Worldline | SIX Payment Services

Všeobecné obchodní podmínky pro přijímání karet

Verze 11.2019 (EULUX)

Tento dokument je nezávazným překladem anglického zdrojového textu. Pokud by nastal rozpor ve výkladu, je rozhodující anglická verze.

1 Rozsah použití, vymezení zákonných požadavků, týkajících se platebních služeb a definice

1.1 Rozsah použití

Tyto všeobecné obchodní podmínky (dále jen "VOP") se vztahují na všechny produkty a služby, dohodnuté mezi Obchodníkem a SIX Payment Services (Europe) S.A. (dále jen "SPS") v modulech pro přijímání karet, např. "Přijetí karty na prodejním místě" nebo "Přijetí karty pro bezpečné elektronické a mailové/telefonní objednávky" (dále samostatně uváděny jako "Smluvní modul" nebo souhrnně "Smluvní moduly").
Tyto VOP tvoří nedílnou součást uzavřených Smluvních modulů. Uzavřené Smluvní moduly tvoří nedílnou součást "Rámcové smlouvy o bezhotovostních platbách" (dále jen "Rámcová smlouva"), uzavřené mezi Obchodníkem a SPS.

1.2 Vyloučení zákonných požadavků, týkajících se platebních služeb

Dle článku 38 a 61 Směrnice EU 2015/2366 z 25. listopadu 2015 (dále uváděna jako „Směrnice o platebních službách") a národních prováděcích zákonů, se smluvní strany dohodly na vyloučení aplikace veškerých nepovinných předpisů, obsažených ve Směrnici o platebních službách a v národních zákonech o převodech.

1.3 Definice

Následující definice odpovídají použití odpovídajících termínů v těchto VOP.

Autorizace	V rámci procesu autorizace vydavatel karty ověřuje, zda je karta platná/není blokovaná a zda je částka transakce ve stanoveném limitu.
Bezkontaktní (bezkontaktní karta, bezkontaktní čtečka, bezkontaktní transakce)	Provedení transakcí pomocí "komunikace v blízkém poli" (NFC), mezinárodní normy pro přenos dat radiovou technologií. To vyžaduje terminál s bezkontaktní čtečkou a kartu s NFC-kompatibilním čipem, např. Visa s funkcí "PayWave" nebo Mastercard s funkcí "PayPass". Data čipu jsou načítána podržením karty u bezkontaktní čtečky.
Debetní karta	Karta, používaná k platbě za zboží a služby, přičemž částka je okamžitě zaúčtována na vrub držitele karty (např. V PAY, Maestro).
Distanční transakce	Transakce, kde držitel karty ani karta nejsou fyzicky přítomni v místě prodeje. K těmto transakcím dochází především přes Internet, telefon, fax nebo korespondenčně.
Držitel karty	Zákazník, který nakupuje zboží a/nebo služby, nabízené Obchodníkem a platí za ně bezhotovostně pomocí karty (transakce).
Elektronické zpracování	Realizace a předání transakce s použitím hardwarového nebo virtuálního terminálu a elektronického předání do systému.

116.1305.08/EULUX_CZ/11.2019

EMV (EMV karta, EMV čip, EMV terminál)	Specifikace pro karty, které jsou vybaveny procesorovým čipem a také souvisejícím zařízením pro čtení čipových karet (např. POS terminály, přístroje na jízdenky, bankomaty, systémy pro čerpací stanice). EMV transakce jsou platby, které jsou zpracovány na základě elektronického načtení dat karty na EMV terminálu z procesorového čipu karty.
Infrastruktura	Technické instalace, které náleží Obchodníkovi a jsou určeny pro přijímání a provádění kartových plateb prostřednictvím elektronického zpracování, t.j. hardwarové nebo virtuální terminály, včetně periferních zařízení, jako jsou registrační pokladny nebo telekomunikační zařízení, routery, servery, atd.
Kartová společnost	Poskytovatel licence (jako je Visa International, Mastercard International) na vydávání a přijímání karet.
Karty	Obecný termín pro platební karty, které se používají k provádění bezhotovostních plateb, t.j. kreditní/debetní karty.
Komerční karta	Karta, která je vydána společnostem, subjektům veřejné správy nebo výhradním vlastníkům a je omezena k obchodnímu nebo oficiálnímu použití; kde transakce provedené kartou jsou natíženy na vrub účtu společnosti, subjektu sektoru veřejné správy nebo výhradního vlastníka.
Kreditní karta	Karta, používaná k platbě za zboží a služby, přičemž částka je následně zaúčtována na vrub držitele karty (např. Visa, Mastercard, Diners Club/Discover, UnionPay, JCB).
mPOS terminál	Mobilní čtečka karet, která je provozována pomocí kompatibilního koncového zařízení (např. smartphone nebo tablet) a aplikace.
Nabyvatel	Nabyvatel umožňuje svým obchodníkům přijímat karty jako prostředky bezhotovostních plateb (v rámci prezenční či distanční realizace) a zajišťuje zpracování takto generovaných transakcí. Aby tak mohl činit, má v držení licence od příslušných kartových společností.
(SPS)	Nabyvatel umožňuje svým obchodníkům přijímat karty jako prostředky bezhotovostních plateb (v rámci prezenční či distanční realizace) a zajišťuje zpracování takto generovaných transakcí. Aby tak mohl činit, má v držení licence od příslušných kartových společností.
Obchodník	Norma Payment Card Industry Data Security Standard (PCI DSS) představuje PCI normu, která se zaměřuje na to, aby bylo zajištěno, že společnosti implementují bezpečnostní standardy.
kód kategorie (MCC)	Kategorizace, specifikovaná kartovými společnostmi, která umožňuje přiřazení obchodních aktivit Obchodníka nabyvatelem do jedné nebo více sektorových kategorií.
PCI DSS	Norma Payment Card Industry Data Security Standard (PCI DSS) představuje PCI normu, která se zaměřuje na to, aby bylo zajištěno, že společnosti implementují bezpečnostní standardy.
PCI standardy	Bezpečnostní normy pro kartový průmysl, definované Radou Payment Card Industry Security Standards Council (PCI SSC), jejichž aplikace je stanovena kartovými společnostmi. Podrobnější informace lze najít na www.pcisecuritystandards.org.
PIN (osobní identifikační číslo)	Osobní kombinace číslic, která ověřuje držitele karty jako oprávněného uživatele karty.
Platforma Alipay	Alipay.com Co Ltd. (dále jako «Alipay») provozuje mezinárodní elektronickou platební platformu. Smlouva o spolupráci uzavřenámezi Alipay a SPS umožňuje smluvnímu partnerovi akceptaci bezhotovostních plateb uživateli platformy Alipay.
Poskytovatel platebních služeb (PSP)	PSP nabízí řešení plateb, například aplikaci (virtuální terminál), která umožňuje akceptování elektronických platebních prostředků pro platbu v internetovém obchodu.
Prezenční transakce	Transakce, kde jsou jak držitel karty, tak karta fyzicky přítomni v místě prodeje.
SEPA: jednotná evropská platební oblast	Standardizovaná oblast plateb v Euro, v níž lze vyrovnávat přeshraniční platby stejně účinně jako domácí platby v jednotlivých zemích.
Spotřebitelská karta	Karta vydaná fyzické osobě, jejíž používání nemůže být vztaženo k jejím obchodním, firemním nebo profesním aktivitám; přičemž transakce provedené kartou jsou natěžovány přímo na vrub účtu fyzické osoby.
Stvrzenka	Fyzické nebo elektronické potvrzení realizace transakce, generované terminálem nebo internetovým obchodem.
Systém	Systém elektronických autorizací a vyrovnání, provozovaný SPS pro zpracování transakcí. Služba "myPortal" dle bodu 4.4 tvoří jeho součást.
Terminál (hardwarový nebo virtuální terminál)	Hardwarové terminály jsou pevná nebo mobilní zařízení, používaná pro zpracování transakcí. Softwarové komponenty, které umožňují připojení hardwarových terminálů k dalším periferním zařízením (systémy registračních pokladen, hotelové rezervační systémy, systémy čerpacích stanic, atd.), jsou přiřazovány k hardwarovému terminálu.
	Virtuální terminály jsou aplikace, které umožňují provedení distanční transakce a její zpracování. Softwarové terminály jsou obvykle provozovány a prodávány poskytovateli platebních služeb (tedy SPS).
Transakce	Procedura bezhotovostní platby, realizovaná Obchodníkem prostřednictvím elektronického zpracování, přičemž data transakce jsou následně zpracována systémem SPS.
Úvěr/kredit	Plné či částečné proplacení transakcí na kartě, které byly původně zaúčtovány na vrub.
Verifikační kód karty	Sekvence číslic, vytištěná na kreditní kartě (např. Visa [CVV2], Mastercard [CVC2]), která se používá jako dodatečný bezpečnostní prvek při distančních operacích.
Vydavatel karty	Společnost oprávněná kartovým systémem k vydávání karet držitelům karet.
Zpětná platba	Zrušení transakce, zadané Obchodníkem nebo úhrady již odeslané, a to v důsledku oprávněné reklamace, týkající se transakce, a to držitelem karty nebo vydavatelem karty. Nárok na úhradu na straně Obchodníka propadá.

2 Smluvní strany

2.1 Obchodník

2.1.1 Identifikace Obchodníka

SPS je povinen identifikovat Obchodníka, jeho právní zástupce a oprávněné majitele a také zaznamenávat obchodní aktivity Obchodníka a správně je alokovat do odpovídající kategorie sektoru (MCC). Za tímto účelem poskytne Obchodník SPS kopie dokumentů, specifikované v Rámcové smlouvě a také – případ od případu – veškeré další vyžadované dokumenty. SPS si vyhrazuje právo, v souladu s legislativou, vztahující se k boji proti praní špinavých peněz, vyžadovat v intervalech, požadovaných SPS za adekvátní, aktualizaci dokumentů, poskytnutých pro účely identifikace Obchodníka.
SPS je pro účely řízení rizik oprávněna posoudit obchodní aktivity (produkty a služby) a finanční situaci obchodníka. Obchodník poskytne SPS požadované informace (včetně účetní závěrky) do 10 dnů od žádosti SPS.

2.1.2 Přidružení prodejních míst a internetových obchodů

Prodejní místa a internetové obchody Obchodníka mohou být přidruženy k Rámcové smlouvě v okamžiku uzavření smlouvy. Následné přidružení prodejních míst a internetových obchodů bude odsouhlaseno Smluvními stranami samostatně.

2.1.3 Přidělení sektoru (kód kategorie obchodníka, MCC)

Obchodník pracuje v sektorových kategoriích, specifikovaných ve Smluvních modulech a prodává zboží a/nebo poskytuje služby držitelům karet, kdy tyto jsou výhradně alokovány k uvedeným sektorovým kategoriím. Samostatný Smluvní modul musí být uzavřen pro každou sektorovou kategorii.

2.1.4 Změny na straně Obchodníka

Změny na straně Obchodníka (například týkající se právní formy, obchodní činnosti, adresy, detailů účtu, právních zástupců, oprávněných vlastníků,

prodejních míst nebo infrastruktury) budou Obchodníkem neprodleně oznámeny SPS písemnou formou. SPS má právo fakturovat Obchodníkovi náklady, spjaté se změnami.
V případě významné změny ve vlastnické struktuře a kontrole Obchodníka, je tento povinen písemně informovat SPS alespoň jeden měsíc předem. SPS bude oprávněn v takovém případě požadovat, aby byla aktualizována identifikace Obchodníka dle bodu 2.1.1. Pokud by z tohoto vyplývalo zvýšené riziko, je SPS oprávněn ukončit Smluvní modul, a to s okamžitou účinností. Za dobu, kdy nebyl SPS písemně informován o právním nástupnictví, může připsat veškeré kompenzace s vylučujícím důsledkem na předchozího Obchodníka.
Pokud dojde k výraznému zhoršení úvěrového ratingu Obchodníka (například k zahájení insolvenčního řízení), bude Obchodník informovat SPS. SPS bude oprávněn – dle svého výhradního rozhodnutí – okamžitě přijmout vhodná opatření, jako je úprava podmínek kompenzací, zadržení kompenzací nebo požadování náležité jistiny. Obchodník bude neprodleně informován o všech přijatých opatřeních.

2.2 SIX Payment Services (Europe) S.A.

SIX Payment Services (Europe) S.A. je společnost se sídlem v Lucembursku ("Société Anonyme"), se sídlem na 10, rue Gabriel Lippmann, L-5365 Munsbach (Lucemburský obchodní rejstřík č. B144087). Jako licencovaná platební instituce (číslo licence 06/10) je SPS pod dohledem lucemburského dozorového finančního úřadu (Commission de Surveillance du Secteur Financier/CSSF, 110, route d'Arlon, L-1150 Lucembursko). SPS je držitelem licencí od kartových společností, které jsou pro akceptaci karet nezbytné.

3 Infrastruktura Obchodník

3.1 Obecně

Obchodník ponese plnou odpovědnost za získání, provozování a údržbu infrastruktury, která je vhodná pro elektronické provádění kartových transakcí a také za přijetí technických bezpečnostních opatření, aby se zabránilo jakémukoli zneužití infrastruktury; především dodržování PCI DSS dle bodu 14.3. Výše uvedené bude platit i na změny infrastruktury v důsledku úprav systému na straně SPS v souladu s bodem 4.1, odst. 3.
Pouze terminály (hardwarové a/nebo virtuální terminály), které byly certifikovány v souladu s platnou normou PCI a požadavky, stanovenými kartovými společnostmi, mohou být používány pro provádění kartových transakcí. EMV certifikace je povinným požadavkem pro hardwarové terminály. Dále, certifikované terminály vyžadují odsouhlasení jedním nebo několika Nabyvateli, v souladu se specifickými požadavky odpovědného orgánu v dané zemi.

3.2 Povinnosti Obchodníka

3.2.1 Obecné povinnosti náležité péče

Obchodník je povinen zajistit prostřednictvím náležitých opatření, aby nebyla možná žádná manipulace, především žádné neoprávněné transakce a aby byly terminály chráněny proti neoprávněnému přístupu třetích stran. Obchodník proškolí svůj personál z hlediska správné manipulace a používání infrastruktury, a to v náležitých intervalech, především při zahájení provozu. Poučí personál také o opatřeních, která je třeba provádět v rámci prevence proti zneužití a podvodu.

3.2.2 Povinnosti, týkající se hardwarových terminálů

Obchodník umístí všechny hardwarové terminály do místa prodeje takovým způsobem, aby měl držitel karty přímý přístup k terminálu (především k displeji, klávesnici a čtečce karet) a nemohl být sledován v případě, že je vyžadováno zadání PIN.

3.2.3 Povinnosti, týkající se virtuálních terminálů

Obchodník bude s náležitou péčí chránit infrastrukturu, používanou k provozování virtuálních terminálů, především počítače (včetně všech souvisejících síťových komponent) a nosiče dat, které obsahují data z karet (především čísla karet, data platnosti nebo data o transakcích).

