T Business

OBCHODNÍ PODMÍNKY SLUŽBY INLINE SECURITY

společnosti T-Mobile Czech Republic a.s. se sídlem Tomíčkova 2144/1, 148 00 Praha 4, IČO: 64949681, zapsané v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 3787

(dále jen „Podmínky“)

Tyto Podmínky definují pravidla zřízení a poskytování služby Inline Security, na jejímž základě společnost T-Mobile Czech Republic a.s. (dále jen „Operátor“) zajišťuje svým zákazníkům (dále jen „Účastník“) ochranu jejich mobilních datových služeb za podmínek uvedených níže.

V otázkách neupravených v těchto Podmínkách se přiměřeně užijí zejména ustanovení aktuálních Všeobecných podmínek společnosti T-Mobile Czech Republic a.s. (dále jen „VPST“), Podmínek pro zpracování osobních, identifikačních, provozních a lokalizačních údajů Účastníka a dalších podmínek Účastníkem využívaných služeb a nabídek Operátora uveřejněných na webových stránkách Operátora na adrese www.t-mobile.cz/podnikatele-firmy/podminky-mobilni-sluzby, dále platný Ceník služeb a ustanovení platného právního řádu České republiky.

Podmínky jsou uveřejněny na výše uvedených webových stránkách Operátora a nejsou samostatně bez splnění dalších podmínek návrhem na uzavření smlouvy. Podmínky či jejich část mohou být dále komunikovány dalšími prostředky, např. tiskovou inzercí, plakáty atd. V případě rozporu mezi zněním Podmínek uveřejněným na internetu a zněním Podmínek uveřejněným jiným způsobem je vždy rozhodující znění uveřejněné na shora uvedených webových stránkách.

Charakteristika Služby

1 Podmínkou služby Inline Security (dále též jen „Inline Security“ nebo „Služba“) je využívání mobilních dat v rámci aktivní účastnické smlouvy s Operátorem (na mobilní hlas/data).

2 Služba je určena pouze pro firemní zákazníky s uzavřenou účastnickou smlouvou na své IČO. Účastníkem se rozumí smluvní strana účastnické smlouvy na konkrétní telefonní službu, uživatelem se rozumí subjekt, který telefonní číslo (SIM) reálně využívá pro své pracovní a příp. i soukromé účely.

3 Účastník je povinen informovat všechny skutečné uživatele telefonních čísel (zejména své zaměstnance a další, kterým umožnil užívání telefonního čísla) o aktivaci Služby a jejích podmínkách, včetně možnosti zrušení Služby. Účastník bere na vědomí a výslovně souhlasí s tím, že Operátorovi uhradí veškerou příp. újmu vzniklou v souvislosti s neoprávněnou aktivací Služby či jiným neoprávněným použitím Služby.

4 O aktivaci i deaktivaci Služby (balíčku) Operátor informuje Účastníka, resp. uživatele konkrétního telefonního čísla prostřednictvím notifikační SMS. Účastník si Službu může zrušit i znovu nastavit.

5 Uživatel bere na vědomí, že pokud nedisponuje potřebným oprávněním jednat za své telefonní číslo, musí pro administraci (aktivaci/zrušení) kontaktovat Účastníka.

6 **Služba Inline Security**

6.1 Služba je vázána na telefonní číslo Účastníka, pro které byla objednána (není přenosná, resp. využitelná na jiném čísle).

6.2 Účelem Služby je zajištění ochrany před kybernetickými hrozbami na síťové úrovni, jako jsou viry, ransomware, phishing apod. Služba nenahrazuje další bezpečnostní opatření pro koncové zařízení Účastníka/uživatele (např. antivirový program), ale tyto nástroje vhodně doplňuje. Služba chrání Účastníka/uživatele pouze v rámci provozu na mobilní síti, nechrání ho při využití dat prostřednictvím Wi-Fi a při využívání privátní APN.

