ZMLUVA O ZABEZPEČENÍ SLUŽBY PLATOBNÉHO SYSTÉMU PROSTREDNÍCTOM MOBILNEJ APLIKÁCIE PRE ÚHRADU DOČASNÉHO PARKOVANIA

uzavretá podľa ustanovenia § 269 ods. 2 a § 276 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v platnom znení

medzi:

Objednávateľ

Názov:	Hlavné mesto Slovenskej republiky Bratislava
Sídlo:	Primaciálne námestie č. 1, 814 99 Bratislava, Slovenská republika
IČO:	00 603 481
DIČ:	2020372596
IČ DPH:	SK2020372596
IBAN:	
Zastúpený:	Ing. arch Matúš Vallo, primátor

(ďalej len ako „Objednávateľ" v príslušnom gramatickom tvare)

a

Poskytovateľ

Názov:	EasyPark Slovakia s.r.o.
Sídlo:	Zámocká 3, 811 01 Bratislava, Slovenská republika
IČO:	50929411
DIČ:	2120550333
IČ DPH:	-
IBAN:	SK8511110000001693039008
Zastúpený:	Ing. Patrik Piščák, Country Director CZ & SK

(ďalej len ako „Poskytovateľ" v príslušnom gramatickom tvare)

(Objednávateľ a Poskytovateľ ďalej spolu len ako „Zmluvné strany" alebo jednotlivo ako „Zmluvná strana" v príslušnom gramatickom tvare)

Preambula

Objednávateľ je prevádzkovateľom parkovacích miest na území Objednávateľa. Objednávateľ všeobecne záväzným nariadením č. 8/2019 o dočasnom parkovaní motorových vozidiel (ďalej ako „VZN 8/2019") ustanovil úseky miestnych komunikácií na dočasné parkovanie motorových vozidiel na svojom území, určil spôsob zabezpečenia prevádzky parkovacích miest, výšku úhrady za dočasné

parkovanie, spôsob jej platenia a spôsob preukázania jej zaplatenia. Objednávateľ umožnil vo VZN 8/2019 vykonávanie úhrady za parkovací lístok prostredníctvom internetového rozhrania, vrátane mobilných aplikácií, ktoré sú bežným a veľmi využívaným platobným nástrojom v oblasti úhrady za dočasné parkovanie v rámci krajín Európskej únie. Objednávateľ považuje úhradu parkovacích lístkov prostredníctvom mobilnej aplikácie za dlhodobo preferovaný spôsob predaja a distribúcie dočasných parkovacích oprávnení na území Objednávateľa.

Objednávateľ v snahe zabezpečiť poskytovanie kvalitných služieb pre svojich obyvateľov, ako aj návštevníkom na najvyššej možnej úrovni aj v oblasti predaja a distribúcie parkovacích oprávnení (parkovacích lístkov) podporuje otvorenú súťaž pre všetkých poskytovateľov služieb súvisiacich s predajom a distribúciou parkovacích oprávnení, ktorá ako jediná dokáže zabezpečiť a kontinuálne udržať požadovanú kvalitu poskytovaných služieb.

Poskytovateľ má záujem poskytnúť mobilnú aplikáciu na úhradu parkovacích lístkov prostredníctvom tejto mobilnej aplikácie, umožniť jej bezplatné stiahnutie a užívanie každej osobe, ktorá o to prejaví záujem a prevádzkovať túto aplikáciu za odplatu poskytovanú Objednávateľom.

Objednávateľ má záujem vytvoriť efektívnu hospodársku súťaž medzi poskytovateľmi mobilných aplikácií a preto sa verejným návrhom na uzavretie zmluvy zaviazal uzavrieť zmluvu s každým poskytovateľom, ktorý o to v lehote na prijatie verejného návrhu prejaví záujem. Objednávateľ sprostredkuje Zákazníkovi v rovnakej miere informácie o každom poskytovateľovi mobilnej aplikácie, ktorý uzatvoril túto Zmluvu, a to najmä na webovej stránke Bratislavský parkovací asistent – www.paas.sk. a odkazom na túto webovú stránku, umiestneným na vyhradených miestach, najmä na informačných tabuliach parkovacích zón.

Prijatím verejného návrhu na uzavretie zmluvy každý Poskytovateľ potvrdí, že spĺňa podmienky oprávnenosti definované Objednávateľom. Objednávateľ po nadobudnutí účinnosti tejto Zmluvy overí splnenie podmienok oprávnenosti poskytovateľmi. Poskytovateľom, ktorí splnia podmienky oprávnenosti, vznikne právo aj povinnosť preukázať, že mobilná aplikácia spĺňa požiadavky Objednávateľa prevádzkovať a bezplatne poskytnúť mobilnú aplikáciu každej osobe, ktorá o to prejaví záujem.

Na účely zabezpečenia prístupu na trh je Objednávateľ oprávnený na ročnej báze zverejňovať nové verejné návrhy na uzavretie zmluvy, v ktorých na základe skúseností s plnením Zmluvy nanovo upraví požiadavky na mobilnú aplikáciu a spôsob preukazovania ich splnenia ako aj podmienky prevádzky mobilnej aplikácie na ďalšie obdobie. Objednávateľ umožní Poskytovateľovi poskytovať služby podľa tejto Zmluvy aj v ďalšom období, a to na základe dodatku k tejto Zmluve, ktorý bude zodpovedať podmienkam nového verejného návrhu na uzavretie zmluvy, čím Objednávateľ zabezpečí rovnaké podmienky poskytovania služieb pre všetkých (pôvodných aj pristupujúcich) poskytovateľov.

Článok 1.

Definície pojmov

Nasledujúce výrazy a pojmy v tejto Zmluve majú nižšie definovaný význam, ktorý sa ďalej použije na účely výkladu ustanovení tejto Zmluvy:

„Aplikácia" znamená mobilnú aplikáciu, ktorú na základe a podľa podmienok tejto Zmluvy poskytne a bude prevádzkovať Poskytovateľ a ktorej účelom je zabezpečenie bezproblémovej, časovo a administratívne efektívnej úhrady Parkovného Zákazníkmi.

„***Fáza akceptácie Aplikácie***" znamená fázu plnenia tejto Zmluvy, ktorá sa začína dňom doručenia Potvrdenia o splnení Podmienok oprávnenosti a končí dňom doručenia doručením oznámenia Objednávateľa o preukázaní splnenia Technických a funkčných požiadaviek Poskytovateľovi podľa bodu 5.7 tejto Zmluvy.

„***Fáza prevádzkovania Aplikácie***" znamená fázu plnenia tejto Zmluvy, ktorá sa začína doručením súhlasu so začatím Fázy prevádzkovania Aplikácie podľa bodu 5.9 tejto Zmluvy a končí

(i) uplynutím doby trvania Zmluvy podľa bodu 14.1 tejto Zmluvy;

(ii) ukončením Zmluvy odstúpením od Zmluvy podľa bodu 14.2 tejto Zmluvy;
(iii) zánikom Zmluvy podľa bodu 14.3 tejto Zmluvy.

„Prevádzkovanie Aplikácie" znamená poskytovanie služieb Poskytovateľom vo Fáze prevádzkovania Apiikácie podľa špecifikácie uvedenej v tejto Zmluve;

„Skúšky Apiikácie" znamenajú všetky relevantné skúšky alebo testy, ktorých účelom je preukázanie, že Aplikácia spĺňa Technické a funkčné požiadavky.

„Technické a funkčné požiadavky" znamenajú podrobnú špecifikáciu technických parametrov a funkcionality Aplikácie vypracovanú Objednávateľom; Technické a funkčné požiadavky tvoria Prílohu č .1 tejto Zmluvy;

„Audítor" predstavuje subjekt, ktorý u Objednávateľa vykonáva kontrolu *inter alia* výberu Parkovného a nákladov spojených s prevádzkou regulovaného parkovania na miestnych komunikáciách. Minimálny okruh týchto subjektov zahŕňa Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre verejné obstarávanie Slovenskej republiky, štatutárneho audítora Objednávateľa a mestského kontrolóra hlavného mesta SR Bratislavy, vrátane zamestnancov nimi poverených na výkon kontroly;

„Banková záruka" má význam uvedený v bode 7.13 až 7.15 tejto Zmluvy;

„Dôverná informácia" znamená akúkoľvek informáciu, ktorá nie je verejne prístupná, a ktorú Zmluvná strana poskytujúca informáciu označí za dôvernú, okrem tej, ktorá sa stane alebo stala verejne prístupnou inak ako neoprávnenou manipuláciou Zmluvnou stranou, ktorá sa oboznamuje s dôvernou informáciou; Dôverné informácie môžu byť poskytnuté vo verbálnej (telefonát, rozhovor), písomnej (zadanie, pripomienkovanie) alebo elektronickej forme (email, textový editor, zdrojový kód);

„Hraničný podiel 1" znamená podiel na trhu vo výške 20 (dvadsať) % určený spôsobom podľa Prílohy č. 3 tejto Zmluvy;

„Hraničný podiel 2" znamená podiel na trhu vo výške 40 (štyridsať) % určený spôsobom podľa Prílohy č. 3 tejto Zmluvy;

„Incident" znamená akékoľvek prerušenie fungovania Apiikácie alebo jej funkcionality alebo akékoľvek zníženie kvality Aplikácie najmä v porovnaní s Technickými a funkčnými požiadavkami;

„Kritický incident" alebo ***„A-blocker"*** znamená Incident, ktorý sa prejavuje výpadkom fungovania Aplikácie, čo znemožňuje jej využívanie ako celku, resp. spôsobuje zásadné obmedzenie jej funkcionality a rýchlosti pri obsluhe Zákazníkmi alebo Objednávateľom počas doby trvania Incidentu (najmä úhrada Parkovného). Kritický incident sa zväčša opakuje globálne voči všetkým užívateľom Aplikácie. Za Kritický incident sa považuje aj prejav, ktorý je opakovane vyvolateľný alebo má trvalý charakter alebo sa prejavuje hromadne. Kritickým incidentom môže byť aj výskyt viacerých Závažných incidentov alebo Nekritických incidentov, ktorých súčasné pôsobenie znemožňuje prevádzkovanie Aplikácie alebo spôsobuje zásadné obmedzenie jej funkcionality alebo rýchlosti pre Zákazníka alebo Objednávateľa. Akékoľvek narušenie bezpečnosti Aplikácie alebo systému ParkSys, na ktorý bude Aplikácia integrovaná, sa považuje za Kritický incident, a to aj vtedy, ak nemá vplyv na funkčnosť Apiikácie.

„Závažný incident" alebo **„B-major"** znamená Incident, ktorý sa prejavuje výpadkom fungovania Aplikácie (jej funkcií a modulov v rámci dôležitých biznis funkcionalít Apiikácie) voči Zákazníkom v rozsahu čiastočne obmedzenej funkcionality Aplikácie, v dôsledku ktorého je používanie Aplikácie zo strany Zákazníkov alebo Objednávateľa obmedzené počas doby trvania incidentu. Za Závažný incident sa považuje aj prejav, ktorý je opakovane vyvolateľný alebo má trvalý charakter alebo sa prejavuje hromadne. Závažným incidentom, môže byť aj výskyt viacerých Nekritických incidentov, ktorých súčasné pôsobenie závažným spôsobom obmedzuje funkcionalitu Aplikácie pre Zákazníkov alebo Objednávateľa.

„Nekritický incident" alebo ***„C-minor"*** znamená Incident, ktorý nespôsobí výpadok Aplikácie, resp. ktorý závažným spôsobom neznižuje funkčný rozsah a rýchlosť Aplikácie (napr. drobná funkčná chyba).

„Mesačný výkaz Parkovného" znamená prehľad uhradeného Parkovného v štruktúre uvedenej v Prílohe č. 4 tejto Zmluvy;

„***Mesačný výkaz prevádzky***" znamená prehľad Monitorovania prevádzky v štruktúre uvedenej v Prílohe č. 5 tejto Zmluvy;

„***Model odmeňovania***" znamená spôsob určenia výšky odplaty Poskytovateľa zadefinovaný v Prílohe č. 7 tejto Zmluvy;

„***Monitorovanie prevádzky***" znamená činnosť Poskytovateľa, ktorou preukazuje riadnu a bezporuchovú prevádzku Aplikácie, zabezpečuje evidenciu predchádzania vzniku Incidentov, ako aj všetku ďalšiu činnosť v zmysle Technických a funkčných požiadaviek;

„***Nové obdobie***" znamená obdobie poskytovania služieb úhrady Parkovného cez mobilnú aplikáciu určené Objednávateľom vo verejnom návrhu na uzavretie zmluvy, ktorý Objednávateľ uverejní podľa bodu 12.1 tejto Zmluvy;

„***Odplata***" má význam uvedený v bode 6.1 Zmluvy;

„***ParkSys***" znamená informačný systém Objednávateľa, v ktorom sú implementované prijaté pravidlá parkovacej politiky, a ktorý slúži na ich uplatňovanie v praxi v súlade s Právnym poriadkom ako aj pravidlami prijatými Objednávateľom; Aplikácia komunikuje s ParkSys pomocou API rozhrania definovaného v prílohe č. 6 k tejto Zmluve – ParkSysAPI;

„***Obchodný zákonník***" znamená zákon č. 513/1991 Zb. Obchodný zákonník v platnom znení;

„***Parkovacie miesta***" znamenajú úseky miestnych komunikácií určené na dočasné parkovanie motorových vozidiel určené všeobecne záväzným nariadením Objednávateľa pričom ku dňu uzavretia tejto Zmluvy ide o VZN 8/2009 ako aj ďalšie parkovacie miesta uvedené v Prevádzkovom poriadku;

„***Parkovné***" znamená poplatok za úhradu parkovacieho lístka určený všeobecne záväzným nariadením Objednávateľa; ku dňu uzavretia tejto Zmluvy ide o VZN 8/2009 (§ 4 VZN 8/2019) alebo v Prevádzkovom poriadku;

„***Podmienky oprávnenosti***" znamenajú podmienky uvedené v Prílohe č. 2 tejto Zmluvy;

„***Poskytovateľ služieb pre ParkSys***" je poskytovateľ, ktorý poskytuje Objednávateľovi (okrem iného) servisné služby pre ParkSys;

„***Potvrdenie o splnení Podmienok oprávnenosti***" má význam uvedený v bode 4.2 (ii) alebo 4.4 tejto Zmluvy;

„***Právny poriadok***" znamená právny poriadok Slovenskej republiky, ktorý zahŕňa všetky platné a účinné všeobecne záväzné právne predpisy Slovenskej republiky s relevantným zohľadnením európskej legislatívy, ktorou je Slovenská republika viazaná;

„***Prevádzkový poriadok***" znamená prevádzkový poriadok Objednávateľa, zverejnený na webovom sídle Objednávateľa, ktorý upravuje niektoré podmienky prevádzky Aplikácie a môže obsahovať zoznam Parkovacích miest neuvedených vo VZN 8/2019 a upraviť výšku Parkovného za Parkovacie miesta neuvedené vo VZN 8/2019; Prevádzkový poriadok môže Objednávateľ jednostranne meniť; v prípade rozporu medzi Prevádzkovým poriadkom a touto Zmluvou vrátane jej Príloh má prednosť táto Zmluva;

„***Verejný návrh***" znamená verejný návrh na uzavretie tejto Zmluvy podľa § 276 a nasl. Obchodného zákonníka, zverejnený Objednávateľom dňa 20.7.2021 pod č. MAG 399921/2021;

„***Vyššia moc***" znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo Zmluvných strán pred uzatvorením Zmluvy predvídať, ktorá je mimo kontroly ktorejkoľvek zo Zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek Zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy ktoroukoľvek zo Zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä, nie však výlučne, vojna, teroristický útok, občianske nepokoje, vzbura, prítomnosť ionizujúceho alebo rádioaktívneho žiarenia, požiar, výbuch, povodeň či iné živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že Vyššou mocou nie je štrajk zamestnancov ani hospodárske pomery Zmluvných strán, ani iné okolnosti osobnej povahy a tiež nie také okolnosti, ktoré síce náklady na plnenie zvyšujú, ale plnenie neznemožňujú, t.j. predovšetkým zmeny ovplyvňujúce len ekonomickú situáciu tzn. prekážky, kvôli ktorým je plnenie náročnejšie, a strana tak dosiahne nižší zisk, než aký predpokladala v dobe

uzatvárania tejto Zmluvy, prípadne bude na celej obchodnej transakcii stratová. Pre vylúčenie pochybností sa dojednáva, že opatrenia orgánov verejnej moci vo vzťahu k predchádzaniu šírenia ochorenia COVID-19 platné v čase uzavretia tejto Zmluvy a ich následky nemôžu byť považované za udalosti, resp. okolnosti Vyššej moci;

„***Zákazník***" je právnická osoba alebo fyzická osoba, ktorá prejavila záujem o úhradu Parkovného cez Aplikáciu;

„***Zákon o e-Governmente***" znamená zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente);

„Zástupca Poskytovateľa" znamená osoba preukázateľne určená Poskytovateľom na konanie v mene Poskytovateľa voči Objednávateľovi pri plnení záväzkov a výkone práv Poskytovateľa podľa tejto Zmluvy;

„Zástupca Objednávateľa" znamená osoba preukázateľne určená Objednávateľom na konanie v mene Objednávateľa voči Poskytovateľovi pri plnení záväzkov a výkone práv Objednávateľa podľa tejto Zmluvy;

„***Zberný účet***" znamená bankový účet Poskytovateľa, vedený v banke alebo pobočke zahraničnej banky na území krajín Európskej menovej únie, na ktorý Poskytovateľ prijíma úhrady Parkovného a poukazuje z neho tieto úhrady na účet Objednávateľa;

„***Zmluva***" znamená túto Zmluvu o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania uzatvorenú na základe Verejného návrhu medzi Objednávateľom a Poskytovateľom vrátane jej príloh.

Článok 2.

Úvodné ustanovenia a vyhlásenia strán

2.1 Účelom, na ktorý Objednávateľ s Poskytovateľom uzatvárajú túto Zmluvu, je záujem Objednávateľa, v súlade so štandardmi definovanými v Prevádzkovom poriadku, zabezpečiť bezproblémovú, časovo a administratívne efektívnu úhradu Parkovného prostredníctvom Aplikácie a umožniť Zákazníkom bezplatné použitie Aplikácie ako jedného z platobných kanálov na úhradu Parkovného podľa VZN 8/2019. Objednávateľ zavedením systému platieb Parkovného cez mobilné aplikácie Objednávateľom sleduje zvýšenie komfortu služieb pre Zákazníkov.