3.2.4 Povinnost informovat/právo na informace

Na žádost SPS bude Obchodník poskytovat písemné informace o tom, které terminály jsou aktivně využívány. Dále Obchodník opravňuje SPS, aby získával tyto informace přímo od koncových výrobců/poskytovatelů softwaru či dodavatelů jakékoli jiné infrastruktury. Obchodník poskytne v tomto ohledu pomoc SPS.
Obchodník bude okamžitě písemně informovat SPS o jakýchkoli změnách, vztahujících se k hardwarovým terminálům nebo jeho internetovému obchodu, o veškerých odpojeních, výměnách nebo změnách umístění/URL.

3.2.5 Směrování transakcí třetími stranami

Obchodník bude oprávněn vstupovat do smluv s třetími stranami, certifikovanými PCI DSS (jako jsou poskytovatelé platebních služeb, síťoví operátoři), které předávají transakce SPS jménem Obchodníka. SPS neodmítne uznání, přijetí takových třetích stran, pokud k tomu nemá dobré důvody. Veškeré náklady, vznikající ve spojitosti s třetí stranou a jejím zapojením, především za aktivaci, poplatky, zpoždění a neplnění, ponese Obchodník. SPS bude oprávněn fakturovat Obchodníkovi takové náklady a poplatky nebo je započíst proti veškerým kreditům, splatným k úhradě Obchodníkovi.
Obchodník bude okamžitě písemně informovat SPS o veškerých změnách ve vztahu k zpracování transakcí prostřednictvím třetích stran nebo o případech, kdy mění třetí využívanou stranu. SPS bude oprávněn odmítnout takové změny či změnu třetí strany ze závažné příčiny.

3.2.6 Akceptace karty prostřednictvím více nabyvatelů

Při současném zajišťování získávání služeb od více než jednoho poskytovatele je třeba vždy zajistit, aby byly údaje o transakci, vztahující se ke každému Nabyvateli, ukládány samostatně. Při spolupráci s třetí stranou nesmí Nabyvatelé žádným negativním způsobem ovlivňovat realizaci a bezpečnost transakcí, které mají být zpracovány SPS.

3.2.7 Používání log produktů

Obchodník je povinen jasně prezentovat loga produktů, získaná od SPS. Kromě toho je Obchodník povinen získat písemný souhlas SPS s dokumenty, které připravil, a to ještě před jejich vytištěním či jakýmkoli publikováním (např. na Internetu), pokud tyto dokumenty obsahují loga SPS nebo výslovně uvádějí SPS.

4 Systém vyrovnání a autorizace SPS

4.1 Obecně

SPS provozuje a podporuje systém z technického, organizačního a administrativního hlediska.
Obchodník nebude mít právo na to, aby byl systém neustále k dispozici a v činnosti bez přerušení. SPS neposkytuje v tomto ohledu žádnou záruku. SPS bude oprávněn přerušit – dle svého rozumného posouzení – provoz systému, pokud bude považovat takové přerušení za nezbytné z nezbytných podstatných důvodů, jako jsou například úpravy a aktualizace systému, přerušení, riziko zneužití.
SPS si vyhrazuje právo provádět technické nebo organizační změny či doplňky do systému. Pokud tyto přinesou modifikace do infrastruktury, Obchodník je bude implementovat v souladu s pokyny od SPS na své vlastní náklady. Obchodník je rovněž povinen akceptovat úpravy a aktualizace systému, především za účelem zvýšení standardů bezpečnosti, které provádí SPS a dodavatelé systému/infrastruktury nebo výrobci terminálů.

4.2 Autorizace

Pokud není výslovně dohodnuto jinak, Obchodník je povinen získat oprávnění od SPS pro jakoukoli formu akceptace karet prostřednictvím postupu, specifikovaného SPS. To se nevztahuje na výjimky, výslovně schválené SPS (např. přijímání bezkontaktní karty pomocí offline transakcí).
Obchodník potvrzuje, že v kontextu autorizačního postupu si lze pouze ověřit, zda karta není blokovaná a zda nebyl překročen nějaký limit. Udělená autorizace tedy nedává Obchodníkovi jakýkoli nárok na proplacení transakce od SPS.

4.3 Zpracování transakce a vyrovnání

Transakce, dodané Obchodníkem, jsou zpracovány a vyrovnány systémem. Výsledné nároky na úhrady jsou započteny ve prospěch Obchodníka a banka SPS dostane pokyn, aby převedla splatnou částku do finanční instituce Obchodníka.

4.4 Webová služba "myPortal"

Tyto všeobecné obchodní podmínky platí pro služby, které nabízí SIX Payment Services (Europe) S.A. (dále jen "SPS") pod názvem "myPortal". Tyto služby zahrnují elektronické poskytování zpráv o vrácené úhradě, informací o transakci a terminálu, stejně jako zpráv a funkcí samoobslužnosti v souvislosti s přijímáním bezhotovostních plateb.
Obchodník musí pro SPS specifikovat osoby, kterým budou poskytnuta přístupová práva k oblasti správy Platformy myPortal. Personalizované přihlašovací údaje (dále jen „Přihlašovací údaje") poskytnuté ze strany SPS tyto osoby opravňují k provádění změn nakoupených služeb a konfigurace jménem Obchodníka.
Obchodník odpovídá za řádnou ochranu Přihlašovacích údajů před přístupem neoprávněných třetích osob. Kromě toho se pravidelně mění hesla. Jakákoli osoba, která se identifikuje vůči SPS jako uživatel Přihlašovacích údajů, se považuje za osobu, které dal Obchodník svolení s používáním Platformy myPortal. SPS Přihlašovací údaje pouze ověřuje, žádné další prokazování platnosti se neprovádí.
Jestliže existuje důvod k podezření, že k Přihlašovacím údajům získaly přístup neoprávněné třetí osoby, musí Obchodník neprodleně požádat SPS (kontaktní údaje viz www.six-payment-services.com/contact) o zablokování Přihlašovacích údajů. Obchodník je odpovědný za veškeré

kroky učiněné třetími osobami používajícími Přihlašovací údaje jako za své vlastní jednání.
Obchodník má přístup k datům uloženým na platformě myPortal po dobu minimálně šesti měsíců. SPS však není odpovědná za pravost a neměnnost dat po jejich stažení, zaznamenání a uložení Obchodníkem.

5 Přijetí karty

5.1 Povinnosti Obchodníka

5.1.1 Obecné povinnosti

Bez ohledu na částku, o kterou se jedná, Obchodník je povinen přijímat všechny karty dohodnutých značek a všechny typy karet (kreditní, debetní nebo předplacené karty) jako platební prostředek za zboží a/nebo služby. Výjimkou z této povinnosti jsou komerční obchodní karty (Commercial Cards), vydávané v rámci EEA – pokud jsou v zemi vydání karty uplatňována ustanovení předpisu (EU) 2015/751 – a také karty z kartového platebního systému třetí strany.
Obchodníci, kteří nepřijímají všechny typy karet dohodnutých značek, oznámí tuto skutečnost držiteli karty, a to jasně, nezpochybnitelně a současně budou držitele karty také informovat o ostatních typech karet téže značky- to vše v každém případě před provedením transakce. Při prezenční transakci musí být tato informace jasně uvedena u vstupu a současně také na pokladně. Při distanční transakci musí být tato Informace zobrazena na webovém obchodě Obchodníka či na jiném elektronickém či mobilním médiu.
Ve všech případech v kontextu použití platí, že Obchodník

- nebude dělit transakce mezi několik karet nebo do několika částek na téže kartě; pokud
  - se nejedná u první platby o zálohu a u druhé o konečnou platbu za službu nebo zboží, které jsou dodány později,
  - se nejedná o splátkovou platbu, které splatnost a jednotlivé částky jsou písemně dohodnuty mezi prodejcem a držitelem karty,
  - držitel karty nezaplatí část celkové částky kartou a zbývající částku kupní ceny v jiné formě (např. hotovost nebo šek).
- nebude znevýhodňovat spotřebitelské karty vydané v EU ve srovnání s jinými způsoby platby, zejména nepožadovat příplatek za platbu.
- nebude zatěžovat kartu výměnou za hotovostní platby nebo poskytnuté úvěry; hotovostní platby (Cash Advance/hotovostní záloha, Purchase with Cash Back/nákup s vyplacením částky) vyžadují (tam, kde jsou k dispozici) doplňkovou dohodu;
- bude přijímat kartu za služby, které nemohou být poskytnuty okamžitě, pokud držitel karty obdrží písemnou informaci (také e-mailem), že služba bude poskytnuta později;
- nezmění/neopraví žádná data na stvrzence poté, co byla podepsána; pokud je vyžadována oprava, je třeba vydat novou stvrzenku;
- přijme očekávaná opatření Obchodníka pro prevenci zneužití karty a neprodleně oznámí SPS jakékoli podezření na zneužití.

5.1.2 Speciální povinnosti pro akceptaci Alipay

Smluvní partner se v rámci akceptace Alipay zavazuje poskytnout SPS následující marketingové údaje:

- ID smluvního partnera;
- druh podnikání (jídlo, nákupy, služby, jiné);
- jméno, adresa a otevírací doba každého prodejního místa;
- popis prodejních míst.

Toto umožní smluvnímu partnerovi propagovat své podnikání na platformě Alipay a jsou předpokladem pro akceptaci Alipay.

5.2 Vyloučení akceptace karty

Obchodník nesmí přijmout karty za

- transakce, které zahrnují zboží a/nebo služby, které nejsou nabízeny nebo poskytovány Obchodníkem, ale třetí stranou (zákaz sub-získávání);
- transakce, které neodpovídají dohodnutým sektorovým kategoriím: musí být uzavřen dodatečný Smluvní modul za účelem realizace transakcí mimo sektorové kategorie, specifikované ve Smluvních modulech;
- transakce, které jsou nelegální nebo nemorální v jeho zemi, v místě přijetí a/nebo dle zákona, platného pro zákonné transakce s držitelem karty nebo které vyžadují oficiální schválení, které Obchodník nemá;
- transakce, přiřaditelné do sektoru zábavy pro dospělé (pornografie, erotika), tabáku, farmaceutik, her a hráčství nebo aukcí; transakce v těchto sektorových kategoriích mohou být prováděny pouze na základě dodatečné smlouvy;
- transakce, používané k dobití jiných platebních prostředků (např. předplacené karty, dárkové karty nebo elektronické peněženky či elektronická řešení); provádění těchto transakcí požaduje uzavření dodatečné smlouvy.

5.3 Akceptace karty v prezenčních transakcích

Při přijímání karet na základě elektronického provádění prostřednictvím hardwarových terminálů Obchodník zajistí, aby mohlo být čtení dat karty a tam, kde je to nezbytné i zadávání autentizace (např. zadáním PIN kódu), provedeno osobně držitelem karty na terminálu – tohoto se nesmí účastnit ani Obchodník ani žádná třetí strana.
Pokud terminál nevyžaduje autentizaci (např. zadáním PIN kódu), musí být stvrzenka, generovaná terminálem, v každém případě vlastnoručně podepsána držitelem karty na zvláštním řádku, určeném pro podpis. Při používání mPOS terminálu se držitel karty podepisuje přímo na obrazovku mobilního koncového zařízení. Následující platí pro UnionPay transakce: Kód PIN/kombinace šesti číslic je vyžadován pro každou transakci. Kromě toho musí být každá stvrzenka podepsána držitelem karty.
Pro bezkontaktní transakce se platný bezpečnostní standard řídí prostřednictvím hardwarového terminálu. Pokud to bezpečnostní parametry, uložené na kartě a/nebo hardware terminálu umožní, není podle technických regulačních standardů vydaných Evropskou komisí v rámci Směrnice o platebních službách vyžadována autentizace (např. zadáním PIN kódu). Jinak bude po držiteli karty vyžadováno, aby se autentizoval např. zadáním PIN kódu.
Pokud je pro akceptaci karty vyžadován podpis držitele karty, smí Obchodník přijmout kartu pouze pokud

- je předložena v průběhu platnosti, která je na ní vytištěna;
- nejde o rozpoznatelný padělek;
- karta má všechny relevantní bezpečnostní prvky; a
- byla podepsána držitelem karty.

Dále platí, že pro transakce, které jsou potvrzovány podpisem, musí Obchodník zajistit, aby

- držitel karty vlastnoručně podepsal stvrzenku v jeho přítomnosti;
- podpis na papírové stvrzence nebo obrazovce (pro mPOS terminály) odpovídal podpisu na zadní straně karty; a
- poslední čtyři číslice z čísla karty byly shodné s posledními čtyřmi číslicemi, vytištěnými na stvrzence.

V případě pochybností Obchodník zkontroluje identitu držitele karty na základě průkazu totožnosti (kontroluje, zda se shoduje jméno a příjmení) a uvede poznámku, že identifikační údaje na průkazu totožnosti a na kartě byly porovnány a ověřeny. Tato (mPOS terminály) poznámka musí být zapsána s odkazem na odpovídající ID transakce. U některých karet UnionPay není jméno držitele karty a doba její platnosti uvedeno na kartě. V těchto případech není Obchodník povinen provádět kontroly s ohledem na dobu platnosti karty a průkaz totožnosti držitele karty.
Pokud držitel karty nemá možnost autentizace (např. držitel karty zapomněl PIN kód nebo systém nedovoluje žádná další zadání PIN kódu), karta nesmí být přijata v souladu s ochrannými postupy, popsanými v kapitolách 11.2 a 11.3.

5.4 Akceptování karty v distančních transakcích

5.4.1 Obecně

Pro provádění distančních obchodních transakcí musí Obchodník vždy získat jméno, příjmení a adresu bydliště držitele karty a také číslo karty a platnost karty nebo, si nechat potvrdit u předem uložených údajů, a ověřit si věrohodnost daných informací; to platí především v případě odlišné adresy dodání a adresy bydliště. Obchodník musí uvést jméno společnosti používané v internetovém obchodě na všech dokumentech předávaných držiteli karty (např. objednávka, potvrzení dodávky a transakce, faktura).

5.4.2 Bezpečná e-komerce v internetovém obchodě (3-D bezpečnostní procedura)

Tím, že si ověří držitele karty v rozsahu takzvaných "bezpečných" elektronických obchodních transakcí, může Obchodník snížit riziko nezákonných transakcí následně rozporovaných držitelem karty. Podle národních zákonů pro realizaci Směrnice o platebních službách se musí Obchodník postarat o to, aby se mohl držitel karty autentizovat. Za tímto účelem je do Obchodníkova e-shopu integrován virtuální terminál s přípojkou (dále označován jako "MPI"). Tento virtuální terminál lze získat od SPS nebo jiného poskytovatele platebních služeb s certifikací dle PCI DSS. Terminál MPI je vyžadován pro provádění transakcí v souladu s 3-D bezpečnostními standardy kartových společností (např. "Verified by Visa", "Mastercard SecureCode" nebo "ProtectBuy"). V průběhu transakce naváže MPI kódované spojení se serverem vydavatele karty a ověří autentizační údaje držitele karty pro bezpečné internetové transakce, což umožňuje ověření a následné schválení transakce vydavatelem karty. Výjimky v souvislosti s autentizací držitele karty jsou možné podle technických regulačních standardů vydaných Evropskou komisí: SPS se postará o to, aby mohl Obchodník z těchto výjimek pokud možno profitovat.
Transakce e-komerce, které jsou uskutečněny bez MPI (např. ruční zadání údajů karty na virtuálním terminálu) jsou povoleny pouze ve výjimečných případech a jsou spojeny s vyšším rizikem zpětného zúčtování odměny v souladu s bodem 10.3.

