

# Podmínky služby UPC Anti-DDoS

## 1. Definice

Není-li uvedeno jinak, mají výrazy s velkými počátečními písmeny význam definovaný v tomto článku 1.

1.1 „Výstražné upozornění“ znamená data, jež by mohla naznačovat potenciální DDoS útok na základě Internetového provozu Účastníka, který se odchyluje od profilu Účastníka, přičemž taková odchylka přesahuje předem stanovenou minimální hodnotu.

1.2 Účastník, na něhož se vztahuje omezení, znamená účastníka, jehož obchodní činnost spadá do některé z kategorií uvedených v článku 12.1 v definici „zakázaných činností“.

1.3 „Protokol BGP“ (Border Gateway Protocol) znamená směrovací protokol, který může použít Účastník k ohlášení svých prefixů, nebo UPC k přesměrování provozu na Stránky ochrany před útoky DDoS.

1.4 „Důvěrné informace“ znamená materiály, data, systémy a další informace týkající se provozu, obchodní činnosti, prognóz, tržních cílů, finančních záležitostí, produktů, služeb, účastníků a práv k duševnímu vlastnictví druhé smluvní strany, jež nemusí být přístupné nebo známé široké veřejnosti. Důvěrné informace zahrnují zejména (avšak nikoli výlučně) podmínky a ustanovení Specifikace objednané služby UPC Anti-DDoS (dále jen „Specifikace Anti-DDoS“), jakož i veškeré informace týkající se technických podmínek provozu jakýchkoli Služeb UPC poskytovaných na základě této smlouvy.

1.5 „Účastník“ znamená zákazník UPC Česká republika, s.r.o.

1.6 „Portál Účastníka“ znamená webový portál, kde může Účastník sledovat svůj Internetový provoz, zprávy, Výstražná upozornění a informace o účtech. Zřízení Portálu účastníka není automatickou součástí služby UPC Anti-DDoS. Zřizuje se na požádání Účastníka a je zpoplatněno dle Ceníku. Ustanovení v této specifikaci vztahující se k Portálu účastníka se uplatní pouze v případě, že Účastník o zřízení této doplňkové služby požádal.

1.7 „Případ DDoS“ (distributed denial of service) znamená pokus z externích zdrojů způsobit nedostupnost internetových služeb Účastníka pro jeho zamýšlené uživatele. Existenci takových pokusů měří a určuje UPC.

1.8 „Naléhavá údržba“ znamená odstávku mimo termín „Pravidelné plánované údržby z důvodu instalace naléhavě vyžadovaných patchů nebo provádění oprav či jiné urgentně vyžadované údržby.“

1.9 „Filtrovaný případ DDoS“ nastává, když dojde k přesměrování Internetového provozu Účastníka na Stránku ochrany před útoky DDoS provozované společností UPC a toto přesměrování trvá až do některé z následujících událostí, která nastane dříve: (a) okamžik navrácení Účastníka k běžnému provozu (tj. Internetový provoz Účastníka již není přesměrován na Stránku ochrany před útoky DDoS provozovanou společností UPC); nebo (b) uplynutí čtyřiceti osmi (48) hodin bez ohledu na to, kolik Případů DDoS u Účastníka v mezidobí nastane. Pokud bude Filtrovaný případ DDoS trvat i po uplynutí čtyřiceti osmi (48) hodin, bude považován za nový Filtrovaný případ DDoS.

1.10 „Hackerská činnost“ znamená (a) nelegální nebo neoprávněný přístup k počítačům, účtům, informacím nebo komunikačním zařízením či zdrojům nebo sítím třetí strany (včetně UPC); (b) obejití či narušení nebo pokus o obejití či narušení bezpečnostních opatření třetí strany; nebo (c) provádění jakékoli činnosti, která by mohla předcházet pokusu o proniknutí do systému.

1.11 „Omezení infrastruktury“ znamená, že určitý Případ DDoS u Účastníka (a) nelze zmírnit pomocí Služby ochrany před útoky DDoS poskytované společností UPC; nebo (b) může mít dopad na provozní stabilitu sítě UPC nebo jiných účastníků UPC.

1.12 „Práva k duševnímu vlastnictví“ znamená veškeré v současné době známá nebo v budoucnu existující práva související s autorskými právy (zejména, avšak nikoli výlučně, včetně práva na používání, reprodukce, úpravy, distribuci, veřejné vystavování a veřejné předvádění autorských děl), práva k databázím, ochranné známky (zejména, avšak nikoli výlučně, charakteristické vizuální prvky, obchodní názvy, značky, firemní označení a loga), vynálezy, patenty (zejména, avšak nikoli výlučně, práva na výrobu, používání, nabízení k prodeji a prodej), žádosti o patenty, software, firmware, know-how, obchodní tajemství, morální práva a veškerá další práva nebo formy ochrany chráněných práv jakékoli povahy nebo obdobného charakteru nebo s obdobným účinkem na cokoli z výše uvedeného, jež mohou existovat kdekoli na světě a mohou být označena jakkoli, bez ohledu na to, zda jsou kterákoli z nich registrována, a včetně případných žádostí o registraci čehokoli z výše uvedeného.

