zařízení kapacitně nezvládlo.

Vzhledem k redundantní přístupové infrastruktuře nebude nijak omezena dostupnost www.cnb.cz ani v případě technické závady na inline zařízení. V případě technické závady na inline zařízení, dojde k automatickému přepnutí (hw bypass) do plně transparentního režimu, který nebude nijak ovlivňovat provoz.

Technické parametry řešení

Navržené řešení je postaveno na hardwaru Arbor AED 8100.



1. VGA connector
2. **USB1** (top) and **USB2** (bottom) (USB 3.0)
3. (Not supported) Remote Management NIC
4. **USB3** (top) and **USB4** (bottom) (USB 3.0)
5. **mgt0**: 10GBASE-T Ethernet management port 0
6. **mgt1**: 10GBASE-T Ethernet management port 1
7. Protection ports
8. Two ground studs for DC-input system
9. Power supply 2 (DC module is shown)

   DC connector pinout:
   - Pin 3 (top): Return
   - Pin 2 (middle): DC
   - Pin 1 (bottom): Ground

   You must assemble the DC power cables by using the connector assemblies that come with the DC power supplies.
10. Power supply 1 (AC module is shown)

Features	8100	8100-CI
Physical Dimensions	**Chassis:** 2U rack height; **Height:** 3.45 inches (8.67 cm); **Width:** 17.14 inches (43.53 cm); **Depth:** 20 inches (50.8 cm); **Weight:** 36.95 lbs. (17.76 kg)	
Power Options	**DC:** 2 x DC redundant, hot swap capable power supplies; **DC Power Ratings:** -40 to -72 Vdc, 28/14 A max (per DC input); **AC:** 2 x AC redundant, hot swap capable power supplies; **AC Power Ratings:** 100 to 240 VAC, 50 to 60 Hz, 12/6 A max; Both AC and DC power options are 850-watt.	
Hard Drives	2 x 240GB SSD in RAID 1 Configuration	
Environmental	**Operating:** Temperature : 41°F to 104°F (5° to 40°C) Humidity: 5–85%; **Non-Operating:** Temperature -40° to 158°F (-40° to 70°C); Humidity 95%	
Operating System	Our proprietary ArbOS® operating system	
Management Interfaces	2 x 1G or 2 x 10G Copper, RJ-45 serial console support	
Protection Interfaces	• 4 x 1 GigE bypass ports (LX, SX or copper) • 8 x 1 GigE bypass ports (LX, SX, copper or mixed) • 12 x 1 GigE bypass ports (LX, SX, copper or mixed) • 4 x 10 GigE bypass ports (LR or SR) • 8 x 10 GigE bypass ports (LR, SR, or mixed) • 4 x 10 GigE bypass ports (LR or SR) plus 4 x 1GigE bypass ports (LX, SX or copper) • 4 x 10 GigE bypass ports (LR or SR) plus 8 x 1GigE bypass ports (LX, SX or copper) • 8 x 10 GigE bypass ports (LR or SR) plus 4 x 1GigE bypass ports (LX, SX or copper) • 2 x 40 GigE bypass ports (LR or SR) • 4 x 40 GigE bypass ports (LR or SR) • 2 x 40 GigE bypass ports (LR or SR) plus 4 x 10 GigE bypass ports (LR or SR) • 2 x 40 GigE bypass ports (LR or SR) plus 8 x 10 GigE bypass ports (LR or SR)	
Traffic Bypass Options	Integrated hardware bypass; Internal "software" bypass to pass traffic without inspection	
Latency	Less than 80 microseconds	
Availability	Inline bypass, dual power supplies, solid-state hard drive RAID cluster	

DDoS Ochrana - inline support

DDoS Ochrana - inline support - poskytování (provoz) hardware inline, který obsahuje:

- Správu hardware a zajištění jeho trvalé funkčnosti dle definovaných garantovaných parametrů v bodě 2.2.4. této nabídky.
- Technickou podporu a konfiguraci služby v rozsahu 2 hodiny/kalendářní měsíc (technickou podporou se rozumí především vzdálené úpravy konfigurace služby dle požadavků ČNB nad rámec odsouhlasené iniciální konfigurace)
- Havarijní zásah v případě poruchy zařízení.
- Upgrade firmwaru a softwaru zařízení, kontrola licenční politiky výrobce.
- Hodnocení výkonnosti systému.
- Vytvoření a uchování zálohy poslední změny konfigurace.

Poskytování (provoz) DDoS Ochrana - inline neobsahuje:

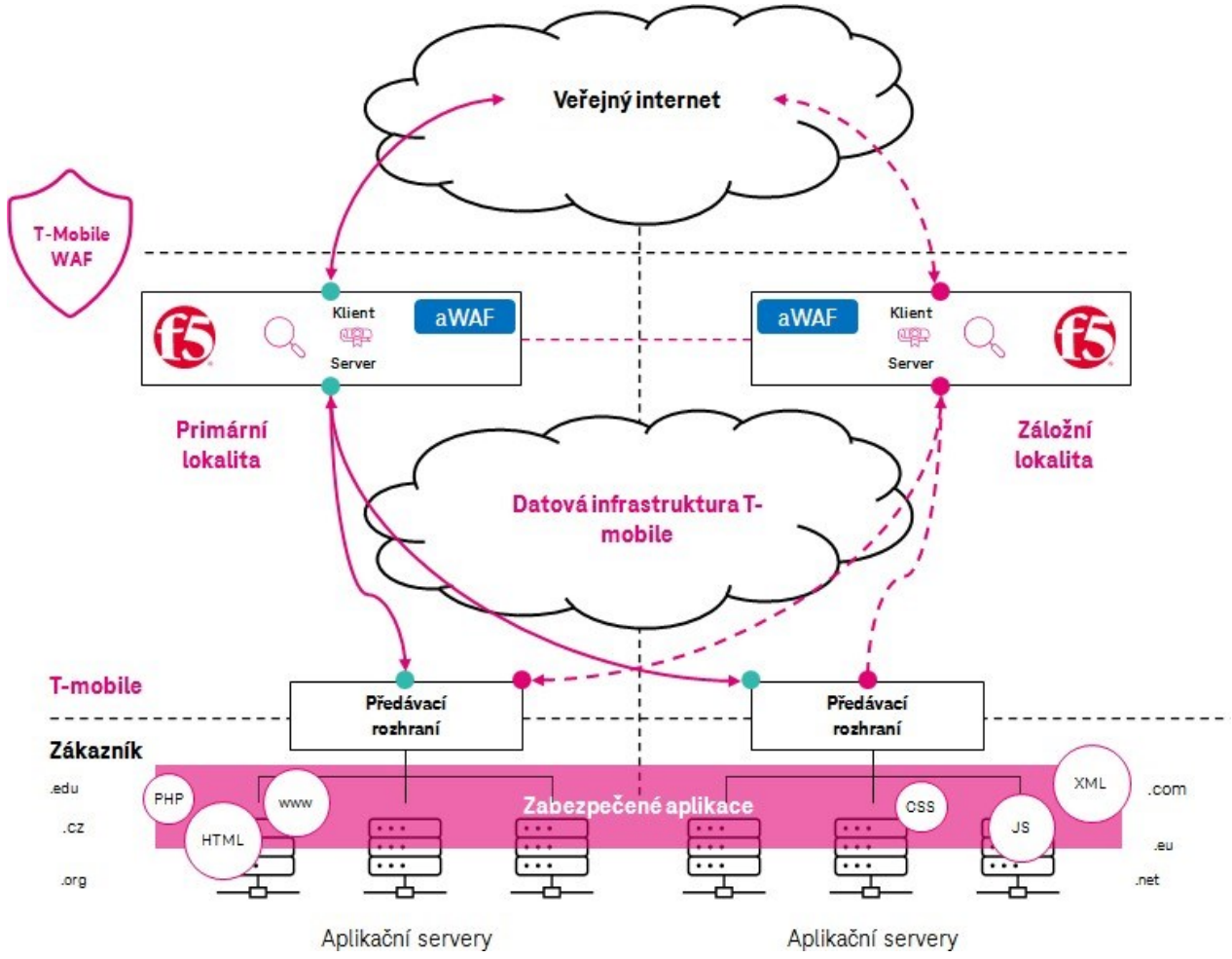
- Technickou podporu vyžádanou ČNB nad rámec odsouhlasené iniciální konfigurace, která přesáhne časový objem 2 hod v kalendářním měsíci (re)konfiguračních prací a technické podpory.
- Havarijní zásah, pokud závada či nefunkčnost zařízení byla způsobena ČNB, uživatelem, třetí osobu, apod. – tzn. z příčin, které neleží na straně poskytovatele.