6.3 Předmětem Služby je prevence kybernetických hrozeb prostřednictvím blokování potenciálně nebezpečné datové komunikace Účastníka/uživatele. Součástí Služby je poskytnutí řešení určeného k detekci kybernetických bezpečnostních událostí, ověření a kontrole přenášených dat na síťovém perimetru komunikační sítě a aktivnímu

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

OBCHODNÍ PODMÍNKY SLUŽBY INLINE SECURITY

blokování nežádoucí komunikace v rámci perimetru komunikační sítě a jinak nebezpečného obsahu na internetu (dále jen „Řešení"). Řešení je na základě aktivace Služby Účastníkem implementováno mezi koncový bod mobilní sítě Operátora a koncové zařízení Účastníka/uživatele, tj. na síťovém perimetru komunikační sítě Účastníka/uživatele. Toto Řešení kontroluje datový provoz na síťovém perimetru komunikační sítě Účastníka/uživatele, aniž by realizovalo dešifrování obsahu komunikace. Při šifrované komunikaci jsou analyzovány zejména hlavičky datových paketů a metadata. Strojové rozhodování o blokaci komunikace probíhá především na základě IP adres, portů, protokolu nebo metadat v hlavičkách (např. detekce anomálií v chování sítě) za využití kontinuálně aktualizovaných dat globálně uznávaných expertních společností a skupin v oblasti kyberbezpečnosti.

6.4 Rozsah Služby a základní funkcionality jsou blíže popsány v příloze č. 1 k Podmínkám.

6.5 Pokud dojde k identifikaci hrozby a zablokování komunikace na síťovém perimetru komunikační sítě Účastníka/uživatele, je o takovéto události každý dotčený uživatel konkrétního telefonního čísla informován prostřednictvím SMS. Uživatel může na portálu firma nebo v aplikaci Můj T-Mobile zhlédnout přehled všech zablokovaných hrozeb souvisejících s jeho tel. číslem za posledních 60 dnů včetně detailu o konkrétní hrozbě. Účastník má na portálu Moje firma k dispozici statistické souhrnné informace o celkovém počtu zamezených hrozeb za každé firemní telefonní číslo za posledních 30 dnů.

6.6 Služba negarantuje zachycení veškeré potenciálně nebezpečné komunikace. V případě pochybností, zda je konkrétní doména nebo komunikace skutečně potenciálně nebezpečná, má za účelem ověření Účastník právo kontaktovat Operátora telefonicky nebo e-mailem. Operátor si vyhrazuje právo neposkytnout odblokování přístupu na jednotlivé zablokované domény na žádost Účastníka.

6.7 Účastník bere na vědomí, že příp. porucha Služby může ovlivnit využívání mobilních dat, aplikací fungujících na mobilních datech či jiná řešení Účastníka/uživatele využívající mobilní datový přenos, a to včetně úplné nefunkčnosti datového provozu a některých aplikací na straně Účastníka/uživatele za síťovým perimetrem komunikační sítě Účastníka/uživatele. Operátor se zavazuje jakékoliv poruchy řešit v rámci SLA definovaného v příloze č. 1 těchto Podmínek.

6.8 Přestože se Operátor zavazuje vynaložit úsilí k identifikaci a omezení dopadu kybernetických událostí, vzhledem k neustálému vývoji nových typů útoků, jejich kombinací a modifikací a rozsahu nemůže zaručit, že ochrana poskytovaná prostřednictvím Služby bude vždy a bezpodmínečně plně účinná. Operátor nenese odpovědnost za případnou újmu (včetně škody způsobené zejména nedostupností Služby, ztrátou, narušením integrity či autenticity dat, znepřístupněním dat, přerušením provozu nebo únikem informací, popř. vzniklé v důsledku sankcí a nároků třetích osob, a ušlého zisku), kterou Účastník a/nebo uživatel utrpí v důsledku jakékoliv kybernetické události vedené prostřednictvím mobilní datové sítě Operátora, a to nad rámec sjednaných nároků z porušení SLA.

6.9 Služba není kompatibilní se službou Statická IP adresa. Před aktivací Služby musí Účastník zrušit statickou IP adresu užívanou na telefonním čísle.

6.10 Služba není slučitelná se službou OnNet Securita a Security – aktivací Služby se tyto služby automaticky zruší.

7 Operátor pro účely poskytování Služby zpracovává údaje o komunikaci Účastníka, a to výhradně na telefonních číslech, pro něž je Služba aktivní. Osobní údaje jsou zpracovávány výhradně za účelem poskytnutí Služby, pro jiné účely nebudou využívány. Po provedení analýzy v rámci Řešení nejsou žádná data o komunikaci dále zpracovávána s výjimkou informací o zamezené hrozbě za účelem informačního reportu Účastníkovi. Pro tento účel jsou ukládány údaje v rozsahu: IP adresa, doména/URL, čas, MSISDN, důvod blokace (tj. druh zablokované hrozby), a to po dobu maximálně 60 dnů.