2.2 Zmluvné strany vyhlasujú, že údaje uvedené v Zmluve sú v súlade so skutočným stavom ku dňu uzavretia Zmluvy.

2.3 Poskytovateľ vyhlasuje, že:

2.3.1 sa riadne oboznámil s Technickými a funkčnými požiadavkami a s Prevádzkovým poriadkom,

2.3.2 spĺňa všetky požiadavky kladené Právnym poriadkom na výkon činností podľa tejto Zmluvy,

2.3.3 spĺňa Podmienky oprávnenosti,

2.3.4 je oprávnený túto Zmluvu uzavrieť a riadne plniť záväzky v nej obsiahnuté a

2.3.5 Verejný návrh prijal bez výhrad.

2.4 Objednávateľ vyhlasuje, že

2.4.1 je prevádzkovateľom systému ParkSys, s ktorým bude integrovaná Aplikácia Poskytovateľa cez rozhranie systému ParkSys špecifikované v Technických a funkčných požiadavkách resp. prílohe č. 6 k tejto Zmluve - ParkSysAPI.

2.4.2 je oprávnený túto Zmluvu uzavrieť a riadne plniť záväzky v nej obsiahnuté.

Článok 3.

Predmet Zmluvy

3.1 Predmetom tejto Zmluvy je

(i) záväzok Poskytovateľa preukázať, že Aplikácia spĺňa Technické a funkčné požiadavky *inter alia* včítane integrácie s ParkSys spôsobom podľa článku 5. tejto Zmluvy,

(ii) záväzok Poskytovateľa riadne prevádzkovať Aplikáciu, umožniť bezplatné stiahnutie a užívanie Aplikácie Zákazníkmi podľa podmienok tejto Zmluvy

(iii) záväzok Poskytovateľa zabezpečovať možnosť platby Parkovného Zákazníkmi cez Aplikáciu na Zberný účet a záväzok Poskytovateľa poukazovať Parkovné zo Zberného účtu na účet Objednávateľa a

(iv) záväzok Objednávateľa zaplatiť Poskytovateľovi dohodnutú Odplatu podľa článku 6 tejto Zmluvy.

3.2 Poskytovateľ sa zaväzuje, že Aplikácia a Prevádzkovanie Aplikácie budú zodpovedať účelu, na ktorý sa Zmluva uzatvára najmä, aby pre Objednávateľa zabezpečila bezproblémový, časovo a administratívne efektívny výber Parkovného, ako aj kontrolu úhrady Parkovného na základe integrácie Aplikácie so systémom ParkSys.

3.3 Poskytovateľ je povinný v zmysle tejto Zmluvy zabezpečiť si vo svojom mene, na vlastné náklady, na vlastnú zodpovednosť a riziko všetko potrebné technické vybavenie a systémové softvérové vybavenie, licencie a iné práva k predmetom duševného vlastníctva potrebným na preukázanie splnenia Technických a funkčných požiadaviek a Prevádzkovanie Aplikácie v súlade s touto Zmluvou.

3.4 Zmluvné strany sa zaväzujú dodržiavať pri plnení záväzkov podľa tejto Zmluvy ustanovenia Právneho poriadku. Poskytovateľ je povinný vo svojom mene zaobstarať si všetky oznámenia, povolenia, vyjadrenia, licencie a súhlasy vyžadované Právnym poriadkom pre preukázanie splnenia Technických a funkčných požiadaviek a Prevádzkovanie aplikácie. Poskytovateľ uznáva, že akékoľvek zmeny tejto Zmluvy môžu vyžadovať zmenu alebo dodatok k povoleniam, súhlasom a licenciám, ktoré je Poskytovateľ povinný zabezpečiť. Zmluvné strany sa dohodli, že Aplikácia musí okrem vlastností výslovne dohodnutých v Zmluve spĺňať požiadavky Právneho poriadku.

Článok 4.

Preukazovanie splnenia Podmienok oprávnenosti

4.1 Poskytovateľ sa zaväzuje v lehote do 10 (desiatich) pracovných dní odo dňa účinnosti tejto Zmluvy preukázať Objednávateľovi splnenie Podmienok oprávnenosti v rozsahu a spôsobom upraveným v Prílohe č. 2 k tejto Zmluve.

4.2 Objednávateľ posúdi splnenie Podmienok oprávnenosti a v lehote do 10 (desiatich) pracovných dní od uplynutia lehoty podľa bodu 4.1 tejto Zmluvy:

(i) písomne vyzve Poskytovateľa, aby v lehote do 5 (piatich) pracovných dní vysvetlil alebo doplnil predložené doklady, ak tieto doklady nepreukazujú splnenie Podmienok oprávnenosti alebo

(ii) vydá Poskytovateľovi písomné Potvrdenie o splnení Podmienok oprávnenosti, ak doklady predložené Poskytovateľom preukazujú splnenie Podmienok oprávnenosti.

4.3 V prípade, ak Poskytovateľ ani na výzvu Objednávateľa podľa bodu 4.2 (i) tejto Zmluvy nepredloží doklady, ktorými preukáže splnenie Podmienok oprávnenosti, Objednávateľ zašle Poskytovateľovi písomné oznámenie o nesplnení Podmienok oprávnenosti. Doručením písomného oznámenia o nesplnení Podmienok oprávnenosti Poskytovateľovi táto Zmluva zaniká.

4.4 V prípade, ak Poskytovateľ na výzvu Objednávateľa podľa bodu 4.2 (i) tejto Zmluvy predloží doklady, ktorými preukáže splnenie Podmienok oprávnenosti, Objednávateľ vydá Poskytovateľovi písomné Potvrdenie o splnení Podmienok oprávnenosti.

4.5 Doručením písomného potvrdenia o splnení Podmienok oprávnenosti podľa bodu 4.2 (ii) alebo bodu 4.4 tejto Zmluvy sa začína Fáza akceptácie Apiikácie.

Článok 5.

Preukazovanie splnenia Technických a funkčných požiadaviek

5.1 Poskytovateľ sa zaväzuje preukázať splnenie Technických a funkčných požiadaviek v lehote do 45 (štyridsiatich piatich) kalendárnych dní od dňa začatia Fázy akceptácie Apiikácie podľa bodu 4.5 tejto Zmluvy. Poskytovateľ je povinný poskytnúť a prevádzkovať Aplikáciu s vynaložením odbornej starostlivosti a v súlade s najlepšími profesionálnymi zvyklosťami tak, aby bol splnený účel tejto Zmiuvy.

5.2 Ak hrozí, že Poskytovateľ nesplní povinnosti podľa bodu 5.1 tejto Zmluvy včas alebo hrozí omeškanie pri plnení povinností Poskytovateľa vo Fáze prevádzkovania Aplikácie, Poskytovateľ bude o tejto skutočnosti písomne informovať Objednávateľa bez zbytočného odkladu po tom, čo sa o tejto skutočnosti dozvie. Toto oznámenie bude obsahovať dôvody omeškania a predpokladaný deň a čas nápravy omeškania povinností podľa tejto Zmluvy.

5.3 Splnením oznamovacej povinnosti Poskytovateľa podľa bodu Zmiuvy nie sú dotknuté ostatné nároky Objednávateľa vyplývajúce z porušenia záväzku Poskytovateľa vo Fáze akceptácie Apiikácie alebo vo Fáze prevádzkovania Aplikácie, predovšetkým nárok na zmluvnú pokutu a na náhradu škody. Objednávateľ je po splnení oznamovacej povinnosti Poskytovateľa podľa bodu 5.2 Zmiuvy oprávnený lehotu podľa bodu 5.1 tejto Zmiuvy predĺžiť o čom Poskytovateľa písomne informuje.

5.4 Poskytovateľ preukazuje splnenie Technických a funkčných požiadaviek predložením vyhlásenia o splnení Technických a funkčných požiadaviek podľa Prílohy č. 9 k tejto Zmluve, v ktorom popíše spôsob naplnenia jednotlivých Technických a funkčných požiadaviek.

5.5 Objednávateľ v lehote do 10 (desať) pracovných dní odo dňa doručenia vyhlásenia podľa bodu 5.4 tejto Zmluvy posúdi Poskytovateľom uvedený spôsob naplnenia jednotlivých Technických a funkčných požiadaviek a v rovnakej lehote buď oznámi Poskytovateľovi, že preukázal splnenie Technických a funkčných požiadaviek alebo Poskytovateľovi oznámi svoje výhrady k popisu spôsobu splnenia Technických a funkčných požiadaviek a vyzve ho na predloženie upraveného vyhlásenia o splnení Technických a funkčných požiadaviek.

5.6 Objednávateľ v lehote do 5 (piatich) pracovných dní odo dňa doručenia upraveného vyhlásenia podľa bodu 5.5 tejto Zmluvy posúdi Poskytovateľom uvedený spôsob naplnenia jednotlivých Technických a funkčných požiadaviek a v rovnakej lehote buď oznámi Poskytovateľovi, že preukázal splnenie Technických a funkčných požiadaviek aiebo Poskytovateľovi oznámi, že splnenie Technických a funkčných požiadaviek nepreukázal. Momentom doručenia oznámenia Objednávateľa o nepreukázaní splnenia Technických a funkčných požiadaviek Poskytovateľovi aiebo márnym uplynutím lehoty podľa bodu 5.1 tejto Zmluvy táto Zmluva zaniká bez nároku Poskytovateľa na akúkoľvek odplatu či kompenzáciu.

5.7 Fáza akceptácie Aplikácie sa považuje za dokončenú doručením oznámenia Objednávateľa o preukázaní splnenia Technických a funkčných požiadaviek Poskytovateľovi.

5.8 Vyhlásenie o splnení Technických a funkčných požiadaviek alebo upravené vyhlásenie o spinení Technických a funkčných požiadaviek bude tvoriť Prílohu č. 9 tejto Zmiuvy a spôsob naplnenia Technických a funkčných požiadaviek uvedený v Prílohe č. 9 je pre Poskytovateľa záväzný.

5.9 Objednávateľ vydá Poskytovateľovi písomný súhlas so začatím Fázy prevádzkovania Apiikácie v lehote do 5 (piatich) pracovných dní odo dňa doručenia oznámenia o preukázaní splnenia

Technických a funkčných požiadaviek, nie však skôr ako Poskytovateľ splní povinnosti podľa bodu 7.13 tejto Zmluvy.

5.10 Poskytovateľ sa zaväzuje kontinuálne preukazovať splnenie Technických a funkčných požiadaviek počas Fázy prevádzkovania apiikácie za podmienok dojednaných v bode 8.17 alebo 8.18 tejto Zmluvy.

Článok 6.

Odplata a platobné podmienky

6.1 Objednávateľ sa zaväzuje vyplácať Poskytovateľovi odplatu určenú v súlade s Modelom odmeňovania, na základe počtu Bezplatných transakcií a Platených transakcií.

6.2 K odplate bude Poskytovateľ účtovať daň z pridanej hodnoty (DPH) v zmysle platných právnych predpisov.

6.3 V odplate sú zahrnuté všetky náklady Poskytovateľa spojené s realizáciou plnení podľa tejto Zmluvy, vrátane akýchkoľvek vecí a práv potrebných na preukázanie splnenia Technických a funkčných požiadaviek a Prevádzkovanie Aplikácie, nákladov spojených s dodávaním technického vybavenia (hardvér) a systémového softvérového vybavenia, licencií, autorských odmien, ako aj nákladov, správnych a obdobných poplatkov vyberaných akýmkoľvek orgánom štátnej správy, ceny dokumentácie potrebnej na preukázanie splnenia Technických a funkčných požiadaviek alebo Prevádzkovanie Aplikácie, nákladov na poplatky súvisiace s úhradou Parkovného cez platobné karty, či nákladov súvisiacich s vedením a užívaním Zberného účtu.

6.4 Objednávateľ sa zaväzuje uhrádzať odplatu mesačne na základe Mesačného výkazu Parkovného schváleného podľa bodu 6.5 tejto Zmluvy a Mesačného výkazu prevádzky schváleného podľa bodu 8.5 tejto Zmluvy počnúc začatím Fázy prevádzkovania Aplikácie. Pre vylúčenie pochybností sa uvádza, že za plnenie povinnosti Poskytovateľa počas Fázy akceptácie Aplikácie nevzniká Poskytovateľovi žiaden nárok na peňažné ani akékoľvek iné plnenie od Objednávateľa.

6.5 Objednávateľ má právo počas trvania tejto Zmluvy podať voči Mesačnému výkazu Parkovného námietky v prípade, ak tento výkaz obsahuje nepravdivé alebo neoveriteľné údaje alebo neobsahuje Objednávateľom požadované údaje, a to v lehote do 10 (desiatich) kalendárnych dní odo dňa doručenia Mesačného výkazu Parkovného. Inak Mesačný výkaz Parkovného v rovnakej lehote schváli. Poskytovateľ je povinný Mesačný výkaz Parkovného upraviť v súlade s námietkami Objednávateľa v lehote do 5 (piatich) kalendárnych dní. Objednávateľ Mesačný výkaz Parkovného upravený v súlade s námietkami Objednávateľa schváli v lehote do 5 (piatich) kalendárnych dní od jeho doručenia. Súčasťou schváleného Mesačného výkazu Parkovného je aj aplikovaný podiel na trhu a celková výška odplaty za daný mesiac pre Poskytovateľa, ktoré Objednávateľ vypočíta v súlade s prílohami č. 3 a č. 7 tejto Zmluvy.

6.6 Poskytovateľ vystaví faktúru v súlade so schváleným Mesačným výkazom Parkovného a schváleným Mesačným výkazom prevádzky najneskôr 15. (pätnásty) deň kalendárneho mesiaca nasledujúceho po kalendárnom mesiaci, ku ktorému sa platba vzťahuje a bezodkladne ju doručí do sídla Objednávateľa.

6.7 Faktúry vystavené Poskytovateľom musia obsahovať všetky náležitosti vyplývajúce z platnej legislatívy, najmä, nie však výlučne zo zákona č. 222/2004 Z. z. o dani z pridanej hodnoty a zákona č. 431/2002 Z. z. o účtovníctve. Prílohou faktúry bude schválený Mesačný výkaz Parkovného a schválený Mesačný výkaz prevádzky.

6.8 Bankové spojenie Poskytovateľa uvedené na faktúre musí byť zhodné s bankovým spojením Poskytovateľa uvedeným v záhlaví tejto Zmluvy. O prípadnej zmene bankového spojenia (účtu) Poskytovateľ písomne informuje Objednávateľa v najneskôr v lehote 5 (päť) pracovných dní pred doručením faktúry, ktorá má byť uhradená na nový bankový účet Poskytovateľa.

6.9 Splatnosť faktúr bola dohodou Zmluvných strán určená na 30 (tridsať) dní od ich preukázateľného doručenia v listinnej podobe na adresu Objednávateľa.

6.10 Záväzok Objednávateľa zaplatiť Poskytovateľovi odplatu sa považuje za splnený dňom odpísania dlžnej fakturovanej sumy z bankového účtu Objednávateľa v prospech Poskytovateľa. V prípade, ak Poskytovateľ zmení počas účinnosti tejto Zmluvy číslo účtu a o tomto riadne neinformuje Objednávateľa spôsobom podľa bodu 6.8 tejto Zmluvy, záväzok Objednávateľa sa považuje za splnený bez ohľadu na to, či budú finančné prostriedky pripísané na účet Poskytovateľa.

6.11 Objednávateľ je oprávnený vrátiť Poskytovateľovi faktúru v lehote jej splatnosti, ak nespĺňa podmienky podľa bodu 6.7 tejto Zmluvy, spolu s písomnou výhradou.

6.12 V prípade nedoručenia faktúry v zmysle bodu 6.7 tejto Zmluvy alebo nesplnenia povinnosti Poskytovateľa v zmysle bodu 6.8 tejto Zmluvy, nezačne Objednávateľovi plynúť lehota podľa bodu 6.9 tejto Zmluvy. Nová lehota splatnosti začne Objednávateľovi plynúť riadnym doručením opravenej alebo doplnenej faktúry.

6.13 Poskytovateľ nie je oprávnený požadovať a nárokovať si náhradu bankových a iných poplatkov týkajúcich sa úhrady odplaty. Poskytovateľ rovnako nie je oprávnený požadovať preddavkové alebo zálohové platby.

Článok 7.

Práva a povinnosti pri Prevádzkovaní Aplikácie

7.1 Poskytovateľ sa zaväzuje vo Fáze prevádzkovania Aplikácie zabezpečiť pre Zákazníkov možnosť úhrady Parkovného prostredníctvom Aplikácie podľa podmienok tejto Zmluvy.

7.2 Na základe tejto Zmluvy je Poskytovateľ oprávnený v mene a na účet Objednávateľa prijímať úhrady Parkovného Zákazníkmi na Zberný účet. Uhradené Parkovné sa stáva vlastníctvom Objednávateľa momentom jeho pripísania na Zberný účet. Poskytovateľ nie je oprávnený vyberať Parkovné vo vlastnom mene a v žiadnom okamihu mu nevzniká k uhradenému Parkovnému vlastnícke právo.

7.3 Poskytovateľ je povinný zabezpečiť, aby výška Parkovného uhrádzaného Zákazníkmi cez Aplikáciu zodpovedala výške Parkovného stanoveného aktuálne platným všeobecne záväzným nariadením Objednávateľa upravujúcim dočasné parkovanie na Parkovacích miestach alebo Prevádzkovým poriadkom. Objednávateľ je povinný písomne oznámiť Poskytovateľovi zmenu výšky Parkovného v dostatočnom predstihu tak, aby mohol Poskytovateľ nové sadzby Parkovného včas implementovať. Pokiaľ sa zmení len výška Parkovného a nezmení sa vymedzenie Parkovacích miest, považuje sa za dostatočný časový predstih lehota 10 (desať) pracovných dní pred účinnosťou zmeny. Pokiaľ sa zmení vymedzenie Parkovacích miest, považuje sa za dostatočný časový predstih lehota 20 (dvadsať) pracovných dní pred účinnosťou zmeny.