(1) V rámci Služby garantuje Poskytovatel Smluvnímu partnerovi včasnou implementaci standardních ochranných postupů (scénářů) dle Zadání a zajišťuje podporu specialistů Poskytovatele.
(2) Poskytovatel se zavazuje poskytovat Službu na základě Best Practice principů s využitím aktuálně dostupné sady funkcí Platformy.
(3) Poskytovatel nenese odpovědnost za případné škody, které Smluvní partner utrpí v důsledku jakéhokoli útoku nebo jakýmkoliv opatřením přijatým Poskytovatelem pro ochranu příchozího provozu do sítě Smluvního partnera.
(4) Poskytovatel upozorňuje Smluvního partnera, že v souladu se zák. č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), v platném znění, je povinen poskytovat přednostní připojení pro určené subjekty, zajišťovat bezpečnost a integritu své sítě elektronických komunikací a bezpečnost služeb, které poskytuje, a plnit další zákonné povinnosti či povinnosti uložené mu na základě zákona soudním či správním rozhodnutím či opatřením. Za účelem zachování integrity a bezpečnosti sítě T-Mobile, služeb poskytovaných prostřednictvím této sítě a koncových zařízení koncových Uživatelů, může Poskytovatel uplatňovat dočasná opatření spočívající v blokování IP adres a jejich rozsahů, blokování síťových portů, protokolů a doménových jmen, dále pak aktualizaci firmware a řízení konfigurace koncových zařízení, které má Poskytovatel ve své správě, jsou-li tyto známým zdrojem nebo cílem útoků a nebo představují hrozbu pro bezpečnost a integritu sítě.
(5) Poskytovatel není odpovědný za neposkytnutí nebo vadné poskytnutí Služby, resp. za újmu, vzniklou v důsledku následujících skutečností, které pokud nastanou, nejsou považovány za Poruchu Služby a Služba není v jejich důsledku považována za nedostupnou (resp. vadně poskytnutou):
   (a) V případech, kdy za poruchu Služby neodpovídá Poskytovatel v souladu s příslušnými právními předpisy.
   (b) Poruchy Služby vzniklé vnitřní chybou operačního systému a dalšího programového vybavení třetích stran. Případnou odpovědnost nesou tyto třetí strany dle jejich licenčních ujednání.
   (c) Poruchy Služby vzniklé v důsledku nefunkčnosti služeb Smluvního partnera. Případnou odpovědnost nese Smluvní partner.
   (d) Poruchy Služby zapříčiněné počítačovými viry, červy, spamy apod., pokud není způsobeno zanedbáním povinností Poskytovatele sjednaných ve Smluvním dokumentu.
   (e) Doba, po kterou je Smluvní partner v prodlení s poskytnutím součinnosti,
   (f) Nesprávné užití Služby ze strany Smluvního partnera – např. nevhodné nastavení parametrů software, síťového prvku, či nevhodná volba software nebo síťového prvku apod.
   (g) Plánované výpadky a údržba či update Služby, popř. jiné služby se Službou provázané, ze strany Poskytovatele, a to při splnění podmínek stanovených v ustanovení čl. III odst. 3 této smlouvy,
   (h) Doba, po kterou Smluvní partner nemůže přistoupit přes webové rozhraní Portálu, pokud je Portál prokazatelně dostupný.

Příloha č. 4: Popis služby WAF.

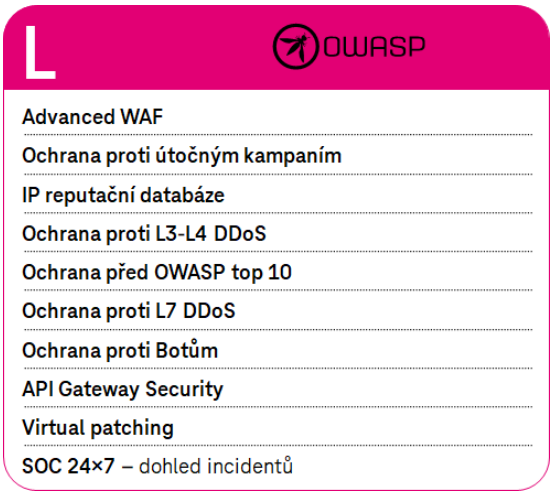
1.1 Předmět plnění

Předmětem plnění je poskytování služeb **Webového Aplikačního Firewallu** (dále také jen WAF) s cílem ochránit definované aplikační prostředky zákazníka před komplexními internetovými útoky.



Službu WAF T-Mobile provozuje jako jednu z dalších bezpečnostních služeb v rámci své vlastní infrastruktury. Nasazení služby je rychlé a nevyžaduje od zákazníka žádnou prvotní investici do infrastrukturních prvků. Zákazník si v rámci služby pronajímá část výkonu sdílené platformy poskytovatele určené k aplikaci ochranných opatření v rámci služby, která odpovídá jeho aktuálním potřebám. T-Mobile zajišťuje nastavení a pravidelnou údržbu platformy, a dále pravidelný reporting a konzultace související s vyhodnocením provozu služby.

Služba zahrnuje **ochranu 5 aplikací zákazníka** ve variantě **WAF L**. Seznam aplikací si vymění pověřené osoby objednatele a poskytovatele provozu v domluveném termínu.