8 Bližší informace, jak Operátor nakládá s osobními údaji, jsou k dispozici v Podmínkách pro zpracování osobních, identifikačních, provozních a lokalizačních údajů účastníků a Zásadách zpracování osobních údajů na webu t-mobile.cz v sekci Ochrana osobních údajů.

9 V rámci Služby může/bude docházet ke zpracování osobních údajů Operátorem v postavení zpracovatele osobních údajů. Práva a povinnosti při zpracování osobních údajů se řídí Podmínkami zpracování osobních údajů, které tvoří přílohu č. 2 těchto Podmínek.

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

OBCHODNÍ PODMÍNKY SLUŽBY INLINE SECURITY

10 Operátor si vyhrazuje právo kdykoliv aktualizovat a měnit tyto Podmínky v části týkající se popisu a charakteristiky Služby, možností aktivace a zrušení Služby a okruhu Účastníků/uživatelů, pro které je Služba určena, jakož i související Podmínky zpracování osobních, identifikačních, provozních a lokalizačních údajů. Operátor si zároveň vyhrazuje právo Službu částečně či v plném rozsahu zrušit. O této změně bude Operátor Účastníky informovat způsobem stanoveným ve VPST.

11 **Nedílnou součástí je:**

Příloha č. 1 – Rozsah Služby a základní funkcionality

Příloha č. 2 – Podmínky zpracování osobních údajů

12 **Podmínky jsou platné a účinné od 15. 6. 2026.**

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

T Business

PŘÍLOHA Č. 1: ROZSAH SLUŽBY A ZÁKLADNÍ FUNKCIONALITY

Funkce	Popis
Dedikovaná pravidla	Pravidla vytvořená a spravovaná dodavateli i bezpečnostními experty CERT/SOC T-Mobile, využívající databáze indikátorů kompromitace (IP adresy, domény, URL, hashe souborů apod.) získané v rámci každodenních operací kybernetické zpravodajské činnosti (CTI).
Filtrování IP adres	Blokuje přístup ke škodlivým internetovým zdrojům odmítnutím připojení k IP adresám kategorizovaným jako *škodlivé webové stránky, phishing, spamové URL adresy a řídicí servery botnetů (C&C).*
Blokování řídicích serverů botnetů (C&C)	Detekuje a blokuje pokusy o připojení k řídicím serverům *Command & Control*, které kyberzločinci používají ke správě botnetů.
Filtrování DNS	Blokuje přístup ke škodlivým internetovým zdrojům odmítnutím DNS dotazů spojených se *škodlivými webovými stránkami, phishingem, spamovými URL adresami a řídicími servery botnetů (C&C).*
Filtrování URL	Blokuje přístup ke škodlivým webovým stránkám prostřednictvím HTTP požadavků. Pokud je aktivní DNS-over-HTTPS (DoH), analyzuje pole SNI ve zprávách TLS Client Hello, aniž by přistupovalo k šifrovanému obsahu.
Antivirus	Detekuje a blokuje škodlivý software přenášený na mobilní nebo stacionární zařízení prostřednictvím HTTP.
Antimalware (Sandboxing)	Analyzuje přenášené soubory ve virtuálním izolovaném prostředí (sandboxu) za účelem detekce škodlivého softwaru.
Detekce a prevence průniku (IPS)	Blokuje potenciální kritické nebo vysoce závažné síťové hrozby detekované v nešifrovaném provozu.
Reporty	Agreguje data Služby (události a upozornění). Účastníci mohou generovat reporty prostřednictvím portálu nebo aplikace *Můj T-Mobile*.

Pro všechny SIM využívající Službu platí stejná bezpečnostní pravidla. (Službu nelze customizovat per SIM ani per IČO!)

Garance SLA

Měsíční dostupnost Služby – 99,5 %
Garance vyřešení poruchy – 16 pracovních hodin od nahlášení

Smluvní pokuta pro případ porušení SLA:

V případě nedodržení garantované dostupnosti Služby může Účastník uplatnit nárok na smluvní pokutu ve výši měsíčního paušálu Služby (po zohlednění všech poskytnutých slev), a to v rámci reklamace Služby.