5.4.3 Distanční transakce, realizované poštou, telefonem nebo faxem (telefonické/poštovní objednávky)

Pro přijímání karet při "telefonických/poštovních objednávkách" je zapotřebí použít certifikovaný virtuální terminál. Obchodník musí zničit všechny

ručně zaznamenané údaje z karty (především číslo karty, datum platnosti a verifikační číslo karty) poté, co byla transakce provedena.
Poštovní a telefonické objednávky bez MPI a 3-D bezpečné procedury. Proto je riziko zpětného účtování úhrady dle sekce 10.3 vždy vyšší.

5.5 Realizace kreditů
Pokud má být transakce plně nebo částečně refundována držiteli karty poté, co byla provedena, Obchodník vydá kredit na tutéž kartu. Kredit může být realizován s ohledem na dříve vyrovnaný debet a částka kreditu nesmí překročit původní strženou částku.
Při elektronické realizaci bude kreditní transakce iniciována a vytištěna stvrzenka. Pro mPOS terminály, nabízené SPS, je Obchodník schopen vyžádat si následný úplný/částečný kredit pro transakci písemnou formou od Zákaznického servisu SPS.
Poté, co Obchodník realizoval kredit, je SPS oprávněn požadovat od Obchodníka splacení nebo započtení transakce dříve vyrovnané nebo vyplacené.
Pro akceptaci Alipay platí:
Alipay umožňuje technickou realizaci dobropisů ve lhůtě do 365 dnů. Po skončení této lhůty již není dobropis možný. Smluvní partner zajistí, aby byl uživatel Alipay informován v okamžiku transakce o 365-denní lhůtě pro dobropis tím, že poskytne příslušné podmínky zákaznických služeb nebo vhodným písemným oznámením.

6 Stvrzenky
6.1 Obecně
V případě nedodržení povinností dle bodů 6.2 a 6.3 bude vyšší riziko zpětného účtování úhrady dle bodu 10.3.

6.2 Předání držiteli karty
V prezenčních transakcích si originální kopii stvrzenky, vytištěnou terminálem, ponechá Obchodník (“Stvrzenka pro obchodníka”). Obchodník předá kopii (“Stvrzenka pro zákazníka”) držiteli karty. Při používání mPOS terminálu je stvrzenka převedena na držitele karty prostřednictvím e-mailu, pokud je to vyžadováno.
V distančních transakcích poskytuje Obchodník držiteli karty písemné potvrzení o transakci.

6.3 Povinnost zachování bezpečnosti
Obchodník je povinen ukládat všechny originální papírové stvrzenky a kopie elektronických stvrzenek, všechna data o transakcích a každodenní uzávěrky (včetně dat o jednotlivých transakcích) a také veškerá další související data a dokumentaci na bezpečném místě, nejméně 36 měsíců od data transakce.
Elektronická data musí být uložena v kódovaném formátu a chráněna proti neoprávněnému přístupu. V tomto ohledu je Obchodník povinen dodržovat relevantní pokyny, vydané SPS (dle bodu 14.3).

7 Dodání transakce
7.1 Lhůty dodání
Obchodník je povinen dodat transakce SPS do 48 hodin po jejich realizaci.
Pro transakce, které přijdou do systému SPS později, než je stanoveno ve výše uvedených ustanoveních, si SPS vyhrazuje právo zamítnout Obchodníkovi nárok na úhradu či vymáhat/započíst úhrady dříve poukázané.
V distančních transakcích (bezpečná e-komerce, mailové/telefonické objednávky) bude Obchodník povinen předat transakce v průběhu 48 hodin, i pokud nebude schopen odeslat/dodat předmětné zboží okamžitě nebo okamžitě poskytnout službu.
Obchodník nese výhradní riziko, týkající se přenosu dat z infrastruktury Obchodníka do systému, provozovaného SPS, bez ohledu na to, zda jej provádí sám Obchodník nebo třetí strana, kterou pro tento účel najal.

7.2 Měna dodávky
Obchodník dodá transakce v měnách, stanovených ve Smluvním modulu.

7.3 Následné zadání
Za předpokladu, že Obchodník splní termín předání, uvedené v bodě 7.1, bude možné ručně znovu zadat ztracené, nesprávné nebo neúplně dodané transakce v případech, způsobených technickou poruchou přenosu dat či zpracování. Nesprávné zaúčtování (např. účtovaná částka je příliš vysoká či nízká) nemohou být znovu zadány.
Transakce, které jsou předány po více než 60 dnech (debetní karty) nebo 180 dnech (kreditní karty) nemohou být znovu zadány. Totéž platí pro transakce, jejichž údaje nejsou zadány do systému SPS.

8 Úhrada
8.1 Nárok Obchodníka na úhradu
SPS provede úhradu Obchodníkovi ve vztahu k dodané transakci – po stržení dohodnutých poplatků a na základě následné zpětné výplaty – v dohodnuté frekvenci úhrad. Detaily vyrovnání jsou uvedeny na potvrzení o úhradě.
O státních svátcích SPS nezpracovává žádné platby. Obchodník akceptuje jakákoli prodlení v převodech, vyplývající z výše uvedeného. Specifické svátky jiných zemí nebo regionální svátky mohou vést k dalším prodlením.

8.2 Účet pro přijímání plateb
Obchodník bude mít otevřený účet u finanční instituce na jméno společnosti nebo majitele za účelem přijímání plateb. Pro náležité zpracování je vyžadován IBAN a BIC daného účtu.
Obchodník potvrzuje, že pokud budou poskytnuty nesprávné nebo neúplné údaje o účtu, nemusí být převody/vklady na účet provedeny nebo může dojít k převodu na jiného příjemce. Veškeré náklady a poplatky za zjišťování nebo jiné související výdaje plně ponese Obchodník.
SPS bude připisovat úhrady, vyplývající ze Smluvních modulů, na Obchodníka formou souhrnné platby. Pokud Obchodník požaduje převody pro každou značku karty, ponese veškeré dodatečné náklady, které v tomto ohledu vzniknou.

8.3 Měna úhrady
V zásadě platí, že úhrady jsou Obchodníkovi poukazovány v místní měně, platné v místě platného sídla Obchodníka. Pokud Obchodník požaduje úhradu v jiné měně, je měna, dodaná Obchodníkem konvertována přes EUR na požadovanou měnu úhrady. Platí mezinárodní směnné kurzy, specifikované SPS. Obchodník bude akceptovat směnné kurzy, aplikované SPS.

8.4 SEPA platební transakce
V případě, že má Obchodník v úmyslu využívat výhod platebních transakcí SEPA, zajistí, aby se finanční instituce, kterou si zvolil, účastnila SEPA platebních transakcí a měla účet v Eurech. Pokud nebudou tyto požadavky splněny, mohou vznikat vyšší poplatky za zpracování. Účet, vyhovující SEPA kritériím, může být používán jak pro přijímání úhrad, tak i pro výběr přímých úhrad mezi podniky SEPA.

8.5 Oznámení o úhradě a předběžné oznámení
Oznámení o úhradě je poskytováno Obchodníkovi ve formě, dohodnuté ve Smluvním modulu. V každém případě bude oznámení o úhradě dostupné ve webové aplikaci “myPortal”.
Obchodník bude písemně informovat SPS v průběhu 30 dnů od poskytnutí v rámci WebService nebo v případě jiných forem dodání po přijetí, o jakýchkoli námitkách ve vztahu k oznámení o úhradě; jinak bude oznámení o úhradě, včetně všech informací které obsahuje, považováno za správné a úplné a za schválené bez výhrad.
Pokud jsou reklamace vůči Obchodníkovi (např. v případě zpětných úhrad nebo záporného zůstatku) vyrovnány prostřednictvím SEPA bezhotovostní úhrady mezi subjekty, dostává Obchodník žádost o úhradu na zbývající částky ve formě předběžného oznámení. Bezhotovostní vyrovnání bude provedeno k avizovanému datu splatnosti. Pokud je k datu vyrovnání na účtu Obchodníka nedostatečná hotovost a je zahájena procedura zpětného zúčtování, dostane se Obchodník do prodlení od data zpětného účtování.

9 Poplatky
9.1 Obecně
Všechny poplatky, které má platit Obchodník SPS, jsou stanoveny ve Smluvním modulu. Tyto poplatky se stanou splatnými poté, co bude poskytnuta služba SPS a budou započteny v rozsahu úhrad a uvedeny na oznámení o vyrovnání (bod 8.1).
Pokud je dohodnuto použití plánu úhrady poplatků ve Smluvním modulu, verze platná při uzavření Smluvního modulu (je k dispozici na www.six-payment-services.com/downloads) tvoří nedílnou součást Smluvního modulu. Nároky Obchodníka vůči SPS mohou být započteny pouze s předchozím souhlasem SPS. SPS je oprávněn kdykoli započíst nároky vůči Obchodníkovi. Takové započtení nároků se bude řídit lucemburským právem pro finanční kolaterální dohody z 5.srpna 2005, ve znění pozdějších dodatků.

9.2 Poplatky „Interchange“
Obchodník může od SPS požadovat informace, týkající se částky interchange poplatků, a to písemně nebo se na ně podívat na www.six-payment-services.com/interchange.

9.3 Poplatky za platby třetí straně
Obchodník ponese poplatky za převod nebo poplatky za platby v cizí měně, účtované finanční institucí Obchodníka a tyto mu budou přímo účtovány po převedení platby. V případě zákonných změn a/nebo změn poplatků, účtovaných třetími stranami, si SPS vyžaduje právo změnit své postupy úhrady.

9.4 Porušení platby
Pokud započtení částek, které dluží Obchodník, nevede k jejich úplnému vyrovnání, SPS předá Obchodníkovi žádost o úhradu zbývající částky. Termín úhrady je 10 dnů; po jeho vypršení se Obchodník bez dalšího upozornění dostane do prodlení.
V případě, že se Obchodník dostane do prodlení, SPS bude oprávněn účtovat Obchodníkovi standardní úrok z prodlení v zákonné sazbě ze zbývající částky plus všechny náklady na upomínky a vymáhání dluhů.

9.5 Daně

Poplatky, specifikované ve Smluvních modulech za produkty a služby SPS jsou – pokud není specifikováno jinak – uváděny bez nepřímých daní (např. DPH), srážkových daní a dalších povinností. Všechny daně a povinnosti dle legislativy země Obchodníka, které jsou nebo mohou být v budoucnu splatné ve vztahu k plnění služeb, poskytovaných SPS v rozsahu Smluvních modulů, ponese Obchodník. V každém případě platí, že Obchodník je povinen dodržovat ustanovení, platná v jeho zemi ve vztahu k nepřímým daním (např. zpětné účtování), srážkovým daním a dalším povinnostem. Obchodník bude plně chránit SPS proti veškerým nárokům, vzneseným proti SPS třetími stranami.

10 Zpětné účtování a monitoring podvodů

10.1 Zpětné účtování (Chargeback)

Držitel karty a vydavatel karty jsou oprávněni vznést stížnost na transakci za předpokladu splnění předpokladů pro otevření postupu zpětné úhrady (chargeback), především při existenci důvodu pro zpětnou výplatu.
Pokud je otevřena procedura zpětného vyúčtování, Obchodní na žádost SPS předá SPS – do 10 dnů a prostřednictvím doporučeného dopisu – kopie všech stvrzenek a dokumentace (dle kapitoly 6), vhodné pro vyvrácení nároku na zpětné vyúčtování. Pokud nelze nárok na zpětné vyúčtování vyvrátit stvrzenkami, dodanými Obchodníkem, nebo pokud nejsou požadované stvrzenky dodány včas, je SPS oprávněn nárokovat transakce již vyplacené nebo tyto započítat formou kreditu obchodníkovi („zpětné zúčtování"). To platí i v případech, kdy nedochází k dodání/poskytnutí zboží nebo služeb přímo smluvním partnerem, nýbrž třetí osobou, například pokud smluvní partner vystupuje jako zprostředkovatel nebo agent těchto třetích stran.
Pokud obchodník po otevření procedury zpětného vyúčtování chce realizovat kredit ve prospěch karty, použité v rozporované transakci, bude informovat Oddělení zpětného účtování v SPS o tomto svém záměru. Po schválení ze strany SPS Obchodník zrealizuje kredit v souladu s ustanovením, uvedeným v bodě 5.5.
V průběhu procedury zpětného vyúčtování se Obchodník zdrží jakýchkoli právních postupů proti držiteli karty.

10.2 Důvody zpětného účtování v presenčním obchodování

Ve vztahu k akceptaci karty v prezenčním obchodování bude mít SPS právo zpětného účtování především tehdy, pokud držitel karty zpochybní transakci a Obchodník nemůže prokázat, že karta byla přítomna v místě prodeje v okamžiku transakce. To platí především tehdy, pokud Obchodník
– při přijímání EMV karet načítá data karty prostřednictvím "non-EMV terminálu" (bez čipové čtečky EMV); nebo
– nečte data karty z EMV čipu nebo magnetického pásku, ale zadává je manuálně prostřednictvím klávesnice terminálu (v souladu s postupy, uváděnými v kapitolách 11.2 a 11.3.).

Tento seznam důvodů pro zpětné účtování není úplný.

10.3 Důvody zpětného vyúčtování v distančním obchodování

Ve vztahu k akceptaci karty v distančním obchodování platí především následující důvody zpětného účtování:
– držitel karty zpochybní objednávku a/nebo přijetí zboží nebo služeb;
– držitel karty odmítne přijaté zboží jako vadné nebo jako odlišné od toho, které specifikoval v objednávce;
– držitel karty vypoví koupi zboží a/nebo služeb v rámci zákonné doby pro odstoupení od smlouvy;
– držitel karty uplatňuje nároky vůči Obchodníkovi či z jakéhokoli jiného důvodu odmítne splnit nároky, vyplývající z transakce;
– transakce byla realizována bez procedury 3-D Secure.

Tento seznam důvodů pro zpětné vyúčtování není úplný.

10.4 Monitorování podvodů

V kontextu monitorování podvodů je SPS oprávněn kdykoli vydat pokyn pro Obchodníka, zaměřený na prevenci případů podvodu (např. povinnost držitelů karet poskytnout ID). Tyto pokyny vstupují v platnost ihned poté, co je o nich Obchodník informován a Obchodník je povinen je plně dodržovat.
V případě odůvodněného podezření na podvod je SPS oprávněn zadržet úhrady Obchodníkovi do okamžiku vyjasnění podezření. Toto i nadále podléhá bodům 10.2 a 10.3. V případě vysokého počtu případů podvodu si SPS rovněž vyhrazuje právo ukončit Smluvní moduly s okamžitou platností.

10.5 Dodržování limitů

Každý měsíc Obchodník zajistí, aby byly pro dohodnuté značky karet dodržovány následující limity:
– poměr celkového objemu zpětných zúčtování plus kreditů k hrubému měsíčnímu obratu nepřekročí 2%;
– poměr počtu zpětných zúčtování plus kreditů k počtu transakcí za měsíc nepřekročí 1%.
– poměr celkového objemu transakcí zpětných zúčtování k hrubému měsíčnímu obratu nepřekročí 0,75%;
– poměr počtu podvodných transakcí k počtu transakcí za měsíc nepřekročí 3% a méně než 3 podvodné transakce.