V rámci provozního zajištění služba zahrnuje:

- **Provoz a dohled v celkové kapacitě 7 MH měsíčně (**z pohledu nasazování hlavních aplikačních release počítá s periodicitou **6 měsíců):**
    - Reporting a konzultace
    - Revize bezpečnostních politik v souvislosti s aktualizací signatur
    - Revize bezpečnostních politik v souvislosti s novými release aplikací
    - 24×7 SOC proaktivně (6x řešený incident v ceně služby

Nabídka rovněž zahrnuje prémiovou funkci **IP Intelligence**, která prostřednictvím online reputační databáze umožňuje detekci uživatelů, jejichž zdrojová IP adresa má špatnou reputaci. Bezpečnostní politika tak může automaticky blokovat přístupy ze známých:

- anonymizačních proxy serverů
- botnetů
- adres, které provádí webové útoky
- skenerů webových aplikací
- IP adres provádějící DoS útoky
- phishingových proxy serverů

2 Popis služby WAF

2.1 Potřeba specializované aplikační ochrany

Dnešní moderní síťové firewally (NGFW) často disponují i základní funkcí ochrany webových aplikací na základě průběžně aktualizované sady signatur (princip IPS – Intrusion Prevention System). Nasazení aplikační IPS v rámci NGFW je vhodné zejména k zabezpečení aplikační infrastruktury (Windows Server, Apache, MySQL DB apod.) proti známým typům aplikačních útoků a má tedy bezesporu svůj význam. Je však zároveň důležité vnímat i její omezení, které souvisí především se skutečností, že chráněné objekty není schopna vnímat jako sadu několika odlišně fungujících částí a často není schopna se zaměřit na potřebný detail odlišující škodlivý provoz od toho legitimního (např. pokud je jako součást prevence Cross Site Scripting útoků potřeba zakázat použití scriptů v konkrétních uživatelských formulářích, ale neblokovat scripty v jiné části webové aplikace, kde je jejich použití legitimní).

Zajištění komplexní ochrany webových aplikací vyžaduje nasazení specializované aplikační ochrany v podobě Webových Aplikačních Firewallů (WAF). WAF na rozdíl od IPS pracují na principu přesné definice legitimní komunikace, která je na webové aplikaci povolena, a to z pohledu jednotlivých komponent, které se týkají HTTP provozu. Vyhodnocována jsou povolená URL, parametry formulářových polí, HTTP hlavičky apod. WAF je schopna detekovat vše, co se jakkoliv odchýlí od definované sady pravidel, a v případě útoku takovou komunikaci zablokovat. WAF spolehlivě rozezná automatizovanou komunikaci botů od chování legitimních uživatelů. Ochranu lze z principu cílit na konkrétní části webů, např. webové uživatelské formuláře a zabránit tak jejich prostřednictvím vytěžování databáze.

2.2 Charakteristika služby WAF

Služba WAF je postavena na T-Mobile operátorské platformě F5 BIG-IP aWAF (Advanced WAF) kombinované s F5 BIG-IP LTM (Load Traffic Manager). Jedná se o plně multi-tenantní platformu, která zajišťuje logické oddělení WAF instancí, webových aplikací a webových služeb jednotlivých zákazníků, přičemž každý zákazník disponuje dedikovaným síťovým rozhraním.

Použitím funkcí automatického učení, dynamického profilování, unikátních metod detekce anomálií a politik založených na rizicích, dokáže služba WAF zajistit potřebnou ochranu aplikačních prostředků zákazníka před neustále se vyvíjejícími útoky.

2.3 Hlavní přínosy služby WAF

Mezi hlavní přínosy poskytované služby WAF patří především tyto:

- Zajištění aplikační bezpečnosti a shody s předpisy
- Okamžité nasazení ochrany díky před-připraveným bezpečnostním politikám
- Možnost automatizace vytváření bezpečnostních politik na základě swagger souborů
- Rychlé ošetření zranitelností prostřednictvím pro-vazby na výstupy z penetračních testů (virtual patching)
- Vysoká dostupnost a škálovatelnost
- Pokročilá technologie prokazující 99,89% celkové účinnosti zabezpečení
- Přehledný reporting aktuálního stavu zabezpečení
- Možnosti detailní analýzy bezpečnostních událostí

2.4 Funkční rozsah nabízené služby WAF

V rámci této nabídky je služba WAF nabídnuta v následujícím rozsahu funkcionalit a služeb:

- Ochrana proti prolomení hrubou silou
- Aplikační IPS
- Ochrana citlivých informací
- Ochrana proti Code Injection útokům
- Ochrana proti SQL Injection útokům
- Ochrana proti Cross-Site Scripting (XSS)
- Ochrana proti L3/4 DDoS útokům
- http Compliance
- SSL Offload ochrana pro zabezpečení proti SSL útokům včetně SSL floods, POODLE, Heartbleed a různých memory-cracking nástrojů
- Šifrování klíči do velikosti 2048 bitů

3 Provoz služby WAF

3.1 Běžný provozní režim

Provoz služby v běžném provozním režimu zahrnuje následující oblasti:

- Správa platformy
- Reporting, konzultace, aktualizace

Rozsah činností za jednotlivé oblasti je blíže popsán v následujících odstavcích.

6.2.1 Správa platformy

- Pronájem veškerého zařízení (hardware), pronájem softwarových licencí pro provoz služby
- Správu služby a zajištění její trvalé funkčnosti dle definovaných garantovaných parametrů
- Upgrade firmwaru a softwaru zařízení, kontrola licenční politiky výrobce
- Nasazování bezpečnostních záplat
- Vytvoření a uchování zálohy poslední změny konfigurace

6.2.2 Reporting, konzultace, aktualizace

- Generování pravidelných měsíčních provozních reportů
- Konzultace související s vyhodnocením provozních reportů
- Aktualizace bezpečnostních pravidel včetně souvisejících aktivit tj.:
  - U stávajících pravidel ověření, že nedochází ke generování false positive
  - U nových pravidel vyhodnocení jejich chování v prostředí zákazníka (monitoring s vyhodnocením a doporučením nastavení v rámci provozu)
- V souladu s plánovaným release plánem zákazníka zajištění následujících aktivit:
  - Revize politik
  - 1-2 iterace pro odladění stávajících a nasazení nových politik
  - Workshopy a konzultace se zákazníkem
  - Aktualizace dokumentace

Příloha č. 5 - Specifikace cen služeb

Název	Pravidelná cena
Virtuální datová centra (VDC) + Virtuální záloha	56 896,- Kč měsíčně
DDoS ochrana	50 500,- Kč měsíčně
WAF	34 590,- Kč měsíčně
DDoS Inline	98 400,- Kč ročně

Příloha č. 6 - Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději den před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků poskytovatele. Poskytovatel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů 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 jen „GDPR“). Poskytovatel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že poskytovatel předá jejich osobní údaje v rozsahu: 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 budovy ČNB z důvodu ochrany majetku a osob a správy přístupového systému ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči poskytovateli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese poskytovatel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle bodu 2. nahradí poskytovatel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků poskytovatele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Při příchodu do objektů ČNB pracovníci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny v seznamu, nebudou do objektů ČNB vpuštěny.
6. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostor ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.
7. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB, a dále instrukcemi vyhlašovanými vnitřním rozhlasem ČNB.

8. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
9. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
10. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
11. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či odcizování majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
12. Pracovníci poskytovatele uvedení v seznamu se musí před započetím výkonu práce v objektech ČNB seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifiky daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka poskytovatele uvedeného na seznamu ohledně dodržování těchto předpisů a ustanovení.

Příloha č. 7 - 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).

Příloha č. 8 - Obchodní podmínky pro změnu poskytovatele služby zpracování dat společnosti T-Mobile Czech Republic, a.s.

Článek 1 Obecná ustanovení

1.1. Tyto Obchodní podmínky pro změnu poskytovatele služby zpracování dat společnosti T-Mobile Czech Republic, a.s. (dále jen "Podmínky") upravují práva a povinnosti mezi T-Mobile Czech Republic, a.s. jako poskytovatelem (dále jen "Poskytovatel" a/nebo "zdrojový Poskytovatel") a zákazníkem (dále jen "Zákazník") služeb zpracování dat v souvislosti s převodem služby na jiného poskytovatele nebo přenosem dat do lokální infrastruktury Zákazníka, popř. v souvislosti s požadavkem Zákazníka na výmaz dat bez jejich přenosu. Tyto Podmínky tvoří /budou tvořit nedílnou součást smlouvy uzavřené mezi Poskytovatelem a Zákazníkem, jejímž předmětem je poskytování služeb zpracování dat a kterou má Zákazník zájem přenést k jinému Poskytovateli nebo na svou lokální infrastrukturu.