Operátor nenese odpovědnost za zajištění souladu činností Účastníka (včetně činností, při nichž užívá/čerpá Službu) s jakýmikoliv právními předpisy, regulačními požadavky, standardy nebo rámci v oblasti kybernetické bezpečnosti, digitální provozní odolnosti, ochrany osobních údajů či jiných oblastí, které se vztahují na činnost Účastníka. Operátor garantuje poskytování Služby jen v souladu s právními předpisy, regulačními požadavky, standardy nebo rámci v oblasti kybernetické bezpečnosti, digitální provozní odolnosti, ochrany dat (včetně osobních údajů) či jiných oblastí, které upravují poskytování Služby výhradně ve vztahu k němu (a to v obvyklém standardu využitelném běžným zákazníkem). Rozhodnutí o tom, zda a jaké právní předpisy, regulační požadavky, standardy nebo rámce jsou relevantní pro poskytování Služby z hlediska poskytovatele, jakož i způsob jejich aplikace, náleží výhradně Operátorovi. Při definici parametrů Služby Operátor vychází z předpokladu, že infrastruktura Účastníka, pro kterou hodlá Službu užívat, je provozována v minimálně běžném režimu zabezpečení odpovídajícím stavu techniky, právním předpisům a relevantním certifikačním rámcům, případně jejich ekvivalentům, přičemž systémy a koncová zařízení Účastníka jsou průběžně zálohovány, pravidelně aktualizovány a podléhají odpovídající provozní údržbě.

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

PŘÍLOHA Č. 2: PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1.1 Ukládání a jiné zpracování dat, která mají charakter osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 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“) a zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění (dále jen „Zákon o zpracování osobních údajů“) (společně dále jako „Aplikovatelné právo“), v rámci Služby se řídí níže uvedenými podmínkami.

1.2 V rámci Služby může docházet ke zpracování osobních údajů fyzických osob, např. zaměstnanců (dále jen „**Subjekty údajů**“). Účastník (dále také jen „**Správce**“) je při zpracování osobních údajů v souladu s ustanovením článku 4 bodu 7 GDPR v postavení správce osobních údajů. Operátor (dále také jen „**Zpracovatel**“) je v souladu s ustanovením článku 4 bodu 8 GDPR v postavení zpracovatele osobních údajů.

Zpracování osobních údajů

1.3 Správce pověřuje Zpracovatele zpracováním osobních údajů a Zpracovatel tyto údaje bude zpracovávat výhradně za účelem zajištění plnění Služby na základě sjednaného smluvního vztahu (dále jen „Specifikace služby“). Zpracovatel zpracovává osobní údaje vždy transparentně, korektně, pouze v nezbytném rozsahu, po nezbytnou dobu a v souladu s Aplikovatelným právem. Zpracovatel nepoužije osobní údaje k žádnému jinému účelu a neposkytne je žádným neoprávněným třetím stranám. Bez souhlasu Správce nesmí být pořizovány kopie a duplikáty osobních údajů – to neplatí v případě provádění záloh k zajištění řádného zpracovávání osobních údajů a/nebo řádnému poskytování Služby nebo činnosti k zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů Zpracovatele nebo plnění zákonné povinnosti.

1.4 Předmětem zpracování jsou osobní údaje předávané Zpracovateli prostřednictvím poskytované služby nebo v souvislosti s ní. O rozsahu zpracovávaných osobních údajů rozhoduje Správce.

1.5 Správce odpovídá za to, že osobní údaje, které jsou předmětem zpracování, jsou přesné, byly shromážděny v souladu s právními předpisy, zejména v souladu s GDPR a Zákonem o zpracování osobních údajů.

1.6 Správce nese výhradní odpovědnost za posouzení, zda lze osobní údaje zpracovávat v souladu s platnou právní úpravou v oblasti ochrany osobních údajů, zejména v souladu s Aplikovatelným právem, jakož i za ochranu práv subjektů údajů, a to zejména tak, aby Zpracovatel mohl poskytovat Služby dohodnutým způsobem, který není v rozporu s právními předpisy. Správce se zavazuje informovat Zpracovatele o jakémkoliv podezření, které může mít vliv na poskytovanou Službu.