Pokud je kterýkoli z těchto limitů překročen, je SPS oprávněn účtovat Obchodníkovi výdaje, specifické pro každý případ, za každé zpětné účtování/kredit/podvodnou transakci nad tyto limity. Dále je SPS oprávněn předat dále jakoukoli pokutu a/nebo poplatky za zpracování, uložené kartovými společnostmi, na Obchodníka, zadržet úhradu předaných transakcí až na 180 dnů a ukončit Smluvní moduly s okamžitou účinností/platností.

11 Funkční poruchy a nouzové postupy

11.1 Obecně

Mohou nastat následující funkční poruchy:
– Funkční porucha systému;
– Funkční porucha infrastruktury nebo terminálu;
– Funkční porucha karty (poškozená karta).

V případě funkčních poruch může Obchodník použít ruční nouzové postupy dle bodů 11.2 a 11.3. Obchodník akceptuje, že pro transakce, realizované nouzovými postupy, nese vyšší riziko zpětného účtování úhrady dle bodu 10.3.
Při použití nouzových postupů bude Obchodník v každém případě vyžadovat od držitele karty oficiální ID a porovná data z ID (příjmení a jméno) proti údajům na kartě. Po provedení nouzového postupu je Obchodník povinen okamžitě zničit všechna manuálně zapsaná data karty. Za žádných okolností si Obchodník nesmí nechat nebo ukládat verifikační číslo karty ani žádná data, načtená a uložená z magnetických pásků karet poté, co byla transakce schválena.
Neexistuje žádný nouzový postup pro transakce s Visa Electron, V PAY, Maestro a UnionPay, a ani na transakce dynamické konverze měn (DCC).

11.2 Nouzové postupy pro funkční poruchy systému/terminálu

Pokud plně či částečně selže systém či terminál Obchodníka, bude Obchodník autorizovat každou transakci se SPS po telefonu, dokud nebude chod systému obnoven/dokud nebude terminál opět funkční. Poté, co byla činnost systému obnovena, budou data transakce a také číslo oprávnění zadávány ručně Obchodníkem na terminálu, pomocí funkce "Platba schválena telefonem".
V případě funkční poruchy na mPOS terminálu není k dispozici žádný nouzový postup.

11.3 Nouzové postupy pro funkční poruchy karty

Pokud je funkční porucha výsledkem poškození karty, může Obchodník ručně zadat data karty na terminálu. Obchodník bude takové transakce předem autorizovat se SPS po telefonu. Ruční zadávání dat formou zápisu dat karty na terminálu musí být provedeno pomocí funkce "Ruční zadání dat karty". Terminálem vytištěnou stvrzenku musí vlastnoručně podepsat držitel karty.

12 Dodatečná ustanovení pro rezervace hotelů a pronájmů aut

Ve vztahu k přijímání kreditních karet pro rezervace hotelového ubytování či pronájmu auta bude Obchodník dále dodržovat ustanovení, uvedená na odpovídajícím listu "Garance hotelové rezervace s kreditní kartou"/"Hotelová rezervace platbou na místě pomocí kreditní karty (Zálohový depozit pro hotel)"/"Rezervace pronájmu auta s kreditní kartou". Daný datový list tvoří nedílnou součást Smluvního modulu.

13 Dodatečná ustanovení pro dynamickou konverzi měny (DCC)

Služba dynamické konverze měny (DCC) umožňuje dynamickou směnu měny na terminálu. Přehled dostupných cizích měn si lze vyžádat od SPS.
Obchodník zajistí, aby držitel karty ve všech případech nezávisle zvolil, zda si přeje provést transakci v měně karty (DCC transakce) nebo v místní měně.
Pro DCC transakce bude pro držitele karty platit směnný kurs zahraniční měny (místní měna/měna karty), specifikovaný SPS pro akceptované zahraniční karty. Obchodník bude akceptovat směnný kurs, specifikovaný SPS.
SPS bude oprávněn – dle svého rozumného rozhodnutí – přerušit provádění služby DCC nebo jednotlivých zahraničních měn, pokud bude takové přerušení považovat za nezbytné z vážných a podstatných důvodů, jako jsou například závady, riziko zneužití či mimořádná nestálost na trzích zahraničních měn.

14 Ochrana dat

14.1 Obecně

Smluvní strany jsou povinny dodržovat ustanovení odpovídajících platných zákonů ve vztahu k ochraně dat.
V tomto ohledu je Obchodník povinen požadovat, aby jeho personál, stejně tak jako veškeré jím najaté třetí strany, které mají přístup k důvěr-

ným či jinak chráněným datům (především údajům o kartě), splňovaly ustanovení o ochraně dat a také bezpečnostní požadavky PCI DSS (dle bodu 14.3).

14.2 Zpracování a přenos dat

Obchodník výslovně opravňuje SPS, a to předtím, než Smluvní modul vstoupí v platnost a po celou dobu jeho trvání, aby získával veškeré informace včetně osobních údajů, které považuje SPS za důležité ve vztahu ke Smluvnímu modulu a plnění služeb zde stanovených. Dále je SPS oprávněn přenášet data ze Smluvních modulů a Rámcové smlouvy v rozsahu, vyžadovaném pro třetí strany, jmenované SPS, aby zhodnotil potenciální rizika nebo zpracovával transakce. K tomu jsou osobní údaje předávány karetním organizacím pro marketingové účely. Obchodník bere na vědomí, že data (především hlavní data a transakční data), vztahující se k uzavření a plnění Smluvních modulů, jsou zpracovávána ve Švýcarsku a v zemích EU. V rámci akceptování Alipay bere smluvní partner kromě toho na vědomí, že kmenové, transakční a marketingové údaje jsou zpracovávány společností Alipay také v Čínské lidové republice.

SPS ve své funkci kontrolora zpracování dat shromažďuje a zpracovává osobní údaje Obchodníka a/nebo dalších fyzických osob, napojených na organizaci Obchodníka, aby zajistil následující:

- identifikace Obchodníka a/nebo fyzických osob, spjatých s organizací Obchodníka;
- správná realizace Smluvních modulů, a
- dodržení zákonných závazků.

SPS přijme odpovídající technická opatření a zavede náležitou organizaci tak, aby zajistil ochranu takových osobních údajů a bude je zpracovávat pro výše uvedené účely a v souladu s platnými zákony o ochraně dat, včetně Směrnice o platebních službách a národních prováděcích zákonů a od 25. května 2018 Obecného předpisu o ochraně dat (EU) 2016/679. Obchodník s tímto souhlasí a poskytuje svůj výslovný souhlas se zpracováním dat.

Obchodních a dle situace i fyzické osoby, napojené na organizaci Obchodníka, mají právo na přístup ke svým osobním údajům a také právo dané údaje opravovat a mazat a od 25.května 2018 také právo na přenosnost osobních údajů v souladu s platnými zákony.

Obchodník je povinnen zavést veškerá opatření a informovat všechny fyzické osoby spojené se svou organizací o zpracování osobních dat ve smyslu významu tohoto oddílu a zajistit souhlas se zpracováním těchto osobních dat ve formě požadované příslušným zákonem.

14.3 PCI DSS norma pro bezpečnost dat

Údaje o kartě (především čísla karet, data platnosti) budou chráněny proti ztrátě a přístupu neoprávněných třetích stran. Ustanovení kartových společností o bezpečnosti dat, která musí být v tomto ohledu splněna, jsou definována v normě PCI DSS. V tomto ohledu bude Obchodník vždy dodržovat a kompletně plnit aktuálně platnou verzi "bezpečnostních norem PCI DSS pokynů pro shodu", vydaných SPS, která tvoří nedílnou součást těchto VOP. Především je Obchodník povinen provádět certifikační opatření, např. sebe-hodnotící dotazník, a potvrdí SPS dodržování PCI DSS ze své strany.

V případě, že by byla data karty zcizena nebo pokud by existovalo podezření, že byla data karty zcizena, Obchodník bude okamžitě informovat SPS. V takovém případě Obchodník výslovně opravňuje SPS, aby zmocnil společnost, akreditovanou kartovými společnostmi pro provádění auditu k vytvoření takzvané "PCI Zprávy o auditu". Ta bude zahrnovat prozkoumání okolností, za nichž nastala škoda a ověření, zda Obchodník splnil PCI DSS. Obchodník je povinen plně spolupracovat s auditorskou společností; především poskytne auditorské společnosti neomezený přístup do svých prostor a své infrastruktury. Poté, co byla vytvořena Zpráva o auditu PCI Audit Report, Obchodník na své vlastní náklady dokonale vyřeší všechny zjištěné bezpečnostní závady, a to v termínu, oznámeném SPS. Pokud šetření ukáže, že nebyly splněny bezpečnostní normy v souladu s PCI DSS v okamžiku, kdy byla data zcizena, náklady na vytvoření Zprávy o auditu PCI Audit Report ponese rovněž Obchodník.

SPS bude oprávněn předat veškeré nároky na škodu, předložené kartovými společnostmi Obchodníkovi a/nebo ukončit Smluvní modul s okamžitou platností, pokud Obchodník nesplňuje PCI DSS nebo pokud Obchodník na požádání nepotvrdí, že splňuje PCI DSS. Toto bude stejně platit i v případě, kdy byla data karty ukradena nebo když existuje podezření, že byla data ukradena.

15 Odpovědnost

Bez ohledu na doplňková zákonná ustanovení, a pokud není výslovně stanoveno jinak, Obchodník bude odpovědný především za škody, které SPS utrpí v důsledku toho, že výše uvedený nebo jakákoli jiná jím zjednaná třetí strana, nesplní své povinnosti, a to především v technickém, organizačním a administrativním ohledu. SPS je především oprávněn přenést na Obchodníka jakékoli možné nároky na škody, vyplývající ze zaviněného porušení povinnosti Obchodníka nebo jakékoli jím zjednané třetí strany a stejně tak předat jakoukoli pokutu a/ nebo poplatky za zpracování, uložené kartovými společnostmi nebo jakékoli další výdaje, vztahující se k dané záležitosti. Obchodník bude plně chránit SPS před veškerými závazky v tomto ohledu a ponese odpovědnost za takové nároky a veškeré související dodatečné výdaje, spjaté s případem.

Pokud není výslovně regulováno jinak, SPS či jakákoli jiná jím najatá strana, ponese odpovědnost v případě úmyslného chybného chování či hrubé nedbalosti v souladu se zákonnými ustanoveními.

Odpovědnost každé smluvní strany za zaviněné poškození na životě, těle nebo zdraví a také zákonná odpovědnost za produkt zůstávají nedotčeny.

16 Oznámení

Veškerá oznámení budou vydávána v písemné formě, pokud nebyla jiná forma výslovně dohodnuta ve Smluvním modulu. Písemná forma zahrnuje i elektronicky přenášené zprávy (např. prostřednictvím e-mailu nebo prostřednictvím platformy, poskytnuté SPS v rámci servisu).

17 Modifikace a dodatky do Smluvních modulů, včetně poplatků

Modifikace a dodatky do Smluvních modulů, především do VOP a dalších nedílných součástí, musí být provedeny v písemné formě (a také v elektronické formě), aby vstoupily v účinnost.

SPS si vyhrazuje právo modifikovat či provádět dodatky do Smluvních modulů, především do VOP a dalších nedílných součástí, stejně jako i poplatky, a to kdykoli. Tyto modifikace či dodatky budou oznámeny Obchodníkovi písemně alespoň 60 dnů před vstupem v platnost, ledaže jsou tyto změny, resp. doplňky předepsány ze zákona a vyžadují kratší lhůtu. Pokud není Obchodník ochoten akceptovat oznámenou modifikaci či dodatek, bude oprávněn ukončit Smluvní modul, dotčený modifikací či dodatkem, a to doporučeným dopisem v průběhu 30 dnů po obdržení oznámení o modifikaci nebo dodatku, s účinností k okamžiku vstupu modifikace či dodatku v platnost. Pokud Obchodník opomene ukončení, bude tato skutečnost považována za akceptaci modifikace nebo dodatku.

Přijetí bezpečnostních opatření v souladu s ustanovením bodu 2.1.4, odst. 3, provádění změn v systému v souladu s bodem 4.1, odst. 3 a modifikace poplatků v rámci dohodnutého rozsahu plateb, nejsou považovány za modifikace ve významu tohoto bodu a nepředstavují tedy důvod pro ukončení.

18 Vstoupení v platnost, doba trvání a ukončení

18.1 Vstoupení v platnost

V zásadě vstupuje Smluvní modul v platnost poté, co SPS odešle potvrzení o aktivaci Obchodníkovi. Pokud ovšem Smluvní modul explicitně předpokládá podepsání ze strany SPS, Smluvní modul vstoupí v platnost poté, co bude podepsán oběma Smluvními stranami.

18.2 Doba trvání

Smluvní modul je uzavírán na dobu neurčitou.

18.3 Řádné ukončení

Smluvní modul může být ukončen ke konci měsíce doporučeným dopisem. Pokud je Smluvní modul ukončen Obchodníkem, výpovědní lhůta je jeden měsíc. Pokud je ukončen ze strany SPS, platí dvouměsíční výpovědní lhůta.

Právo Obchodníka na ukončení dle bodu 17 a právo na okamžité ukončení z náležité příčiny Smluvních stran dle bodu 18.4 zůstává vyhrazeno.

Oznámení o ukončení jednoho Smluvního modulu nezpůsobí ukončení ostatních zbývajících smluvních modulů. Pokud už neexistují žádné další smluvní moduly, ukončení posledního/jediného Smluvního modulu automaticky vede k ukončení Rámcové smlouvy.

18.4 Mimořádné ukončení

Pokud existuje náležitá příčina, Smluvní strany budou oprávněny kdykoli ukončit Smluvní moduly s okamžitou účinností. Náležitá příčina zahrnuje především následující:

- závažná či opakovaná porušení ustanovení Smluvního modulu některou ze Smluvních stran;
- opakované stížnosti/vrácené platby a/nebo transakce, nahlášené vydavateli karet jako podvodné (dle bodu 10.2);
- jiné nesoulady v uskutečněných transakcích;
- významná změna vlastnické struktury a kontroly nad Obchodníkem
- zahájení insolvenčního řízení vůči aktivům Obchodníka.

Mimořádné ukončení Smluvního modulu o akceptaci karet opravňuje SPS okamžitě zrušit všechny existující smluvní moduly, Okamžité ukončení všech smluvních modulů vede k automatickému zrušení Rámcové smlouvy.

18.5 Automatické ukončení

Všechny existující Smluvní moduly jsou automaticky ukončeny bez nutnosti písemného oznámení, pokud Obchodník nedodá žádnou transakci po dobu 2 let.

Automatické ukončení Smluvních modulů o akceptaci karet vede také k automatickému ukončení rámcové smlouvy.

18.6 Důsledky ukončení smlouvy

Závazky, vyplývající z bodů 6.3 (Závazek bezpečného uložení), 14 (Ochrana dat), 15 (Odpovědnost), 18.6 (Důsledky ukončení smlouvy), 19 (Důvěrnost), 20.3 (Zákaz postoupení) a 20.7 (Rozhodné právo a místo jurisdikce), zůstanou v platnosti po ukončení Smluvního modulu.
Po ukončení Smluvního modulu odstraní Obchodník veškeré reference na odpovídající služby SPS, viditelné pro zákazníky.
Po oznámení o ukončení Smluvního modulu, je SPS oprávněn a to s účinností ihned, zadržet kompenzace pro Obchodníka na dobu 180 dnů po datu ukončení Smluvního modulu, aby započetl všechny následné nároky, a to především zpětné úhrady, proti těmto odměnám.
Pokud je proti obchodníkovi zahájeno trestní či jiné zákonné řízení, nebo pokud proti němu byla vznesena obvinění, vyhrazuje si SPS právo zpozdit převod kompenzací alespoň do okamžiku, kdy bylo dané řízení ukončeno.