1.2. Tyto podmínky jsou vydány za účelem plnění povinností vyplývajících z nařízení (EU) 2023/2854 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (dále jen "Nařízení o datech).

1.3 Těmito Podmínkami nejsou dotčena práva a povinnosti Poskytovatele a/nebo Zákazníka plynoucí z unijních a vnitrostátních právních předpisů o ochraně osobních údajů, soukromí a důvěrného charakteru sdělení, které se použijí na osobní údaje zpracovávané v souvislosti s právy a povinnostmi stanovenými v těchto Podmínkách, zejména pokud jde o nařízení (EU) 2016/679 a (EU) 2018/1725 a směrnice 2002/58/ES, ani pravomoci a kompetence dozorových úřadů a práva subjektů údajů. V případě rozporu mezi těmito Podmínkami a unijními právními předpisy o ochraně osobních údajů nebo soukromí nebo vnitrostátními právními předpisy přijatými v souladu s těmito právními předpisy Unie mají přednost příslušné unijní nebo vnitrostátní právní předpisy o ochraně osobních údajů nebo soukromí.

1.4. Definice

"Službou zpracování dat" se rozumí služba definovaná v čl. 2 odst. 8 Nařízení o datech, poskytovaná Poskytovatelem Zákazníkovi na základě Smlouvy (dále také jen „Služba“).

"Cílovým poskytovatelem" se rozumí poskytovatel služby zpracování dat, ke kterému Zákazník přechází dle Žádosti předložené Poskytovateli za účelem použití jiné služby zpracování dat stejného typu nebo jiných služeb.

„Cílovým prostředím“ se rozumí služba (prostředí) Cílového poskytovatele nebo místní infrastruktura informačních a komunikačních technologií určená Zákazníkem.

„Digitálními aktivy“ jsou prvky v digitální podobě, včetně aplikací, k nimž má Zákazník právo k jejich užívání, nezávisle na smluvním vztahu pro Službu, již hodlá změnit;

„Exit plánem“ je ujednání Smlouvy upravující mimo jiné práva a povinnosti stran při ukončení Smlouvy relevantní pro Službu,

"Exportovatelnými daty" se rozumí vlastní data Zákazníka, tj. vstupní a výstupní data, včetně metadat, přímo či nepřímo vytvořená nebo společně vytvořená užíváním Služby Zákazníkem, s výjimkou jakýchkoli aktiv nebo dat Poskytovatele nebo třetí strany, které jsou chráněny právy duševního vlastnictví nebo představují obchodní tajemství.

"Přenosem" se rozumí proces zahrnující Poskytovatele, Zákazníka a případně Cílového poskytovatele, v jehož rámci Zákazník přechází z používání Služby na používání jiné služby zpracování dat stejného typu nebo jiné služby v Cílovém prostředí, a to i prostřednictvím extrakce, transformace a nahrání dat.

„Přechodné období“ je definováno v čl. 3.2 Podmínek.

"Poplatky za přenos" jsou poplatky účtované Poskytovatelem Zákazníkovi za úkony realizované Poskytovatelem v souvislosti s přenosem, odlišné od standardních poplatků za služby nebo poplatků za předčasné ukončení, které zahrnují poplatky za výstup dat.

„Smlouvou“ se rozumí smluvní závazek sjednaný mezi Poskytovatelem a Zákazníkem, jehož předmětem je mimo jiné poskytování Služby (zejména Specifikace služby nebo jiná smlouva/dohoda).

„stranou“ Poskytovatel a/nebo Zákazník

„Žádost“ je projev vůle Zákazníka doručený Poskytovateli za účelem přenosu Služby do Cílového prostředí nebo za účelem ukončení Služby s výmazem dat Zákazníka.

1.5. Vyloučení z oblasti působnosti

Tyto Obchodní podmínky se nevztahují na službu zpracování dat poskytovanou třetí osobou a/nebo na službu třetí osoby, kterou Poskytovatel pouze zprostředkoval/zajistil Zákazníkovi, pokud se její poskytování řídí výhradně obchodními podmínkami této třetí osoby.

Tyto Podmínky se nevztahují na služby zpracování dat, které jsou poskytovány jako neprodukční verze pro účely testování a hodnocení, a po omezenou dobu.

1.6 Zvláštní režim

Pokud se strany písemně nedohodnou jinak, vztahují se tyto Podmínky také na služby zpracování dat uvedené v článku 31 odst. 1 Nařízení o datech, s vyloučením těch ustanovení, která se neuplatní ve smyslu článku 31 odst. 1 Nařízení o datech.

Článek 2 Specifikace údajů přenosu

2.1 Konkrétní specifikace kategorií dat a digitálních aktiv, která mohou být do Cílového prostředí přenesena v rámci jednotlivých Služeb poskytovaných Poskytovatelem, a datových formátů, ve kterých jsou exportovatelná data k dispozici, jsou zveřejněny v aktuálním online registru na webových stránkách Poskytovatele: https://www.t-mobile.cz/ke-stazeni#/.

Poskytovatel je oprávněn přiložené specifikace a/nebo online registr zveřejněný na webových stránkách kdykoli jednostranně aktualizovat a měnit, aniž by o tom byl povinen informovat Zákazníka v případě, že změnou není Zákazník přímo negativně dotčen.

2.2. Přenos dat prostřednictvím sebeobslužných automatizovaných nástrojů

Automatizované nástroje jsou k dispozici především pro Služby typu infrastructure-as-a-service (IaaS). Zákazník může svá data samostatně bez další součinnosti Poskytovatele přenést kdykoliv do ukončení Přechodného období, a to v rozsahu určeném specifikací kategorií dat a digitálních aktiv uvedenou pro příslušnou Službu ve zveřejněném online registru, pokud nebylo mezi stranami výslovně písemně sjednáno jinak, a to zejména v rámci Exit plánu.

2.3 Přenos dat na základě plánu přenosu

V případě, že nejsou k dispozici nástroje pro automatizované předávání dat, a/nebo Zákazník pro přenos Služby vyžaduje součinnost a/nebo individuální přístup Poskytovatele, mohou se Smluvní strany dohodnout na plánu přenosu (dále jen "Plán"), který Poskytovatel a Zákazník společně písemně sjednají. Obdobně se postupuje v případě dříve sjednaného Exit plánu.

Plán zahrnuje zejména:

a) specifikaci kategorií dat a digitálních aktiv, která lze přenášet, včetně alespoň všech exportovatelných dat;

(b) specifikace kategorií dat, které jsou specifické pro vnitřní fungování Služby a které zprošťují dle Nařízení o datech Poskytovatele povinnosti k přenosu z důvodu rizika porušení obchodního tajemství Poskytovatele;

(c) informace o známých rizicích pro kontinuitu poskytování funkcí nebo služeb ze strany Poskytovatele;

d) podrobnosti o pomoci při změně poskytovatele a ukončení Smlouvy, včetně způsobů a formátů přenosu a kroků potřebných k provedení procesu změny služby;

(e) kontaktní údaje Zákazníka pro realizaci Plánu;

(f) odhad doby potřebné k přesunu dat a digitálních aktiv od Poskytovatele;

g) překážky Služby a technická omezení, včetně těch, které vyplývají z uchovávání údajů mimo území Evropské unie;

h) popis sledu operací směřujících k přenosu Služby v oblasti odpovědnosti Poskytovatele navržený Poskytovatelem;

(i) popis bezpečnostních opatření k zabezpečení dostupnosti, důvěrnosti, autenticity a integrity přenášených dat, a dále popis zkušební metody navržené Poskytovatelem, pokud mají být provedeny testy

(j) cenu, pokud není Plán sjednán na základě písemné dohody Smluvních stran bezplatně, popř. pokud je cena za jeho plnění již zahrnuta v ceně Služby.