1.7 Zpracovatel se zavazuje zpracovávat osobní údaje pouze na základě těchto Podmínek zpracování osobních údajů a doložených písemných pokynů Správce. Pro vyloučení pochybností se zpracování osobních údajů v souladu s povinnostmi Zpracovatele vyplývajícími ze Specifikace služby považuje za zpracování prováděné v souladu s instrukcemi Správce, resp. Správcem k tomu pověřených osob. Pokud je určitý pokyn podle názoru Zpracovatele nezákonný, bez zbytečného odkladu o tom informuje Správce. V takovém případě je oprávněn pozastavit plnění pokynu, dokud jej Správce písemně nepotvrdí. V případě, že Správce trvá na splnění pokynu, který Zpracovatel i nadále odůvodněně považuje za nezákonný, Zpracovatel je oprávněn ukončit poskytování Služby bez výpovědní doby, a to bez nároku Správce na jakoukoliv finanční kompenzaci.

1.8 Zpracovatel zpracovává osobní údaje zejména automatizovaným způsobem a v nezbytných případech manuálně.

Zabezpečení osobních údajů

1.9 Správce a Zpracovatel jsou povinni přijmout veškerá vhodná technická a organizační opatření, aby zajistili úroveň ochrany odpovídající riziku a poskytované Službě. Opatření Zpracovatele, která jsou v současné době pokládána za adekvátní, jsou popsána v bodě 1.22 těchto Podmínek zpracování osobních údajů. Jakékoliv pokyny nebo opatření, které představují odchylku od zde uvedených opatření, se pokládají za žádost o úpravu, jejíž náklady, pokud bude úprava technicky realizovatelná a možná, nese Správce. Smluvní strany v takovém případě uzavřou samostatnou dohodu o rozsahu činností, výši a úhradě nákladů.

1.10 Zpracovatel přijal a udržuje adekvátní technická a organizační opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k osobním údajům Správce, k jejich změně, zničení či ztrátě, neoprávněným přenosům,

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

PŘÍLOHA Č. 2: PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, a to s přihlédnutím k poskytované Službě.

1.11 Zpracovatel je oprávněn prokázat plnění závazků, zejména potom technických a organizačních opatření, prostřednictvím následujících nástrojů: a) Kodexem chování (čl. 40 GDPR); b) závaznými podnikovými pravidly; c) osvědčením (čl. 42 GDPR); d) aktuálními certifikáty, zprávami nebo výpisy ze zpráv od nezávislých osob (např. auditoři, oddělení auditu); e) vhodnou certifikací ve formě auditu bezpečnosti IT nebo ochrany údajů; f) čestnými prohlášeními Zpracovatele.

1.12 Zpracovatel je povinen bez zbytečného odkladu informovat Správce o jakýchkoliv případech porušení zabezpečení Údajů, a to na e-mailovou adresu kontaktní osoby uvedenou ve Specifikaci služby.

Povinnost mlčenlivosti

1.13 Zpracovatel zajistí, že každá osoba, která bude mít přístup k osobním údajům, bude zavázána povinností mlčenlivosti nebo se na ni bude vztahovat zákonná povinnost mlčenlivosti. Povinnost mlčenlivosti trvá rovněž po ukončení hlavní smlouvy.

Poskytování součinnosti

1.14 Zpracovatel bude s přihlédnutím k charakteru zpracování a k informacím, kterými disponuje, poskytovat Správci součinnost při plnění povinností Správce dle Aplikovatelného práva.

1.15 **Zpracovatel je povinen zajistit součinnost v následujících bodech:**

1.15.1 Správce je oprávněn na vlastní náklady prověřovat soulad s plněním povinností dle smlouvy o zpracování osobních údajů a čl. 28 GDPR (povinnosti zpracovatele osobních údajů). Zpracovatel umožní Správci na jeho žádost, ne však častěji než 1× za kalendářní rok, vykonat kontrolu či audit. Správce se zavazuje oznamovat kontroly s přiměřeným předstihem, minimálně 30 (třicet) pracovních dnů předem, aby byla ze strany Zpracovatele zajištěna dostatečná součinnost. Správce je povinen kontroly provádět pouze v rozsahu nezbytně nutném pro ověření plnění ve vztahu ke zpracování osobních údajů pro jemu konkrétně poskytovanou Službu, a pouze pokud mu Zpracovatel nedoloží plnění závazků: **a)** Kodexem chování (čl. 40 GDPR); b) závaznými podnikovými pravidly; c) osvědčením (čl. 42 GDPR); d) aktuálními certifikáty, zprávami nebo výpisy ze zpráv od nezávislých instancí (např. auditoři, oddělení auditu); e) vhodnou certifikací ve formě auditu bezpečnosti IT nebo ochrany údajů; f) čestnými prohlášeními Zpracovatele; a vždy tak, aby nenarušoval běžnou činnost Zpracovatele a byla zachována důvěrnost. Správce nemůže mít přístup k informacím, které jsou předmětem obchodního tajemství Zpracovatele. Zpracovatel je zároveň oprávněn podmínit umožnění kontroly či auditu uzavřením zvláštní dohody o ochraně důvěrnosti informací a dodržením předem sdělených interních pravidel Zpracovatele.

