## 1. POPIS SLUŽBY

**1. 1.** GP WebPay je online služba přijímání plateb, kterou společnost KB SmartPay zpřístupňuje Obchodníkovi, a kterou poskytuje společnost Global Payments Europe, s.r.o. (V Olšinách 626/80, Praha 10, identifikační číslo (IČO): 27088936) (dále jen „Dodavatel"). Tato služba umožňuje Obchodníkům, kteří nabízejí zboží/služby k prodeji na Internetu, přijímat platby Kartou prostřednictvím Mezinárodních karetních schémat. Služba GP WebPay mimo jiné umožňuje Kupujícím předkládat objednávky, požádat o předautorizaci dané částky na bankovním účtu Kupujícího, požádat o vypořádání částky, provést vrácení peněz nebo připsání částky k dobru za vrácené zboží.

**1. 2.** Služba GP WebPay může být aktivována pouze po vytvoření a aktivaci v systémech Dodavatele a aktivaci služeb akceptace karet pro situace „Card Not Present" („Bez přítomnosti karty").

**1. 3.** Po vytvoření Obchodníka v systémech Dodavatele:

- bude Obchodníkovi přiřazeno uživatelské jméno a heslo pro přístup ke službě GP WebPay;
- Dodavatel poskytne Obchodníkovi svůj veřejný klíč pro ověřování přenášených zpráv. Obchodník bude následně povinen poskytnout svůj veřejný klíč pro ověření přenášených zpráv.

## 2. POVINNOSTI OBCHODNÍKA

**2. 1.** Obchodník se zavazuje využívat službu GP WebPay v souladu se Smlouvou a s pokyny společnosti KB SmartPay a/nebo Dodavatele. Používáním služby GP WebPay bude Obchodník rovněž jednat v souladu s jakýmikoliv pokyny zobrazenými touto aplikací.

**2. 2.** Obchodník obdrží od Dodavatele specifikaci rozhraní mezi Obchodníkem a systémem GP WebPay, které bude sloužit k úpravě a nastavení aplikace Obchodníka. Tato specifikace obsahuje důvěrné údaje, které musí Obchodník zabezpečit proti neoprávněnému použití.

**2. 3.** Obchodník zajistí, aby jeho webové stránky byly bezpečné, a bude informovat společnost KB SmartPay o každém podvodném použití služby GP WebPay.

**2. 4.** Obchodník zajistí ochranu všech údajů, které obdrží od Držitelů platebních karet. Tyto údaje zahrnují: především citlivé autentizační údaje (PIN, CAV2, CVC2 a CVV2), jakož i údaje týkající se platby Držitelů karet (číslo platební karty, jméno Držitele platební karty, datum vypršení platnosti a kód služby). V případě, že budou přijaty citlivé autentizační údaje, nemohou být ukládány. Údaje týkající se Držitelů platebních karet mohou být ukládány pouze za podmínky úplného souladu s podmínkami požadavku č. 3 bezpečnostního standardu PCIDSS (https://www.pcisecuritystandards.org). Obchodník je odpovědný za jakékoliv škody, které by mohly vzniknout v důsledku zveřejnění nebo neoprávněného použití takovýchto údajů, včetně vypořádání finančních sankcí uložených sdruženími karet a dalšími subjekty.

**2. 5.** V případě jakékoliv poruchy aplikace GP WebPay bude Obchodník neprodleně informovat KB SmartPay, aby tak zajistil rychlou opravu této poruchy.

**2. 6.** Obchodník bude dodržovat veškeré platné zákony a výslovně zaručí, že bude dodržovat veškeré zákony týkající se prodeje na dálku a elektronického obchodu;

**2. 7.** Na webové stránce Obchodníka bude jasně uvedeno, že přenosy dat jsou zabezpečeny pomocí protokolu SSL.

**2. 8.** Obchodník sám odpovídá za produkty a služby nabízené svým klientům. Společnost KB SmartPay neodpovídá za žádné informace, zprávy, fotografie a obecný obsah pocházející od Obchodníka nebo jeho webových stránek.

**2. 9.** Obchodník nese plnou odpovědnost za veškeré důsledky každé změny, kterou provede sám nebo třetí strana ve službě GP WebPay, zejména pak za důsledky každé změny a/nebo narušení softwaru, které mohou změnit povahu služby GP WebPay.