7.4 Poskytovateľ sa zaväzuje, že:

7.4.1 umožní prostredníctvom Aplikácie vyhľadanie Parkovacieho miesta;

7.4.2 vo Fáze prevádzkovania Aplikácie bude poskytovať Zákazníkom v pracovné dni 9x5 8:00-17:00 zákaznícky servis na bezplatnom telefónnom čísle alebo e-mailovej/chat adrese podpory v slovenskom a anglickom jazyku,

7.4.3 Zákazníkom bude poskytovať informácie o prípadnej nedostupnosti funkcionalít Aplikácie, najmä o nemožnosti platby, neúspešnosti platby spolu s postupom nápravy.

7.4.4 zabezpečí bezpečné spracovanie osobných údajov Zákazníkov v súvislosti s plnením tejto Zmluvy a za podmienok dojednaných v Prílohe č. 8 tejto Zmluve,

7.4.5 zabezpečí poskytnutie zjednodušenej faktúry podľa § 74 ods. 3 písm. a) zákona o DPH Zákazníkovi v mene Objednávateľa ku každej úhrade Parkovného.

7.5 Poskytovateľ je povinný poukázať celý výťažok z Parkovného na účet Objednávateľa č. účtu (IBAN SK72 7500 0000 0000 2582 7813) vždy najneskôr do 5 (piatich) kalendárnych dní po skončení príslušného kalendárneho mesiaca.

7.6 Poskytovateľ nie je oprávnený žiadnym spôsobom nakladať s peňažnými prostriedkami zodpovedajúcimi uhradenému Parkovnému inak než spôsobom podľa bodu 7.5 tejto Zmluvy. Náklady spojené so zriadením a vedením Zberného účtu znáša Poskytovateľ.

7.7 Poskytovateľ sa zaväzuje bezodplatne sprístupniť Objednávateľovi alebo Audítorovi kompletné údaje týkajúce sa Zberného účtu na účely kontroly výšky úhrady za Parkovné a výšky odplaty Poskytovateľa, a to na základe písomnej žiadosti Objednávateľa alebo Audítora, v lehote do 5 (piatich) pracovných dní od doručenia žiadosti Poskytovateľovi.

7.8 Poskytovateľ poskytne Objednávateľovi Mesačný výkaz Parkovného za predchádzajúci mesiac vždy najneskôr do 5. dňa nasledujúceho mesiaca.

7.9 V prípade, ak Poskytovateľovi bude brániť v plnení niektorej jeho povinnosti podľa Zmluvy Vyššia moc, je Poskytovateľ povinný oznámiť Objednávateľovi udalosť a/alebo okolnosti, ktoré predstavujú Vyššiu moc, a uviesť povinnosti, v ktorých plnení mu Vyššia moc bráni a/alebo bude brániť. Oznámenie musí byť urobené bezodkladne, najneskôr v lehote 3 (troch) pracovných dní potom, čo sa Poskytovateľ dozvedel a/alebo sa pri vynaložení riadnej odbornej starostlivosti mal a mohol dozvedieť o príslušnej udalosti a/alebo okolnostiach predstavujúcich dôvod Vyššej moci. Poskytovateľ vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizoval omeškanie pri plnení svojich povinností podľa Zmluvy, ktoré vzniklo v dôsledku Vyššej moci. Poskytovateľ oznámi druhej Objednávateľovi okamih ukončenia pôsobenia Vyššej moci v rovnakej lehote ako pri oznámení o jej vzniku. Vyššie uvedené platí obdobne aj pre Objednávateľa.

7.10 V prípade, ak účinky Vyššej moci trvajú nepretržite viac ako 15 (pätnásť) kalendárnych dní a dotýkajú sa povinnosti a/alebo povinností podľa Zmluvy, bez plnenia ktorých nemá plnenie ostatných povinností podľa Zmluvy pre druhú Zmluvnú stranu zrejmý hospodársky význam, alebo ak sa dotýkajú všetkých povinností podľa Zmluvy, je druhá Zmluvná strana oprávnená od Zmluvy odstúpiť.

7.11 Objednávateľ je oprávnený kedykoľvek priebežne kontrolovať Prevádzkovanie Aplikácie a Poskytovateľ je povinný na tento účel Objednávateľovi poskytnúť nevyhnutnú súčinnosť.

7.12 Poskytovateľ je pri plnení Zmluvy povinný postupovať tak, aby jeho činnosťou ani činnosťou tretích osôb nedošlo ku škode na majetku Objednávateľa ani na majetku Zákazníkov, za prípadné škody spôsobené svojou činnosťou alebo činnosťou tretích osôb zodpovedá v plnej výške.

7.13 Poskytovateľ sa zaväzuje v lehote podľa bodu 5.1 tejto Zmluvy zriadiť a Objednávateľovi predložiť originál Bankovej záruky v zmysle ust. § 313 a nasl. Obchodného zákonníka, vystavenej tuzemskou bankou alebo pobočkou zahraničnej banky zriadenou na území Slovenskej republiky, ktorej obsahom bude je bezpodmienečné, neodvolateľné a časovo obmedzené vyhlásenie banky, že uspokojí na základe písomnej žiadosti Objednávateľa ako osobu oprávnenú z Bankovej záruky do výšky 25 000 EUR (slovom dvadsaťpäťtisíc euro) a to bez skúmania právnych vzťahov a bez výhrad.

7.14 Poskytovateľ Bankovou zárukou zabezpečí splnenie akejkoľvek peňažnej povinnosti Poskytovateľa podľa tejto Zmluvy, vrátane prípadného nároku Objednávateľa na náhradu škody spôsobenej Poskytovateľom v súvislosti s plnením predmetu tejto Zmluvy.

7.15 Poskytovateľ zabezpečí, aby Banková záruka bola platná počas celého trvania tejto Zmluvy a aspoň 3 mesiace po zániku záväzkov Poskytovateľa podľa tejto Zmluvy. Po dobu trvania Bankovej záruky nesmie byť Banková záruka odvolateľná bez písomného súhlasu Objednávateľa a práva z nej musia byť prevoditeľné na tretiu osobu spolu so zabezpečovanou pohľadávkou alebo jej časťou.

7.16 V prípade, ak Objednávateľ uspokojí svoju pohľadávku voči Poskytovateľovi z tejto Zmluvy z Bankovej záruky je povinný túto skutočnosť oznámiť Poskytovateľovi, ktorý je povinný bez zbytočného odkladu, najneskôr do 10 (desiatich) kalendárnych dní odo dňa doručenia oznámenia, zabezpečiť doplnenie Bankovej záruky do výšky podľa bodu 7.13 tejto Zmluvy a na celú dobu trvania Bankovej záruky. Splnenie povinnosti podľa tohto bodu Zmluvy preukáže Poskytovateľ predložením úradne osvedčenej kópie potvrdenia o doplnení Bankovej záruky

vydaného bankou. V prípade, ak Poskytovateľ nedoplní Bankovú záruku v lehote uvedenej v tomto bode Zmluvy vznikne Objednávateľovi právo odstúpiť od Zmluvy.

Článok 8.

Zodpovednosť za vady Aplikácie

8.1 Poskytovateľ zodpovedá za vady, chyby a nedostatky Aplikácie počas celej Fázy prevádzkovania Aplikácie. Za vadu Aplikácie sa považuje najmä nespĺňanie Technických a funkčných požiadaviek.

8.2 Poskytovateľ počas celej Fázy prevádzkovania Aplikácie vykonáva Monitorovanie prevádzky spôsobom a v rozsahu, aby bolo zabezpečené riadne a nepretržité Prevádzkovanie Aplikácie v súlade s Technickými a funkčnými požiadavkami.

8.3 Poskytovateľ zasiela Objednávateľovi Mesačný výkaz prevádzky vždy do 5. (piateho) dňa mesiaca nasledujúceho po mesiaci, v ktorom bolo Monitorovanie prevádzky vykonávané.

8.4 Mesačný výkaz prevádzky je základným podkladom na vykonávanie kontroly plnenia Technických a funkčných požiadaviek a záväzným podkladom pre odstraňovanie vád Aplikácie. Poskytovateľ zodpovedá za pravdivosť údajov uvedených v Mesačnom výkaze prevádzky.

8.5 Objednávateľ má právo počas trvania tejto Zmluvy podať voči Mesačnému výkazu prevádzky námietky v prípade, ak tento výkaz obsahuje nepravdivé alebo neoveriteľné údaje alebo neobsahuje Objednávateľom požadované údaje, a to v lehote do 10 (desiatich) kalendárnych dní odo dňa doručenia Mesačného výkazu prevádzky. Poskytovateľ je povinný Mesačný výkaz prevádzky upraviť v súlade s námietkami Objednávateľa v lehote do 5 (piatich) kalendárnych dní.

8.6 Poskytovateľ je povinný počas celej doby Prevádzkovania Aplikácie zabezpečiť na vlastné náklady odstránenie akýchkoľvek vád Aplikácie tak, aby bolo počas celého trvania tejto Zmluvy zabezpečené riadne a nepretržité Prevádzkovanie Aplikácie, a to v súlade s Technickými a funkčnými požiadavkami.

8.7 Poskytovateľ sa zaväzuje počas Fázy prevádzkovania Aplikácie detegovať, neutralizovať a hlásiť Incidenty Objednávateľovi. Poskytovateľ zaznamenáva údaje o Incidentoch a ich neutralizovaní v Mesačnom výkaze prevádzky.

8.8 Poskytovateľ je povinný obnoviť funkciu Aplikácie na úroveň definovanú v Technických a funkčných požiadavkách v čo najkratšom čase od detegovania Incidentu. Incident sa považuje za detegovaný momentom jeho identifikácie Poskytovateľom pri Monitorovaní prevádzky, alebo momentom nahlásenia Incidentu Poskytovateľovi Objednávateľom alebo treťou osobou telefonicky, emailom alebo prostredníctvom Aplikácie.

8.9 Poskytovateľ je povinný potvrdiť nahlásenie Incidentu Objednávateľom alebo treťou osobou ohlasovateľovi Incidentu a prípadne si vyžiadať od Objednávateľa alebo tretej osoby dodatočné informácie nevyhnuté pre analýzu a úspešné vyriešenie Incidentu.

8.10 Poskytovateľ je povinný zabezpečiť reakciu na Incident v dobe, ktorej dĺžka nesmie presiahnuť nasledujúce doby tzv. Response Time:

a) 60 (šesťdesiat) minút od identifikácie Kritického incidentu,
b) 2 (dve) hodiny od identifikácie Závažného incidentu,
c) 1 (jeden) kalendárne deň od identifikácie Nekritického incidentu.

Doba reakcie na Incident sa začína rátať od momentu detegovania Incidentu v zmysle bodu 8.7 tejto Zmluvy.

8.11 Za reakciu na Incident sa považuje formálna kontrola nahlásenej udalosti, identifikácia možnej príčiny s riadnou klasifikáciou, prioritizácia a ohlásenie Incidentu, jeho možnej príčiny, klasifikácie a prioritizácie Objednávateľovi na adresu servicedesk@bratislava.sk.

8.12 Poskytovateľ je povinný zabezpečiť neutralizáciu Incidentu v dobe, ktorej dĺžka nesmie presiahnuť nasiedujúce doby tzv. Fix Time:

a) 8 (osem) hodín v prípade Kritického incidentu,
b) 4 (štyri) kalendárne dni v prípade Závažného incidentu,
c) 14 (štrnásť) kalendárnych dní v prípade Nekritického incidentu.

Doba neutralizácie incidentu začína plynúť od najbližšej celej hodiny po uplynutí Response Time podľa bodu 8.10 tejto Zmluvy.

8.13 Incident sa považuje za neutralizovaný obnovením riadnej funkcionality Aplikácie v súlade s touto Zmluvou, najmä Technickými a funkčnými požiadavkami. Po neutralizácii Incidentu je Poskytovateľ povinný túto skutočnosť oznámiť Objednávateľovi na adresu servicedesk@bratislava.sk. Priebeh každého Incidentu spolu s popisom príčin vzniku Incidentu a spôsobu jeho vyriešenia zaznamená Poskytovateľ v Mesačnom výkaze prevádzky.

8.14 V prípade, ak Poskytovateľ v priebehu kalendárneho mesiaca opakovane (aspoň dvakrát) poruší povinnosti uvedené v bode 8.10 tejto Zmluvy, zníži Objednávateľ celkovú odplatu Poskytovateľa podľa bodu 6.1 tejto Zmluvy za príslušný kalendárny mesiac o 3 (tri) percentá. Každé ďalšie porušenie povinnosti uvedenej v bode 8.10 tejto Zmluvy potom vedie k zníženiu celkovej odplaty Poskytovateľa podľa bodu 6.1 tejto Zmluvy za príslušný kalendárny mesiac o 1,5 (jeden a pol) percenta.

8.15 V prípade, ak Poskytovateľ v priebehu kalendárneho mesiaca poruší povinnosti uvedené v bode 8.12 tejto Zmluvy, zníži Objednávateľ celkovú odplatu Poskytovateľa podľa bodu 6.1 tejto Zmluvy nasledovným mechanizmom. Objednávateľ udelí za každé porušenie povinnosti uvedené v bode 8.12 tejto Zmluvy sankčné body takto:

a) 2 (dva) sankčné body za každé porušenie vo vzťahu ku Kritickému incidentu,
b) 1 (jeden) sankčný bod za každé porušenie vo vzťahu k Závažnému Incidentu
c) 0,5 (nula celá päť desatín) sankčného bodu vo vzťahu ku každému Nekritickému incidentu.

Súčet sankčných bodov predstavuje percento, o ktoré sa zníži celková odplata Poskytovateľa podľa bodu 6.1 tejto Zmluvy za príslušný kalendárny mesiac. V prípade ak súčet sankčných bodov za ktorýkoľvek kaiendárny mesiac dosiahne 10 (desať) bodov, vznikne Objednávateľovi právo odstúpiť od Zmiuvy.

8.16 Úprava (zníženie) odplaty Poskytovateľa podľa bodov 8.14 a 8.15 sa neuplatní v prípade, ak Poskytovateľ preukáže, že incident boi spôsobený Vyššou mocou.

8.17 V prípade, ak Poskytovateľ poruší povinnosti uvedené v bode 8.12 tejto Zmiuvy, vznikne Poskytovateľovi povinnosť preukázať splnenie Technických a funkčných požiadaviek vo vzťahu k technickej a/alebo požiadavke, ktorej sa týka Incident Skúškami Aplikácie v rozsahu uvedenom v Prílohe č. 1 k tejto Zmluve a v lehote 10 (desiatich) pracovných dní. Povinnosť Poskytovateľa neutralizovať Incident tým nie je dotknutá.

8.18 Objednávateľ je oprávnený kedykoľvek počas trvania Fázy prevádzky vyzvať Poskytovateľa na preukázanie splnenia Technických a funkčných požiadaviek Skúškami Aplikácie v rozsahu uvedenom v Prílohe č. 1 k tejto Zmluve a v lehote 10 (desiatich) pracovných dní.

8.19 V prípade ak Poskytovateľ nepreukáže splnenie Technických a funkčných požiadaviek podľa bodu 8.17 alebo 8.18 tejto Zmluvy, vznikne Objednávateľovi právo odstúpiť od Zmiuvy.

Článok 9.

Zmluvné sankcie

9.1 Poskytovateľ má právo uplatniť si v prípade omeškania s plnením peňažných záväzkov Objednávateľa úrok z omeškania vo výške 0,05 % z nezaplatenej sumy za každý deň omeškania

formou vystavenia faktúry splatnej do 30 (tridsiatich) dní od jej doručenia Objednávateľovi.

9.2 Objednávateľ má právo uplatniť si zmluvnú pokutu vo výške 1 (jedno) percento z nezaplatenej sumy za každý deň omeškania Poskytovateľa so splnením povinnosti previesť Parkovné zo Zberného účtu na účet Objednávateľa podľa bodu 7.5 tejto Zmluvy formou vystavenia faktúry splatnej do 30 (tridsiatich) dní od jej doručenia Poskytovateľovi.

9.3 V prípade porušenia povinnosti Poskytovateľa podľa bodu 7.6 tejto Zmluvy má Objednávateľ právo uplatniť si zmluvnú pokutu vo výške 5.000,- EUR (slovom päťtisíc euro) za každé také porušenie povinnosti formou vystavenia faktúry splatnej 30 (tridsať) dní od jej doručenia Poskytovateľovi.

9.4 Objednávateľ si môže v prípade, že Poskytovateľ poruší niektorú z povinností ustanovených v bodoch 7.8 a 8.3 Zmluvy uplatniť zmluvnú pokutu vo výške 5.000,- EUR (slovom päťtisíc euro) za každé také porušenie povinnosti formou vystavenia faktúry splatnej 30 (tridsať) dní od jej doručenia Poskytovateľovi.

9.5 V prípade neoprávnenej manipulácie s Dôvernými informáciami podľa článku 10 tejto Zmluvy vzniká poskytovateľovi Dôvernej informácie nárok na zmluvnú pokutu vo výške 5.000,- EUR (slovom päťtisíc euro) voči prijímateľovi Dôvernej informácie, za každý jednotlivý prípad neoprávnenej manipulácie. Nárok na náhradu škody týmto nie je dotknutý.

9.6 Uplatnením zmluvných pokút podľa tohto článku nie je dotknutý nárok Zmluvnej strany na náhradu škody v plnej výške.

Článok 10.

Dôverné informácie a ochrana osobných údajov

10.1 Prijímateľ Dôvernej informácie je oprávnený:

- použiť Dôverné informácie výlučne na účely plnenia tejto Zmluvy a počas trvania tejto Zmluvy;
- poskytnúť Dôverné informácie tretím osobám iba v nevyhnutnom rozsahu a len s predchádzajúcim súhlasom poskytovateľa Dôvernej informácie, pričom zodpovedá za neoprávnenú manipuláciu s Dôvernými informáciami treťou osobou a poskytnutie Dôverných informácií tretej osobe je povinný bezodkladne oznámiť poskytovateľovi Dôvernej informácie;
- poskytnúť Dôverné informácie bez súhlasu poskytovateľa Dôvernej informácie len v prípadoch a v rozsahu určených Právnym poriadkom.