Dobu přenosu dat určí Poskytovatel přiměřeně s ohledem na rozsah dat, požadovaný způsob jejich přenosu a své aktuálně dostupné kapacity. Některé úkony Poskytovatele při přenosu Služby nad rámec základních úkonů pro standardní přenos Služby mohou být podmíněny splněním všech finančních a smluvních závazků Zákazníka vůči Poskytovateli.

Není-li předem písemně sjednáno jinak, v rámci přenosu Služby bude umožněn přístup k datům způsobem a ve formátu dohodnutém mezi stranami (např. JSON, XML, CSV a další), a to prostřednictvím jedinečného URL odkazu doručeného bez zbytečného odkladu e-mailem Zákazníkovi (obdrží ADSR a administrátor administračního portálu). Přenášená data jsou šifrována a šifrovací klíč doručí Poskytovatel bez zbytečného odkladu odpovědnému zástupci Zákazníka (ADSR, pokud je sjednán).

Poskytovatel je povinen přijmout veškerá nezbytná opatření, aby zabránil neoprávněnému přístupu při přenosu dat, včetně šifrovacích klíčů. Poskytovatel neodpovídá za případný neoprávněný přístup při přenosu dat v případě, kdy neoprávněný přístup mohla umožnit aplikace individuálního technického požadavku Zákazníka na přenos (zejména v případě API zajištěného Zákazníkem). V rámci zpřístupnění údajů podle Plánu bude Poskytovatel sdílet se Zákazníkem takové informace a dokumentaci, které umožní Zákazníkovi získat potřebné znalosti pro zajištění budoucí nezávislosti při nakládání s těmito daty.

Článek 3 Proces přenosu Služby

3.1. Žádost Zákazníka 3.1.1 Zákazník může Poskytovateli oznámit své rozhodnutí provést po uplynutí výpovědní doby jeden nebo více z těchto kroků: a) přejít k jinému poskytovateli služeb zpracování dat, přičemž Zákazník o tomto Poskytovateli uvede nezbytné údaje; b přejít do místní infrastruktury informačních a komunikačních technologií Zákazníka; c) vymazat svá exportovatelná data a digitální aktiva.

3.1.2 Zákazník může požádat o přenos Služby do Cílového prostředí podáním Žádosti. Žádost lze podat na Zákaznickém centru business nebo prostřednictvím ICT Portálu.

3.1.3 Žádost lze podat pouze po dobu trvání Smlouvy, nejpozději však dva pracovní dny před uplynutím výpovědní doby, popř. před uplynutím v dohodě o ukončení Smlouvy sjednaného okamžiku ukončení Smlouvy.

3.1.4 Zákazník v Žádosti uvede, zda

(a) žádá o přechod k jinému poskytovateli služeb zpracování dat, přičemž v takovém případě poskytne případné potřebné údaje o Cílovém poskytovateli; nebo

(b) vyžaduje přechod na místní infrastrukturu informačních a komunikačních technologií;

a dále v případě potřeby v Plánu uvede data, které požaduje přednést.

3.1.5 Poskytovatel potvrdí přijetí Žádosti Zákazníkovi nejpozději do 3 pracovních dnů stejným způsobem komunikace, jaký Zákazník použil při podání Žádosti. V případě, že Žádost nesplňuje požadavky a/nebo nevyhovuje těmto podmínkám (např. je vyžadován export dat mimo online registr), vyhrazuje si Poskytovatel právo požádat Zákazníka o doplnění, přičemž pokud Zákazník Žádost nedoplní ani v přiměřené lhůtě, nejpozději však do 5 pracovních dnů, a přenos Služby bez takového doplnění nelze realizovat ani standardní cestou (ve smyslu obecné technické specifikace pro přenos), je Poskytovatel oprávněn Žádost Zákazníka odmítnout, o čemž Poskytovatel Zákazníka bezodkladně informuje.

3.1.6 Doručení Žádosti Poskytovateli se považuje za podání výpovědi ze strany Zákazníka v souladu s podmínkami Smlouvy pro příslušnou Službu, přičemž dnem následujícím po dni doručení výpovědi Poskytovateli začíná běžet dvouměsíční výpovědní doba. V případě, že je výpovědní doba ve Smlouvě sjednána na dobu kratší než dva měsíce, platí výpovědní doba/lhůta sjednaná ve Smlouvě. Výpovědní doba nepřesáhne dva měsíce. Tím není dotčena případná dohoda stran ve smyslu článku 7.4 těchto Podmínek.

3.2. Přechodné období pro přenos Služby

3.2.1 Smluvní strany se dohodly na Přechodném období v délce maximálně 30 kalendářních dnů, které začíná běžet dnem následujícím po dni uplynutí výpovědní doby dle čl. 3.1.3 a 3.1.6 těchto podmínek, případně jiným okamžikem určeným těmito Podmínkami.

3.2.2 Přechodné období skončí:

- pokud Zákazník oznámil (doručil) Poskytovateli úspěšné dokončení procesu změny poskytovatele před zahájením Přechodného období, prvním pracovním dnem Přechodného období, nebo

- pokud Zákazník oznámil Poskytovateli úspěšné dokončení procesu změny poskytovatele v průběhu Přechodného období, prvním pracovním dnem následujícím po tomto oznámení, nebo

- k datu sjednanému dohodou stran; nebo

- uplynutím náhradního Přechodného období dle čl. 3.2.5 těchto Podmínek, nebo

- uplynutím 60 kalendářních dnů, pokud Zákazník v průběhu Přechodného období písemně požádal dle čl. 3.2.4 Podmínek o prodloužení standardní doby Přechodného období stanovené v čl. 3.2.1 těchto Podmínek; nebo

- uplynutím 30 kalendářních dnů následujících po dni uplynutí výpovědní doby, pokud nenastala některá z výše uvedených okolností ukončení Smlouvy (Služby).

3.2.4 V souladu s čl. 25 odst. 5 Nařízení o datech je Zákazník oprávněn jednou písemně požádat Poskytovatele o prodloužení přechodného období, a to na dobu, kterou považuje za vhodnější pro své vlastní účely, nejdéle však o dodatečné období 30 kalendářních dnů. Zákazník je povinen podat žádost o prodloužení Přechodného období způsobem, jakým podal Žádost, a to nejméně dva pracovní dny před uplynutím Přechodného období dle čl. 3.2.1 těchto Podmínek.

3.2.5 Nelze-li Přechodné období v délce 30 dnů z technických důvodů dodržet, informuje o tom Poskytovatel Zákazníka do 14 pracovních dnů od obdržení Žádosti spolu s vhodným zdůvodněním technické neproveditelnosti a současně uvede náhradní Přechodné období, které nepřesáhne sedm (7) měsíců (dále jen "Náhradní přechodné období").