19 Důvěrnost

Smluvní strany se vzájemně zavazují držet v tajnosti dohodnuté smluvní podmínky a také veškeré informace, dokumentaci, data a postupy zpracování – označené nebo identifikovatelné jako důvěrné nebo takové, které nejsou veřejně ani obecně přístupné – o kterých se dozví při plnění Smluvních modulů a také všechny dohodnuté podmínky; smějí je dát k dispozici třetím stranám pouze s předchozím písemným souhlasem druhé Smluvní strany. To nebrání žádné ze Smluvních stran v prozrazení důvěrných informací, pokud to představuje povinné naplnění zákonných ustanovení.

20 Závěrečná ustanovení

20.1 Právo vydávat pokyny SPS

Obchodník je povinen plnit technické, organizační a administrativní pokyny a instrukce, vydané SPS a také dodavateli terminálu a infrastruktury.

20.2 Zprostředkovatelská činnost SPS

SPS rovněž působí jako prostředník pro ostatní vlastníky a poskytovatele infrastruktury a při této činnosti uzavírají své smlouvy pod svým jménem, na své riziko a na svůj účet. Smluvní strany pro služby, poskytované tímto způsobem, jsou jednotlivý poskytovatel služeb a Obchodník.

20.3 Zákaz postoupení

Obchodník může postoupit kterékoli ze svých práv nebo povinností, kterými disponuje, vůči a ve vztahu k SPS, pouze s předchozím písemným souhlasem SPS.

20.4 Účast třetích stran/Postoupení na společnosti ve skupině

SPS si vyhrazuje právo převést plnění svých smluvních závazků na třetí strany, a to kdykoli, aniž by musel informovat Obchodníka.
SPS je oprávněn postoupit Smluvní modul na jiné společnosti ve Skupině. V takovém případě musí být Obchodník vhodně informován.

20.5 Zřeknutí se práv

Pokud nejsou jakákoli práva, vyplývající ze Smluvních modulů, zajištěna ze strany SPS, pak toto žádným způsobem nepředstavuje zřeknutí se těchto práv, pokud SPS nevydal výslovné písemné prohlášení o zřeknutí se v tomto ohledu.

20.6 Klauzule o oddělitelnosti

Pokud bude ustanovení Smluvních modulů (včetně poplatků) prohlášeno za neplatné, zbývající ustanovení tímto nebudou dotčena a budou sepsána takovým způsobem, jako kdyby byl daný Smluvní modul uzavřen bez neplatného ustanovení. Totéž se vztahuje na jakákoli smluvní opomenutí.

20.7 Rozhodné právo a místo jurisdikce

Všechny právní vztahy mezi Obchodníkem a SPS, vznikající z Rámcové smlouvy a všech uzavřených Smluvních modulů, podléhají lucemburským zákonům, s výjimkou Konvence SN o obchodu. Výhradním místem jurisdikce je Lucembursko.

20.8 Postup při mimosoudním řešení sporů

CSSF může řešit mimosoudně spory týkající se práv a povinností podle hlav III a IV Směrnice o platebních službách a národních prováděcích předpisů, pokud tato práva a povinnosti nebyla vyloučena v souladu s oddílem 1.2.
Další informace o CSSF a podmínky pro uplatnění naleznete na internetových stránkách CSSF http://www.cssf.lu/.

Worldline | SIX Payment Services

General Business Conditions for Card Acceptance

Version 11.2019 (EULUX)

1 Scope of application, abrogation of the legal provisions concerning payment services and definitions

1.1 Scope of application

These General business conditions (hereinafter "GBC") shall apply with respect to the products and services agreed between the Merchant and SIX Payment Services (Europe) S.A. (hereinafter "SPS") in the modules for card acceptance, e.g. "Card acceptance at the point of sale" or "Card acceptance for secure e-commerce and mail/phone order" (hereinafter individually "Contract Module" or collectively "Contract Modules").
These GBC form an integral part of the Contract Modules concluded. The Contract Modules concluded form an integral part of the "Framework agreement for cashless payments" (hereinafter "Framework Agreement") concluded between the Merchant and SPS.

1.2 Exclusion of the legal provisions concerning payment services

Pursuant to Art. 38 and Art. 61 of Directive (EU) 2015/2366 of 25 November 2015 ("Payment Services Directive") and the national transposition acts, the Contracting Parties agree to exclude the application of all non-mandatory provisions contained in the Payment Services Directive and the national transposition acts.

1.3 Definitions

The following definitions correspond to the use of the respective terms in these GBC.

Acquirer (SPS)	An acquirer enables its merchants to accept **cards** as a means of cashless payment (within **presence** or **distance business**) and ensures the processing of the **transactions** thus generated. To do so, it holds the licenses from the relevant **card schemes.**
Alipay platform	Alipay.com Co Ltd. (hereinafter known as "Alipay") operates an international e-payment platform. The collaborative agreement established between Alipay and SPS allows the Merchant to the accept cashless payments made by Alipay users.
Authorization	As part of the authorization process, the **card issuer** verifies whether a **card** is valid/not blocked and whether the transaction amount is within the set limit.
Card issuer	Company authorized by the **card scheme** for the issuing of **cards** to **cardholders.**
Card scheme	Licensor (such as Visa International, Mastercard International) for the issuance (issuing) and acceptance (acquiring) of **cards.**
Card verification code	Sequence of digits printed on a **credit card** (e.g. Visa [CVV2], Mastercard [CVC2]), which is used as an additional security feature in **distance business.**
Cardholder	Customer that purchases goods and/or services offered by the Merchant and pays for them on a cashless basis using a **card (transaction).**
Cards	Generic term for payment cards that are used to make cashless payments, i.e. **credit/debit cards.**
Chargeback	Reversal of a **transaction** delivered by the Merchant or of a reimbursement already credited as a result of a justified objection regarding the **transaction** by the **cardholder** or the **card issuer.** The claim to reimbursement on the part of the Merchant lapses.

116.1305.02/EULUX_EN/11.2019

Commercial Card	**Card** that is issued to companies, public sector entities or sole proprietors and is limited to a commercial or official use; whereby the **transactions** executed with the **card** are debited to the account of the company, the public sector entity or the sole proprietor.
Consumer Card	**Card** that is issued to natural persons and its use cannot be attributed to their commercial, corporate or professional activity; whereby the **transactions** executed with the **card** are debited to the account of the natural person.
Contactless (contactless card, contactless reader, contactless transaction)	Execution of **transactions** using "near field communication" (NFC), an international standard for the transmission of data via radio technology. This requires a **terminal** with a contactless reader and a **card** with an NFC-compatible chip, e.g. a Visa with "PayWave" or Mastercard with "PayPass" functionality. The chip data is read by holding the **card** to the contactless reader.
Credit	Full or partial refund of a **transaction** to the **card** that was originally debited.
Credit card	**Card** used to pay for goods and services whereby the **cardholder** is debited subsequently (e.g. Visa, Mastercard, Diners Club/Discover, UnionPay, JCB).
Debit card	**Card** used to pay for goods and services whereby the account of the **cardholder** is debited immediately (e.g. V PAY, Maestro).
Distance business	**Transactions** where neither the **cardholder** nor the **card** are physically present at the point of sale. In particular, these are carried out via the Internet, telephone, fax or letter.
Electronic execution	Execution and delivery of a **transaction** making use of a hardware or virtual **terminal** and the electronic delivery to the **system.**
EMV (EMV card, EMV chip, EMV terminal)	Specification for **cards** that are equipped with a processor chip as well as the associated chip card reader device (e.g. POS **terminals,** ticket machines, ATMs, fuel pump systems). EMV transactions are payments that are processed by having the card data read electronically at an EMV terminal from the processor chip of the **card.**
Infrastructure	The technical installations attributable to the Merchant for the acceptance of card payments by means of **electronic execution,** i.e. hardware or virtual **terminals** incl. peripheral devices such as cash registers and telecommunication equipment, routers, servers, etc.
Merchant Category Code (MCC)	Grid specified by the **card schemes** that enables the Merchant's business activities to be allocated by the **acquirer** to one or more sector categories.
mPOS terminal	Mobile card reader that is operated by means of a compatible mobile end device (e.g. smartphone or tablet) and an app.
Payment service provider (PSP)	A PSP offers payment solutions, e.g. an application (virtual **terminal**) that allows electronic means of payment to be accepted in a webshop.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a **PCI standard** which aims to ensure companies implement security standards.
PCI standards	Security standards for the card industry defined by the Payment Card Industry Security Standards Council (PCI SSC) whose application is imposed by the **card schemes.** More information can be found at www.pcisecuritystandards.org.
PIN (personal identification number)	Personal combination of digits that authenticates the **cardholder** as a legitimate user of a **card.**
Presence business	**Transactions** where both the **cardholder** and the **card** are physically present at the point of sale.
Receipt	Physical or electronic confirmation of the execution of a **transaction** generated by a **terminal** or in the webshop.
SEPA: Single Euro Payments Area	Standardized euro payments area in which cross-border payment transactions can be settled as efficiently as domestic payment transactions in the individual countries.
System	The electronic authorization and settlement system operated by SPS for processing **transactions.** The "myPortal" service pursuant to section 4.4 forms a part thereof.
Terminal (hardware or virtual terminal)	Hardware terminals are stationary or mobile devices used to execute **transactions.** Software components that allow hardware terminals to be connected to other peripheral devices (cash register systems, hotel reservation systems, fuel pump systems, etc.) are assigned to the hardware terminal. Virtual terminals are applications that allow **distance business** transactions to be executed. Software terminals are usually operated and sold by **payment service providers** (also SPS).
Transaction	Cashless payment procedure carried out by the Merchant by means of **electronic execution,** with the transaction data subsequently being processed by the **system** of SPS.

2 The Contracting Parties

2.1 The Merchant

2.1.1 Identification of the Merchant

SPS is obliged to identify the Merchant, its legal representatives and beneficial owners as well as to record the business activities of the Merchant and correctly allocate them to the corresponding sector category (MCC). For this purpose, the Merchant shall provide SPS with copies of the documents specified in the Framework Agreement as well as, on a case-by-case basis, with any further documents required.
SPS reserves the right, in conformity with the legislation related to the fight against money laundering and terrorist financing, to request, at intervals deemed adequate by SPS, the update of the documents submitted for the purpose of identifying the Merchant.
SPS is entitled to, for the purpose of its risk management, assess the business activities (products and services) and the financial situation of the Merchant. The Merchant shall provide SPS with the required information (including financial statements) within 10 days following SPS' request.

2.1.2 Affiliation of points of sale and webshops

The Merchant's points of sale and webshops can be affiliated to the Framework Agreement at the time the contract is concluded. The subsequent affiliation of points of sale and webshops shall be agreed separately by the Contracting Parties.

2.1.3 Sector allocation (Merchant Category Code, MCC)

The Merchant operates in the sector categories specified in the Contract Modules and sells goods and/or provides services to cardholders that are exclusively allocated to these sector categories. A separate contract module must be concluded for each sector category.

2.1.4 Changes on the part of the Merchant

Changes on the part of the Merchant (e.g. regarding its legal form, business activity, address, account details, legal representatives, beneficial owners, points of sale or infrastructure) shall be immediately communicated by the Merchant to SPS in writing. SPS is entitled to invoice the Merchant for the expenses associated with changes.
In the event of a significant change in the ownership structure and control of the Merchant, the latter is obliged to inform SPS in writing at least one month in advance. In such an instance, SPS shall be entitled to request that the Merchant's identification, pursuant to section 2.1.1, be updated. Should higher risks arise therefrom, SPS is entitled to terminate the Contract Modules with immediate effect. For as long as SPS is not informed in writing of a legal succession, it may credit all reimbursements with discharging effect to the previous Merchant.
If the Merchant's credit rating deteriorates considerably (e.g. the opening of insolvency proceedings), the Merchant shall inform SPS without delay. SPS shall be entitled, at its equitable discretion, to immediately take suitable measures, such as adjusting reimbursement terms, withholding reimbursements or demanding appropriate collateral. The Merchant shall be notified without delay of the measures taken.

2.2 SIX Payment Services (Europe) S.A.

SIX Payment Services (Europe) S.A. is a Luxembourg company ("Société Anonyme"), with its registered seat at 10, rue Gabriel Lippmann, L-5365 Munsbach (Luxembourg Commercial Register no. B144087). As a licensed payment institution (license no. 06/10) SPS is under the supervision of the Luxembourg Financial Supervisory Authority (Commission de Surveil-

lance du Secteur Financier/CSSF, 283, route d'Arlon, L-1150 Luxembourg). SPS holds the licenses from the card schemes that are necessary for acquiring.

3 Infrastructure of the Merchant

3.1 General

The Merchant shall be completely responsible for obtaining, operating and maintaining an infrastructure that is suitable for the electronic execution of card payments as well as for taking the technical security measures to prevent any misuse of the infrastructure; in particular compliance with PCI DSS pursuant to section 14.3. This shall also apply to changes to the infrastructure as a result of system adjustments on the part of SPS in accordance with section 4.1, para. 3.

Only terminals (hardware and/or virtual terminals) that have been certified in accordance with the applicable PCI standard and the requirements set forth by the card schemes may be used for the execution of card payments. EMV certification is a mandatory requirement for hardware terminals. Furthermore, certified terminals require approval, by one or more acquirers, in accordance with the country-specific requirements of the responsible body.

3.2 Obligations of the Merchant

3.2.1 General due diligence obligations

The Merchant is obliged to ensure through appropriate measures that no manipulation is possible, in particular no improper transactions, and that the terminals are protected against access by unauthorized third parties. The Merchant shall train its personnel in the correct handling and use of the infrastructure at adequate intervals, in particular upon its entry into operation. It shall also instruct its personnel about measures to be taken to prevent misuse and fraud.

3.2.2 Obligations regarding hardware terminals

The Merchant shall place all hardware terminals at the point of sale in such a way that the cardholder has direct access to the terminal (in particular the display, keypad and card reader) and cannot be observed in case a PIN entry is required.

3.2.3 Obligations regarding virtual terminals

The Merchant shall, with the appropriate level of care, protect the infrastructure used to operate virtual terminals, in particular the computers (including all related network components) and the data carriers that contain card data (particularly card numbers, expiry dates or transaction data).

3.2.4 Information obligation/Right to information

At the request of SPS, the Merchant shall provide information in writing on which terminals are in productive use. Furthermore, the Merchant authorizes SPS to obtain this information directly from the terminal manufacturers/software providers or any other infrastructure suppliers. The Merchant shall provide assistance to SPS in this respect.

The Merchant shall immediately notify SPS in writing of any changes relating to hardware terminals or its webshop, in particular any shutdowns, replacements or changes of location/URL.