1.13 „Internetový provoz“ znamená zejména, avšak nikoli výlučně, veškeré internetové přenosy, VPN, elektronickou poštu, přenosy souborů a další data procházející některou veřejnou sítí s přepojováním paketů.

1.14 „Právní předpisy“ znamená veškerou místní a evropskou legislativu, zákony, prohlášení, vyhlášky, směrnice, právní úpravy, nařízení, předpisy, zásady nebo jiná závazná omezení.

1.15 „Routery pro zmírňování dopadů útoků“ znamená určitý počet routerů, pomocí nichž UPC přesměrovává Internetový provoz Účastníka, jak je popsán v článku 2.3.

1.16 „Normální podmínky“ znamená situace, kdy u Účastníka neprobíhá žádný Případ DDoS.

1.17 „Pravidelná plánovaná údržba“ znamená jakoukoli údržbu prováděnou v rámci vyčleněného okna na údržbu, přičemž taková údržba musí respektovat požadavek na 99,99% dostupnost služby.

1.18 „Datum komerční aktivace Služby“ znamená datum, kdy UPC zašle Účastníkovi e-mail v souladu s článkem specifikujícím kontaktní údaje v dokumentu o zprovoznění služeb pro Účastníka oznamující zprovoznění IP objektů v souladu s pokyny UPC. Datem technické aktivace služby se rozumí datum, kdy bude Účastník přidán do příslušného nástroje pro detekci / zmírňování následků útoků DDoS.

1.19 „Daně“ znamená daně, cla, poplatky a další státem uložené částky jakékoli povahy (včetně daní z obchodní činnosti, prodeje, služeb, používání a přidané hodnoty a veškeré příslušné sankce, úroky a další příplatky, avšak s výjimkou daní z čistého příjmu UPC), jež jsou uloženy jakoukoli vládou nebo jakoukoli její politickou součástí nebo z jejich pověření z poplatků účtovaných za jakékoli ze Služeb ochrany před útoky DDoS poskytovaných společností UPC neboze související dokumentace přeprdané Účastníkovi na základě této smlouvy.

1.20 „Stránky ochrany UPC proti útokům DDoS“ znamená stránky určené ke zmírňování škod, kde UPC zmírňuje škody vzniklé v důsledku Událostí filtrovaných útoků DDoS.

1.21 „Systém Arbor“ je komplexní řešení zajišťující detekci a filtrování škodlivého provozu.

## 2. Popis Služeb

V souladu s podmínkami a ustanoveními této Smlouvy o ochraně bude UPC poskytovat Účastníkovi následující služby prostřednictvím sdílené platformy označované jako Služba ochrany před útoky DDoS poskytovaná společností UPC (dále jen jako „UPC Anti-DDoS“):

2.1 **Nastavení Účastníka.** UPC zahájí proces nastavování Účastníka po odsouhlasení Specifikace Anti-DDoS a této Přílohy. Účastník souhlasí a bere na vědomí, že UPC může dle vlastního uvážení z jakéhokoli důvodu odmítnout nebo zamítnout provedení jakéhokoli zřízení služeb předložené UPC, přičemž v takovém případě UPC nebude povinna Účastníkovi poskytovat UPC Anti-DDoS.

(a) **Portál Účastníka.** Na základě žádosti zřídí UPC Účastníkovi účet na Portálu služby Anti-DDoS a poskytne Účastníkovi uživatelské jméno a heslo pro přístup k Portálu. UPC poskytne Účastníkovi jedno (1) základní školení na Portálu Účastníka.

(b) **Informace nutné pro zprovoznění služeb.** UPC může dle vlastního uvážení od Účastníka požadovat poskytnutí informací pro zprovoznění služeb v podobě určené společností UPC. Po předání požadovaných informací pro zprovoznění služeb provede UPC kontrolu těchto informací. Poskytnutá data jsou využita pro nastavení profilu pro příslušnou šablonu účastníka.

2.2 Účastník tímto bere na vědomí a souhlasí, že sám odpovídá za veškeré monitorování své interní sítě a svého vybavení a že UPC nebude Účastníkovi poskytovat žádné monitorovací služby ve vztahu k jeho interní síti a k jeho vybavení. Účastník dále bere na vědomí a souhlasí, že je povinen informovat UPC, pokud u něho nastane nějaký Případ DDoS nebo pokud se bude Účastník domnívat, že u něho nastal Případ DDoS.

### 2.3 Zmírňování škod.

Během útoku se k účastníkovi (tj. k jeho serveru, IP adresám atd.) snaží dostat škodlivý provoz a současně i normální/legální provoz. Provoz se měří podle síťových uzlů a odesílá se do centrální sběrnice. Přítomnost škodlivého provozu se zjišťuje na základě stanovených minimálních/maximálních hodnot a vzorců. Automatické zmírňování škod se spouští při dosažení určité konfigurovatelné maximální hodnoty v určitém časovém intervalu způsobené útokem. Po skončení útoku se tento systém opět vypne. Routery v síti jsou naprogramovány tak, aby přesměřovaly provoz spojený s útokem DDoS cílený na účastníka na čistící server TMS. Škodlivý provoz se odfiltrovává a běžný legální provoz se odesílá zpět k účastníkovi.

Služba ochrany proti útokům DDoS nabízená společností UPC chrání zejména před volumetrickými útoky, jež jsou především důsledkem útoků využívajících amplifikaci.