## 3. ROZSAH PODPOROVANÝCH FUNKCÍ

### 3. 1. Doručování příkazů

**3. 1. 1.** Po uzavření Smlouvy obdrží Obchodník URL adresu pro doručování příkazů. V případě, že Kupující na webové stránce Obchodníka zvolí „Pay" („Platit"), musí webová stránka Obchodníka na tuto adresu zavolat se zadanými parametry a předem definovanou zprávou. Zpráva zaslaná Obchodníkem neobsahuje žádné údaje o platební kartě. Takovéto údaje (číslo platební karty, datum vypršení platnosti karty a kód CVV/CVC) musí být zadány přímo v aplikaci GP WebPay. Podrobná specifikace a struktura předávaných zpráv budou Obchodníkovi poskytnuty po podpisu smlouvy.

**3. 1. 2.** Dodavatel musí používat servlet pro přenos příkazů, který umožní Obchodníkům minimalizovat počet odeslaných parametrů a používat předem dohodnuté a předem nastavené parametry.

### 3. 2. Uživatelské rozhraní

Obchodníkovi, který využívá službu GP WebPay, je také přiřazena URL adresa uživatelského rozhraní s jedním nebo více jmény a hesly. Ve výchozím nastavení je Obchodníkovi přiděleno jedno oprávnění Administrátora (správce), který může měnit nastavení Obchodníka a zakládat další uživatele.

### 3. 3. Uzávěrka šarží

Povolení každého příkazu (pokud je požadováno) se uskutečňuje okamžitě (online). Platby a kredity (tj. transakce) se stávají součástí šarže. Příkaz k převodu částky z účtu klienta na účet Obchodníka není odesílán z GP WebPay, dokud není uzavřena šarže (dávka) s danou transakcí. Obchodník může uzavírat šar-

že (dávky) tak často, jak si přeje, nebo Zúčtovací banka (Acquirer) a Obchodník se mohou dohodnout, že Dodavatel bude automaticky jednou denně uzavírat šarže pro Obchodníka.

**3. 4. Ostatní služby**

Ve výchozím nastavení je Obchodníkům k dispozici Servlet plateb, kterému mohou být zasílány autentizované žádosti o zavedení příkazu, autorizaci příkazu, vypořádání atd. Servlet plateb také Obchodníkům umožňuje získávat seznam jejich příkazů, plateb, částek připsaných k dobru (tj. kreditů) za vrácení zboží.

**3. 5. Testování**

Společnost KB SmartPay také nabízí – prostřednictvím Dodavatele – testovací prostředí, které umožňuje otestovat všechny typy transakcí, jakmile je Obchodník zadán do databáze. Testování je k dispozici zdarma.

## 4. OVĚŘENÍ AUTORIZACE KARTY

**4. 1.** Ověřování autorizace Karty bude prováděno postupně, jakmile údaje dorazí na aplikaci GP WebPay, a sice na základě informací poskytnutých a potvrzených Kupujícími (číslo Karty, datum vypršení platnosti a vizuální kryptogram) ve formátu používaném pro zadávání bankovních údajů.

**4. 2.** Tato ověřování se budou skládat z následujících prvků:

- Bude ověřováno datum vypršení platnosti, aby se zajistilo, že se jedná o pozdější datum, než je datum transakce.
- Bude ověřována přítomnost a numerické složení vizuálního kryptogramu.
- Bude ověřováno číslo Karty za účelem zjištění, zda obsahuje počet znaků v souladu s příslušnými specifikacemi Karty, a zda se skládá z číselných znaků.
- Bude ověřována matematická pravděpo¬dobnost čísla Karty.

**4. 3.** Pokud tyto řídicí mechanismy nevyvolají žádné negativní prvky, bude se poté aktivovat proces zahájení žádosti o autorizaci.

**4. 4.** Pokud tyto řídicí mechanismy přece jen způsobí negativní prvky, potom bude Kupující požádán o opakování tohoto postupu. Transakce bude zrušena po třech neúspěšných pokusech.

## 5. SPRÁVA PLATEBNÍHO SYSTÉMU

Obchodník může mít online přístup k platebním transakcím, které jsou zaznamenány službou GP WebPay, aby do nich mohl nahlédnout, aby je mohl potvrzovat (zcela nebo částečně) nebo rušit, aby mohl provádět náhrady nebo urychlovat transakce.

## 6. PODÁVÁNÍ ZPRÁV

**6. 1.** Služby GP WebPay nebudou s Obchodníkem provádět výměny žádných citlivých informací o Držiteli karty (jako jsou například jméno, adresa, číslo Karty atd.).