10.2 Prijímateľ Dôvernej informácie je povinný:

- zdržať sa neoprávnenej manipulácie s Dôvernými informáciami;
- prijať a dodržiavať také technické, organizačné a iné opatrenia potrebné na ochranu Dôverných informácií, ktoré mu boli alebo mu budú poskytnuté, alebo sprístupnené, aby bolo účinne zabránené pred neoprávnenou manipuláciou s Dôvernými informáciami;
- bez zbytočného odkladu oznámiť poskytovateľovi Dôvernej informácie každú neoprávnenú manipuláciu s Dôvernými informáciami;
- poskytnúť poskytovateľovi Dôvernej informácie všetku súčinnosť potrebnú na odstránenie následkov neoprávnenej manipulácie s Dôvernými informáciami;
- zabezpečiť oboznámenie sa s povinnosťami podľa tejto Zmluvy tretie osoby, ktorým poskytne Dôverné informácie;
- po skončení trvania Zmluvy vrátiť poskytovateľovi Dôvernej informácie všetky originály, kópie, reprodukcie alebo iné zhrnutia Dôverných informácií a všetky Dôverné informácie nahraté v systémoch prijímateľa Dôvernej informácie alebo tretích osôb podľa bodu 10.1 tejto Zmluvy preukázateľne zničiť.

10.3 Poskytovateľ Dôvernej informácie má právo odmietnuť poskytnutie Dôverných informácii, ak takéto poskytnutie nebude nevyhnutne potrebné k naplneniu účelu tejto Zmluvy.

10.4 Prijímateľ Dôvernej informácie zodpovedá za každú neoprávnenú manipuláciu s Dôvernými informáciami, ktoré mu boli poskytnuté a zodpovedá za neoprávnenú manipuláciu s Dôvernými informáciami, ktoré poskytol tretej osobe.

10.5 Poskytnutím Dôverných informácii neprechádza na prijímateľa Dôvernej informácie vlastnícke alebo iné právo alebo licencia k Dôverným informáciám.

10.6 Poskytovateľ sa zaväzuje pri plnení tejto Zmluvy plniť všetky povinnosti, ktoré mu vyplývajú z Právneho poriadku vo vzťahu k ochrane osobných údajov. Pri spracúvaní osobných údajov Zákazníkov zabezpečí Poskytovateľ splnenie všetkých povinností sprostredkovateľa voči dotknutým osobám podľa Právneho poriadku vo vzťahu k ochrane osobných údajov.

10.7 Poskytovateľ sa najmä zaväzuje získavať osobné údaje dotknutých osôb výlučne na účely plnenia povinností Poskytovateľa podľa tejto Zmluvy, vrátane. riadneho plnenia informačnej povinnosti vo vzťahu k dotknutým osobám.

10.8 Poskytovateľ je povinný preukázateľne poučiť svojich zamestnancov o povinnostiach ochrany údajov a záväzku mlčanlivosti o údajoch podľa Právneho poriadku vo vzťahu k ochrane osobných údajov, s ktorými prídu/by mohli prísť do styku pri vykonávaní činností pre Objednávateľa.

10.9 Pravidlá a podmienky spracúvania osobných údajov Poskytovateľom sú predmetom samostatnej zmluvy uzatvorenej medzi Objednávateľom a Poskytovateľom, ktorá tvorí prílohu č. 8 k tejto Zmluve.

10.10 Poskytovateľ sa zaväzuje zakotviť vo svojich zmluvách so subdodávateľmi obdobnú úpravu práv a povinností vo vzťahu k výmene dôverných informácií a ochrany osobných údajov ako je uvedená v tomto článku Zmluvy.

Článok 11.

Doručovanie

11.1 Odstúpenie od Zmluvy, oznámenie o nesplnení Podmienok oprávnenosti podľa bodu 4.3 tejto Zmluvy, oznámenie o nepreukázaní splnenia Technických a funkčných požiadaviek podľa bodu 5.6 tejto Zmluvy, dodatky k Zmluve, faktúry, oznámenie zmeny údajov podľa bodu 6.8 alebo 11.3 tejto Zmluvy budú vyhotovené písomne a doručené druhej Zmluvnej strane osobne, prostredníctvom elektronickej schránky podľa zákona o e-Governmente, ak je zriadená a funkčná alebo zaslané poštou. Odstúpenie od Zmluvy doručujú Zmluvné strany formou doporučenej listovej zásielky.

11.2 Listovú zásielku je možné doručovať prostredníctvom poštového podniku alebo kuriéra na adresu Zmluvnej strany uvedenú v záhlaví tejto Zmluvy. Za doručenú sa považuje každá listová zásielka, ktorá:

a) bola adresátom prevzatá dňom jej prevzatia,

b) prevzatie bolo adresátom odmietnuté, dňom, kedy bolo prevzatie odmietnuté,

c) bola uložená na pobočke poštového podniku uplynutím tretieho dňa od uloženia, aj keď sa adresát s jej obsahom neoboznámil.

11.3 Ostatné prejavy vôle Zmluvných strán, na ktoré sa nevzťahuje bod 11.1 tejto Zmluvy, môžu byť doručované tiež na nasledovné adresy:

11.3.1 Objednávateľovi elektronicky na adresu: mpa@bratislava.sk

11.3.2 Poskytovateľovi elektronicky na adresu: patrik.piscak@easypark.net

11.4 Zmluvné strany sú oprávnené adresy podľa bodu 11.3 Zmluvy jednostranne meniť bez potreby

uzavretia dodatku. Takáto zmena je voči druhej Zmluvnej strane účinná dňom, keď jej bude doručené písomné oznámenie o zmene.

11.5 Elektronická správa sa považuje za doručenú deň nasledujúci po jej odoslaní na emailovú adresu podľa bodu 11.3 tejto Zmluvy a to aj vtedy, ak sa adresát o jej obsahu nedozvedel. Uvedené neplatí, ak je odosielateľovi doručená automatická správa o nemožnosti adresáta oboznámiť sa so správou spolu s uvedením inej kontaktnej osoby.

11.6 V prípade vyhlásenia mimoriadnej situácie alebo mimoriadnej udalosti v zmysle zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov alebo v prípade vyhlásenia vojny, vojnového stavu, výnimočného alebo núdzového stavu v zmysle ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov, je možné doručovať tie písomnosti, ktoré môžu mať za následok vznik, zmenu alebo zánik práv a povinností Zmluvných strán vyplývajúcich z tejto Zmluvy aj prostredníctvom elektronickej schránky v zmysle zákona o e-Governmente. Doručovanie písomností zaslaných prostredníctvom elektronickej schránky v zmysle zákona o e-Governmente sa riadi príslušnými ustanoveniami tohto zákona.

11.7 Zmluvné strany sú povinné minimálne raz denne kontrolovať kontaktné emailové schránky.

Článok 12.

Zmenové konanie

12.1 Zmluvné strany sa dohodli, že Objednávateľ je oprávnený jedenkrát ročne, v čase, ktorý určí Objednávateľ, otvárať okruh poskytovateľov služby úhrady Parkovného cez mobilnú aplikáciu a na základe skúseností s prevádzkou mobilných aplikácií na úhradu Parkovného a situácie na trhu poskytovateľov týchto služieb pripraviť a zverejniť nový verejný návrh na uzavretie zmluvy na Nové obdobie.

12.2 Objednávateľ je oprávnený, najneskôr v lehote do 30 (tridsiatich) kalendárnych dní pred uplynutím doby trvania tejto Zmluvy, vypracovať a doručiť Poskytovateľovi návrh dodatku k tejto Zmluve, ktorým sa úprava vzájomných práv a povinností podľa tejto Zmluvy zosúladí s úpravou verejného návrhu na uzavretie zmluvy na Nové obdobie podľa bodu 12.1 tejto Zmluvy.

12.3 V prípade, ak Poskytovateľ návrh dodatku neprijme do 10 (desiatich) kalendárnych dní pred uplynutím doby trvania tejto Zmluvy, Zmluva zanikne uplynutím doby jej trvania podľa bodu 14.1 tejto Zmluvy.

12.4 Po uzavretí dodatku podľa bodu 12.2 tejto Zmluvy Poskytovateľ preukáže splnenie Podmienok oprávnenosti spôsobom dojednaným v bode 4.2 tejto Zmluvy.

12.5 Pre vylúčenie pochybností Zmluvné strany výslovne uvádzajú, že zmeny podľa tohto článku Zmluvy sa môžu týkať akéhokoľvek dojednania v tejto Zmluve alebo jej prílohách. V prípade, ak sa zmeny budú týkať Technických a funkčných požiadaviek, Objednávateľ poskytne Poskytovateľovi primeraný čas na úpravu Aplikácie. Ak to bude povaha zmien vyžadovať, obdobne sa uplatní úprava Skúšok Aplikácie podľa bodu 8.18 tejto Zmluvy. Do momentu úspešného absolvovania Skúšok Aplikácie prevádzkuje Poskytovateľ Aplikáciu v súlade s pôvodnými Technickými a funkčnými požiadavkami.

Článok 13.

Spoločné ustanovenia

13.1 Zmluvné strany sa v súlade s ustanovením § 364 Obchodného zákonníka dohodli, že Objednávateľ si môže započítať voči Poskytovateľovi akékoľvek svoje pohľadávky vyplývajúce z tejto Zmluvy voči akýmkoľvek pohľadávkam Poskytovateľa vyplývajúcim z tejto Zmluvy, a to bez ohľadu na to, či pohľadávky Objednávateľa sú budúce, súčasné, podmienené alebo nepodmienené, splatné alebo sú premlčané. Objednávateľ bezodkladne písomne oznámi Poskytovateľovi realizáciu zápočtu. Poskytovateľ nie je oprávnený jednostranne započítať svoje

pohľadávky bez predchádzajúceho písomného súhlasu Objednávateľa.

13.2 Poskytovateľ nie je oprávnený bez predchádzajúceho písomného súhlasu Objednávateľa postúpiť alebo previesť Zmluvu, jej časť, resp. výhody, úžitky či pohľadávky z nej vyplývajúce. Poskytovateľ nie je taktiež oprávnený bez predchádzajúceho písomného súhlasu Objednávateľa svoje pohľadávky z tejto Zmluvy založiť alebo iným spôsobom zaťažiť právom tretích osôb. Ak Poskytovateľ postúpi alebo prevedie Zmluvu, jej časť resp. výhody, úžitky či pohľadávky z nej vyplývajúce alebo založí alebo inak zaťaží právom tretích osôb svoje pohľadávky bez predchádzajúceho písomného súhlasu Objednávateľa, bude sa to považovať za podstatné porušenie zmluvných povinností zo strany Poskytovateľa, ktoré bude Objednávateľa oprávňovať na odstúpenie od Zmluvy.

13.3 Súhlas Objednávateľa s postúpením alebo prevedením Zmluvy alebo jej časti na tretiu osobu nezbavuje Poskytovateľa jeho záväzkov a zodpovednosti vyplývajúcich z časti Zmluvy, ktorá už bola splnená alebo za časť Zmluvy, ktorá nebola postúpená.

13.4 Postupník musí spĺňať všetky požiadavky ustanovené pre uzatvorenie Zmluvy medzi Objednávateľom a Poskytovateľom.

13.5 Objednávateľ je oprávnený postúpiť svoje práva a povinnosti zo Zmluvy na akúkoľvek tretiu osobu z dôvodu zmien v platných právnych predpisoch alebo iných zmien, ktoré môžu viesť k úprave oprávnení alebo kompetencií Objednávateľa, s čím Poskytovateľ vyjadruje svoj výslovný predchádzajúci súhlas. Zmenu údajov uvedených v tejto Zmluve a ostatných údajov, ktoré si Zmluvné strany oznamujú v zmysle tejto Zmluvy, ako aj osôb oprávnených konať v mene Zmluvnej strany, je Zmluvná strana povinná oznámiť druhej Zmluvnej strane písomne.

13.6 Poskytovateľ je povinný oznámiť Objednávateľovi začatie vstupu do likvidácie Poskytovateľa, začatie exekučného konania na majetok Poskytovateľa a začatie konania podľa zákona č. 7/2005 Z. z. o konkurze a reštrukturalizácii v znení neskorších predpisov. Poskytovateľ je počas trvania Zmluvy tiež povinný písomne oznámiť Objednávateľovi dátum zrušenia registrácie platiteľa DPH, dátum registrácie platiteľa DPH a to bezodkladne po tomto dátume.

Článok 14.
Trvanie Zmluvy

14.1 Zmluva sa zatvára na dobu určitú do 31.12.2022.

14.2 Zmluvné strany sa dohodli, že Zmluvu je možné ukončiť okamžitým odstúpením od Zmluvy v prípade podstatného porušenia Zmluvy, za ktoré sa popri dôvodoch v zmysle Obchodného zákonníka alebo dôvodoch uvedených na inom mieste v tejto Zmluve považuje, ak:

14.2.1 Poskytovateľ:

a) poruší povinnosti vyplývajúce z bodu 7.1, 7.3, 7.4, 7.5, 7.6 alebo 7.7 tejto Zmluvy;

b) je v omeškaní so splnením povinnosti podľa bodu 7.8 alebo 8.3 Zmluvy o viac ako 10 (desať) kalendárnych dní;

c) neplní Zmluvu v dôsledku Vyššej moci po dobu uvedenú v bodu 7.10 tejto Zmluvy;

d) dostane sa do omeškania s plnením povinností podľa bodu 7.13 až 7.16 tejto Zmluvy;

e) dosiahne počet sankčných bodov v zmysle bodu 8.15 tejto Zmluvy;

f) nepreukáže splnenie Technických a funkčných požiadaviek podľa bodu 8.17 alebo 8.18 tejto Zmluvy;

g) poruší ktorúkoľvek povinnosť podľa bodu 13.2 tejto Zmluvy;

h) poškodzuje dobré meno a oprávnené záujmy Objednávateľa alebo sa angažuje v akomkoľvek korupčnom správaní;

i) podlieha zákonu č. 7/2005 Z.z. o konkurze a reštrukturalizácii v znení neskorších predpisov a podľa tohto zákona boi podaný návrh na vyhlásenie konkurzu na majetok Poskytovateľa.

14.2.2 Objednávateľ:

a) nezaplatí Odplatu v lehote viac ako 30 (tridsať) kalendárnych dní po splatnosti faktúry napriek predchádzajúcemu písomného upozorneniu Poskytovateľa.

14.3 Odstúpenie od Zmluvy je účinné dňom jeho doručenia druhej Zmluvnej strane.

14.4 Zmluva tiež zaniká:

a) doručením písomného oznámenia o nesplnení Podmienok oprávnenosti Poskytovateľovi podľa bodu 4.3 tejto Zmluvy;

b) doručením oznámenia o nepreukázaní splnenia Technických a funkčných požiadaviek podľa bodu 5.6 tejto Zmluvy;

c) uplynutím doby podľa bodu 14.1 tejto Zmluvy, na ktorú bola dojednaná.

14.5 Zánikom tejto Zmluvy zaniká oprávnenie Poskytovateľa prijímať úhradu Parkovného v mene a na účet Objednávateľa. Poskytovateľ je v prípade zániku Zmluvy povinný najmä:

a) bezodkladne informovať Zákazníkov, ktorí majú Aplikáciu stiahnutú, o ukončení poskytovania služieb Poskytovateľom podľa tejto Zmluvy,

b) bezodkladne znefunkčniť Aplikáciu tak, aby ďalej neumožňovala Zákazníkom uskutočňovať úhradu Parkovného,

c) v lehote do 3 (troch) pracovných dní od zániku Zmluvy poukázať výťažok z Parkovného na účet Objednávateľa podľa bodu 7.6 tejto Zmluvy,

d) v lehote do 5 (piatich) pracovných dní od zániku Zmluvy doručiť Objednávateľovi Mesačný výkaz Parkovného a Mesačný výkaz prevádzky.

Článok 15.

Záverečné ustanovenia

15.1 Táto Zmluva nadobúda platnosť dňom prijatia Verejného návrhu a účinnosť deň nasledujúci po dni jej zverejnenia na webovom sídle Objednávateľa v zmysle ust. § 5a a nasl. zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií).

15.2 Táto Zmluva je vyhotovená v 4 (štyroch) rovnopisoch, z ktorých má každý právnu silu originálu, z ktorých každá Zmluvná strana dostane po 2 (dvoch) rovnopisoch.

15.3 Právne vzťahy vyplývajúce Zmluvným stranám z tejto Zmluvy sa riadia Právnym poriadkom, a to najmä, nie však výlučne, Obchodným zákonníkom a Občianskym zákonníkom.

15.4 Zmluvné strany sa zaväzujú, že žiadne ustanovenie tejto Zmluvy ani jej príloh nebude vykladané spôsobom, ktorý by bol v rozpore s Preambulou, účelom Zmluvy podľa článku 2 alebo predmetnom Zmluvy podľa článku 3.

15.5 Zmena tejto Zmluvy je možná len formou písomného dodatku k tejto Zmluve očíslovaného vo vzostupnom poradí, ktorý bude podpísaný štatutárnymi orgánmi Zmluvných strán.

15.6 Neplatnosť, neúčinnosť alebo neaplikovateľnosť niektorého ustanovenia tejto Zmluvy nespôsobuje neplatnosť, neúčinnosť alebo neaplikovateľnosť tejto Zmluvy ako celku.

15.7 V prípade neplatnosti, neúčinnosti alebo neaplikovateľnosti niektorého ustanovenia tejto Zmluvy sú Zmluvné strany povinné vyvinúť všetku súčinnosť, ktorú od nich možno spravodlivo požadovať, aby neplatné, neúčinné alebo neaplikovateľné ustanovenie tejto Zmluvy nahradili novým ustanovením v súlade s účelom a predmetom tejto Zmluvy. V prípade, ak bude právny predpis citovaný v tejto Zmluve zrušený a nahradený iným právnym predpisom, odkazy tejto Zmluvy na nahradený právny predpis sa budú považovať za odkazy na právny predpis, ktorý ho nahradil.

15.8 Keď táto Zmluva stanovuje lehoty alebo termíny v dňoch alebo mesiacoch a neustanovuje v konkrétnom prípade inak, dňom alebo mesiacom sa vždy rozumie kalendárny deň alebo kalendárny mesiac.

15.9 Táto Zmluva bude vykladaná v súlade so všeobecnými pravidlami slovenského jazyka. Vzájomná komunikácia medzi Zmluvnými stranami bude prebiehať v slovenskom jazyku, prípadne v českom jazyku, pokiaľ sa Zmluvné strany nedohodnú inak.

15.10 Zmluvné strany sa zaväzujú vynaložiť primerané úsilie pri riešení vzájomných sporov vyplývajúcich z tejto Zmluvy, ktoré budú riešené v prvom rade zmierlivým spôsobom a dialógom. V prípade, ak zmierlivý spôsob riešenia vzájomných sporov nebude úspešný, právomoc riešiť spory vyplývajúce z tejto Zmluvy majú súdy Slovenskej republiky.