UPC nabízí ochranu před zdroji ze své sítě (onnet) i před zdroji mimo síť LGI (offnet).

Na žádost UPC bude UPC pracovat na zmírnění následků Případu DDoS tak, že poskytne doporučení dalšího postupu. Pokud bude doporučeným dalším postupem přesměrování Internetového provozu Účastníka, pak se bude postupovat následovně:

Nastavení v systému Arbor definuje, co je považováno za normu (standardní provoz) a kdy má být vydáno upozornění na útok DDoS. Jakmile systém Arbor zjistí útok DDoS, nainstaluje kontrola trasu pro čištění a veškerý provoz z útoku DDoS bude přesměrován na základě adresy destinace do systémů TMS.

Systémy TMS vyřadí veškerý provoz, který bude dle nastavení vyhodnocen jako škodlivý.

### Odhalení útoku

Vybavení používané společností UPC, Arbor Networks SP, provádí analýzu vzorku provozu získaného z routerů.

Útok může spustit standardní výstražné upozornění DoS Host nebo upozornění na útok v podobě rychlé záplavy Fast Flood DoS Host. Standardní výstražné upozornění DoS Host se spustí, když provoz na monitorovaném routeru směřujícím k jedinému hostiteli přesáhne konfigurovanou mezní hodnotu povoleného typu zneužití za určitý stanovený čas. Výstražné upozornění na útok v podobě rychlé záplavy Fast Flood DoS Host se spustí při zjištění velkého objemu provozu směřujícího k jedinému hostiteli pro určitý povolený typ zneužití.

### Zmírňování škod způsobených útokem

Zařízení TMS umožňují společnosti UPC zmírnit dopady útoků pomocí protipatření, zpráv a výstražných upozornění. Zařízení TMS rovněž umožňují UPC monitorovat nejdůležitější aplikace a síťové služby za účelem zajištění dostupnosti služeb a poskytnutí včasného upozornění v případě útoků na síť.

Když systém Arbor Networks SP odhalí nějakou neobvyklou událost, přesměruje provoz prostřednictvím zařízení TMS tak, aby bylo možno provést ověření a v případě potřeby zareagovat na útok. Zařízení TMS a systém Arbor Networks SP si mezi sebou předávají základní data a data o provozu, aby bylo zajištěno přesné blokování škodlivého provozu.

Systém automatického zmírňování škod umožňuje systému Arbor Networks SP automatické spuštění procesu zmírňování dopadů pomocí TMS, jakmile dojde k útoku na určitý objekt spravovaný účastníkem.

Útoky DDoS se odhalují na základě získaných dat o provozu v síti z předem definovaných okrajových routerů společnosti UPC (PEs).

UPC bude aplikovat vrstvené filtry na Internetový provoz přesměrovaný do systému UPC Anti-DDoS, kde bude progresivním způsobem blokován provoz, jehož cílem je narušit nebo vyřadit z provozu internetové služby Účastníka. Účastník tímto bere na vědomí a souhlasí, že UPC bude filtrovat pouze takové objemy Internetového provozu Účastníka, jaké jsou nezbytné k zajištění dostupnosti internetových služeb Účastníka pro jeho koncové uživatele.

### Návrat k běžnému fungování:

Jakmile systém vyhodnotí, že Případ DDoS skončil, vrátí Účastníka do normálního provozu.

Účastník se může rozhodnout pro ukončení přesměrování svého Internetového provozu do systému UPC Anti-DDoS, a to kdykoli v průběhu trvání Filtrovaného případu DDoS v souladu s Plánem eskalace. V takových případech nevniká UPC jakákoli odpovědnost vůči Účastníkovi a Účastník nese plnou odpovědnost za zmírňování dopadů Filtrovaného případu DDoS od okamžiku ukončení procesu filtrace na žádost Účastníka, kdy Internetový provoz Účastníka již není nadále filtrován; *současně však* Účastník nese veškeré náklady vzniklé v době, kdy byl Internetový provoz Účastníka přesměrováván do systému UPC Anti-DDoS a/nebo kdy byl Filtrovaný případ DDoS spravován společností UPC.

## 2.4 Podmínky služby

Pro připojení ke službě UPC Anti-DDoS musí Účastník splňovat následující podmínky:

- Využívat služby UPC Internet nebo IP konektivita – služba UPC Anti-DDoS nemůže být nabízena jako samostatná služba
- Být připojen do sítě UPC pomocí optických vláken s minimální přenosovou rychlostí 100Mbit/s.
- Služba ochrany před útoky DDoS bude k dispozici pro účastníky využívající služeb internetu pro firmy s připojením pomocí optických vláken.

Další pravidla a popis služby UPC Anti-DDoS:

- Jakýkoli přístup přes coaxiální kabel je mimo rámec sjednaného rozsahu.
- Služba je nabízena pouze v podobě automatického zmírňování dopadů útoků. Automatické zmírňování dopadů útoků vyžaduje monitorování internetového provozu směřujícího k účastníkovi a odebírání vzorků z tohoto provozu. Automatizovaná nápravná opatření budou přijímána bez lidského zásahu.
- Při dosažení maximální kapacity začne UPC provoz namísto čištění vyřazovat.
- Služba obrany proti útokům DDoS může být aplikována pouze na internetové služby poskytované společností Liberty Global, nikoli na připojení poskytované třetími stranami, jež může účastník využívat od dalších poskytovatelů.