1.15.2 Pokud je Správce povinen poskytnout orgánům státní správy nebo osobám informace o zpracovávání osobních údajů, Zpracovatel poskytne Správci při poskytování takových informací součinnost, pokud se tyto informace týkají zpracovávání údajů v souladu se Specifikací služby a poskytovanou Službou. Zpracovatel rovněž Správce vyrozumí – pokud to zákon připouští – o jakýchkoliv sděleních dozorových orgánů (např. šetření, oznámení o opatřeních nebo požadavcích) Zpracovateli v souvislosti se zpracováváním osobních údajů podle Specifikace služby.

1.15.3 Zpracovatel je povinen poskytnout Správci součinnost ve vztahu k povinnosti Správce reagovat na žádost o uplatnění práv Subjektů údajů dle čl. 15 až 22 GDPR, a to v rozsahu, v němž je to s ohledem na podmínky příslušné Služby a technické a organizační podmínky možné. V případě potřeby budou smluvní strany koordinovat obsah a rozsah činnosti ve formě podpory poskytované Zpracovatelem podle tohoto odstavce. Pokud se Subjekt údajů obrátí přímo na Zpracovatele a z podání bude možné určit, že se žádost týká Správce, Zpracovatel žádost Subjektu údajů bezodkladně postoupí Správci.

1.15.4 Zpracovatel je povinen poskytnout na základě žádosti Správce odeslané na Zákaznické centrum T-Mobile (nejméně 10 pracovních dnů předem) informace potřebné k doložení plnění povinností Zpracovatele dle článku 28 GDPR (povinnosti zpracovatele osobních údajů).

1.15.5 Zpracovatel je povinen poskytovat na základě žádosti Správce odeslané na Zákaznické centrum T-Mobile (nejméně 10 pracovních dnů předem) součinnost při zajišťování souladu s povinnostmi Správce dle článků

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

PŘÍLOHA Č. 2: PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

32 a 36 GDPR, a to při zohlednění povahy zpracování a informací, jež má Zpracovatel od Správce k dispozici.

1.15.6 Pokud Správce provede posouzení dopadu na ochranu soukromí (osobních údajů) a/nebo konzultace s dozorovým orgánem k posouzení dopadu na ochranu soukromí, smluvní strany budou koordinovat obsah a rozsah případné podpory poskytované Zpracovatelem, bude-li nutná.

1.16 Výše uvedené činnosti a součinnosti Zpracovatele jdou na náklad Správce a hradí se zvlášť podle časové náročnosti nebo využitých prostředků, a to zpětně za měsíc, ve kterém byly smluvnímu partnerovi poskytnuty.

Pověřenec pro ochranu osobních údajů

1.17 Zpracovatel se zavazuje ustanovit nezávislého, kvalifikovaného a spolehlivého pověřence pro ochranu osobních údajů, pokud to vyžadují právní předpisy Evropské unie nebo členského státu, které se na Zpracovatele vztahují.

Předávání do třetích zemí

1.18 V případě, že by ze strany Zpracovatele docházelo k předání osobních údajů do tzv. třetích zemí (tj. zemí, které nejsou členskými státy Evropské unie a nedisponují patřičnou úrovní ochrany osobních údajů) nebo mezinárodní organizace, Zpracovatel bude zpracovávat osobní údaje v souladu s příslušnými právními předpisy Evropské unie. V takovém případě Zpracovatel předem informuje Správce, ledaže by takové informování právní předpisy zakazovaly z důležitých důvodů veřejného zájmu.