15.11 Neoddeliteľnou súčasťou tejto Zmluvy sú nasledujúce prílohy:

Príloha č. 1: Technické a funkčné požiadavky

Príloha č. 2: Podmienky oprávnenosti a spôsob ich preukázania

Príloha č. 3: Spôsob určenia výšky podielu na trhu

Príloha č. 4: Mesačný výkaz Parkovného (formulár)

Príloha č. 5: Mesačný výkaz prevádzky (formulár)

Príloha č. 6: ParkSysAPI

Príloha č. 7: Model odmeňovania

Príloha č. 8: Zmluva o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností a ochrany osobných údajov

Príloha č. 9: Vyhlásenie k splneniu Technických a funkčných požiadaviek

V Bratislave dňa _____

V Bratislave dňa 21.1.2022

Za objednávateľa:

Za poskytovateľa:

PRÍLOHA 1
Rozsah činností Dodávateľa v zmysle Základného kontraktu

Predmetom Základného kontaktu je vytvorenie mobilnej aplikácie na zabezpečenie:

- bezproblémovej, časovo a administratívnej efektívnej úhrady parkovného zákazníkmi Prevádzkovateľa,
- kontroly úhrady parkovného na základe integrácie aplikácie do systému ParkSys.

Dodávateľ apilkáciu vytvorí, otestuje a integruje do systému ParkSys v súlade s požiadavkami Prevádzkovateľa uvedenými v Základnom kontrakte.

Dodávateľ je v zmysle Základného kontraktu povinný:

- umožniť zákazníkovi Prevádzkovateľa bezodplatne inštalovať aplikáciu do mobilného zariadenia zákazníka;
- umožniť prostredníctvom aplikácie vyhľadanie parkovacieho miesta,
- zabezpečiť zákazníkovi Prevádzkovateľa prostredníctvom apiikácie bezpečné pripojenie na platobný systém banky a umožniť zaplatiť parkovné prostredníctvom platobnej karty na zberný účet Prevádzkovateľa;
- zabezpečiť bezpečné spracovanie osobných údajov zákazníkov Prevádzkovateľa v súvislosti s plnením Základného kontraktu,
- zabezpečiť poskytnutie zjednodušenej faktúry podľa § 74 ods. 3 písm. a) zákona o DPH zákazníkovi Prevádzkovateľa v mene Prevádzkovateľa ku každej úhrade parkovného;
- prostredníctvom aplikácie upozorniť zákazníka Prevádzkovateľa na to, že sa mu končí doba, za ktorú má zaplatené parkovné;
- zabezpečiť zákazníkovi Prevádzkovateľa možnosť prostrednictvom aplikácie predĺžiť dobu užívania parkovacieho miesta.

PRÍLOHA 2
Špecifikácia a rozsah bezpečnostných opatrení

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

1. Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre Dodávateľa záväzný a obsahuje najmenej
   a) určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
   b) základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré Dodávateľ má zavedené a riadi sa nimi v oblastiach:
      - organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
      - riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
      - personálna bezpečnosť,
      - riadenie prístupov,
      - riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
      - bezpečnosť pri prevádzke informačných systémov a sieti,
      - hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
      - ochrana proti škodlivému kódu,
      - sieťová a komunikačná bezpečnosť,
      - akvizícia, vývoj a údržba informačných technológií,
      - zaznamenávanie udalostí a monitorovanie,
      - riadenie kontinuity procesov, fyzická bezpečnosť a bezpečnosť prostredia,
      - riešenie kybernetických bezpečnostných incidentov,
      - kryptografické opatrenia,
      - kontinuita prevádzky informačných technológií,
      - audit a kontrolné činnosti.

B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:
1. Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Návrh a prijatie bezpečnostných opatrení.
3. Periodické preskúmavanie rizík.
   a) identifikácia všetkých významných informačných aktív Dodávateľa a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
   b) Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
   c) Vypracovanie a implementácia interného riadiaceho aktu na riadenie bezpečnostných rizík, ktorý obsahuje najmenej:
      - zodpovednosť za vykonanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
      - proces vykonávania analýzy rizík,
      - maticu určenia závažnosti rizika,
      - periodicitu vykonávania analýzy rizík,
      - spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v podľa matice určenia závažnosti rizika.
4. Vykonávanie analýzy rizík najmenej raz za rok.
5. Vytvorenie a udržiavanie zoznamu informačných aktív.

C. Personálna bezpečnosť

1. Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.
2. Dodávateľ zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.

3. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
4. Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí:
   a) vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
   b) zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
   c) zrušenie prístupových práv v informačných systémoch verejnej správy,
   d) odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
5. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
6. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.
7. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, najmä:
   a) prideľovanie prístupových práv,
   b) zásady tvorby a používania hesiel,
   c) zásady ochrany pred infiltráciou škodlivým kódom,
   d) zásady bezpečného používania elektronickej pošty,
   e) zásady bezpečného používania internetu,
   f) zásady bezpečného používania komunikačných nástrojov a sociálnych sietí,
   g) zásady používania prenosných zariadení a médií,
   h) zálohovanie údajov,
   i) riešenie kybernetických bezpečnostných incidentov,
   j) ochranu fyzického majetku,
   k) pohyb v priestoroch Dodávateľa.
8. Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
9. Zavedenie procesu preukázateľného oboznámenia správcov informačných technológií verejnej správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.
10. Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za rok.
11. Na prístup k informačným technológiám verejnej správy sa vyžaduje:
   a) oboznámenie so spôsobom používania informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy v rozsahu svojej pracovnej náplne,
   b) poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente,
   c) oboznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy.

D. Riadenie prístupov

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy.
2. Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy.
3. Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok.
4. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.
5. Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
6. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
7. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.

8. Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá umožni používateľom najmä:
   a) zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,
   b) presadzovať určenú štruktúru hesla,
   c) vyžadovať pravidelnú zmenu hesla,
   d) uchovávať a prenášať používateľské heslá bezpečným spôsobom.
9. Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do informačných technológii verejnej správy a ich obmedzenie len na nevyhnutné prípady.
10. Preskúmavanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok.
11. Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií verejnej správy a na prácu na diaľku.
12. Automatické zaznamenávanie každého prístupu administrátora do informačných technológii verejnej správy a automatické zaznamenávanie prístupu používateľa.
13. Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy.
14. implementácia centrálnej správy identít (IDM).
15. Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.
16. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov.
17. Implementácia, vynucovanie prístupových rolí v Informačných technológiách verejnej správy.
18. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov.

E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

1. V zmluve so Subdodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií verejnej správy.
3. Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú najmenej záväzok:
   a) plnenia určených požiadaviek a kritérií pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti pri dodávke predmetu zmluvy,
   b) ochrany informácií, ku ktorým je poskytnutý prístup,
   c) oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti a ďalších opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti špecifických na plnenie predmetu Základného kontraktu a tejto Zmluvy,
   d) riadenia a monitorovania prístupov do informačných technológií verejnej správy vrátane spôsobu a mechanizmu,
   e) možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
   f) oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľnosti informačných technológií verejnej správy zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,
   g) spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
   h) zachovania úrovne kybernetickej bezpečnosti a informačnej bezpečnosti pri významných zmenách vrátane spôsobu a formy prechodu k inému Subdodávateľovi.
4. Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti a posúdia sa najmä
   a) kritické komponenty a prvky služby,
   b) možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
   c) možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch medzi Dodávateľom a Subdodávateľmi,
   d) ďalšie možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému Subdodávateľovi.
5. Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.

6. Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti Dodávateľa.
7. Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.
8. Pre informačné technológie verejnej správy, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.
9. Interný predpis ustanovujúci zásady kybernetickej bezpečnosti a informačnej bezpečnosti pre Subdodávateľov a tretie strany obsahuje najmenej bezpečnostné požiadavky:
   a) pri riadení vzťahov so Subdodávateľmi,
   b) pri ošetrení kybernetickej bezpečnosti a informačnej bezpečnosti v zmluvách so Subdodávateľmi,
   c) dodávateľských reťazcov informačných technológií verejnej správy,
   d) monitorovania a preskúmavania dodávateľských služieb,
   e) riadenia zmien v službách Subdodávateľa,
   f) na prístupové práva a účty,
   g) na fyzickú bezpečnosť,
   h) na ochranu a zálohovanie dát,
   i) na mobilné prostriedky a vzdialený prístup.
10. Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu so Subdodávateľmi.

F. Bezpečnosť pri prevádzke informačných systémov a sietí

1. Na účinnú prevenciu pred stratou dát u Dodávateľa sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru.
2. Dodávateľ vypracuje a dodržiava politiku zálohovania, ktorá definuje požiadavky Prevádzkovateľa na zálohovanie vrátane doby uchovávania, testovania záloh, ako aj opatrenia na ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.
4. Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.
5. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
6. Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.
7. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.
8. Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú.
9. Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.
10. Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.
11. Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.
12. V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.
13. Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:
   a) operačné systémy,
   b) virtualizačné prostredia,
   c) aplikačný softvér,
   d) pracovné stanice,
   e) sieťové zariadenia, vrátane bezpečnostných zariadení,
   f) databázové prostredia.

14. Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.
15. Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

G. Hodnotenie zraniteľností a bezpečnostné aktualizácie

Nastavenie automatickej aktualizácie operačného systému a aplikácií.

1. Dodávateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
2. Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.
3. Vykonávanie hodnotenie zraniteľnosti najmenej raz ročne.
4. Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií verejnej správy.
5. Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológii verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľnosti a aktualizácií.
6. Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy.
7. Primárnymi zdrojmi na identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú
   a) informácie zo systémov a automatizovaných technológií pre aktualizáciu,
   b) informačný servis výrobcov technológií,
   c) výstupy z bezpečnostných technológií,
   d) výsledky penetračných testov,
   e) oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti,
   f) webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti.
8. Výnimky z implementácie bezpečnostných aktualizácií sa schvaľujú a evidujú manažérom kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý určuje bezpečnostné opatrenia na ochranu pred zneužitím zraniteľnosti, na elimináciu ktorej je bezpečnostná aktualizácia vydaná.
9. Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií.
10. Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.
11. Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verejnej správy verifikovaný, najmä jeho správna funkcionalita.
12. Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.
13. Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

H. Ochrana proti škodlivému kódu

1. Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.
3. Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na
   a) používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
   b) škodlivé emailové prílohy a odkazy,
   c) podozrivé a škodlivé webové stránky a odkazy,
   d) externú a internú sieťovú komunikáciu u Dodávateľa vrátane webových sídiel,
   e) prenos súborov z externých sietí.
4. Vytvorenie procesu alebo postupu na prenos súborov z externých sieti, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.
5. Zavedenie ochrany informačných technológií verejnej správy pred škodlivým kódom najmenej v rozsahu
   a) kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,

b) detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách verejnej správy,
c) kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
d) detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu.

6. Zavedenie ochrany pred nevyžiadanou elektronickou poštou.
7. Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu.
8. Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov.
9. Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom.

I. Sieťová a komunikačná bezpečnosť

1. Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.
2. Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:
   a) pravidelná aktualizácia firmvéru,
   b) zmena továrensky nastavených autentifikačných údajov,
   c) pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
   d) vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.
3. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.
4. Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.
5. Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.
6. Správa počítačových sietí je riadená a kontrolovaná.
7. Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb.
8. Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.
9. Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni.
10. Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.
11. Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.
12. Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.
13. Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.
14. Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.
15. Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii.
16. Vzdialený prístup do vnútornej siete Dodávateľa musí podliehať autentifikácii a autorizácii.
17. Dodávateľ implementuje technológiu detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.
18. Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
19. Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.

J. Akvizícia, vývoj a údržba informačných technológií verejnej správy

1. Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Pri vytváraní nových alebo úprave existujúcich informačných technológii verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.
3. Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov.
4. informácie prenášané prostredníctvom verejných sieti sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.
5. Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.
6. Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.
7. Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológii verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.
8. Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácii, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.
9. Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre Prevádzkovateľa, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.

K. Zaznamenávanie udalosti a monitorovanie

Zaznamenávanie úspešných a neúspešných autentifikačných udalostí.

1. Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy.
2. Pre každý prvok informačných technológii verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované.
3. Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:
   a) úspešné a neúspešné autorizačné udalosti,
   b) úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
   c) úspešné a neúspešné prístupy k log súborom,
   d) úspešné a neúspešné prístupy k systémovým zdrojom,
   e) vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
   f) zmeny v prístupových oprávneniach,
   g) aktivácia a deaktivácia bezpečnostných mechanizmov,
   h) spustenie a zastavenie procesov,
   i) konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
   j) spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
   k) významné aktivity v sieťovej komunikácii,
   l) požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
   m) IP adresy pridelené prostredníctvom služby DHCP.
4. Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:
   a) čas a dátum udalosti,
   b) identifikácia používateľa,

c) identifikácia zariadenia,
d) informácia týkajúca sa udalosti,
e) indikácia úspešnosti, alebo zlyhania operácie,
f) pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port.

5. Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.
6. Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.
7. Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.
8. Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja.
9. Dodávateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy.
10. Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
11. Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.
12. Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.
13. Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.
14. Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.
15. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

L. Fyzická bezpečnosť a bezpečnosť prostredia

1. Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.
2. Umiestnenie informačných technológií verejnej správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa.
3. Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.
4. Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám.
5. Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá
   a) údržby, uchovávania a evidencie technických komponentov informačných technológií verejnej správy a zariadení informačných technológií verejnej správy,
   b) používania zariadení informačných technológií verejnej správy na iné účely, než na aké sú pôvodne určené,
   c) používania zariadení informačných technológií verejnej správy mimo určených priestorov,
   d) vymazávania, vyraďovania a likvidovania zariadení informačných technológií verejnej správy a všetkých typov relevantných záloh,
   e) prenosu technických komponentov informačných technológií verejnej správy alebo zariadení informačných technológií verejnej správy mimo priestorov orgánu riadenia,
   f) narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií verejnej správy tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.
6. Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.
7. Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.
8. Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.

M. Riešenie kybernetických bezpečnostných incidentov

1. Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe.
2. Dodávateľ má na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov.
3. Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.
4. S interným riadiacim aktom, najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy.
5. Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto.
6. Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.
7. Proces odborného posúdenia a analýzy oznámení realizuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT.
8. Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.
9. Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy.
10. Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov.
11. Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
12. Dodávateľ má vytvorené plány na riešenie kybernetických bezpečnostných incidentov.

N. Kryptografické opatrenia

Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS
https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=181

1. Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
2. Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä
   a) elektronických dokumentov,
   b) dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
   c) emailovej komunikácie prostredníctvom PGP alebo S/MIME,
   d) komunikačných kanálov na výmenu nešifrovaných dát,
   e) centrálnych úložísk,
   f) záloh.
3. Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä
   a) princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
   b) definovanie požadovanej úrovne ochrany a štandardy šifrovania,
   c) roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
   d) riadenie šifrovacích kľúčov.

4. Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.
5. Dodávateľ pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.

O. Kontinuita prevádzky informačných technológií verejnej správy

1. Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.
2. Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.
3. Plán kontinuity prevádzky obsahuje najmä:
   a) roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
   b) možné vplyvy na prevádzku informačných technológií verejnej správy,
   c) časový rámec obnovy,
   d) identifikáciu zdrojov potrebných na obnovu prevádzky,
   e) identifikáciu zamestnancov potrebných na obnovu prevádzky,
   f) identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
   g) identifikáciu priestorov potrebných na obnovu prevádzky,
   h) stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),
   i) identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
   j) spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
   k) konkrétne havarijné procedúry slúžiace na obnovu prevádzky.
4. Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.

P. Audit a kontrolné činnosti

1. Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa tejto Zmluvy.
2. Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy.
3. Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti.
4. Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.
5. Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.

PRÍLOHA 3
Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle Základného kontraktu

Prevádzkovateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	Email
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej bezpečnosti		
		Zodpovedná osoba na úseku ochrany osobných údajov		
		Technická podpora		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou základnej služby	Telefónny kontakt	Email
Ing. Patrik Piščák	Country director CZ & SK	Zodpovednosť za realizáciu projektu	+46 72 222 72 48	patrik.piscak@easypark.net
Eddy Baltazar	Head of IT Security	Riadenie informačnej bezpečnosti	+46 73 372 83 06	edelson.baltazar@easypark.net
Katrin Bjarnebrand	DPO	Zodpovedná osoba na úseku ochrany osobných údajov	-	katrin.bjarnebrand@easypark.net
Eva Dubenova	Partner Success manager	Technická podpora	-	eva.dubenova@easypark.net

PRÍLOHA 4
Zoznam schválených Subdodávateľov

Obchodné meno	Sídlo	IČO	Rozsah činností v zmysle Základného kontraktu

PRÍLOHA 5
Špecifikácia spracúvania osobných údajov

Základný kontrakt
Základným kontraktom, ktorý upravuje predmet zmluvného vzťahu medzi Prevádzkovateľom a Dodávateľom je Zmluva o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania špecifikovaná v Preambule tejto Zmluvy.

Prevádzkovateľ
Prevádzkovateľom podľa či. 4 ods. 7 Všeobecného nariadenia o ochrane údajov je Hlavné mesto Slovenskej republiky Bratislava, ktorý určuje prostriedky a účely spracúvania osobných údajov.

Sprostredkovateľ
Sprostredkovateľom podľa čl. 4 ods. 8 všeobecného nariadenia o ochrane údajov je Dodávateľ:
EasyPark Slovakia s.r.o. , ktorý spracúva osobné údaje v mene Prevádzkovateľa pri výkone činností špecifikovaných v Základom kontrakte.

Účel spracovania
Osobné údaje budú spracúvané na účely plnenia služieb definovaných Základným kontraktom:
bezproblémová, časovo a administratívne efektívna úhrada parkovného zákazníkmi Prevádzkovateľa prostredníctvom Dodávateľom vytvorenej a prevádzkovanej aplikácie a kontrola týchto úhrad integráciou aplikácie do systému ParkSys

Kategória dotknutých osôb
Zákazníci Prevádzkovateľa

Kategória údajov a ich jednotlivé atribúty (typy)
Bežné osobné údaje: titul, meno, priezvisko, adresa trvalého alebo prechodného pobytu, EČ motorového vozidla, vzťah k motorovému vozidlu, vzťah k držiteľovi/používateľovi motorového vozidla, miesto podnikania, miesto výkonu práce, vlastníctvo k nehnuteľnosti, vzťah k majiteľovi nehnuteľnosti, transakčné údaje
Osobitná kategória osobných údajov: zdravotný stav (ZŤP)

Prevádzkovateľom povolené operácie s osobnými údajmi
Dodávateľ spracúva osobné údaje automatizovanými prostriedkami, pričom ich môže získavať, zaznamenávať, usporadúvať, uchovávať, poskytovať Prevádzkovateľovi, prípadne schváleným Subdodávateľom prenosom, vymazávať alebo likvidovať len za podmienok uvedených v Základom kontrakte a v tejto Zmluve.