## 2.5 Parametry dostupnosti služby

Relevantním aspektem Služby UPC Anti-DDoS je reakční doba zmírňování dopadů útoky DDoS, tj. čas, který uplyne do okamžiku zahájení procesu zmírňování dopadů.

Parametr	Hodnota
Reakční doba v případě útoku	UPC povolila funkci detekce útoku v podobě rychlé záplavy, která odhalí útok během méně než 60 sekund a zahájí automatický proces zmírňování dopadů, jakmile se spustí výstražné upozornění na útok.
Garantovaná roční dostupnost služeb (Platforma Arbor)	99,99 %

Dopad na latenci, jitter a ztrátu paketů v internetové službě během čištění provozu?	Účastník vidí více skoků, ale nedochází ke ztrátě paketů.  Dopad na reakční dobu v případě zmírňování dopadů útoku: < 50 ms.
Maximální doba čištění provozu po skončení útoku DDoS	5 minut

2.6 Zákaznická podpora. Tým B2B podpory společnosti UPC poskytuje (a) telefonickou a e-mailovou podporu Účastníkovi; (b) odpovědi na otázky týkající se fakturace za službu UPC Anti-DDoS; (c) přiměřené úsilí k bezodkladnému informování Účastníka (forma e-mailu se považuje za dostatečnou) o případné Naléhavé údržbě. UPC poskytne Účastníkovi otázky/doporučení k odstranění problémů týkající se Služby UPC Anti-DDoS poskytované společností UPC.

2.7 Úprava nebo přerušení Služeb. Účastník tímto bere na vědomí a souhlasí, že UPC může dle vlastního uvážení kdykoli, avšak pouze na základě konzistentní změny provedené společností UPC, upravit nebo přerušit službu UPC Anti-DDoS jako celek nebo jakoukoli její část nebo jinak upravit jakékoli jiné podmínky vztahující se na službu UPC Anti-DDoS poskytovanou společností UPC na základě písemného oznámení (postačuje e-mailem) zaslání Účastníkovi třicet (30) dnů předem nebo s okamžitou účinností na základě písemného oznámení (postačuje e-mail) zaslání Účastníkovi, pokud je to nutné k dodržení platných Právních předpisů (každý z bodů výše je dále označován jako „Datum účinnosti úpravy Služby“).

## 3. Ověření správného fungování vyčištěného provozu.

3.1 Jako součást nastavení Účastníka nadefinuje UPC profil statického provozu na základě informací poskytnutých Účastníkem v přihlašovacím formuláři a z toho pak nadefinuje seznam statických mezních hodnot, kde budou stanoveny hodnoty, při jejichž překročení se automaticky spustí výstražná upozornění a (v závislosti na závažnosti) opatření směřující ke zmírňování dopadů. Při poklesu pod nastavené hodnoty se provoz vrátí do normálního stavu a proces zmírňování dopadů a přesměrování provozu se ukončí.

3.2 Pokud některý Filtrovaný případ DDoS překročí hranici čistého provozu, pak bude provoz Účastníka přesměrován na stránku (stránky) ochrany před útoky DDoS provozované společností UPC.

Není-li ve Smlouvě o ochraně sjednáno jinak, smí UPC tato data používat pouze k poskytování služby UPC Anti-DDoS.

## 4. Podmínky a omezení.

4.1 Pokud UPC na základě vlastního uvážení s přihlédnutím k obvyklým komerčním standardům dospěje k závěru, že došlo nebo dochází k Omezení infrastruktury, může se UPC bezodkladně rozhodnout, že (a) nebude nadále přijímat žádný Internetový provoz Účastníka nebo jeho část; nebo (b) vyřadí (zablokuje) veškerý Internetový provoz Účastníka nebo jeho část ze služby UPC Anti-DDoS. Pokud UPC využije svých práv vyplývajících z Omezení infrastruktury, může UPC pozastavit plnění

svých závazků vyplývajících z této Přílohy a po dobu takového pozastavení plnění nebude služba UPC Anti-DDoS (resp. jakákoli jejich část) Účastníkovi k dispozici. Jakmile UPC na základě vlastního uvážení dospěje k závěru, že Omezení infrastruktury pominulo, obnoví UPC plnění svých závazků vyplývajících z této Přílohy a služba UPC Anti-DDoS bude Účastníkovi opět zpřístupněna.

4.2 Účastník tímto bere na vědomí a souhlasí, že UPC (a) bude používat Výstražná upozornění a Informace pro spuštění služeb pro účely poskytování služby UPC Anti-DDoS; (b) může zveřejňovat data v agregované podobě, přičemž však takové zveřejnění musí vždy být zcela anonymní; (c) může být povinná poskytnout informace nebo data související s Případy DDoS vnučovacím orgánům a/nebo národním útvarům pro počítačovou bezpečnost („CERT“), přičemž UPC neponese odpovědnost za žádné takové požadované poskytnutí informací či dat. Pokud se takové informace či data o Případu DDoS týkají Účastníka, pak UPC (i) v rozsahu povoleném právními předpisy bude Účastníka o takovém požadovaném poskytnutí informovat; a (ii) bude se Účastníkem v přiměřeném rozsahu spolupracovat na získání ochranného příkazu nebo jiného právního prostředku ochrany zabráňujícího takovému poskytnutí informací či dat.