3.2.5 Transaction routing through third parties

The Merchant shall be entitled to enter into an agreement with PCI DSS-certified third parties (such as payment service providers, network operators) which deliver transactions to SPS on behalf of the Merchant. SPS shall not refuse acknowledgement of such third parties unless for reasons of good cause. Any costs arising in relation to connecting the third party, in particular for activation, fees, delays and faults, shall be borne by the Merchant. SPS shall be entitled to invoice the Merchant for such costs and fees or to offset these against any reimbursements due for crediting to the Merchant.

The Merchant shall immediately notify SPS in writing of any changes in relation to transaction routing via third parties or if it switches the third party used. SPS shall be entitled to refuse such changes or such a switch of third party for good cause.

3.2.6 Card acceptance through multiple acquirers

If the Merchant simultaneously procures acquiring services from more than one provider, it must be ensured at all times that the transaction data relating to each acquirer is kept separate. Working with third-party acquirers must in no way negatively impact the execution and security of the transactions to be processed by SPS.

3.2.7 Use of product logos

The Merchant is obliged to clearly present the product logos received from SPS. In addition, the Merchant is obliged to obtain written consent from SPS for documents it has drawn up prior to printing or any publication (e.g. on the Internet) if these documents contain logos of SPS or specifically mention SPS.

4 Authorization and settlement system of SPS

4.1 General

SPS operates and supports the system in technical, organizational and administrative respects.

The Merchant shall have no right to the system being available at all times and operating without disruption. SPS provides no warranty in this respect. SPS shall be authorized to interrupt, at its equitable discretion, the operation of the system if it deems such an interruption to be necessary for imperative material reasons, for example system adjustments and updates, disruptions, risk of misuse.

SPS reserves the right to make technical or organizational changes or additions to the system. If these entail modifications to the infrastructure, the Merchant shall implement these in accordance with the instructions from SPS at its own cost. The Merchant is also obliged to accept the system adjustments and updates, in particular for the purpose of increasing security standards, carried out by SPS and the system/infrastructure suppliers or terminal manufacturers.

4.2 Authorization

Unless otherwise expressly agreed, the Merchant is obliged to obtain authorization from SPS for any form of card acceptance by means of a procedure specified by SPS. This does not apply to exceptions explicitly authorized by SPS (e.g. contactless card acceptance by means of offline transactions).

The Merchant acknowledges that within the context of the authorization procedure, it can only be verified whether a card is not blocked and no limit has been exceeded. An authorization granted therefore does not confer on the Merchant any claim to the reimbursement of the transaction by SPS.

4.3 Transaction processing and settlement

The transactions delivered by the Merchant are processed and settled by the system. The resulting claims to reimbursement are credited to the Merchant and the bank of SPS is instructed to remit the amount due to the Merchant's financial institution.

4.4 Web service "myPortal"

These general business conditions apply to the services offered by SIX Payment Services Ltd (hereinafter "SPS") under the name of "myPortal". They comprise the electronic provision of reimbursement notices, transaction and terminal information, as well as reports and self-service functionalities, in connection with the acceptance of cashless means of payment.

The Merchant must specify vis-à-vis SPS the individuals to be given access rights to the administration area of the myPortal platform. The personalized login credentials (hereinafter "login credentials") provided by SPS entitle them to make changes to the services purchased and to the configuration on behalf of the Merchant.

The Merchant is responsible for ensuring that the login credentials are adequately protected against access by unauthorized third parties. Furthermore, the passwords shall be changed on a regular basis. Any party that identifies itself to SPS using the login credentials, shall be considered as having been authorized by the Merchant to use the myPortal platform. SPS only verifies the login credentials; no further authentication is carried out.

If there are grounds to suspect that unauthorized third parties have gained access to the login credentials, the Merchant must ask SPS (contacts to be found at www.six-payment-services.com/contact) immediately to block the login credentials. The Merchant shall be liable for any actions taken by third parties using the login credentials as it is for its own actions.

The Merchant can access the data stored on the myPortal platform for a period of at least 6 months. However, SPS assumes no responsibility regarding the authenticity and immutability of data when downloaded, recorded or stored by the Merchant.

5 Card acceptance

5.1 Obligations of the Merchant

5.1.1 General obligations

Irrespective of the amount involved, the Merchant is obliged to accept all cards of the agreed card brands and agreed card types (credit, debit or prepaid card) as a means of payment for goods and/or services. Commercial Cards issued within the EEA – insofar as the provisions of the regulation (EU) 2015/751 are applied in the country of card issuance – as well as cards from a three-party card payment system are exempt from this rule.

Merchants that do not accept all card types of the agreed card brands shall communicate this to the cardholder clearly, unmistakably and at the same time as they inform the cardholder about the acceptance of other card types of the same card brand – in any case prior to the execution of the transaction. In presence business, this information is to be displayed clearly at the entrance as well as at the cashier's desk. In distance busi-

ness, this information is to be displayed within the Merchant's webshop or any other electronic or mobile medium.
In all cases, within the context of the acceptance, the Merchant shall
- not split a transaction across several cards or in several partial amounts on the same card, unless
  - it concerns an initial payment paid in advance and a second payment as the final payment for a service or good that was rendered or delivered at a later date;
  - it concerns an instalment the term and individual instalment amount of which has been agreed in writing between the retailer and the card holder;
  - the card holder pays one part of the total amount by card and the remaining purchase amount in another form (e.g. cash or cheque);
- not disadvantage Consumer Cards issued within the EU in comparison with other means of payment, in particular not request a surcharge for payment with the card;
- not debit the card in return for cash payments or loans granted; cash payments (Cash Advance, Purchase with Cash Back) require (where available) a supplemental agreement;
- only accept the card for services that cannot be provided immediately if the cardholder receives written information (also by e-mail) that the service will be provided subsequently;
- not change/correct any data on a receipt after it has been signed; if a correction is required, a new receipt must be issued;
- take the measures expected of a diligent merchant to prevent the misuse of cards and notify any suspicions of misuse to SPS immediately.

5.1.2 Special obligations for Alipay acceptance

For the purposes of Alipay acceptance, the Merchant undertakes to deliver the following marketing data to SPS:
- Merchant ID;
- Business category (food, shopping, services, other);
- Name, address and opening times of every point of sale;
- Description of points of sale.

These enable the Merchant to promote their business activities on the Alipay platform and are a requirement for Alipay acceptance.

5.2 Exclusion of card acceptance

The Merchant may not accept the card for
- transactions involving goods and/or services that are not offered or provided by the Merchant but by a third party (sub-acquiring prohibition);
- transactions that do not correspond to the agreed sector categories; an additional contract module must be concluded in order to execute transactions outside the sector categories specified in the Contract Modules;
- transactions that are illegal or immoral in its country, at the place of receipt and/or according to the law applicable to the legal transaction with the cardholder or that require an official authorization that the Merchant does not have;
- transactions attributable to the sectors adult entertainment (pornography, eroticism), tobacco, pharmaceuticals, gaming and gambling or auctions; transactions in these sector categories may only be executed based on a supplemental agreement;
- transactions used to load other means of payment (e.g. prepaid cards, gift cards or e-wallet solutions); the execution of these transactions requires a supplemental agreement.

5.3 Card acceptance in presence business

In electronic execution by means of hardware terminals, the Merchant shall ensure that the reading of the card data and, where necessary, authentication (e.g. by entering the PIN) can be carried out on the terminal by the cardholder in person – without this being observed by the Merchant or third parties.
If the terminal does not request authentication (e.g. by entering the PIN), the receipt generated by the terminal must in every case be signed personally by the cardholder on the signature line intended for this purpose. When using an mPOS terminal, the cardholder signs directly on the screen of the mobile end device. The following applies to UnionPay transactions: A PIN/six-digit combination of numbers is required for each transaction. In addition, each receipt must be signed by the cardholder. For contactless transactions, the applicable security standard is managed via the hardware terminal. If the security parameters saved on the card and/or hardware terminal allow, no authentication will be required (e.g. by entering the PIN) in accordance with the regulatory technical standards issued by the European Commission under the Payment Services Directive. Otherwise, the cardholder will be prompted to authenticate themselves, for example, by entering their PIN.
If the cardholder's signature is required for the card to be accepted, the Merchant may only accept the card if it
- is presented within the period of validity printed on it;
- is not a recognizable forgery;
- has all the relevant security features; and
- has been signed by the cardholder.

Furthermore, for transactions with signature confirmation, the Merchant shall ensure that
- the cardholder personally signs the receipt in its presence;
- the signature on the paper receipt/screen (for mPOS terminals) matches the signature on the reverse of the card; and
- the last four digits of the card number are identical to the last four digits of the number printed on the receipt.

In case of doubt, the Merchant shall check the identity of the cardholder against a piece of official ID (check that last and first names match) and note on the receipt that the data on the ID and on the card have been compared and verified. For mPOS terminals this note has to be recorded together with a reference to the corresponding transaction ID. For certain UnionPay cards, the name of the cardholder and expiry date are not shown on the card. In these cases, the Merchant has no obligation to carry out checks with respect to the period of validity of the card and the proof of identity of the cardholder.
If the cardholder is unable to authenticate themselves (e.g. if the cardholder has forgotten their PIN or the system does not allow any further PIN entries), the card may not be accepted in accordance with the fallback procedures described in sections 11.2 and 11.3.

5.4 Card acceptance in distance business

5.4.1 General

For the execution of distance business transactions, the Merchant must always obtain the last name, first name and residential address of the cardholder as well as the card number and expiry date of the card or have it confirmed in the case of previously stored information and validate the plausibility of this information; in particular if the delivery address and residential address differ. The Merchant must specify the company name used in the webshop on all information transmitted to the cardholder (e.g. order, delivery and transaction confirmations, invoice).

5.4.2 Secure e-commerce in the webshop (3-D Secure procedure)

By authenticating the cardholder within the scope of "secure e-commerce" transactions, the Merchant can reduce the risk of fraudulent transactions subsequently disputed by the cardholder. Under the national laws implementing the Payment Services Directive, it is up to the Merchant to ensure that the cardholder can authenticate themselves. For this purpose, a virtual terminal with merchant plug-in (hereinafter "MPI") is integrated into the Merchant's webshop. This virtual terminal can be obtained from SPS or another payment service provider certified in accordance with PCI DSS. The MPI is required in order to execute transactions in accordance with the 3-D Secure standards of the card schemes (e.g. "Verified by Visa", "Mastercard SecureCode" or "ProtectBuy"). During the transaction, the MPI establishes an encrypted connection with the server of the card issuer and verifies the cardholder's authentication credentials for secure e-commerce transactions, which allows the authentication and subsequent authorization of the transaction by the card issuer. Exceptions with respect to the cardholder's authentication are possible under the regulatory technical standards issued by the European Commission; SPS shall ensure that the Merchant can benefit as much as possible from these exceptions.
E-commerce transactions that take place without MPI (e.g. manual entry of card data on the virtual terminal) are only permitted in exceptional cases and are associated with a higher risk of charging back of reimbursements in accordance with section 10.

5.4.3 Distance business transactions by post, telephone or fax (mail/phone order)

The acceptance of cards via "mail/phone order" requires use of a certified virtual terminal. The Merchant must destroy all manually recorded card data (in particular card number, expiry date and card verification number) after the transaction has been executed.
Mail/phone order transactions are executed without MPI and the 3-D Secure procedure. Therefore, the risk of charging back of reimbursements pursuant to section 10 is always higher.

5.5 Execution of credits

If a transaction is to be fully or partially refunded to the cardholder after it has been executed, the Merchant shall issue a credit to the same card. A credit may only be made with respect to a debit previously settled and the amount of the credit may not exceed the amount originally debited.
With electronic execution, a credit transaction shall be initiated and a credit receipt printed out. For mPOS terminals offered by SPS, the Merchant is able to request a subsequent full/partial credit for a transaction in writing from the Customer Service of SPS.

Once the Merchant has executed a credit, SPS is entitled to demand from the Merchant the repayment or offsetting of the transaction previously settled or reimbursed.
The following applies for Alipay acceptance:
Alipay allows credits to be handled which are within a period of 365 days. A credit can no longer be requested after this deadline ends. Using appropriate customer service provisions or with a suitable written notice, the Merchant must ensure that the user is notified of the 365-day deadline at the time of the transaction.

6 Receipts

6.1 General

Non-compliance with the obligations pursuant to sections 6.2 and 6.3 leads to a higher risk of charging back of reimbursements pursuant to section 10.

6.2 Transfer to the cardholder

In presence business, the original copy of the receipt printed out by the terminal is retained by the Merchant ("Merchant Receipt"). The Merchant hands over a copy ("Customer Receipt") to the cardholder. When using an mPOS terminal, the receipt is transmitted to the cardholder via e-mail, if requested.
In distance business, the Merchant provides the cardholder with written confirmation of the transaction.

6.3 Safekeeping obligation

The Merchant is obliged to store all original paper receipts and copies of the electronic receipts, all transaction data and daily closing reports (incl. individual transaction data) as well as the related order data and documentation in a secure location for at least 36 months from the date of the transaction.
Electronic data must be stored in an encrypted form and be protected against unauthorized access. In this respect, the Merchant is obliged to comply with the relevant instructions issued by SPS (pursuant to section 14.3).

7 Transaction delivery

7.1 Delivery deadlines

The Merchant is obliged to deliver the transactions to SPS within 48 hours of their execution.
For transactions that arrive in the system of SPS later than is stipulated in the aforementioned provision, SPS reserves the right to deny the Merchant the claim to reimbursement or to reclaim/offset reimbursements previously credited.
In distance business (secure e-commerce, mail/phone order), the Merchant shall be obliged to deliver the transactions within 48 hours even if it is unable to send/deliver the goods in question immediately or provide the service immediately.
The Merchant bears the sole risk regarding the data transfer from the infrastructure of the Merchant to the system operated by SPS, irrespective of whether this is carried out by the Merchant or a third party it has involved.

7.2 Delivery currency

The Merchant shall deliver the transactions in the currencies set out in the Contract Module.

7.3 Subsequent entry

Provided the Merchant meets the delivery deadlines pursuant to section 7.1, it is possible to manually re-enter lost, incorrect or incompletely delivered transactions in cases attributable to a technical disruption to data transmission or processing. Incorrect bookings (e.g. amount booked is too high or too low) cannot be re-entered.
Transactions that are delivered after more than 60 days (debit cards) or 180 days (credit cards) cannot be re-entered. The same applies to transactions whose data is not entered into SPS' system.

8 Reimbursement

8.1 The Merchant's claim to reimbursement

SPS shall reimburse the Merchant in respect of the transactions delivered – after deducting the agreed fees and subject to a subsequent chargeback – at the agreed reimbursement frequency. The settlement details are shown on the reimbursement notice.
No payments are processed by SPS on bank holidays. The Merchant accepts any delays to crediting resulting therefrom. Other country-specific or regional public holidays may result in additional delays.

8.2 Account for receiving reimbursements

The Merchant shall hold an account at a financial institution in the name of the company or the owner for the purpose of receiving the reimbursements. For proper processing, the IBAN and BIC of the corresponding account are required.
The Merchant acknowledges that if incorrect or insufficient account data is provided, transfers/direct debit collections may either not be executed or transfers may be made to another recipient. All costs and fees incurred for inquiries or any other related expenses shall be fully borne by the Merchant.
SPS shall credit reimbursements resulting from the Contract Modules to the Merchant in the form of a collective payment. If the Merchant requests transfers for each card brand, it shall bear any additional costs arising in this respect.