Doba spracúvania osobných údajov
- odo dňa účinnosti tejto Zmluvy po dobu jej trvania v súlade s jej článkom X. ods. 1

Príloha č. 2

Podmienky oprávnenosti

Na účely riadneho plnenia predmetu Zmluvy vyžaduje Objednávateľ splnenie nasledovných podmienok Poskytovateľom:

Číslo	Podmienka oprávnenosti	Spôsob preukazovania
1.	Poskytovateľ, ani jeho štatutárny orgán, ani člen štatutárneho orgánu ani člen dozorného orgánu, ani prokurista nebol právoplatne odsúdený za trestný čin korupcie, trestný čln poškodzovania finančných záujmov Európskych spoločenstiev, trestný čin legalizácie príjmu z trestnej činnosti, trestný čln založenia, zosnovania a podporovania zločineckej skupiny, trestný čin založenia, zosnovania alebo podporovania teroristickej skupiny, trestný čln terorizmu a niektorých foriem účasti na terorizme, trestný čin obchodovania s ľuďmi, trestný čin, ktorého skutková podstata súvisí s podnikaním alebo trestný čln machinácie pri verejnom obstarávaní a verejnej dražbe.	Výpisom z obchodného registra a výpisom z registra trestov nie starším ako tri mesiace alebo zápisom do zoznamu hospodárskych subjektov[1] alebo obdobného zoznamu v inom členskom štáte EÚ.
2.	Poskytovateľ nemá evidované nedoplatky na poistnom na sociálne poistenie a zdravotná poisťovňa neeviduje voči nemu pohľadávky po splatnosti podľa osobitných predpisov[2] v Slovenskej republike alebo v štáte sídla, miesta podnikania alebo obvyklého pobyt.	Potvrdením zdravotnej poisťovne a Sociálnej poisťovne nie starším ako tri mesiace alebo zápisom do zoznamu hospodárskych subjektov alebo obdobného zoznamu v inom členskom štáte EÚ.
3.	Poskytovateľ nemá evidované daňové nedoplatky voči daňovému úradu a colnému úradu podľa osobitných predpisov[3] v Slovenskej republike alebo v štáte sídla, miesta podnikania alebo obvyklého pobytu.	Potvrdením miestne príslušného daňového úradu a miestne príslušného colného úradu nie starším ako tri mesiace alebo zápisom do zoznamu hospodárskych subjektov alebo obdobného zoznamu v inom členskom štáte EÚ.
4.	Na majetok Poskytovateľa nebol vyhlásený konkurz, nie je v reštrukturalizácii, nie je v likvidácii, ani nebolo proti nemu zastavené konkurzné konanie pre nedostatok majetku alebo zrušený konkurz pre nedostatok majetku.	Potvrdením príslušného súdu nie starším ako tri mesiace alebo zápisom do zoznamu hospodárskych subjektov alebo obdobného zoznamu v inom členskom štáte EÚ.
5.	Poskytovateľ je oprávnený poskytovať službu, ktorá je predmetom Zmluvy.	Dokladom o oprávnení dodávať poskytovať službu, ktorá zodpovedá predmetu Zmluvy

[1] § 152 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov
[2] § 170 ods. 21 zákona č. 461/2003 Z. z. o sociálnom poistení v znení zákona č. 221/2019 Z. z., § 25 ods. 5 zákona č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z.
[3] Zákon č. 199/2004 Z. z. Colný zákon a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

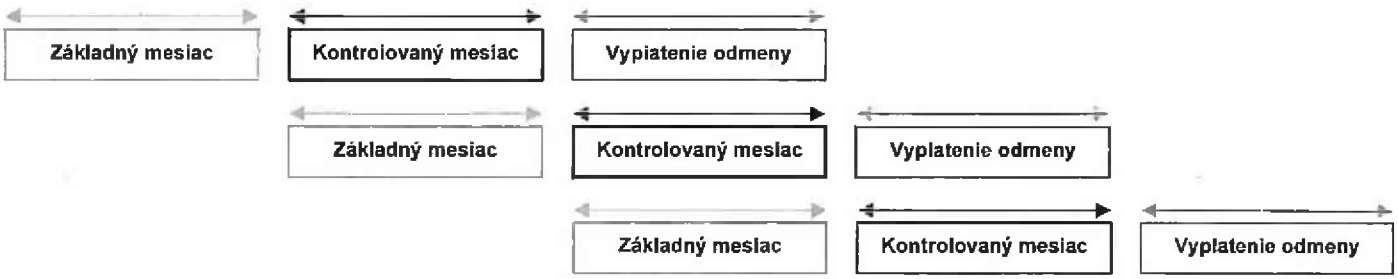
6.	Poskytovateľ je zapísaný do registra partnerov verejného sektora[4]	Overí Objednávateľ lustráciou v registri partnerov verejného sektora.
7.	Poskytovateľ má implementovaný Information Security Management System.	Doloženie ekvivalentného ISO certifikátu vydaného oprávnenou autoritou alebo platného interného popisu procesu Information Security Management System.
8.	Poskytovateľ alebo platobná brána, ktorá je používaná v poskytovanej aplikácií je PCI DSS certifikovaná.	Doloženie PCI DSS certifikátu.
9.	S Poskytovateľom nebola v minulosti ukončená Zmluva z dôvodu porušenia povinností Poskytovateľa	Overí Objednávateľ.

Všetky doklady použité na preukázanie spinenia Podmienok oprávnenosti musia byť predložené v originály a v listinnej podobe. Doklady na preukázanie splnenia podmienok oprávnenosti musia byť vyhotovené v slovenskom, českom alebo anglickom jazyku alebo úradne preložené do slovenského jazyka.

[4] Zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov.

Príloha č. 3: Spôsob určenia výšky podielu na trhu

1. Podiel na trhu sa vyhodnocuje na mesačnej báze, pri schvaľovaní Mesačného výkazu Parkovného (Príloha č. 4).
2. Odmeňovanie za kontroiovaný mesiac prebieha v mesiaci, priamo nasledujúcom po kontrolovanom mesiaci, na základe podielu na trhu, stanoveného na základe mesačných výkazov parkovného za mesiac, priamo predchádzajúci kontrolovanému mesiacu (základný mesiac).
3. Podiel na trhu pre sa stanovuje na základe schválených výkazov parkovného, podľa platených transakcií, realizovaných všetkými zapojenými prevádzkovateľmi mobilných aplikácií v základnom mesiaci.
4. Pre stanovenie podielu na trhu sa vypočíta Celkový objem platených transakcií ako suma v eurách všetkých realizovaných platených transakcií podľa všetkých schválených výkazov parkovného za základný mesiac.
5. Podiel na trhu Poskytovateľa pre odmeňovanie za kontrolovaný mesiac sa vypočíta ako podiel objemu platených transakcií v mesačnom výkaze parkovného Poskytovateľa za základný mesiac a Celkovým objemom platených transakcií, v percentách.
6. Poskytovateľovi, ktorý začal fázu Prevádzkovania aplikácie v kontrolovanom mesiaci, sa pre účely tohto výpočtu a výpočtu Odmeny podľa Prílohy č. 7 priradí 0% podiel na trhu.
7. V prípade, že údaje za základný mesiac nie sú dostupné (napr. ide o úplne prvý výpočet odmeňovania pre prvý kontroiovaný mesiac, aiebo sú údaje za základný mesiac nekompletné z dôvodu chýbajúcich výkazov parkovného), použije sa pre všetkých Poskytovateľov rovnaký podiel na trhu. Ten sa vypočíta ako podiel 1/(počet akceptovaných Poskytovateľov v kontrolovanom mesiaci).



Príloha č. 5: Mesačný výkaz prevádzky

Mesiac rok	_____
Aplikácia	_____

Príloha č. 5: Mesačný výkaz prevádzky

Výpadok od	Výpadok do	Typ výpadku	Popis	Kategória Incidentu	Výpadok nahlásený HMBA (deň)	Výpadok nahlásený HMBA (forma)	Počet sekúnd výpadku

Príloha č. 5: Mesačný výkaz prevádzky

Deň	Uptime
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	
26.	
27.	
28.	
29.	
30.	
31.	
uptime za mesiac	

ParkSys

Integračný manuál pre PEP

VERZIA DOKUMENTU	v1.2
DÁTUM VYDANIA	23.09. 2021
ID DOKUMENTU	07_Priloha_6_Integračný manuál a popis API
AUTOR	mpa@bratislava.sk
ZHOTOVITEĽ	HMBA

Obsah

Záznam o zmenách

Verzia	Popis zmien	Autor zmeny	Dátum
1.0	Prvá úplná verzia dokumentu	HMBA	30.8.2021
1.1	Prepracovaná príloha Pricing API v1.1.zipped	HMBA	8.9.2021
1.2	Opravene chyby URI Pricing API	HMBA	22.9.2021

1 Úvod

Dokument je určený dodávateľom systémov koncových platieb (PEP – Payment End Point) ako sú mobilné parkovacie aplikácie, parkomaty, aplikácie pridružených partnerov (affiliate partners) HMBA, ktorí sa budú integrovať na ParkSys s cieľom nákupu digitálneho parkovacieho lístka pre krátkodobé parkovanie. Cieľom tohto dokumentu popísať všeobecné princípy integrácie ako aj jednotlivé integračné rozhrania.

Integračný manuál je dokument, ktorý sa v čase môže vyvíjať a meniť. Zmeny budú zohľadňovať predovšetkým nové funkčné požiadavky, vždy s ohľadom na existujúce implementácie. Pri každej zmene bude definované obdobie pre zapracovanie zmien, ak budú takej povahy.

2 Skratky

Skratka	Význam
GUID	Globally Unique Identifier
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IS	Informačný systém
JWT	JSON Web Token
MPA	Mobilná Parkovacia Aplikácia
PEP	Payment End Point – MPA, parkomaty, aplikácie affiliate partnerov
REST	Representational state transfer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
PK	Parkovacia karta
NPK	Návštevnícka parkovacia karta
PPP	Prevádzkový poriadok parkovania

3 Základné princípy

Integračné rozhrania ParkSys pre dodávateľov PEP sú publikované ako Web API koncové body definované s použitím OpenAPI špecifikácie vo verzii 3. Prístup k Web API je riadený autentifikačnými a autorizačnými prostriedkami ParkSys založenými na štandarde OpenID Connect vo vezii 1.

Nie všetky rozhranie budú používané všetkými kategóriami PEP, napr.: typicky parkomaty nebudú pristupovať ku vydaným kartám používateľa prostredníctvom mailu.

3.1 Publikácia Web API

Služby sú publikované cez zabezpečený hypertextový prenosový protokol HTTPS použitím TLS protokolu. Čím je zabezpečená dôveryhodnosť publikovanej služby (certifikát servera) ako aj šifrovanie komunikácie. Certifikát servera publikuje verejná dôveryhodná certifikačná autorita.

3.2 Prístup k Web API

Prístup k Web API je realizovaný protokolom OpenID Connect v1. Pre každú interakciu s Web API musí byť použitý prístupový token. Prístupový token sa získa po úspešnej autentifikácii na IAM (Identity and Access Management) serveri ParkSys s poskytnutými povereniami. Prístupový token vo formáte JWT, má definovanú časovú platnosť typicky v minútach, obsahuje identifikáciu klienta, sadu tzv. claims atribútov a je podpísaný certifikátom IAM servera. Účet, ktorý pristupuje k API, musí mať príslušné oprávnenie na úspešné volanie API operácií. Účet pre systém tretej strany je nakonfigurovaný v ParkSys.

3.2.1 Získanie prístupového tokenu

Prístupový token vydáva autorizačný server ParkSys. Príslušný koncový bod vydávania tokenov na základe autentifikačných údajov je prístupný na URI:

https://api.parkdots.com/auth/realms/parkingrealm/protocol/openid-connect/token

Každý systém tretej strany, ktorý sa integruje na Web API má vlastný klientsky účet identifikovaný `client_id` a `client_secret` atribútmi. Tieto údaje je nutné uchovávať na strane klienta v zabezpečenom úložisku.

Príklad volania na získanie prístupového tokenu (`access_token`):

```
curl -kv -H "content-type:application/x-www-form-urlencoded" -X POST
https://api.parkdots.com/auth/realms/parkingrealm/protocol/openid-connect/token -d
'grant_type=client_credentials&client_id=<client-id>&client_secret=<client-secret>'
```

Odpoveď obsahuje JWT `access_token`, `refresh_token` spolu s podrobnosťami o uplynutí platnosti tokenu. Vrátený `access_token` sa používa ako autorizačný token v nasledujúcich volaniach Web API. `access_token` obsahuje všetky role a ďalšie prístupové atribúty potrebné pre prístup k Web API. `refresh_token` je možné použiť na získanie nového `access_token`-u pred uplynutím platnosti aktuálneho tokenu. `refresh_token` je nutné uchovávať na strane klienta v zabezpečenom úložisku a má platnosť typicky v hodinách.

Príklad volania na získanie prístupového tokenu použitím platného `refresh_token`-u:

```
curl -kv -H "content-type:application/x-www-form-urlencoded" -X POST
https://api.parkdots.com/auth/realms/parkingrealm/protocol/openid-connect/token -d
'client_id=parkingclient&grant_type=refresh_token&refresh_token=<refresh_token>'
```

3.2.2 Použitie prístupového tokenu v API voianiach

Prístupový token je nutné použiť pri každom volaní Web API a zasiela sa v http hlavičke `Authorization` ako '`Bearer <access_token>`'.

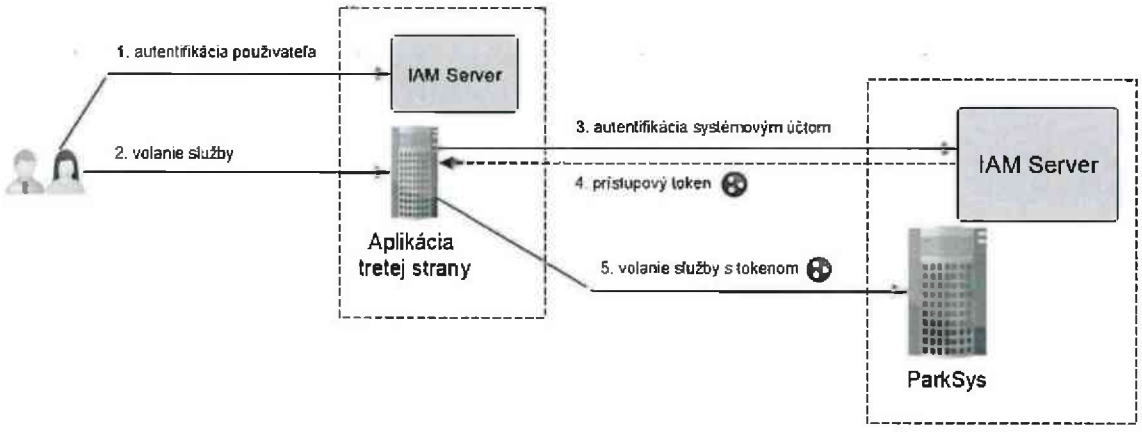
Príklad volania Web API s autorizáciou:

```
curl -kv -H "Accept:application/json" -H "Authorization:Bearer <access_token>"-X GET
"https://api.parkdots.com/api-timecredit"
```

4 Integračné rozhrania

4.1 Overenie registrovaného používateľa ParkSys v PEP aplikácii

Nie je vyžadované, aby PEP aplikácie využívali účty a overovali identitu používateľov ParkSys prostredníctvom IAM servera ParkSys. Predpokladá sa, že PEP aplikácie majú vlastnú implementáciu prístupu k ich službám a IAM server PEP aplikácie nie je prepojený s IAM serverom ParkSys napríklad prostredníctvom identity brokeringu. Backend PEP sa preto autorizuje voči ParkSys jedným klientskym systémovým účtom ako je popísané v kapitole 3.2. Situáciu znázorňuje nasledovný obrázok:



Obrázok 1: Autorizácia volaní ParkSys Web API systémovým účtom

Aby bolo možné komunikovať s ParkSys v kontexte ParkSys používateľa (napríklad získanie kariet používateľa) z PEP aplikácie je nutné prvotné overenie používateľa prostredníctvom jeho e-mail účtu pod ktorým je registrovaný v ParkSys. Detaily implementácie prvotného ako aj následného overenia e-mail účtu používateľa ParkSys sú v zodpovednosti dodávateľa PEP. Jednou z možností je napríklad vygenerovanie a zaslanie jednorázového kódu na e-mail a jeho následné overenie v PEP aplikácii. e-mail adresa slúži ako jednoznačný identifikátor používateľa ParkSys a využíva sa v niektorých Web API operáciách.

4.2 Rozhranie pre získanie informácií o PK

Web API pre získanie údajov o parkovacích kartách umožňuje získať aktuálne dáta o kartách používateľa registrovaných v ParkSys podľa je účtu (e-mail) alebo podľa EČV, na ktorú sú karty vydané.

Špecifikum: pre získanie informácií o NPK je nutné ísť cez účet žiadateľa (e-mail), nakoľko NPK zo svojej podstaty nie je naviazaná na žiadnu konkrétnu EČV.

Názov	Získanie údajov o kartách	
URI	https://api.parkdots.com/api-permitint/cards https://api.pre-prod.parkdots.com/api-permitint/cards	
Swagger	https://api.prod.parkdots.com/api-permitint/swagger-ui/index.html#/ https://api.pre-prod.parkdots.com/api-permitint/swagger-ui/index.html#/	
Špecifikácia	OpenAPI yaml	
	Viď kapitola 6 Prílohy	
Popis	Web APi umožňuje: • Získanie všetkých kariet používateľa • Získanie všetkých kariet registrovaných na subjekt (EČV) Kontext používateľa je definovaný cez http hlavičku username, ktorá nadobúda hodnotu e-mailu s ktorým je používateľ registrovaný v ParkSys a pod ktorým žiadal o parkovaciu kartu. Pozri tiež kapitolu Overenie registrovaného používateľa ParkSys v PEP aplikácii 4.1.	
APi operácie	Zoznam APi operácií: • List subject's cards » POST /cards/list-subject-cards • List user's cards » POST /cards/list-user-cards	
Use cases	Získanie zoznamu a informácií o vydaných kartách na EČV, prípadne účet pre zobrazenie v aplikácii.	