3.2.6 Zákazník je povinen nejpozději do konce Přechodného období (včetně případně prodlouženého či Náhradního přechodného období) převést Službu a provést vlastní technický přenos svých exportovatelných dat. V případě, že je pro účely přenosu Služby vyžadována součinnost Cílového poskytovatele, je Zákazník povinen zajistit nezbytnou součinnost Cílového poskytovatele tak, aby byl přenos Služby včetně technického přenosu exportovatelných dat dokončen nejpozději poslední den Přechodného období.

3.2.4 Po dobu sjednaného Přechodného období (včetně případně prodlouženého či Náhradního přechodného období) zůstává předmětná Smlouva v platnosti a Poskytovatel je oprávněn účtovat cenu za Službu v souladu s podmínkami Smlouvy.

3.2.5 Po dobu Přechodného období Poskytovatel vyvine maximální úsilí k zajištění kontinuity Služby.

3.3 Spolupráce s třetími stranami

3.3.1 V případě, že Zákazník zmocní třetí osobu (včetně Cílového poskytovatele), aby jednala jeho jménem při převodu služby a podala/změnila jeho jménem Žádost, je povinen ji za tímto účelem vybavit plnou mocí s úředně ověřeným podpisem Zákazníka a zajistit, aby tento taková třetí osoba své oprávnění jednat jménem Zákazníka na výzvu Poskytovatele vždy prokázala.

3.3 2 Poskytovatel se zavazuje v přiměřeném rozsahu v rámci procesu přenosu Služby zohledňovat závislosti na jiných subjektech, jako jsou dodavatelé Zákazníka, kteří se podílejí na realizaci přenosu Služby. Má se za to, že pokud dodavatel Zákazníka jedná jménem Zákazníka, zejména při technických úkonech během Přechodného období, činí tak s jeho souhlasem, jeho jménem a na jeho účet. Tím není dotčeno právo Poskytovatele kdykoli ověřit oprávnění třetí strany jednat jménem a na účet Zákazníka a třetí strana a/nebo Zákazník jsou povinni toto Poskytovateli hodnověrně prokázat.

3.3.3 Zákazník je povinen uhradit Poskytovateli dodatečné náklady, které mu v souvislosti s plněním dle tohoto odstavce vznikly.

Článek 4 Povinnosti Poskytovatele během procesu změny poskytovatele

4.1. Poskytovatel se zavazuje poskytnout Zákazníkovi a třetím osobám schváleným Zákazníkem přiměřenou pomoc v procesu změny Poskytovatele od jeho počátku a po celou dobu jeho trvání tak, aby Zákazník mohl v Přechodném období ukončit přenos Služby. Za tímto účelem je Poskytovatel povinen zejména:

a) podporovat Zákazníkovu strategii pro odchod a poskytnout mu odpovídající informace nezbytné k dokončení změny poskytovatele a odpovídající technickou podporu; v případě, že

budou v procesu přenosu zjištěny problémy, Poskytovatel a Zákazník v dobré víře analyzují příčiny a dohodnou se na řešení;

b) jednat s náležitou péčí o zachování kontinuity poskytování Služby podle Smlouvy až do jejího ukončení;

c) zajistit, aby byla po celou dobu procesu změny poskytovatele zachována vysoká úroveň bezpečnosti, zejména pokud jde o bezpečnost dat během jejich přenosu a/nebo soustavná bezpečnost během doby jejich zachování a zpřístupnění, v souladu s platnými právními předpisy. Přenos dat bude prováděn v souladu s technickými a organizačními standardy poskytovatele, které zajišťují ochranu důvěrnosti, integrity a dostupnosti údajů – za bezpečnost samotného procesu přesunu dat a integraci do cílového prostředí zodpovídá Zákazník. Osobní údaje mohou být předávány pouze za podmínek stanovených obecně závaznými právními předpisy a dalšími pravidly ochrany osobních údajů stanovenými Poskytovatelem. V případě, že Zákazník požaduje přenos osobních údajů k Cílovému poskytovateli umístěnému nebo do Cílového prostředí umístěného mimo Evropskou unii nebo Evropský hospodářský prostor, Poskytovatel provede tento přenos na základě pokynu Zákazníka. Zákazník je odpovědný za zajištění souladu takového přenosu s platnými ustanoveními upravující předávání osobních údajů do třetích zemí (zejména čl. 44 a násl. GDPR). Zákazník bere na vědomí, že ve třetích zemích nemusí být zajištěna srovnatelná úroveň ochrany osobních údajů.

Ujednáním o závazcích podle tohoto článku nejsou dotčena práva Poskytovatele podle § 30 odst. 6 Nařízení o datech. Poskytovatel není povinen zpřístupnit informace a digitální aktiva, ani umožnit jejich přenos do Cílového prostředí, pokud jsou chráněna právy duševního vlastnictví a/nebo pokud představují obchodní tajemství Poskytovatele, nebo pokud by ohrozila bezpečnost a integritu Služby Zákazníka nebo služeb Poskytovatele.

Článek 5 Povinnosti Zákazníka během procesu změny poskytovatele

5.1. Zákazník se zavazuje přijmout veškerá nezbytná opatření k dosažení účinné změny poskytovatele služby zpracování dat. Zákazník je odpovědný za import a implementaci dat a digitálních aktiv v Cílovém prostředí, a to i v případech, kdy Zákazník pro tyto operace využívá služby třetí strany (včetně Cílového poskytovatele) a zavazuje se nahradit Poskytovateli škodu, pokud mu tato vznikla v důsledku porušení povinnosti Zákazníka (včetně povinností přenesených Zákazníkem na Cílového poskytovatele a/nebo jinou třetí stranu).

5.2 V případě potřeby, a aniž by byl dotčen čl. 30 odst. 6 Nařízení o datech, se Zákazník zavazuje respektovat práva duševního vlastnictví ke všem materiálům poskytnutým v procesu změn Poskytovatelem, jakož i obchodní tajemství Poskytovatele, a plnění tohoto závazku zajistit i u schválených třetích stran (včetně Cílového poskytovatele). Zákazník se zavazuje zpřístupnit tyto materiály a umožnit jejich použití třetím osobám k tomu oprávněným, a to pouze v rozsahu nezbytném pro dokončení procesu změny poskytovatele a pouze s předchozím výslovným souhlasem Poskytovatele. Přístup k materiálům Poskytovatele, které jsou chráněny právy duševního vlastnictví a/nebo obchodním tajemstvím souvisejícím s procesem změny Poskytovatele, a jejich používání, bude ukončen nejpozději s koncem Přechodného období

(včetně Náhradního nebo prodlouženého Přechodného období), a to v plném souladu s povinností mlčenlivosti a právy duševního vlastnictví udělenými Poskytovatelem.

5.3 Zákazník je povinen jednat v dobré víře tak, aby splnil veškeré pokyny Poskytovatele týkající se přenosu Služby, které mu Poskytovatel za tímto účelem sdělil.

5.4 Pokud Zákazník podal Žádost před uplynutím sjednané doby užívání Služby dle Smlouvy, podle které se Zákazník zavázal nepřetržitě využívat Službu po určitou dobu (tzv. závazková povinnost), je povinen uhradit Poskytovateli sjednanou smluvní pokutu/finanční vypořádání a/nebo jiné dodatečné peněžité nároky a/nebo náhradu újmy sjednané pro případ ukončení Smlouvy před uplynutím sjednané doby závazku.