4.3 Účastník bere na vědomí a uděluje svolení společností UPC a UPC BV nebo dalším třetím stranám k vzájemnému sdílení veškerých relevantních informací, včetně (avšak nikoli výlučně) Důvěrných informací Účastníka, v souvislosti s poskytováním Služeb dle této Přílohy.

4.4 Účastník tímto bere na vědomí a souhlasí s tím, že služba UPC Anti-DDoS podléhá určitým technickým omezením a je určena k obraně proti známým formám Případů DDoS. Účastník má možnost o těchto omezeních informovat. V důsledku toho nemusí služby UPC Anti-DDoS vždy odhalit všechny Případy DDoS a zmírnit jejich dopady a přestože UPC vynakládá a bude i nadále vynakládat veškeré z komerčního hlediska přiměřené úsilí k tomu, aby službu Anti-DDoS provozovala tak, aby dokázala odhalit známé i neznámé Případy DDoS a zmírňovat jejich dopady, nemůže UPC garantovat, že budou odhaleny a zmírněny veškeré Případy DDoS.

## 5. Platby poplatků a daní.

### 5.1 Pozastavení Služeb z důvodu neuhrazení dlužných částek.

Účastník tímto bere na vědomí a souhlasí, že (i) Účastník bude hradit společnosti UPC příslušné poplatky za Službu; (ii) UPC může pozastavit plnění a/nebo přístup k službě UPC Anti-DDoS nebo přerušit poskytování služby UPC Anti-DDoS v případě neuhrazení nebo opakovaného prodlení s úhradou jakýchkoli plateb, a to na základě písemného oznámení svého záměru tak učinit (jez může být zasláno i e-mailem); (iii) UPC může vypovědět tuto Specifikaci Anti-DDoS v případě neuhrazení nebo opakovaného prodlení s úhradou jakýchkoli plateb;

5.2 Poplatky. Účastník tímto bere na vědomí a souhlasí, že poplatky za službu UPC Anti-DDoS poskytovanou společností UPC se skládají z platby za instalaci a z pravidelných fixních měsíčních poplatků a že poplatky za případná období prodloužení nebo za nové objednávky budou stanoveny ve výši aktuálně platných sazeb v době takového prodloužení nebo nové objednávky.

## 6. Povinnosti Účastníka.

Jako podmínku poskytování Služby UPC Anti-DDoS ze strany UPC Účastník bere na vědomí a souhlasí, že nese výlučnou odpovědnost za plnění následujících závazků:

### 6.1 Mezní hodnoty.

Pokud nebude Účastník spokojen s výchozím profilem nastaveným pro něj společností UPC, pak Účastník navrhne minimální mezní hodnoty Internetového provozu Účastníka, při jejichž překročení bude do zasláno výstražné upozornění.

6.2 Účastník je povinen (a) na vyžádání provést změny nebo vydat svým poskytovatelům hostingových služeb a/nebo poskytovatelům služeb pokyn k provedení změn stávajícího síťového vybavení a/nebo infrastruktury tak, aby UPC mohla poskytovat Službu UPC Anti-DDoS; (b) obstarat veškerá potřebná oprávnění a povolení k provedení takových změn (zejména včetně úhrady veškerých poplatků účtovaných jakýmkoli Prostředími třetích stran za zaslání Výstražných upozornění společností UPC); (c) poskytnout společnosti UPC kontaktní body, které UPC pomohou s Nastavením Účastníka a se zavedením Služby UPC Anti-DDoS a poskytováním průběžné podpory; (d) učinit veškeré přiměřené kroky k zajištění ochrany před neoprávněným přístupem, používáním a sdělováním jeho uživatelského jména a hesla poskytnutého mu společností UPC za účelem přístupu Účastníka k jeho Portálu Účastníka.

6.3 Účastník prohlašuje a zaručuje, že (a) získal veškeré potřebné souhlasy a povolení k tomu, aby mohl UPC a/nebo UPC sdělovat informace a údaje Účastníka a/nebo třetích stran (včetně osobních údajů); (b) bude Službu UPC Anti-DDoS používat pro své vlastní interní účely a nebude ji přeprodávat dalším osobám; (c) nezabývá se ani se nebude zabývat žádnou nelegální činností a bude dodržovat veškeré platné zásady, předpisy a zákony; a (d) veškeré informace pro spuštění služeb poskytnuté Účastníkem (buď prostřednictvím Portálu Účastníka nebo prostřednictvím formuláře dodaného společností UPC) jsou přesné, spolehlivé a úplné a Účastník je bude dle potřeby vždy včas aktualizovat.

## 7. Práva přístupu k Portálu.

Na Doby trvání smlouvy uděluje UPC Účastníkovi a ten tímto přijímá omezenou, nevýhradní, nepřevoditelnou a nepostupitelnou licenci na užívání Portálu Účastníka a na přístup k němu, a to výhradně pro účely využívání Služby UPC Anti-DDoS a přístupu k nim a pro účely prohlížení a správy účtu Účastníka a dat na tomto účtu obsažených, a to výhradně v souladu s veškerými příslušnými pokyny nebo dokumentací, jež může UPC v této souvislosti Účastníkovi poskytnout.