8.3 Reimbursement currency

In principle, reimbursements are credited to the Merchant in the local currency valid at the Merchant's registered seat. If the Merchant requests crediting in another currency, the currency delivered by the Merchant is converted via EUR into the requested reimbursement currency. The foreign currency conversion rates specified by SPS apply. The Merchant shall accept the conversion rates applied by SPS.

8.4 SEPA payment transactions

In the event of the Merchant intending to make use of the benefits of SEPA payment transactions, it shall ensure that the financial institution it has selected participates in SEPA payment transactions and that it holds a euro account. If these requirements are not met, higher processing fees may be incurred. An account corresponding to the SEPA criteria can be used for both, the receipt of reimbursements as well as the collection of SEPA business-to-business direct debits.

8.5 Reimbursement notice and pre-notification

The reimbursement notice is provided by SPS in the form agreed in the Contract Module. In every case, the reimbursement notice shall be made available in the web service "myPortal".
The Merchant shall notify SPS in writing, within 30 days of provision within the web service or, in the case of other agreed forms of delivery, of receipt, of any objections in relation to the reimbursement notice; otherwise the reimbursement notice, including all the information contained in it, is deemed to be correct and complete and to have been approved without reservation.
If claims of SPS vis-à-vis the Merchant (e.g. in case of chargebacks or a negative balance) are settled by means of a SEPA business-to-business direct debit collection, the Merchant receives a request for payment for the outstanding amounts in the form of a pre-notification. The direct debit will be collected on the due date advised. If, at the time of collection, the Merchant's account has insufficient funds and a chargeback procedure is initiated, the Merchant shall fall into arrears from the date of the chargeback.

9 Fees

9.1 General

All fees to be paid by the Merchant to SPS are set out in the Contract Module. The fees shall fall due upon the service being provided by SPS; they shall be offset against accrued reimbursements and listed on the reimbursement notice (section 8.1).
If the application of a schedule of fees is agreed in the Contract Module, the version valid upon conclusion of the Contract Module (available at www.six-payment-services.com/downloads) constitutes an integral part of the Contract Module.
The Merchant's claims vis-à-vis SPS may only be offset with prior written approval of the latter. SPS is entitled at any time to offset its claims vis-à-vis the Merchant. Such offsetting of claims shall be governed by the Luxembourg law on financial collateral arrangements of 5 August 2005, as amended.

9.2 Interchange fees

The Merchant may request information regarding the amount of interchange fees from SPS in writing or access it via www.six-payment-services.com/interchange.

9.3 Third-party crediting fees

The transfer fees or foreign currency crediting fees charged by the Merchant's financial institution, in connection with crediting shall be borne by the Merchant and be directly charged to the latter upon the reimbursement being credited. In the event of statutory changes and/or changes to fees charged by third parties, SPS reserves the right to change its modalities of reimbursement.

9.4 Default of payment

If the offsetting of the amounts owed by the Merchant does not result in entire settlement thereof, SPS will submit to the Merchant a request for payment for the outstanding amount. The term of payment is 10 days; upon its expiration the Merchant shall fall into arrears without further notice.
In the event of the Merchant falling into arrears, SPS shall be entitled to charge default interest at the statutory rate on the outstanding amount and charge all costs for dunning and debt collection to the Merchant.

9.5 Taxes

The fees specified in the Contract Modules for products and services of SPS are, unless otherwise specified, exclusive of indirect taxes (e.g. VAT), withholding taxes and other duties. All taxes and duties which under the legislation of the Merchant's country are due or could in future become due with respect to the services to be rendered by SPS within the scope of the Contract Modules shall be borne by the Merchant. In all cases, the Merchant is obliged to adhere to the provisions applicable in its country in relation to indirect taxes (e.g. reverse charge), withholding taxes and any other duties. The Merchant shall fully indemnify SPS against any claims derived therefrom by third parties against SPS.

10 Chargebacks and fraud monitoring

10.1 Chargebacks

The cardholder and card issuer are entitled to dispute a transaction provided that the prerequisites for the opening of a chargeback procedure, in particular the existence of a chargeback reason, are fulfilled.
In the event of a chargeback procedure being opened, the Merchant shall, following SPS' request, submit to the latter, within 10 days and by registered mail, copies of all receipts and documentation (pursuant to section 6) suitable to refute the chargeback reason. If the chargeback reason cannot be refuted by means of the receipts submitted by the Merchant or if the receipts requested are not submitted in due time, SPS is entitled to reclaim transactions already reimbursed or to offset them with reimbursements to be credited to the Merchant ("chargeback"). This also applies to cases in which goods and/or services are not directly delivered/rendered by the Merchant but by third parties, particularly if the Merchant acts as intermediary or agent of such third parties.
If the Merchant, following the opening of a chargeback procedure, wishes to execute a credit in favor of the card used in the disputed transaction, it shall inform the Chargeback department at SPS about its intention. Following approval by SPS, the Merchant shall execute the credit in accordance with the provisions set out in section 5.5.
During the chargeback procedure, the Merchant shall refrain from taking any legal action against the cardholder.

10.2 Chargeback reasons in presence business

With respect to card acceptance in presence business, SPS shall, in particular, have a chargeback right if the cardholder disputes the transaction and the Merchant cannot prove that the card was present at the point of sale at the time of the transaction. This applies, in particular, if the Merchant
– upon accepting EMV cards, reads the card data via a "non-EMV terminal" (without EMV chip reader); or
– does not read the card data from an EMV chip or magnetic stripe, but enters it manually via the keypad of the terminal (in accordance with the fallback procedures pursuant to sections 11.2 and 11.3).

This list of chargeback reasons is not exhaustive.

10.3 Chargeback reasons in distance business

With respect to card acceptance in distance business, in particular, the following chargeback reasons apply:
– the cardholder disputes the order and/or receipt of goods or services;
– the cardholder rejects the goods received as defective or as not being those specified in the order;
– the cardholder withdraws from a purchase of goods and/or services within the statutory withdrawal period;
– the cardholder asserts claims vis-à-vis the Merchant or for any other reason refuses to fulfill the claim resulting from the transaction;
– the transaction was executed without 3-D Secure procedure.

This list of chargeback reasons is not exhaustive.

10.4 Fraud monitoring

Within the context of fraud monitoring, SPS is entitled at any time to issue instructions to the Merchant aimed at preventing fraud cases (e.g. obligation for cardholders to provide ID). These instructions come into force as soon as the Merchant has been notified thereof and the Merchant is obliged to fully comply with them.
In the event of reasonable suspicions of fraud, SPS is entitled to withhold the reimbursements to the Merchant until the suspicions have been clarified. This remains subject to sections 10.2 and 10.3. In the event of an excessive number of fraud cases, SPS also reserves the right to terminate the Contract Modules with immediate effect.

10.5 Compliance with the limits

Each month the Merchant shall ensure that for the card brands agreed the following thresholds are kept:
– ratio of the total volume of chargebacks plus credits/to gross sales per month shall not exceed 2%;
– ratio of the number of chargebacks plus credits/to the number of transactions per month shall not exceed 1%;
– ratio of the total volume of fraudulent transactions/to gross sales per month shall not exceed 0,75%;
– ratio of the number of fraudulent transactions/ to the number of transactions per month shall not exceed 3% and less than 3 fraudulent transactions.

If either of these thresholds is exceeded, SPS is entitled to charge the Merchant case-specific expenses for each chargeback/credit/fraudulent transaction in excess of these limits. Furthermore, SPS is entitled to pass on any penalty and/or processing fees imposed by the card schemes to the Merchant, to defer the reimbursement of the transactions delivered for up to 180 days and to terminate the Contract Modules with immediate effect.

11 Functional disruptions and fallback procedures

11.1 General

The following functional disruptions may occur:
– functional disruption to the system;
– functional disruption to the infrastructure or the terminal;
– functional disruption to the card (damaged card).

In the event of functional disruptions, the Merchant may use the manual fallback procedures pursuant to sections 11.2 and 11.3. The Merchant acknowledges that for transactions executed using the fallback procedures, there is a higher risk of charging back of reimbursements pursuant to section 10.
When applying the fallback procedures, the Merchant shall in each case request from the cardholder a piece of official ID and match the data on the ID (last name and first name) against that on the card. After completing the fallback procedures, the Merchant is obliged to immediately destroy all manually recorded card data. Under no circumstances may the Merchant file or store the card verification number or any data read and saved from the magnetic stripes of cards after the transaction has been authorized.
There is no fallback procedure for transactions with Visa Electron, V PAY, Maestro and UnionPay as well as for Dynamic Currency Conversion (DCC) transactions.

11.2 Fallback procedures for functional disruptions to the system/terminal

If the system or the terminal of the Merchant fully or partially fails, the Merchant shall authorize each transaction with SPS by telephone until system operation is resumed/the terminal is functioning again. Once system operation has been resumed, the transaction data as well as the authorization number obtained shall be entered manually by the Merchant on the terminal using the "Booking authorized by telephone" function.
In the event of a functional disruption on the mPOS terminal, there is no fallback procedure available.

11.3 Fallback procedures for functional disruptions to the card

If the functional disruption is a result of damage to the card, the Merchant may manually enter the card data on the terminal. The Merchant shall authorize such transactions in advance with SPS by telephone. The manual entry of data by typing in the card data on the terminal must be executed using the "Manual card data entry" function. The receipt printed out by the terminal must be signed personally by the cardholder.

12 Additional provisions for hotel or car rental reservations

With respect to the acceptance of credit cards for hotel or car rental reservations, the Merchant shall additionally adhere to the provisions on the respectively applicable data sheet, "Hotel reservation guarantee per credit card"/"Hotel reservation by means of down payment with a credit card (Hotel Advance Deposit)"/"Rental car reservation with a credit card". The respective data sheet forms an integral component of the Contract Module.

13 Additional provisions for Dynamic Currency Conversion (DCC)

The dynamic currency conversion (DCC) service allows dynamic currency conversion at the terminal. An overview of the foreign currencies available can be requested from SPS.
The Merchant shall ensure that the cardholder can in all cases independently select whether he/she wishes to carry out the transaction in the card currency (DCC transaction) or in the local currency.
For DCC transactions, the foreign currency conversion rate (local currency/card currency) specified by SPS for the accepted foreign card shall apply to the cardholder. The Merchant shall accept the conversion rate specified by SPS.
SPS shall be authorized, at its equitable discretion, to interrupt the operation of the DCC service or of individual foreign currencies if it deems such an interruption to be necessary for imperative material reasons, for example disruptions, risk of misuse or extraordinary volatility on the foreign exchange markets.

14 Data protection

14.1 General

The Contracting Parties are obliged to comply with the provisions of the respectively applicable laws in relation to data protection.
In this respect, the Merchant is obliged to require that its personnel as well as any other third parties involved by it that have access to confidential or otherwise protected data (in particular card data) comply with the data protection provisions as well as with the security requirements of the PCI DSS (pursuant to section 14.3).

14.2 Data processing and data transfer

The Merchant shall expressly authorize SPS, prior to the Contract Module coming into force and throughout its duration, to obtain all information, including personal data that SPS deems to be important in relation to the Contract Module and the fulfillment of the services established therein. Furthermore, SPS is entitled to transfer data from the Contract Modules and Framework Agreement within the scope required to third parties appointed by SPS in order to assess potential risks or execute transactions. Data shall also be forwarded to card schemes for marketing purposes. The Merchant acknowledges that the data (in particular master data and transaction data) related to the conclusion and fulfillment of the Contract Modules is processed in Switzerland and in countries of the EU. As part of Alipay's acceptance, the contracting partner additionally acknowledges that Alipay shall also process master data, transaction data and marketing in the People's Republic of China.
SPS, in its capacity as the entity responsible for data processing, collects and processes personal data of the Merchant and/or the natural persons connected to the Merchant's organization in order to ensure the following:
– identification of the Merchant and/or the natural persons connected to the Merchant's organization;
– correct execution of the Contract Modules; and
– compliance with legal obligations.

SPS shall take the appropriate technical measures and implement an adequate organization in order to ensure the protection of such personal data and shall process it as per the above-mentioned purposes and in accordance with the applicable data protection laws, including the Payment Services Directive as well as the national transposition laws, and from 25 May 2018, the General Data Protection Regulation (EU) 2016/679. The Merchant agrees to this and grants its express consent to the data processing.
The Merchant and, as the case may be, the natural persons connected to the Merchant's organization, have the right to access their personal data as well as the right to correct and delete this data and, as from 25 May 2018, the right to the portability of their personal data in accordance with the applicable laws.
The Merchant is obliged to take all of the necessary measures in order to inform the natural persons connected to its organization of the processing of their personal data within the meaning of this section and to ensure that these persons have consented to the data processing in the form prescribed by the applicable laws.

14.3 PCI DSS data security standard

Card data (in particular card numbers, expiry dates) shall be protected against loss and unauthorized access by third parties. The card schemes' data security provisions that must be met to this effect are defined in the PCI DSS. In this respect, the Merchant shall observe and at all times fully comply with the currently applicable version of the "PCI DSS compliance instructions security standards" issued by SPS, which forms an integral part of these GBC. In particular, the Merchant is obliged to carry out the certification measures, e.g. self-assessment questionnaire, and confirm to SPS its compliance with the PCI DSS.
In the event of card data being stolen or if it is suspected that card data has been stolen, the Merchant shall notify SPS immediately. In such a case, the Merchant expressly authorizes SPS to mandate an audit company accredited by the card schemes to produce a "PCI audit report". This will involve investigating the circumstances in which the damage arose and verifying whether the Merchant complied with the PCI DSS. The Merchant is obliged to cooperate fully with the audit company; in particular, it shall provide the audit company with unrestricted access to its premises and infrastructure. After the PCI audit report has been produced, the Merchant shall, at its own expense, completely resolve all the security defects identified within a period of time notified by SPS. If the investigation reveals that the security standards in accordance with PCI DSS were not met at the time the data was stolen, the costs incurred in producing the PCI audit report shall also be borne by the Merchant.
SPS shall be entitled to pass on any claims for damages put forward by the card schemes to the Merchant and/or to terminate the Contract Module with immediate effect if the Merchant does not comply with the PCI DSS or if the Merchant does not confirm, upon request, that it is complying with the PCI DSS. This shall apply equally in the event of card data being stolen or if it is suspected that card data has been stolen.

15 Liability

Notwithstanding ancillary statutory provisions and unless explicitly regulated otherwise, the Merchant shall be liable, in particular, for damage that SPS incurs as a result of the former, or third parties involved by it, failing to fulfill their obligations, notably in technical, organizational and administrative respects. In particular, SPS is entitled to pass on to the Merchant any potential claims for damages resulting from a culpable breach of duty by the Merchant or by third parties involved by it as well as any penalty and/or processing fees imposed by the card schemes and any other case-related expenses. The Merchant shall fully indemnify SPS in this respect and shall be liable for these claims and any additional case-related expenses.
Unless explicitly regulated otherwise, SPS or third parties involved by it shall be liable in case of wilful misconduct or gross negligence in accordance with the statutory provisions.
The liability of the Contracting Parties for culpable harm to life, body or health as well as the statutory product liability remain intact.