Článek 6 Přístup k datům a výmaz dat

6.1 Po skončení Smlouvy na podkladě Žádosti umožní Poskytovatel Zákazníkovi na základě jeho písemné žádosti získat data, která byla předmětem přenosu Služby, a to ve lhůtě 30 kalendářních dnů, pokud nebyla mezi stranami písemně sjednána delší lhůta (dále jen "Doba přístupu k datům"). Zákazník je oprávněn požádat o přístup k údajům stejným způsobem, jakým podal Žádost a/nebo jiným způsobem, který určí Poskytovatel.

6.2 Po uplynutí Doby přístupu k datům a/nebo po ukončení Služby, pokud Zákazník nepodal Žádost, Poskytovatel vymaže veškerá data a digitální aktiva Zákazníka, která byla Zákazníkem vytvořena nebo s ním přímo souvisejí, a na základě písemné žádosti potvrdí Zákazníkovi na jeho e-mailovou adresu bez zbytečného odkladu, že tak učinil. Poskytovatel není povinen vymazat data, která lze exportovat a která je Poskytovatel povinen uchovávat podle platných právních předpisů a/nebo za účelem ochrany a výkonu práv Poskytovatele.

6.3 Úpravou těchto Podmínek není dotčena jakákoliv povinnost Poskytovatele postupovat na základě závazného pokynu příslušného orgánu veřejné moci k uchovávání dat nebo k pozastavení jejich navrácení nebo výmazu dat a majetku (aktiv) Zákazníka, popř. jiného pokynu s rovnocenným účinkem (znemožňujícím dokončení přenosu nebo výmazu dat na straně Poskytovatele), pokud je takový pokyn doručen Poskytovateli a Poskytovatel je povinen se tímto pokynem řídit, a to až do zrušení nebo změny své právní povinnosti.

§ 7 Ukončení Smlouvy

7.1. Smlouva (a Služba) se považuje za ukončenou:

i) po oznámení Zákazníka o úspěšném dokončení procesu přenosu Služby, podal-li Zákazník včas a řádně Žádost; nebo

ii) posledním dnem výpovědní doby, pokud si Zákazník nepřeje změnit poskytovatele, ale po ukončení Služby si přeje vymazat svá exportovatelná data a digitální aktiva,

pokud není jinde v těchto Podmínkách sjednáno jinak.

7.2 V případě, že Zákazník podal Žádost a přenos byl úspěšný, považuje se Smlouva za ukončenou pracovním dnem následujícím po dni doručení písemného oznámení Zákazníka o

úspěšném dokončení procesu změny poskytovatele, nejpozději posledním dnem Přechodného období.

7.3 Rozhodnutí o tom, zda byl přenos Služby úspěšný, je ve výhradní diskreci a odpovědnosti Zákazníka, přičemž Zákazník je povinen bezodkladně informovat Poskytovatele o úspěšném dokončení přenosu Služby.

7.4 V případě, že Zákazník neoznámí Poskytovateli, že úspěšně dokončil převod Služby a neoznámí, že převod nebyl úspěšný, má se za to, že přenos Služby byl úspěšně dokončen k poslednímu dni Přechodného období a k tomuto dni je ukončena Smlouva (a Služba).

7.5 V případě, že Zákazník oznámí Poskytovateli, že přenos Služby nebyl úspěšně dokončen během Přechodného období, vynaloží strany maximální úsilí, které od nich lze přiměřeně požadovat, k identifikaci a odstranění příčiny výpadku tak, aby přenos Služby mohl být úspěšně dokončen v co nejkratším možném čase, maximálně do 30 dnů. Dokud Zákazník nepotvrdí, že přenos Služby byl úspěšně dokončen, a strany se písemně nedohodnou jinak, neukončí Poskytovatel poskytování Služby a Smlouva zůstává v platnosti až do okamžiku potvrzení úspěšného přenosu Služby Zákazníkem, pokud není zjevně nepřiměřené po Poskytovateli takový závazek vyžadovat. V takovém případě je Poskytovatel oprávněn účtovat Zákazníkovi cenu za Službu v souladu s podmínkami Smlouvy až do ukončení Smlouvy, s výjimkou případů, kdy k neúspěšnému přenosu Služby došlo z důvodů, za které nese výhradní odpovědnost Poskytovatel. Tím nejsou dotčené případné další nároky Poskytovatele umožňující ukončení Smlouvy.

7.6 Pokud Zákazník podá Žádost ke Službě poskytované na podkladě Smlouvy, která má skončit uplynutím doby určité, sjednávají Smluvní strany následující:

i) pokud Zákazník podal Žádost dříve než 30 dnů před koncem sjednané doby určité, Přechodné období dle bodu 3.2 těchto Podmínek začíná běžet 30 dnů před posledním dnem sjednané doby trvání Smlouvy,

ii) pokud Zákazník podal Žádost později než 30 dnů před koncem sjednané doby určité, Přechodné období se zkracuje tak, že uplyne posledním dnem sjednané doby trvání Smlouvy.

V ostatním se uplatní ujednání čl. 3.2 těchto Podmínek.

7.7 Poskytovatel oznámí Zákazníkovi skutečnost, že Smlouva byla ukončena, a to bez zbytečného odkladu na e-mailovou adresu Zákazníka, popř. jiným způsobem určeným Zákazníkem (formou, jakou byla podána Žádost).

Článek 8 Vymazání dat při ukončení Služby

Po ukončení Smlouvy jsou údaje Zákazníka automaticky vymazány, s výjimkou těch údajů, které je Poskytovatel povinen uchovávat podle platných právních předpisů a/nebo za účelem ochrany a výkonu práv Poskytovatele.

Článek 9 Poplatky za přenos služby zpracování údajů

Smluvní strany se dohodly na poplatcích za přenos Služby, pokud přenos dat trvá déle než 30 kalendářních dnů, může být Zákazníkovi účtovány další poplatky, jejich vyjádření je součástí smluvní dokumentace Zákazníka.

Článek 10 Zákonná změna Smlouvy

10.1 Dle čl. 23 Nařízení o datech poskytovatelé služeb zpracování dat přijmou opatření stanovená v článcích 25, 26, 27, 29 a 30, aby zákazníkům umožnili přejít na službu zpracování dat pokrývající službu stejného druhu, kterou poskytuje jiný poskytovatel služeb zpracování dat, nebo na místní infrastrukturu informačních a komunikačních technologií, nebo případně využívat více poskytovatelů služeb zpracování dat současně. V souladu s Nařízením o datech tak ke dni nabytí účinnosti Nařízení o datech (12. 9. 2025) dochází k těmto změnám Smlouvy:

- pokud je pro Službu sjednána výpovědní doba delší než 2 měsíce (počítaná od okamžiku podání výpovědi), zkracuje se výpovědní doba Smlouvy pro účely ukončení Služby na 2 měsíce (počítáno od podání výpovědi), a to v souladu s čl. 25 odst. 2 písm. d) Nařízení o datech;

- Smlouva je v některých případech ukončena až po uplynutí Přechodného období dle čl. 7 Podmínek, k zajištění souladu s čl. 25 odst. 2 písm. a) Nařízení o datech;