**6. 2.** Obchodník chápe a souhlasí s tím, že nelze zaručit integritu (tj. celistvost) přehledů odesílaných e-mailem.

## 7. ZABEZPEČENÍ

**7. 1.** Obchodník bude vždy splňovat následující pravidla minimálního zabezpečení:

- Online obchod Obchodníka musí být provozován způsobem, který minimalizuje riziko odhalení osobních údajů subjektu „s“ způsobeným buď sledováním komunikace mezi subjektem „s“ a Obchodníkem, nebo únikem dat uložených v systémech Obchodníka;
- Aby byla zajištěna bezpečnost, musí Obchodník implementovat SSL připojení, které používá alespoň 128bitovou SSL komunikaci mezi prohlížečem klienta a serverem Obchodníka (online obchod);
- Aby byla zajištěna bezpečnost, bude Obchodník implementovat technologie, které zajistí řízený přístup k systémům pro online transakce, jako je například firewall, proxy server, pravidelné aktualizace softwaru, antivirový software a správné postupy správy systému;
- Ochrana systémů/údajů před neoprávněným přístupem;
- Uchovávání záznamů o jednotlivých transakcích, které proběhly v době, kdy byl systém používán klienty – a to i pokud jde o možný postup prokazování související s pokusem o zneužití systému;
- Aby se zajistilo bezpečné ukládání důvěrných kryptografických klíčů, měla by se používat bezpečná technologie (například čipové karty).

**7. 2.** Obchodník musí provozovat svou aplikaci způsobem, který neohrožuje ani neomezuje ostatní uživatele systému GP WebPay, tj. Obchodník musí zejména:

- implementovat rozhraní přesně v souladu se specifikacemi dodanými Obchodníkovi Dodavatelem;
- informovat společnost KB SmartPay a Dodavatele o jakýchkoliv změnách v podstatných skutečnostech, (o změně kontaktních osob, telefonních čísel, adres atd.) nebo o změně systému Obchodníka (o změně webového serveru, databáze, IP adresy, aplikace, významných změnách systému, atd.).

**7. 3.** Obchodník musí informovat společnost KB SmartPay a Dodavatele o jakýchkoliv ověřených porušeních svého systému, které by mohly ovlivnit zabezpečení systému GP WebPay.

## 8. ÚDRŽBA

**8. 1. Preventivní a bezpečnostní údržba**

Společnost KB SmartPay nebo Dodavatel mohou dočasně pozastavit službu GP WebPay za účelem provádění technické údržby, zejména pokud jde o bezpečnostní záplaty a doporučení PCI/DSS. Společnost KB SmartPay nebo Dodavatel vynaloží přiměřené úsilí, aby ohlásili tuto technickou údržbu jeden kalendářní týden předem, a sice zasláním e-mailu na e-mailovou adresu uvedenou v Objednávkovém formuláři/Krycím dokladu.

**8. 2. Nápravná údržba**

Společnost KB SmartPay nebo Dodavatel vynaloží přiměřené úsilí, aby udělili Obchodníkovi přístup ke službě GP WebPay způsobem, který bude co možná nejméně přerušovaný.

Společnost KB SmartPay nebo Dodavatel budou informovat Obchodníka o přerušeních služby GP WebPay zasláním e-mailu na e-mailovou adresu uvedenou v Objednávkovém formuláři/Krycím dokladu.

Pokud by přerušení byla způsobena externími stranami (např. autorizačním serverem vydavatele nebo finanční instituce), potom bude úloha společnosti KB SmartPay a Dodavatele omezena na informování těchto stran o přerušeních,

aby jim bylo umožněno přijmout nutná opatření.

## 9. DEFINICE

- Kupující: uživatel Internetu, který provádí platby na webové stránce Obchodníka za produkt nebo službu nabízenou Obchodníkem na jeho webové stránce.
- PCI/DSS (Standardy bezpečnosti dat odvětví platebních karet): mezinárodní standardy podporované nejdůležitějšími společnostmi v oblasti kreditních karet, jako jsou například Visa a MasterCard International, jejichž cílem je zabránit zneužívání údajů o kreditní kartě. Viz https://www.pcisecuritystandards.org.
- Produktový certifikát: certifikát, který obsahuje bezpečnostní klíč, jenž umožňuje zabezpečení a integritu platby.
- Konektor GP WebPay: software (API neboli aplikační programovací rozhraní) vyvinutý společností GP Europe s.r.o., který je nainstalován u Obchodníka nebo u jeho poskytovatele hostingu, a který umožňuje bezpečnou výměnu dat se systémem GP WebPay.
- Platba v cizích měnách/MultiCurrency: Obchodník může v Objednávkovém formuláři definovat cizí měny, kterými chce umožnit zaplacení přes platební bránu a ve kterých bude zároveň prováděno zúčtování na účty vedené v daných cizích měnách.