Dílčí zpracovatelé

1.19 Zpracovatel může do zpracování zapojit další zpracovatele/subzpracovatele. Na žádost Správce poskytne Zpracovatel seznam zapojených subzpracovatelů. Zpracovatel souhlasí s možností zapojení společností v rámci skupiny Deutsche Telekom. Zpracovatel informuje Správce o veškerých zamýšlených změnách (přijetí/nahrazení) s tím, že Správce má právo vznést do 14 (čtrnácti) dnů vůči těmto změnám relevantní, objektivní a odůvodněné námitky. Smluvní strany se výslovně dohodly, že v případě, že Správce bezdůvodně odmítá změnu, je Zpracovatel oprávněn ukončit poskytování Služby výpovědí bez výpovědní doby, aniž by Správci vznikal jakýkoliv nárok na finanční náhradu spojenou s takovým ukončením Služby.

Výmaz osobních údajů

1.20 Nebude-li dohodnuto jinak a nevyžaduje-li právo delší uchování osobních údajů, budou v případě ukončení Specifikace služby nevratně vymazány. Správce bere na vědomí, že Zpracovatel není schopen oddělit osobní údaje od ostatních dat, a proto v případě požadavku na vrácení dat splní Zpracovatel své povinnosti dle tohoto ustanovení vrácením či zpřístupněním dat.

Specifikace zpracování

1.21 Osobní údaje budou zpracovávány pro účely poskytování Služby v souladu s jejími Podmínkami. Kategorie zpracovávaných údajů, dotčených subjektů, související operace či doba uložení, jakož i další podrobnosti vyplývají z charakteru a způsobu poskytování Služby a jsou blíže popsány v Podmínkách.

1.22 Technická a organizační opatření

a) Důvěrnost (článek 32 odst. 1 písm. b obecného nařízení EU na ochranu osobních údajů – GDPR)

- **Kontrola vstupu**

Zabezpečení systémů pro zpracovávání údajů před přístupem neoprávněných osob, např. prostřednictvím magnetických nebo čipových karet, klíčů, elektrických otvíračů dveří, bezpečnostní služby a/nebo vrátného, alarmu, videosystémů apod.

- **Kontrola přístupu**

Zabezpečení systémů před neoprávněným použitím, např. prostřednictvím (bezpečnostních) hesel, mechanismů automatického zamykání, dvouúrovňového ověřovacího mechanismu, šifrování nosičů údajů apod.

- **Kontrola přístupových oprávnění**

Zabezpečení, aby osoby bez příslušného oprávnění nemohly údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím autorizačních konceptů, přístupových práv na základě příslušných potřeb a evidence přístupů.

b) Integrita (článek 32 odst. 1 písm. b GDPR)

- **Kontrola zpřístupňování údajů**

Zabezpečení, aby v průběhu elektronického přenosu nebo přepravy nemohly osoby bez příslušného oprávnění tyto údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím šifrování, virtuálních privátních sítí (VPN), elektronického podpisu apod.

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787

PŘÍLOHA Č. 2: PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- **Kontrola zadávání údajů**

Zajištění, aby bylo možné zpětně ověřit a zjistit, zda a kým byly osobní údaje do systémů pro zpracovávání údajů zadány, upravovány nebo z těchto systémů vymazány, např. prostřednictvím evidence oprávnění, vedení záznamů o zadávání údajů apod.

c) Dostupnost a odolnost systémů (článek 32 odst. 1 písm. b GDPR)

- **Kontrola dostupnosti**

Ochrana údajů před náhodným nebo úmyslným zničením a/nebo ztrátou, např. prostřednictvím zálohování (online/offline; on-site/off-site), nepřerušitelných zdrojů napájení (UPS), antivirové ochrany, firewallů, zaznamenávání přenosových tras a krizových plánů.

- Schopnost obnovit dostupnost údajů (článek 32 odst. 1 písm. c GDPR)

d) Proces pravidelného testování, posuzování a hodnocení (článek 32 odst. 1 písm. d GDPR; článek 25 odst. 1 GDPR)

- Řízení ochrany údajů
- Řízení reakcí na incidenty
- Výchozí nastavení, která zajišťují ochranu údajů (článek 25 odst. 2 GDPR)
- Kontrola smluvní strany

Zákaz smluvního zpracovávání údajů ve smyslu článku 28 GDPR bez příslušných pokynů od zákazníka, např. jednoznačná smlouva, formální výběrové řízení, přísný výběr poskytovatele služeb, povinnost provádění důkladných kontrol předem a provádění následných kontrol.

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Česká republika, IČO: 64949681, DIČ: CZ64949681, zapsaná v OR u Městského soudu v Praze pod značkou B 3787