	Informácie o kartách sú informatívneho charakteru z pohľadu toho, že cenu lístka preratúvava aj tak príslušné API so zohľadnením kariet v čase preratúvavania.

4.3 Rozhranie určenie ceny parkovania a kúpu lístkov

Ďalej *Pricing Api*, slúži na zistenie celkovej ceny parkovného pre daný subjekt identifikovaný EČV alebo užívateľským účtom (e-mail) a pripadnú kúpu parkovacieho lístka za danú cenu.

Pozn.: pre čerpanie kreditov z NPK je nutný účet

Pricing API pri určení ceny zohľadňuje:

- Aktuálne tarify podľa miesta a času parkovania
- Históriu parkovania v danom mieste parkovania – max doba parkovania za deň
- Bonusové kredity a zľavové karty pre EČV
- Minimálnu dĺžku platenej transakcie v zmysle PPP (aktuálne 30min)

Pricing API pri čerpaní rozdeľuje transakcie na platené a kreditové, upravuje zvyšné kredity na kreditnom účte.

Názov	Pricing api	
URI	https://api.prod.parkdots.com/api-parkingint/hmba https://api.pre-prod.parkdots.com/api-parkingint/hmba	
Swagger	https://api.prod.parkdots.com/api-parkingint/swagger-ui/index.html#/ https://api.pre-prod.parkdots.com/api-parkingint/swagger-ui/index.html#/	
Špecifikácia	OpenAPI yaml	
	Viď kapitola 6 Prílohy	
Popis	Pricing api umožňuje: • Zistenie ceny lístka • Zaevidovanie parkovacieho lístka Systém tretej strany, ktorý registruje lístky musí byť identifikovaný atribútom `systemId` a musí mať na strane ParkSys zaevidovaný aspoň jeden terminál identifikovaný atribútom `terminalId`. Tieto atribúty sa definujú počas zapojenia externého systému do ParkSys.	
API operácie	Zoznam API operácií: • Get actual balance of NPK » GET /api/visitorparking/{NpkId}/balance • Calculate NPK balance required for parking » POST /api/visitorparking/charging • Use NPK balance for parking » POST /api/visitorparking/ticket • Get pricing calculation for given inputs	

	» POST /api/ecvparking/charging • Create ticket for given inputs Time must be within allowable limit » POST /api/ecvparking/ticket • Request shortening/extension of existing ticket » PATCH /api/ecvparking/ticket/{ticketId} • Request ending of existing ticket » GET /api/ecvparking/ticket/{ticketId}/end • Request extension of existing ticket » PATCH /api/ecvparking/ticket/extension/{ticketId}
Use cases	

5 Testovacie dáta

Typ pouzivatela	Typ A – rezident v regulovanej zóne:	Typ B – abonent v regulovanej zóne – typ FO:	Typ C – rezident v regulovanej zóne, ktorý nemá auto:	Typ D – abonent v regulovanej zóne – typ podnikajúca osoba:	Typ E – obyvateľ Bratislavy, ktorý nemá trvalý pobyt v regulovanej zóne	Typ F – bežný parkujúci, nerezident Bratislavy, neabonent:
Účet/ID	• testba1@parkdots.sk • 5ccc154b-acd3-4572-b699-73d87da3d685	• testba2@parkdots.sk • c530ffb6-c0f9-48c7-9150-73163bb6ff91	• testba3@parkdots.sk • 45546ca3-d71c-43a8-a46a-99e03c4c3cc7	• testba4@parkdots.sk • a1b22196-7c12-4580-8677-811847e0f5ad	• testba5@parkdots.sk • 5abda1f2-5729-4ab3-84c5-9ec09528d838	• testba6@parkdots.sk • 0c3ebfdd-0424-4f87-bcce-c90c5abcfb22
Adresa	Košická 4984/46, Bratislava-Ružinov	Košická 4985/45, Bratislava-Ružinov	Košická 4984/44, Bratislava-Ružinov	Košická 4985/43, Bratislava-Ružinov	Dunajská 2317/32, Bratislava-Staré Mesto	Kollárova 557/23, Trnava
				IČO 44917422 Záhradnícka 30, Bratislava-Ružinov		
Typ karty	**a. 1 x Rezidentská**	**a. 1 x Abonentská**	**a. 1 x Návštevnícka**	**a. 1 x Abonentská**	**a. 1 x Bonusová**	**a. 1 x zľavová elektromobil**
Id karty	f066b754-be9a-4b9d-9a5a-9171f268e557	a98a29ac-daba-403d-b331-7fdd087ce9ab	1c3f1e86-83ff-4f61-9bf1-9e84d4b0d4b5	fe30991b-6990-4534-a5f1-a481cd66655f	aa916b81-6f33-4b88-80cc-2028d2d658da	9d4feac8-32b1-462a-ae4e-cf830381dff0
Typ karty	**b. 1 x Návštevnícka**	**b. Potenciálne ešte v 5-15% prípadov zľavové karty (elektromobil /)**	"	**b. Potenciálne ešte do 10% prípadov zľavová karta elektromobil**	**b. Potenciálne ešte v 5-15% prípadov zľavové karty (/ ŤZP)**	**alebo 1 x zľavová ŤZP – aj obe súčasne (Celkovo to predstavuje predpokladám do 10%):**
Id karty	f6827b8e-22df-4d3c-9cfe-62e6565ce957	d45a3de8-5b13-481f-995f-da0324dfc746		fef1d715-991f-4fe7-9eff-190d0a3a5598	3de81b88-d42a-4573-bfe7-11c276d87e22	e2c668b1-ad6a-4659-b369-7f1ee556d57b
Typ karty	**c. 1 x Bonusová**					
Id karty	5e736da6-fff4-43d7-89a7-d5cd14a6925e					
Typ karty	**d. Potenciálne ešte v 5-15% prípadov zľavové karty (elektromobil /)**					
Id karty	a3582f3d-9e89-4f8a-a989-b8894ff10f9b					

6 Prílohy

Názov prílohy	formát	súbor
4.2 Rozhranie pre získanie informácii o PK	zip/ yaml	permit-card-api.zipped
4.3 Rozhranie určenie ceny parkovania a kúpu lístkov	zip/ yaml	Pricing API v1.2.zipped
Taxonómia parkovacej politiky (zón)	pdf	Taxonómia parkovacej politiky (zón) v1.0.pdf
Parkovacie zóny a úseky – kompletná aktuálna definícia k 8.9.2021	zip/ shapefiles	PZU-PAAS_20210908.zipped
Vyextrahované aktuálne tarify z PZU-PAAS_20210908	txt	Actual tarif 20210908.txt
Kompletná definícia testovacích parkovacích kariet v pre-prod	zipped/ json	PRE-PROD_TestParkingCards v01.zipped

Príloha č. 7: Model odmeňovania

1. Každá transakcia bude finančne ohodnotená.
2. Transakcie sa ohodnocujú na mesačnej báze. Odmeňovanie za kontrolovaný mesiac prebieha v mesiaci, priamo nasledujúcom po kontrolovanom mesiaci.
3. Výpočet odmeny prebieha pri schvaľovaní Mesačného výkazu Parkovného (Príloha č. 4).
4. Transakcie sa delia na bezplatné (napr. časovo obmedzené bezplatné parkovanie /digitálny parkovací kotúč/, parkovanie z bonusovej karty alebo z návštevníckej karty a pod.) a platené (ostatné krátkodobé státie, pri ktorom sa realizuje platba, či už priamo z platobnej karty alebo z vopred nahratého kreditu).
5. Minimálna tarifikácia parkovacieho lístka podľa aktuálne platného návrhu je uvedená v tabuľke 3 tejto prílohy, počty a štruktúra transakcií v tabuľke 2 sú odhadované a nie sú záväzné.
6. Bezplatné transakcie sú odmeňované fixnou sumou, vo výške 0,005 eur za každú realizovanú transakciu.
7. Pre výpočet odplaty pre platené transakcie sa používa podiel na trhu, vypočítaný podľa Prílohy č. 3 tejto zmluvy.
8. Pre objem platených transakcií v eurách pod Hraničným podielom 1 sa uplatní základná percentuálna odplata 7,00 % z hodnoty transakcie.
9. Pre objem platených transakcií v eurách, ktorý prekročí Hraničný podiel 1, ale neprekročí Hraničný podiel 2, sa uplatní znížená percentuálna odplata 5,50 % z hodnoty transakcie.
10. Pre objem platených transakcií v eurách, ktorý prekročí Hraničný podiel 2, sa uplatní znížená percentuálna odplata 4,00 % z hodnoty transakcie.
11. Odmeny sú vyplácané všetkým poskytovateľom aplikácie, bez ohľadu na trhový podiel.
12. Vzorec pre výpočet odplaty pre prevádzkovateľa aplikácie *a* v akýkoľvek mesiac *m* je počítaná na základe údajov v tabuľke 1 nasledovne (*N* je počet transakcií):

$$O_{a,m} = N_{b,a,m}B + \min\left(N_{p,a,m}, H1 \times \sum_a N_{p,m}\right) \times P$$
$$+ \min\left(\max\left(N_{p,a,m} - H1 \times \sum_a N_{p,m}, 0\right), (H2 - H1) \times \sum_a N_{p,m}\right) \times (P + d1)$$
$$+ \max\left(N_{p,a,m} - H2 \times \sum_a N_{p,m}, 0\right) \times (P + d1 + d2)$$

Tabuľka 1: Model odmeňovania

Predmet	Skratka	Jednotka	Hodnota
Bezplatná transakcia	B	eur	0,005
Platená transakcia (základ)	P	%	7 %
Prvá hranica trhového podielu pre zmenu sadzby	H1	%	20 %
Zmena pri prekročení hranice 1	d1	p. b.	-1,5
Druhá hranica trhového podielu pre zmenu sadzby	H2	%	40 %
Zmena pri prekročení hranice 2	d2	p. b.	-1,5

ZMLUVA O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ, NOTIFIKAČNÝCH POVINNOSTÍ A OCHRANY OSOBNÝCH ÚDAJOV

uzatvorená v zmysle § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, čl. 28 ods. 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (**Všeobecné nariadenie o ochrane osobných údajov**) a § 34 ods. 3 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len ako „**Zmluva**")
medzi týmito zmluvnými stranami:

Prevádzkovateľ:
Názov: **Hlavné mesto Slovenskej republiky Bratislava**
Sídlo: Primaciálne námestie č. 1, 814 99 Bratislava, Slovenská republika
IČO: 00 603 481
DIČ: 2020372596
IČ DPH: SK2020372596
IBAN:
Zastúpený: Ing. arch. Matúš Vallo, primátor
(ďalej len ako „**Prevádzkovateľ**" v príslušnom grafickom tvare)

a

Dodávateľ:
obchodné meno: EasyPark Slovakia s.r.o.
sídla: Zámocká 3, 811 01 Bratislava, Slovenská republika
IČO: 50929411
DIČ: 2120550333
IČ DPH: -
údaj o zápise v OR Spoločnosť zapísaná v OR Okresný súd Bratislava I odd. sro, vložka č. 120137/B
údaj o konajúcej osobe: Ing. Patrik Piščák, Country Director CZ & SK
(ďalej ako „**Dodávateľ**" v príslušnom grafickom tvare)

PREAMBULA

Prevádzkovateľ je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**Zákon o kybernetickej bezpečnosti**").

Základnou službou Prevádzkovateľa sú webové sídlo, elektronické služby a informačné systémy, ktoré sú v zmysle ustanovenia § 3 písm. k) prvého bodu Zákona o kybernetickej bezpečnosti činnosťou v sektore Verejná správa, podsektore Informačné systémy verejnej správy a podľa ustanovenia § 17 ods. 2 písm. b) Zákona o kybernetickej bezpečnosti sú zaradené do zoznamu základných služieb.

Dodávateľ je zmluvným partnerom Prevádzkovateľa na výkon činností, ktoré priamo súvisia s prevádzkou elektronických komunikačných sietí (ďalej len „**Siete**") a informačných systémov Prevádzkovateľa, pričom tieto činnosti Dodávateľ uskutočňuje na základe Zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania, uzatvorenej s Prevádzkovateľom dňa 21.1.2022 (ďalej len „**Základný kontrakt**").

Dodávateľ je pri výkone činností podľa predchádzajúceho odseku Prevádzkovateľom poverený na spracúvanie osobných údajov v súlade so špecifikáciou spracúvania osobných údajov uvedenej v Prílohe č. 5 tejto Zmluvy.

Dodávateľ vyhlasuje, že je odborne spôsobilý na plnenie predmetu tejto Zmluvy, má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy. Súčasne vyhlasuje, že prijal primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky Všeobecného nariadenia o ochrane údajov a aby sa zabezpečila ochrana práv dotknutej osoby.

Ak nie je uvedené inak, pojmy používané v tejto Zmluve majú význam im priradený v Zákone o kybernetickej bezpečnosti, jeho vykonávacích predpisoch, Všeobecnom nariadení o ochrane osobných údajov a iných predpisoch v oblasti ochrany osobných údajov.

Článok I.
Predmet Zmluvy

1. Predmetom tejto Zmluvy je zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa.
2. Predmetom tejto Zmluvy je špecifikácia spracúvania osobných údajov a úprava práv a povinností zmluvných strán na úseku ochrany osobných údajov.
3. Táto Zmluva upravuje základné princípy spolupráce zmluvných strán pri uskutočňovaní plnenia bezpečnostných opatrení – úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa počas ich životného cyklu, s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Prevádzkovateľa a na porušenia ochrany osobných údajov (ďalej len „**Ciele**").
4. Súčasťou záväzkov Dodávateľa podľa tejto Zmluvy je povinnosť Dodávateľa prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti a ochrany osobných údajov v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené Ciele tejto Zmluvy. Prevádzkovateľ vyhlasuje, že súhlasí so špecifikáciou a rozsahom bezpečnostných opatrení prijímaných Dodávateľom v zmysle tejto Zmluvy. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
5. Dodávateľ sa na základe tejto Zmluvy zároveň zaväzuje dodržiavať bezpečnostné politiky Prevádzkovateľa, s ktorými ho Prevádzkovateľ oboznámil. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa. Dodávateľ súčasne akceptuje, že bezpečnostné politiky Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu Sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa a ochranu osobných údajov.
6. Na základe tejto Zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti a ochrany osobných údajov v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené jej Ciele.
7. Odplata za plnenie povinností Dodávateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto Zmluvy sú v celom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa Základného kontraktu a za plnenie povinností podľa tejto Zmluvy Dodávateľ nemá nárok na žiadne ďalšie peňažné plnenia od Prevádzkovateľa.
8. *Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto Zmluvy po celú dobu trvania Základného kontraktu.*

Článok II.
Prevencia kybernetických bezpečnostných incidentov

1. Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti Siete a informačného systému alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť Prevádzkovateľa alebo ktorej následkom je:
   a) strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému Prevádzkovateľa,
   b) obmedzenie alebo odmietnutie dostupnosti základnej služby Prevádzkovateľa,
   c) vysoká pravdepodobnosť kompromitácie činností základnej služby Prevádzkovateľa alebo
   d) ohrozenie bezpečnosti informácií Prevádzkovateľa.
2. incident definovaný v čl. I. Základného kontraktu sa považuje sa kybernetický bezpečnostný incident v zmysle tejto Zmluvy, okrem nekritického incidentu, ktorý nespôsobuje výpadok služby ani iné následky podľa čl. II ods. 1. písm. a) až d) tejto Zmluvy.
3. Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa a bezpečnosti spracúvania osobných údajov (ďalej len „**Incidenty**"):
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez Dodávateľa nebolo možné zasiahnuť Siete a informačné systémy Prevádzkovateľa;
   b) prijať primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti spracúvania osobných údajov, najmä pseudonymizáciu a šifrovanie osobných údajov; schopnosť zabezpečiť trvalú dôvernosť,

integritu, dostupnosť a odolnosť systémov spracúvania a služieb; schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade incidentu; proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov;

c) sledovať výstrahy, varovania, ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov Incidentov, tieto vyhodnocovať a vykonať protiopatrenia v záujme ochrany oprávnených záujmov Prevádzkovateľa;
d) prijímať od Prevádzkovateľa varovania pred Incidentmi;
e) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa;
f) vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa alebo kybernetickú bezpečnosť Sietí a informačných systémov Prevádzkovateľa alebo ochranu osobných údajov;
g) predchádzať vzniku Incidentov;
h) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch;
i) zasielať Prevádzkovateľovi včasné varovania pred Incidentmi, o ktorých sa dozvie vlastnou činnosťou podľa tejto Zmluvy alebo iným spôsobom;
j) informovať Prevádzkovateľa o incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti;
k) podávať Prevádzkovateľovi oznámenia, že došlo k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k riziku pre práva a slobody fyzických osôb bez zbytočného odkladu potom, čo sa o porušení ochrany osobných údajov dozvedel;
l) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa v rozsahu Základného kontraktu,
m) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov podieľajúcich sa na plnení základného kontraktu a/alebo tejto zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa.