## 8. Omezení.

Účastník nesmí (a) provádět úpravy, demontáž, dekompilaci, vytvářet odvozená díla nebo se jinak pokoušet odhalit nebo získat zdrojový kód k jakémukoli softwaru nebo systému poskytujícímu Službu ochrany proti útokům DDoS společností UPC; (b) kombinovat jakýkoli software poskytnutý společností UPC v souvislosti se Službou ochrany proti útokům DDoS s jakýmkoli programem nebo softwarem licencovaným na základě Všeobecné veřejné licence nebo jakékoli jiné licence z otevřeného zdroje způsobem, který by mohl vést k tomu nebo by mohl být vykládán jako vedoucí k tomu, že se na takový software (nebo jakoukoli jeho modifikaci) začnou vztahovat podmínky příslušné Všeobecné veřejné licence nebo jiné licence z otevřeného zdroje; nebo

(c) využívat služeb UPC způsobem představujícím nadměrné používání nebo zneužívání nebo způsobem, který jinak nesplňuje podmínky sjednané v této Smlouvě nebo je s nimi v rozporu. Účastník tímto bere na vědomí a souhlasí, že UPC si ponechá veškerá Práva k duševnímu vlastnictví, nároky a práva k veškerým dalším informacím, datům, obsahu, softwaru, námětům, konceptům, technikám, procesům, konfiguracím nebo jinému duševnímu vlastnictví obsaženému ve Službách ochrany proti útokům DDoS poskytovanými společnostmi UPC nebo praktikovaným v souvislosti s těmito službami (včetně Portálu Účastníka). Veškerá taková práva UPC k duševnímu vlastnictví se považují za Důvěrné informace.

## 9. Doba trvání; ukončení smlouvy.

9.1. Smlouva na poskytování služby UPC Anti-DDoS se uzavírá na dobu neurčitou, přičemž ji lze na základě výpovědi Účastníka ukončit nejdříve 6 měsíců od data předání. Službu Anti-DDoS lze poté vypovědět i bez udání důvodu, výpovědní doba služby činí 3 měsíce a začíná běžet první den následujícího měsíce po jejím doručení. V případě ukončení poskytování datové služby je zároveň automaticky ukončena služba Anti-DDoS. Služba Anti-DDoS je také ukončena zároveň s ukončením služby internetového připojení, neboť bez této nelze službu Anti-DDoS poskytovat. Účastník tímto bere na vědomí, že UPC může kdykoli a z jakéhokoli důvodu nebo bez uvedení důvodu Specifikaci Anti-DDoS vypovědět bez ohledu na jakákoli ustanovení Specifikace Anti-DDoS v opačném smyslu je UPC oprávněna tuto Specifikaci Anti-DDoS vypovědět písemnou výpovědí s výpovědní dobou v délce 30 dnů.

### 9.3 Výpověď smlouvy z důvodu podstatného porušení povinností.

Kterákoli ze smluvních stran může tuto Smlouvu o ochraně vypovědět písemnou výpovědí druhé smluvní straně v případě podstatného porušení smluvních povinností touto druhou stranou a nenapravení takového porušení ve lhůtě (30) dnů od obdržení písemné výzvy k nápravě obsahující specifikaci předmětného porušení.

9.4 Insolvence. v rozsahu povoleném platnými Právními předpisy může kterákoli ze smluvních stran tuto Smlouvu o ochraně vypovědět s okamžitou účinností v případě (a) zahájení jakéhokoli řízení vůči smluvní straně nebo z jejího popudu požadujícího úlevu, reorganizaci nebo vypořádání v souladu s jakýmkoli zákony či předpisy upravujícími insolvenční, přičemž takové řízení nebude do třiceti (30) dnů zamítnuto; (b) postoupení majetku ve prospěch věřitelů nebo jmenování nuceného správce, likvidátora nebo konkurzního správce ve vztahu k majetku či aktivům druhé smluvní strany; nebo (c) likvidace, zrušení nebo zániku obchodní činnosti druhé smluvní strany.

### 9.5 Účinky ukončení smlouvy

9.5.1 Výpověď ze strany UPC. v případě výpovědi Specifikace Anti-DDoS dle článku 9.3 nebo 9.4 výše se může UPC dle vlastního uvážení rozhodnout s okamžitou účinností ukončit Službu. Pokud UPC ukončí Službu dle tohoto článku 9.5.1, veškeré licence udělené Účastníkovi na základě příslušné Specifikace Anti-DDoS okamžitě zanikají.

9.5.2 Všeobecná ustanovení. Po uplynutí doby trvání Specifikace Anti-DDoS nebo po jejím ukončení je Účastník povinen přestat využívat Službu UPC Anti-DDoS. Žádné uplynutí doby trvání nebo ukončení smlouvy však Účastníka nezprošťuje jakékoli povinnosti uhradit finanční závazky vzniklé nebo splatné k datu ukončení nebo uplynutí doby trvání smlouvy.