16 Notifications

All notifications shall be issued in writing unless another form has been explicitly agreed in the Contract Module. Written form also includes electronically transmitted messages (e.g. via e-mail or via a platform provided by SPS within the scope of a service).

17 Modifications and additions to the Contract Modules, incl. fees

To be effective, any modifications or additions to the Contract Modules, in particular the GBC and other integral parts, must be made in writing (including in electronic form).
SPS reserves the right at any time to modify or make additions to the Contract Modules, in particular the GBC and other integral parts as well as the fees. These modifications or additions shall be communicated in writing to the Merchant at least 60 days prior to their coming into force, unless these changes or additions are required by law and stipulate a shorter time limit. If the Merchant is not willing to accept the announced modification or addition, it shall be entitled to terminate the Contract Module affected by the modification or addition by registered mail within 30 days of receipt of the modification or addition notification, with effect at the time the modification or addition comes into force. If the Merchant omits the termination, this shall be deemed to represent acceptance of the modification or addition.
Taking security measures in accordance with section 2.1.4, para. 3, making changes to the system in accordance with section 4.1, para. 3 as well as modifying the fees within an agreed charging framework are not deemed to be modifications within the meaning of this section and therefore do not represent grounds for termination.

18 Coming into force, duration and termination

18.1 Coming into force

In principle, the Contract Module comes into force once SPS has sent the activation confirmation to the Merchant. If, however, the Contract Module explicitly foresees countersignature by SPS, the Contract Module shall come into force upon being signed by the Contracting Parties.

18.2 Duration

The Contract Module is concluded for an indefinite duration.

18.3 Ordinary termination

The Contract Module may be terminated as per the end of a month by registered mail. If the Contract Module is terminated by the Merchant, the notice period is one month. In the event of termination by SPS, a two-month notice period shall apply.
The Merchant's right to termination pursuant to section 17 and the right to immediate termination for good cause of the Contracting Parties, pursuant to section 18.4, remain reserved.
Notification of termination of one Contract Module does not cause the termination of the remaining Contract Modules. If no further Contract Modules exist, the termination of the last/sole Contract Module automatically results in the dissolution of the Framework Agreement.

18.4 Extraordinary termination

In the event of good cause, the Contracting Parties shall be entitled at any time to terminate the Contract Modules with immediate effect. In particular, good cause includes the following:
– serious or repeated breaches of the provisions of the Contract Module by either Contracting Party;
– repeated complaints/chargebacks and/or transactions being reported by card issuers as fraudulent (pursuant to section 10);
– other inconsistencies in settled transactions;
– a significant change in the ownership structure and control of the Merchant;

– the opening of insolvency proceedings over the assets of the Merchant.
The extraordinary termination of Contract Modules for card acceptance authorizes SPS to immediately terminate all existing contract modules. The immediate termination of all existing contract modules causes the Framework Agreement to be automatically rescinded.

18.5 Automatic termination
The Contract Modules shall automatically terminate, without requirement of notice, if for a period of 2 years no transaction deliveries by the Merchant have occurred.
The automatic termination of Contract Modules for card acceptance results in the automatic termination of all existing contract modules as well as the Framework Agreement.

18.6 Consequences of contract termination
The obligations arising out of sections 6.3 (Safekeeping obligation), 14 (Data protection), 15 (Liability), 18.6 (Consequences of contract termination), 19 (Confidentiality), 20.3 (Assignment prohibition) and 20.7 (Applicable law and place of jurisdiction) shall remain in place following termination of a Contract Module.
Following termination of the Contract Module, the Merchant shall remove all references to the corresponding services of SPS visible to customers.
Upon notice of termination of a Contract Module, SPS is entitled to withhold the crediting of reimbursements to the Merchant immediately and for 180 days beyond the termination date of the Contract Module in order to offset any subsequent claims, in particular chargebacks, against these reimbursements.
If criminal or any other legal proceedings are opened against the Merchant or charges have been brought against the Merchant, SPS reserves the right to delay the crediting of reimbursements at least until the proceedings have been completed.

19 Confidentiality
The Contracting Parties reciprocally undertake to keep confidential the agreed commercial conditions as well as all information, documentation, data and processing techniques – described or identifiable as being confidential and neither publicly nor generally accessible – that they become aware of in fulfilling the Contract Modules; they may only make these accessible to third parties with prior written consent from the other Contracting Party. This does not prevent any Contracting Party from disclosing confidential information insofar as it constitutes a performance of mandatory provisions of law.

20 Concluding provisions
20.1 Right to issue instructions of SPS
The Merchant is obliged to comply with the technical, organizational and administrative instructions and guidelines issued by SPS as well as the terminal and infrastructure suppliers.

20.2 Intermediary activities of SPS
SPS also acts as an intermediary for other acquirers and infrastructure suppliers and in doing so, brokers their contracts in their name, at their risk and on their account. The contracting parties for services provided in this manner are the respective service provider and the Merchant.

20.3 Assignment prohibition
The Merchant may only assign any of the rights or duties it has vis-à-vis SPS with prior written consent from SPS.

20.4 Involvement of third parties/assignment to Group companies
SPS reserves the right to transfer the fulfillment of its contractual obligations to third parties at any time, without having to inform the Merchant.
SPS is entitled to assign the Contract Module to another Group company. In such a case, the Merchant is to be suitably notified.

20.5 Waiver of rights
If any rights arising from the Contract Modules are not asserted by SPS, this in no way represents a waiver of these rights unless SPS has issued an express written waiver declaration in this regard.

20.6 Severability clause
Should a provision of the Contract Modules (including fees) be declared invalid, the remaining provisions shall not be affected thereby and are to be construed in such a way as if the Contract Module concerned was concluded without the invalid provision. The same applies to any contractual omissions.

20.7 Applicable law and place of jurisdiction
All legal relationships between the Merchant and SPS arising from the Framework Agreement and from all Contract Modules concluded are subject to Luxembourg law, to the exclusion of the UN Sales Convention. The exclusive place of jurisdiction is Luxembourg.

20.8 Procedure for out-of-court settlement of disputes
The CSSF may settle disputes relating to the rights and obligations arising from Titles III and IV of the Payment Services Directive and the national transposition laws out of court, in so far as these rights and obligations have not been excluded under section 1.2
For more information on the CSSF and the conditions for access, please refer to the CSSF website http://www.cssf.lu/.

Worldline | SIX Payment Services

Informace k ochraně dat pro zákazníky

Otázka	Odpověď
Koho se týkají tyto informace ohledně ochrany dat?	Tyto informace o ochraně dat ("informace") směřují na zákazníky a partnery (v rámcové smlouvě společně označováni jako "zákazníci") **SIX Payment Services ("SPS").** Tyto informace se týkají příjemců, kteří jsou zákazníky některé nebo některých následujících právních subjektů: – SIX Payment Services Ltd – SIX Payment Services (Europe) S.A. – SIX Payment Services (Germany) GmbH Právní subjekty jmenované výše budou označovány jednotlivě jako "SPS společnost" nebo společně jako "SPS společnosti" pokud se určité prohlášení nebude týkat pouze některého právního subjektu. V takovém případě by byl právní subjekt označen jménem.
Co je cílem informace?	Tato informace má za úkol obeznámit zákazníky o tom: – která osobni data („data"), která obchodník poskytl, jsou zpracovávaná společnostmi SPS, – co je účelem a na základě čeho splečnosti SPS toto provádějí, – jak a jak dlouho jsou data zpracovávána, – jaká práva ohledně ochrany dat zákazníci mají vůči společnostem SPS, a – oddělení odpovědném za zpracování dat uvnitř společnosti SPS a koho mohou zákazníci v případě dotazů kontaktovat.
Jaká data jsou zpracovávaná společnostmi SPS?	Společnosti SPS zpracovávají data, která jsou jim předána nebo zpřístupněna zákazníkem za účelem uzavření rámcové smlouvy o obchodním vztahu. Toto se vztahuje na kontaktní osoby, jako jsou jejich jména, emailové adresy či pracovní telefonní čísla. Sdělením výše uvedených dat společnosti SPS, zákazník potvrzuje, že informoval fyzické osoby, kterých se to týká (zaměstnance, agenty, atd.) a jejichž osobní data společnosti SPS sděluje. Pokud zákazník používá online služby společností SPS, ochrana osobních dat SPS www.six-payment-services.com/privacy-statement má být konsultována.
Zpracovávají společnosti SPS jiná data?	V souvislosti s plněním povinností prevence praní špinavých peněz a financování teroristů, SIX Payment Services (Europe) S.A. je povinna dle zákona proti praní špinavých peněz sbírat a uchovávat specifické osobní dokumenty a informace. Z tohoto důvodu, SIX Payment Services (Europe) S.A. musí, kromě jiného, zjišťovat a kontrolovat identitu zákazníků, významných majitelů zákazníka či beneficientů zákazníka, posuzovat způsob vykonávání a podstatu obchodu, ke kterému se zákazník hlásí, shromažďovat a kontrolovat informace, původ užitých zdrojů, stejně tak neustále monitorovat obchodní vztah a transakce, které se odvíjejí v rámci uzavřené smlouvy. SIX Payment Services (Europe) S.A. musí uchovávat kopie dokumentů a obdržené informace, které jsou požadovány k plnění výše uvedených povinností, stejně tak jako ústřižky od transakcí a záznamy potřebné k identifikaci transakcí.

Otázka	Odpověď
K jakému účelu společnosti SPS data zpracovávají?	Data jsou zpracovávána společnostmi SPS výhradně za účelem uzavírání smluv se zákazníky. Specifické použití dat je odvislé od smlouvy uzavřené mezi zákazníkem a společností SPS. Společnosti SPS společnosti data vyžadují zejména pro: – obecné udržování zákaznického vztahu; – poskytování služeb, které jsou dle smlouvy povinny poskytovat; – posílání produktů a informací, které jsou dle smlouvy povinny poskytovat; – účely účtování; – účely úhrad; – účely zpracování námitek či stížností podaných zákazníkem; – poskytování informací zákazníkovi ohledně změn a vývoje produktů a služeb; – odesílání informačních dopisů; – hlasového nahrávání. Společnosti SPS neprocesují data za žádných okolností mimo své smluvní vztahy se zákazníky.
Jaké odůvodnění má společnost SPS ke zpracovávání dat?	Společnost SPS data zpracovává v první řadě ve svém vlastním legitimním zájmu, aby zaručila dodržování smluv se zákazníky a pravidel regulátorů.
Jsou data předávána také třetím stranám?	Všechny společnosti SPS jsou přímo či nepřímo zcela vlastněné dceřinné společnosti společnosti Worldline. Společnosti SPS mohou celé nebo částečné zpracování dat a jiných služeb předat Worldline nebo jiným dceřinným společnostem (včetně společností SPS) Worldline a externím třetím stranám ve Švýcarsku a zahraničí. Pokud jsou data přenesená k Worldline, dceřinným společnostem Worldline nebo externím třetím stranám jako součást outsourcingu, je outsourcující SPS společnost povinna obdržet od příjemce předem záruku dodržování důvěrnosti a ochrany společnosti SPS. Každá společnost SPS si ponechává právo sdělit data úřadům a/nebo třetím stranám ve Švýcarsku a v zahraničí pokud je společnost SPS povinna tak učinit dle platných zákonů.
Přenáší společnosti SPS data také do zemí mimo EU, EEA nebo Švýcarsko?	Jako součást vykonávání smlouvy se zákazníky, společnosti SPS smí spolupracovat se třetími stranami (např. dodavateli), kteří poskytují některé ze svých služeb nebo vyrábí některý ze svých výrobků mimo EU, EEA nebo Švýcarsko. Pokud taková třetí strana obdrží přístup k datům jakou součást plnění smlouvy, příslušná společnost SPS a třetí strana vstoupí do písemné smlouvy, která zajistí ochranu dat na stejné úrovni, jaká je požadována regulativy ochrany dat v EU nebo Švýcarsku. Na požádání, smí zákazníci vidět smluvní dohody (úryvky), které společnost SPS implementovala s třetími stranami, které tato zákaznická data zpracovávají.
Jak dlouho jsou data zpracovávána nebo uchovávána společnostmi SPS?	Data jsou standardně uchovávána deset let po skončení smluvního vztahu se zákazníkem. Výjimkou jsou data, která musí být dle místních zákonů smazána před uplynutím této lhůty.

Otázka	Odpověď
Jaká práva fyzických osob ("subjektů dat") jsou dotčena zpracováním jejich dat společnostmi SPS jako součást obchodního vztahu se zákazníky?	Subjekty dat jsou oprávněny k následujícím právům vztahujícím se k údajům o subjektu dat: – obdržet informaci o tom, zda nebo která data může společnost SPS ukládat a uchovávat (kategorie dat, adresáti nebo kategorie adresátů, doba uchování, či kritéria, která takovou dobu určují); – obdržet kopie dat zpracovávaných společnostmi SPS; – požadovat opravu dat, pokud tato nejsou správná; – požadovat vymazání dat; – požadovat omezení zpracování dat; – obdržet data ve strukturované, přístupné a strojově čitelném formátu; – podat námitku proti zpracovávání dat, zejména pro účely přímé reklamy. Práva specifikovaná výše mohou být odmítnuta nebo omezena, pokud zájem, práva a svobody třetích stran převažují nebo pokud je zpracovávání dat nezbytné k vytvoření, výkonu a obraně jakýchkoliv právních námitek společností SPS.
Mají společnosti SPS referenta pro ochranu dat?	Ano. Veškeré dotazy ohledně ochrany dat a dotčených osobních práv mohou být směrovány na referenty ochrany dat (DPOs) v SPS na následujících kontaktních adresách: **SIX Payment Services Ltd** Compliance Hardturmstrasse 201 8021 Zurich Switzerland Pro SIX Payment Services Ltd: dataprotection.switzerland@six-payment-services.com Pro SIX Payment Services (Europe) S.A.: dataprotection.europe@six-payment-services.com Pro SIX Payment Services (Germany) GmbH: dataprotection.germany@six-payment-services.com

Otázka	Odpověď
Kdo je zodpovědný za zpracování dat v jednotlivých společnostech SPS?	Pro jednotlivé společnosti SPS, následující subjekty jsou odpovědné za zodpovězení dotazů vztahujících se ke zpracování dat: **SIX Payment Services Ltd** Global Data Protection Support Hardturmstrasse 201 8021 Zurich Switzerland dataprotection.switzerland@six-payment-services.com **SIX Payment Services (Europe) S.A.** Global Data Protection Support 10, rue Gabriel Lippmann 5365 Munsbach Luxembourg dataprotection.europe@six-payment-services.com **SIX Payment Services (Germany) GmbH** Global Data Protection Support Langenhorner Chaussee 92-94 22415 Hamburg Germany dataprotection.germany@six-payment-services.com

V případě rozdílu mezi německou verzí a překladem, má německá verze přednost.

110.0547.08 INT_CZ/12.2019

Kontaktní osobu ve Vašem regionu naleznete na adrese: www.six-payment-services.com/kontakt

SIX Payment Services Ltd
Hardturmstrasse 201
8021 Curych
Švýcarsko

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Lucembursko

SIX Payment Services (Europe) S.A.
Rakouská pobočka
Marxergasse 1B
A-1030 Vídeň

SIX Payment Services (Germany) GmbH
Langenhorner Chaussee 92-94
22415 Hamburk
Německo