- Byla-li pro účely úpravy práv a povinností při zpracování osobních údajů Poskytovatelem pro Zákazníka sjednána smlouva o zpracování osobních údajů podle čl. 28 GDPR, tato smlouva se použije přiměřeně i po ukončení Služby pro ujednané činnosti po Dobu přístupu k datům, a to zejména s ohledem na povinnost zachování a zpřístupnění dat v souladu s čl. 25 odst. 2 písm. g) Nařízení o datech a související nezbytnou součinnost. - ujednání o technických, organizačních a smluvních opatřeních, která Poskytovatel přijal, aby zabránil mezinárodnímu přístupu orgánů veřejné správy k neosobním údajům uchovávaným v Unii nebo v jejich předávání: Poskytovatel má zavedena opatření, která mají zabránit mezinárodnímu přístupu vlád a orgánů veřejné moci ze třetích zemí k neosobním údajům, pokud by takový přenos nebo přístup vedl k rozporu s právem Evropské unie nebo vnitrostátním právem. Tato opatření zahrnují zejména procesy, které zaručují, že každá taková žádost bude Poskytovatelem individuálně vyhodnocena tak, aby bylo postupováno v souladu s platnou legislativou, včetně předpisů upravujících nakládání s osobními údaji. Poskytovatel garantuje, že přezkoumá zákonnost žádosti cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu Zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky, a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů. V případě pochybností o tom, zda jsou splněny podmínky pro poskytnutí údajů v souladu s Nařízením o datech, bude Poskytovatel konzultovat příslušný vnitrostátní orgán v souladu s čl. 32 odst. Nařízení o datech.

Poskytovatel garantuje v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, že nevyhoví této žádosti a odkáže tohoto žadatele na Zákazníka nebo o takové žádosti Zákazníka bezodkladně informuje, nebo pokud český právní řád Poskytovateli zakazuje informovat Zákazníka, vyvine Poskytovatel veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé, a pokud nedosáhne zrušení povinnosti zákazu informování Zákazníka, pak Poskytovatel Zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem

V případě, že taková žádost o poskytnutí údajů není právně závazná, Poskytovatel nevyhoví takové žádosti cizího orgánu o přístup k údajům Zákazníka nebo o jejich přenos a odkáže žadatele na dotčeného Zákazníka, nebo o takové žádosti Zákazníka neprodleně informuje. Poskytovatel informuje dotčeného Zákazníka o přijetí žádosti orgánu veřejné moci ze třetí země o přístup k jeho neosobním údajům, pokud to není v rozporu s platnými právními předpisy a/nebo uloženým zákazem, pokud žádost slouží pro účely vymáhání práva.

- mění se rovněž další ujednání Smlouvy (zejména případně sjednaného Exit plánu), pokud jsou v rozporu s kogentními ujednáními Nařízení.

10.2 V rozsahu, v jakém poskytování Služby podléhá rovněž zvláštním ujednáním mezi stranami za účelem dodržování Nařízení (EU) 2022/2554 (tzv. Nařízení DORA) uzavřeným stranami ve Smlouvě, mají tato zvláštní ujednání podle Nařízení DORA přednost před uplatňováním těchto Podmínek.

10.3 Ujednání Smlouvy pro Službu poskytovanou v režimu zákona č.134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ“), se mění s odkazem na výše uvedené dle Nařízení pouze v rozsahu přípustném dle § 222 ZZVZ.

10.4 Ujednání Smlouvy, která nejsou v rozporu s kogentními ustanoveními Nařízení o datech, mají přednost před aplikací ujednání těchto Podmínek.

10.5 V případě rozporu mezi těmito Podmínkami a popisem služby vydaným Poskytovatelem pro Službu mají přednost ujednání takového popisu služby, která nejsou v rozporu s kogentními ustanoveními Nařízení o datech.

Článek 11 Odpovědnost stran

Poskytovatel nenese odpovědnost za případné prodlení nebo omezení přístupu k údajům, které mohou vzniknout v důsledku okolností nezávislých na jeho přiměřené kontrole, včetně prodlení Zákazníka s poskytnutím požadovaných informací, součinnosti nebo upřesnění postupu při přenosu dat. Poskytovatel nenese odpovědnost za jednání a činnosti, za které je odpovědný Zákazník (popř. jím schválená třetí osoba), ani za činnosti nebo okolnosti mimo jeho kontrolu. Strany se dohodly, že v případě porušení jejich povinností vyplývajících z těchto Podmínek z nedbalosti, včetně případů, kdy je řada souvisejících událostí považována za jedinou událost, bude jejich odpovědnost omezena na maximální výši odpovídající šestinásobku průměrného

měsíčního paušálu Služby účtovaného Zákazníkovi za poslední rok užívání Služby (popř. průměrného měsíčního paušálu za dobu čerpání Služby, pokud trvá Smlouva méně než rok).

Poskytovatel odpovídá za správnost přenosu až do úkonu předání dat a/nebo digitálních aktiv Zákazníkovi, nejpozději do okamžiku, kdy data a/nebo digitální aktiva opustí infrastrukturu Poskytovatele (v případě přenosu dle čl. 2.2 těchto Podmínek), přičemž za navazující fáze přenosu vč. integrace do Cílového prostředí odpovídá Zákazník, popř. Cílový poskytovatel.

Článek 12 Služba poskytovaná jako komponenta jiné služby Poskytovatele

12.1 Tyto obchodní podmínky se přiměřeně aplikují v případě, kdy je Služba poskytována jako jedna z komponent jiné (hlavní) služby Poskytovatele (ať už fakultativní, nebo obligatorní) v rámci jednoho smluvního vztahu, a to zejména s ohledem na charakter hlavní služby a na individuální požadavky Zákazníka při implementaci a plnění hlavní služby.

12.2 V případě, kdy je Služba poskytována jako jedna z komponent jiné služby Poskytovatele v rámci jednoho smluvního vztahu, lze přenos Služby realizovat (Žádost o přenos Služby lze podat) pouze při výpovědi hlavní služby jako celku.

Článek 13 Závěrečná ustanovení

13.1 Komunikace: Smluvní strany se v těchto Podmínkách dohodly na jiné než listinné formě doručování, a to zejména elektronicky s využitím prostředků komunikace na dálku, při které je zachována písemná forma a jsou splněny podmínky právních předpisů.

13.2 Tyto Podmínky tvoří nedílnou součást Smlouvy.

13.3 Tyto Podmínky může Poskytovatel jednostranně změnit z důvodu změny technických, provozních, organizačních nebo obchodních podmínek na straně TMCZ, na trhu poskytování relevantních služeb nebo z jiného závažného důvodu. Poskytovatel má právo jednostranně změnit Podmínky částečně i v celém jejich rozsahu. Není-li sjednáno jinak, Zákazník má právo do 30 dnů od oznámení takové změny písemně ukončit Službu dotčenou takovou změnou s výpovědní dobou, která uplyne posledním dnem měsíce následujícího po měsíci, ve kterém byla výpověď doručena Poskytovateli, přičemž do okamžiku uplynutí výpovědní doby platí původní smluvní podmínky. Pokud Zákazník výše uvedeným způsobem vypoví Službu, má Poskytovatel právo vzít změnu Podmínek zpět, přičemž strany se dohodly, že v takovém případě se Zákazníkem podaná výpověď ruší a pro Službu nadále platí původní smluvní podmínky. Právo ukončit Službu podle tohoto odstavce nevzniká, pokud dojde ke změně smluvních podmínek na základě změny právní úpravy nebo v případě změn smluvních podmínek, které nejsou v neprospěch Zákazníka.

13.4 Tyto obchodní podmínky nabývají platnosti a účinnosti dne 12.9.2025.