9.5.3 Přechod Účastníka. Jakékoli ukončení či výpověď (z jakéhokoli důvodu), uplynutí doby trvání nebo neobnovení služeb UPC (vyjma

případů uplynutí doby trvání nebo neobnovení Služby UPC Anti-DDoS) nezprošťuje Účastníka jeho povinnosti nadále hradit společnosti UPC veškeré platby za Službu UPC Anti-DDoS, s výjimkou následujících případů a výlučně v rozsahu takových případů: (i) pokud Účastník uzavře s UPC smlouvu týkající se Služeb UPC Anti-DDoS; a (ii) pokud UPC písemně souhlasí s promínutím zbývajících platebních závazků ve vztahu ke Službě UPC Anti-DDoS.

Bez ohledu na cokoli o obsahu této Smlouvy o ochraně v opačném smyslu a vedle dalších práv UPC vyplývajících ze Smlouvy je UPC oprávněna tuto Smlouvu vypovědět s okamžitou účinností písemnou výpovědí doručenou Účastníkovi v případě, že UPC na základě vlastního uvážení dospěje k závěru, že se Účastník dopustil porušení zásad zákazu zneužívání (článek 12).

## 10. Neexistence práva na odškodnění vůči UPC

Účastník tímto bere na vědomí a souhlasí, že není oprávněn a nebude požadovat jakékoli odškodnění od UPC ve vztahu ke Službě UPC Anti-DDoS.

## 11. Prohlášení a záruky; Omezení odpovědnosti

11.1 Prohlášení a záruky Účastníka. Účastník tímto (i) prohlašuje a zaručuje, že není ani nebude Účastníkem, na něhož se vztahuje omezení; a (ii) zaručuje, že bude vždy dodržovat podmínky a ustanovení této Přílohy a řídit se jimi.

11.2 Neexistence záruk. Bez ohledu na cokoli z obsahu tohoto popisu v opačném smyslu platí, že služba UPC Anti-DDoS poskytovaná společností UPC je poskytována „ve své současné podobě“ a „dle aktuální dostupnosti“, bez jakýchkoli záruk. UPC tímto vylučuje veškeré výslovné, implicitní či ze zákona vyplývající záruky, zejména (avšak nikoli výlučně) veškeré implicitní záruky prodejnosti, vhodnosti pro určitý účel, splnění požadavků účastníka, neporušení jakýchkoli práv a veškeré záruky vyplývající z plnění, prodeje nebo obchodního použití. UPC neprohlašuje, nezaručuje ani negarantuje, že služba ochrany proti útokům DDoS poskytovaná dle této smlouvy bude fungovat bez přerušování, poruch a chyb. Účastník si je vědom a souhlasí s tím, že UPC neodpovídá za jakékoli jednání či nejednání účastníka založené na jakýchkoli informacích poskytnutých v rámci služeb ochrany před útoky DDoS poskytovaných společností UPC. UPC neprohlašuje, nezaručuje ani negarantuje, že (a) dojde k odhalení bezpečnostních hrozeb, škodlivých programů a/nebo zranitelných míst; (b) služba UPC Anti-DDoS poskytovaná společností UPC zajistí bezpečnost sítí a systémů účastníka před škodlivými programy, vniknutím nebo jinými formami porušení zabezpečení; (c) bude odhaleno každé zranitelné místo na každém testovaném systému či aplikaci; nebo (d) nevyskytnou se žádná falešná potvrzení útoků.

11.3 Bez ohledu na cokoli v opačném smyslu platí, že v souvislosti se službou ochrany před útoky DDoS poskytovanou společností UPC, nenese UPC jakoukoli odpovědnost ve vztahu k zásadám přijatelného používání (zejména, avšak nikoli výlučně, ve vztahu k jakémukoli jednání či nejednání společnosti UPC).

## 12. Zásady přijatelného používání.

12.1 Zakázané činnosti. Účastník nesmí provádět ani se pokoušet provádět žádné z následujících zakázaných činností: (a) Hackerská činnost, testování dostupnosti (pinging), zahlcování, rozesílání hromadné pošty nebo útoky v podobě DoS (odepření služby) nebo

jakékoli jiné činnosti, které narušují užívání nebo možnost ostatních efektivně používat jakoukoli síť, systém, službu nebo vybavení; (b) podílení se nebo šíření návodných informací ohledně podvodné nebo nelegální činnosti (včetně online hazardu ve všech podobách, bez ohledu na to, zda je či není v rozporu s platnými právními předpisy), porušování nebo zcizování Práv k duševnímu vlastnictví třetích stran (včetně softwarového pirátství), narušování práv na soukromí, publicitu a dalších osobnostních práv dalších osob, shromažďování, inzerování, předávání, uchovávání, zveřejňování, zobrazování, nahrávání nebo jiné zpřístupňování dětské pornografie nebo jiných obscenních verbálních projevů nebo materiálů nebo používání sítě UPC nebo jejich prodejců (dle konkrétní situace) k takovým činnostem; (c) podílení se na jakékoli zákonné či nezákonné činnosti, o níž se UPC domnívá, že by mohla poškodit její provoz, pověst, dobré jméno nebo vztahy se účastníky; (d) rozesílání nevyžádané hromadné pošty a/nebo komerčních elektronických sdělení, virů, červů nebo trojských koní; (e) padělání, vymazávání nebo zkeslování nadpisů zpráv, zpátečních adres nebo adres internetových protokolů nebo jiná manipulace i identifikačními znaky jako celkem nebo zčásti, za účelem skrytí původce příslušné zprávy; (f) podpora nebo podněcování k fyzické újmě nebo násilí na určité skupině osob nebo jednotlivci; nebo (g) reklama, přenos, poskytování nebo jiné zpřístupňování jakéhokoli softwaru, programů, produktů, služeb, možností nebo informací určených k usnadnění porušování těchto Zásad přijatelného používání. Účastník je povinen učinit veškeré přiměřené kroky k zajištění toho, aby žádná třetí strana, již Účastník povolil využívat své služby, neprovozovala ani se nepokoušela provozovat žádnou ze zakázaných činností specifikovaných níže.

**12.2 Potvrzení ze strany Účastníka.** Účastník tímto bere na vědomí a souhlasí, že (a) informace, které se dostanou do zařízení UPC nebo jejich prodejců, mohou mít původ u některého z účastníků Účastníka nebo od jiné třetí strany, a že tudíž UPC popř. její prodejce mohou Účastníka požádat o učinění odpovídajících kroků směřujících přímo vůči jeho účastníkům za účelem prevence porušení Zásad přijatelného používání; a (b) pokud to vyžaduje zákon, může UPC informovat příslušné donucovací orgány, pokud se dozví o jakékoli nelegální činnosti provozované v síti UPC nebo přenášené jejím prostřednictvím.

### 12.3 Práva UPC.

Pokud UPC dospěje k závěru, že Účastník nesplnil některé ustanovení tohoto článku 12 nebo učinil popř. pokusil se učinit něco ze zde popsaných zakázaných činností, souhlasí Účastník s tím, že UPC je oprávněna bezodkladně přijmout nápravná opatření, jež zahrnují zejména, avšak nikoli výlučně, pozastavení Služby UPC Anti-DDoS a/nebo ukončení této Služby na základě oznámení (které může být zasláno též e-mailem) doručeného (48) hodin předem. Takové nápravné opatření existuje vedle případných dalších práv UPC vyplývajících z této Specifikace nebo ze zákona. UPC může Účastníkovi předložit oznámení o svém záměru přijmout opatření dle tohoto článku, avšak není povinna tak učinit.

UPC může dle vlastního uvážení kdykoli provést změny nebo aktualizace těchto Zásad dle ustanovení čl. 2.4. Všeobecných podmínek. Účastník je povinen spolupracovat s UPC a/nebo s jejími prodejci při zavádění jakýchkoli nápravných nebo preventivních opatření, jež mohou UPC nebo její prodejci považovat za nezbytné.

## 13. Dodržování Právních předpisů.

Každá ze smluvních stran souhlasí, že bude v souvislosti s plněním této Smlouvy dodržovat veškeré platné místní zákony, předpisy a nařízení. UPC je oprávněna pozastavit plnění jakýchkoli svých závazků

vyplývajících z této Smlouvy o ochraně, a to i bez předchozího oznámení a bez vzniku jakékoli odpovědnosti, pokud Účastník nedodrží ustanovení tohoto článku 13

## 14. Různé

**14.1 Rozhodné právo.** Tato Smlouva o ochraně se ve všech ohledech řídí právním řádem země založení UPC a bude vykládána a vymáhána v souladu s tímto právním řádem.

**14.2 Vyšší moc.** S výjimkou platebních závazků Účastníka nebude žádná ze smluvních stran v prodlení dle této Smlouvy ani nebude vůči druhé smluvní straně odpovědná za jakékoli pozastavení, přerušení nebo zdržení s plněním svých závazků vyplývajících z této Smlouvy (vyjma platebních závazků), pokud bude takový stav způsoben zemětřesením, povodní, požárem, bouřkou, přírodní katastrofou, působením vyšší moci, válkou, terorismem, ozbrojeným konfliktem, stávkou, odstávkou, bojkotem nebo jinými skutečnostmi mimo rozumnou kontrolu příslušné smluvní strany, avšak s tím, že strana dovolávající se tohoto ustanovení (a) bude bezodkladně písemně informovat druhou stranu o této skutečnosti; a (b) učiní veškeré kroky, jež jsou v přiměřeném rozsahu nezbytné ke zmírnění dopadů takové Vyšší moci, a dále za předpokladu, že pokud bude působení Vyšší moci trvat v souhrnu déle než šedesát (60) dnů, je každá ze smluvních stran oprávněna vypovědět tuto Smlouvu o ochraně s okamžitou účinností nebo na základě písemné výpovědi doručené druhé smluvní straně.

**14.3 Pořadí přednosti při výkladu.** v případě rozporů mezi ustanoveními této Přílohy mají v rozsahu takového rozporu přednost ustanovení Specifikace služeb, avšak pouze ve vztahu ke konkrétní Službě UPC Anti-DDoS na základě příslušné Specifikace. Pokud bude síť UPC vyžadovat kapacitu ze služby UPC Anti-DDoS v rozsahu znemožňujícím zajištění úplné ochrany internetového provozu Účastníka, mají interní a vlastní potřeby ochrany UPC přednost před potřebami Účastníka.