4. Dodávateľ je povinný mať počas trvania tejto Zmluvy také technické, technologické a personálne vybavenie, ktoré je potrebné na riadne a včasné plnenie tejto Zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti v rozsahu potrebnom na efektívne napĺňanie Cieľov tejto Zmluvy.
5. Neoddeliteľnými prílohami tejto Zmluvy sú:
   a) rozsah činnosti Dodávateľa v zmysle Základného kontraktu (Príloha č. 1),
   b) špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma Dodávateľ a s ktorými súhlasí (Príloha č. 2),
   c) zoznam pracovných rolí Dodávateľa, ktoré majú mať prístup k informáciám a údajom Prevádzkovateľa a zoznam zamestnancov Dodávateľa a iných osôb, podieľajúcich sa za Dodávateľa na plnení Základného kontraktu a/alebo tejto Zmluvy a/alebo majúcich prístup k informáciám a údajom Prevádzkovateľa (Príloha č. 3),
   d) zoznam Dodávateľom navrhnutých a Prevádzkovateľom schválených Subdodávateľov (Príloha č. 4),
   e) špecifikácia spracúvania osobných údajov (Príloha č. 5).
6. **Dodávateľ je povinný bezodkladne oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí Dodávateľa.**
7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností a všetky potrebné informácie na preukázanie splnenia povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii a dokumentácii na úseku ochrany osobných údajov, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi na nahliadnutie a zhotovenie kópií.
8. Dodávateľ je povinný prijať a dodržiavať všeobecné a sektorové bezpečnostné opatrenia v dotknutých oblastiach podľa Zákona o kybernetickej bezpečnosti a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, najmenej pre oblasť podľa § 20 ods. 3 písm. b), až h), j), k), m) Zákona o kybernetickej bezpečnosti, v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa a Prílohy k vyhláške Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov, ktorá upravuje opatrenia na elimináciu rizík pre práva fyzickej osoby a Prílohy 2 k vyhláške Úradu podpredsedu vlády SR pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Článok III.
Reaktivita pri hlásení Incidentov

1. Dodávateľ je povinný Prevádzkovateľovi bezodkladne hlásiť každý Incident spôsobom určeným Prevádzkovateľom, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie Incidentov. Ak do okamihu hlásenia Incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie Incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky Siete a informačného systému toto hlásenie doplní.
2. Pri incidentoch definovaných v čl. I Základného kontraktu Dodávateľ postupuje v súlade s čl. VIII Základného kontraktu a touto Zmluvou.
3. Dodávateľ je povinný riešiť Incident najmä odozvou alebo inou reakciou na Incident, ohraničením Incidentu a jeho dopadov, nápravou následkov Incidentu, asistenciou pri riešení Incidentu na mieste, reakciou na incident a podporou reakcií na Incident (ďalej len **„Reaktívne opatrenie"**). Pri riešení Incidentu je Dodávateľ povinný na žiadosť Prevádzkovateľa spolupracovať s Prevádzkovateľom, Národným bezpečnostným úradom a Ministerstvom pre investície a informatizáciu Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie Incidentu.
4. Dodávateľ je povinný Prevádzkovateľovi bezodkladne oznámiť a preukázať vykonanie Reaktívneho opatrenia a jeho výsledok.
5. Dodávateľ je povinný v čase Incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, a poskytnúť ho Prevádzkovateľovi.
6. Dodávateľ je povinný Prevádzkovateľovi oznámiť skutočnosť, že v súvislosti s Incidentom došlo k porušeniu ochrany osobných údajov a súčasne poskytnúť mu súčinnosť pri plnení jeho povinností pri oznamovaní týchto porušení dozornému orgánu a dotknutým osobám.
7. Dodávateľ je povinný Prevádzkovateľovi oznámiť skutočnosť, že v súvislosti s Incidentom mohlo dôjsť k spáchaniu trestného činu.
8. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa v určenej lehote povinný predložiť Prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu Incidentu (ďalej len „**ochranné opatrenia**") na schválenie. Ak dodávateľ nenavrhne ochranné opatrenia v určenej lehote alebo ak sú navrhované ochranné opatrenia zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom na jeho návrhu.
9. Po schválení ochranných opatrení Prevádzkovateľom je Dodávateľ povinný ochranné opatrenia bez zbytočného odkladu vykonať.
10. Po vykonaní ochranných opatrení Dodávateľom je Dodávateľ povinný preveriť ich účinnosť.

Článok IV.
Spracúvanie osobných údajov

1. Dodávateľ je oprávnený pri výkone činnosti podľa Základného kontraktu spracúvať osobné údaje len na základe pokynov Prevádzkovateľa uvedených v Základnom kontrakte a v tejto Zmluve.
2. Dodávateľ je povinný spracúvať osobné údaje v súlade so Všeobecným nariadením o ochrane údajov a súvisiacimi právnymi predpismi.
3. Dodávateľ v čo najväčšej miere pomáha Prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby.
4. Dodávateľ je povinný vytvoriť systém na vybavovanie žiadostí o výkon práv dotknutých osôb. Pokiaľ je Dodávateľovi doručená žiadosť dotknutej osoby, bez zbytočného odkladu ju odstúpi Prevádzkovateľovi, pokiaľ sa spracúvanie jej osobných údajov týka Základného kontraktu alebo tejto Zmluvy.
5. Dodávateľ bezodkladne informuje Prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje Všeobecné nariadenie na ochranu osobných údajov alebo iné súvisiace právne predpisy.

Článok V.
Ochrana informácií a povinnosť zachovávať mlčanlivosť

1. Dodávateľ je povinný chrániť všetky informácie poskytnuté mu Prevádzkovateľom. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sieti a informačných systémov Prevádzkovateľa.
2. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením tejto Zmluvy a/alebo Základného kontraktu a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti.
3. Dodávateľ je povinný zabezpečiť, aby každá osoba zúčastnená na predmete plnenia Základného kontraktu a/alebo tejto Zmluvy za Dodávateľa neodkladne podpísala vyhlásenie o zachovávaní mlčanlivosti o skutočnostiach, o

ktorých sa dozvedela v súvislosti s plnením úloh podľa Zákona o kybernetickej bezpečnosti a ktoré nie sú verejne známe. Rovnako je povinný zabezpečiť, aby každá osoba oprávnená spracúvať osobné údaje v jeho mene bola zaviazaná, že zachová dôvernosť informácii. Dodávateľ je v rámci toho povinný zabezpečiť trvalé zachovávanie mlčanlivosti o všetkých takýchto skutočnostiach každou z týchto osôb, a to aj po skončení plnenia predmetu Zmluvy a/alebo predmetu Základného kontraktu.

Článok VI.
Spôsob a forma hlásenia ďalších informácií požadovaných Prevádzkovateľom na plnenie jeho povinností vyplývajúcich zo Zákona o kybernetickej bezpečnosti a ich vymedzenie, kontaktné osoby na úseku kybernetickej bezpečnosti

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo Zákona o kybernetickej bezpečnosti všetky ďalšie Prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
   a) riešenie kybernetického bezpečnostného incidentu,
   b) hlásenie závažného kybernetického incidentu,
   c) poskytnutie súčinnosti a spolupráce s Národným bezpečnostným úradom,
   d) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
   e) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka.
2. Dodávateľ je povinný realizovať hlásenia podľa ods. 1. tohto článku Zmluvy a komunikovať s Prevádzkovateľom pri plnení povinností podľa tejto Zmluvy spôsobom a formou určeným Prevádzkovateľom, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií. Zmluvné strany berú na vedomie, že hlásenia podľa ods. 1. tohto článku Zmluvy ako aj poskytovanie ďalších informácií pri plnení povinností podľa tejto Zmluvy si budú realizovať telefonicky, e-mailom a/alebo písomne, pričom konkrétny spôsob a formu takého oznámenia budú voliť podľa hľadiska účelnosti a naliehavosti nahlasovaných informácií.
3. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
4. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti:
   meno a priezvisko: Eddy Baltazar
   funkcia/pracovná pozícia Head of Information & IT Security
   telefónne číslo: +46733728306
   e-mailová adresa: edelson.baltazar@easypark.net
5. Zmenu kontaktných osôb na úseku kybernetickej bezpečnosti môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VII.
Spôsob a forma hlásenia ďalších informácií požadovaných Prevádzkovateľom na plnenie jeho povinnosti vyplývajúcich zo Všeobecného nariadenia o ochrane údajov, kontaktné osoby na úseku ochrany osobných údajov

1. Dodávateľ je povinný hlásiť Prevádzkovateľovi za účelom plnenia povinností Prevádzkovateľa vyplývajúcich zo Všeobecného nariadenia o ochrane osobných údajov všetky ďalšie Prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
   a) oznámenie porušenia ochrany osobných údajov dozornému orgánu,
   b) oznámenie porušenia ochrany osobných údajov dotknutej osobe,
   c) výkon práv dotknutých osôb,
   d) poskytnutie súčinnosti a spolupráce s Úradom na ochranu osobných údajov SR,
   e) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v súdnom konaní,
   f) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa porušenie ochrany osobných údajov týka.
2. Oznámenie podľa ods. 1 tohto článku musí obsahovať aspoň:

a) opis povahy porušenia ochrany osobných údajov vrátane kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných Dodávateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

3. V rozsahu, v akom nie je možné poskytnúť informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.
4. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku ochrany osobných údajov:
   meno a priezvisko: _____
   funkcia/pracovná pozícia _____
   telefónne číslo: _____
   e-mailová adresa: _____
5. Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku ochrany osobných údajov:
   meno a priezvisko: Katrin Bjärnebrand
   funkcia/pracovná pozícia DPO
   telefónne číslo: -
   e-mailová adresa: katrin.bjarnebrand@easypark.net
6. Zmenu kontaktných osôb na úseku ochrany osobných údajov môže každá zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme.

Článok VIII.
Podmienky a možnosti zapojenia ďalšieho Dodávateľa

1. Dodávateľ môže za účelom plnenia svojho záväzku podľa Základného kontraktu ustanoviť ďalšieho Dodávateľa (ďalej len „**Subdodávateľ**"), ktorý bude úplne alebo čiastočne zabezpečovať plnenie pre Prevádzkovateľa namiesto Dodávateľa, avšak za splnenia nasledovných podmienok:
   a) Dodávateľ môže ustanoviť Subdodávateľa iba na základe predchádzajúceho písomného súhlasu Prevádzkovateľa; Dodávateľ v žiadosti o udelenie súhlasu písomne oznámi Prevádzkovateľovi obchodné meno a ostatné identifikačné údaje Subdodávateľa,
   b) Dodávateľ je povinný zmluvne zaviazať Subdodávateľa k plneniu povinností podľa Základného kontraktu a tejto Zmluvy, a uložiť mu rovnaké povinnosti týkajúce sa plnenia bezpečnostných opatrení a notifikačných povinností za účelom zabezpečenia kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa, ako sú ustanovené v tejto Zmluve, uložiť mu povinnosť poskytnutia dostatočných záruk na vykonanie primeraných technických opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky všeobecného nariadenia na ochranu osobných údajov,
   c) zodpovednosť voči Prevádzkovateľovi nesie Dodávateľ, ak Subdodávateľ nesplní svoje povinnosti týkajúce Základného kontraktu a tejto Zmluvy; tým nie je dotknutý nárok Dodávateľa na náhradu škody voči Subdodávateľovi.

Článok IX.
Spoločné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto Zmluvy v súlade so Zákonom o kybernetickej bezpečnosti, a inými zákonnými úpravami, vykonávacími predpismi vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto Zmluvy v súlade so sektorovými bezpečnostnými opatreniami (§ 32 ods. 2 Zákona o kybernetickej bezpečnosti), ktoré vydáva Ministerstvo pre investície a informatizáciu Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.

3. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo ktoré by sa mohli týkať kybernetickej bezpečnosti Sietí a informačných systémov Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
4. Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy, v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
5. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto Zmluvy (evidovanie logov a incidentov a dokumentovanie školení svojich zamestnancov – prezenčné listiny) a na žiadosť Prevádzkovateľa mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
6. Dodávateľ je oprávnený plniť Základný kontrakt pre Prevádzkovateľa prostredníctvom svojich Subdodávateľov čiastočne v nevyhnutnom rozsahu v prípade, že toto plnenie priamo súvisí s prevádzkou Sietí a informačných systémov Prevádzkovateľa, pričom je povinný zabezpečiť riadne plnenie povinností na úseku kybernetickej bezpečnosti v rozsahu Zákona o kybernetickej bezpečnosti.. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať kontrolné činnosti a audit v súlade s ustanoveniami čl. XI. tejto zmluvy aj u takýchto Subdodávateľov, zabezpečujúcich úplne alebo čiastočne plnenie Základného kontraktu pre Prevádzkovateľa namiesto Dodávateľa.
7. Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto Zmluvy ohrozuje plnenie Cieľov tejto Zmluvy, pričom za dôsledky Incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Dodávateľa podľa tejto Zmluvy neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Prevádzkovateľovi v plnom rozsahu.

Článok X.
Trvanie a zánik Zmluvy, sankčný mechanizmus

1. Táto Zmluva sa uzatvára na dobu určitú, odo dňa jej uzatvorenia do konca trvania Základného kontraktu definovaného podľa preambuly v ods. 3 tejto Zmluvy.
2. Zmluvný vzťah na základe tejto Zmluvy zanikne súčasne so zánikom Základného kontraktu.
3. Túto Zmluvu je možné ukončiť vždy dohodou zmluvných strán o skončení trvania Zmluvy, a to ku dňu uvedenému v takej dohode.
4. Prevádzkovateľ je oprávnený od tejto Zmluvy písomne odstúpiť v prípadoch, ak Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy. Možnosť ktorejkoľvek zmluvnej strany odstúpiť od tejto zmluvy zo zákonom ustanovených dôvodov týmto nie je dotknutá.
5. Zánik tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po zrušení tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do jej zániku.
6. V prípade každého jednotlivého porušenia ktorejkoľvek povinnosti Dodávateľa, vyplývajúcej z tejto Zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 5.000,-EUR (slovami: tisíc Euro).
7. V prípade opakovaného porušenia identickej povinnosti Dodávateľa, vyplývajúcej z tejto zmluvy, má Prevádzkovateľ právo na zaplatenie zmluvnej pokuty vo výške 1.000,-EUR (slovami: tisíc Euro).
8. Ustanovenia o zmluvných sankciách uvedených v Základnom kontrakte týmto nie sú dotknuté.
9. Zmluvná pokuta je splatná na základe výzvy Prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 30 (tridsať) dní odo dňa jej doručenia Dodávateľovi.
10. Nárok Prevádzkovateľa na náhradu škody voči Dodávateľovi, aj vo výške presahujúcej zmluvnú pokutu, nie je ustanoveniami o dojednaní zmluvnej pokuty, uplatnením zmluvnej pokuty voči Dodávateľovi ani jej zaplatením Dodávateľom dotknutý.
11. Ak vznikne Prevádzkovateľovi ujma z dôvodu pochybenia Dodávateľa, ktorý poruší svoje povinnosti dojednané touto Zmluvou alebo uložené mu právnymi predpismi, a to tak, že Prevádzkovateľ bude na základe alebo v súvislosti s takou skutočnosťou zodpovedný za správny delikt v oblasti kybernetickej bezpečnosti alebo ochrany osobných údajov, vzniká Prevádzkovateľovi nárok na náhradu takejto ujmy voči Dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie.

Článok XI.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu kybernetickej bezpečnosti a ochrany osobných údajov u Dodávateľa Prevádzkovateľom

1. Prevádzkovateľ je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov, ako aj

nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto Zmluvy.

2. Prevádzkovateľ je oprávnený realizovať audit u Dodávateľa sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa pri výkone auditu uskutočňuje taká Prevádzkovateľom poverená tretia osoba.
3. Dodávateľ je povinný pri audite spolupracovať s Prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy.
4. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky osobám, ktoré sa za Dodávateľa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy.
5. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad plnenia povinností Dodávateľom s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti a ochrany osobných údajov podľa tejto Zmluvy, aktuálne bezpečnostné povedomie svojich zamestnancov a iných osôb zúčastnených na predmete plnenia Základného kontraktu a/alebo tejto Zmluvy za Dodávateľa, ich záväzok a poučenie o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
6. Prevádzkovateľ je povinný oznámiť Dodávateľovi svoj zámer realizovať u Dodávateľa audit najmenej 14 pracovných dní vopred.
7. Výsledok auditu Prevádzkovateľ zaznamená do zápisnice. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 30 kalendárnych dní.
8. Ak Dodávateľ neumožní Prevádzkovateľovi, resp. Prevádzkovateľom poverenej tretej osobe, bezdôvodne vykonanie auditu ani po opakovanej písomnej výzve, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti a/alebo ochrany osobných údajov podľa tejto Zmluvy.
9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje Dodávateľa zodpovednosti za plnenie povinnosti Dodávateľa vyplývajúcich z tejto Zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu u Dodávateľa a ktoré nie sú verejne známe. Prevádzkovateľ je povinný zabezpečiť zachovávanie mlčanlivosti v tomto zmysle každou osobou zúčastnenou na audite u Dodávateľa. Povinnosť zachovávať mlčanlivosť trvá aj po skončení trvania tejto Zmluvy a/alebo Základného kontraktu.
11. Prevádzkovateľ a nim poverené osoby pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len **„BOZP"**) a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len **„PO"**), s ktorými musia byť Dodávateľom oboznámení v zmysle nasledujúcich ustanovení tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ je povinný preukázateľne informovať Prevádzkovateľa a ním poverené osoby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory Dodávateľa.

Článok XII.
Záverečné ustanovenia

1. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi udelí, poskytne, prevedie alebo na Prevádzkovateľa postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu s Prevádzkovateľom založeného touto Zmluvou po dobu dohodnutú v trvaní päť rokov po ukončení zmluvného vzťahu.
2. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi vráti, prevedie a podľa pokynov Prevádzkovateľa prípadne aj zničí všetky informácie a osobné údaje vrátane ich kópií, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup.
3. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto Zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na plnenie predmetu tejto Zmluvy.
4. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto Zmluvy na tretiu osobu.

5. Táto Zmluva predstavuje úplnú dohodu zmluvných strán týkajúcu sa predmetu tejto Zmluvy a nahrádza v celom rozsahu akékoľvek predchádzajúce dohody či návrhy uvádzané v korešpondencii či na rokovaniach, či už ústne alebo písomné, ku ktorým došlo pred uzatvorením tejto Zmluvy a ktoré jej uzatvorením zanikajú.
6. Táto Zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto Zmluvou sa spravujú príslušnými ustanoveniami Obchodného zákonníka a ostatnými všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
7. Zmluva je vyhotovená v štyroch vyhotoveniach, ktoré majú povahu originálu, po dvoch vyhotoveniach pre každú zmluvnú stranu.
8. Neoddeliteľnou súčasťou tejto Zmluvy sú jej prílohy v zmysle ustanovenia čl. II, bodu 3. tejto Zmluvy.
9. Akúkoľvek zmenu alebo doplnenie tejto Zmluvy je možné vykonať výlučne formou písomných dodatkov podpísaných oboma zmluvnými stranami.
10. Táto Zmluva je uzatvorená, vzniká a zaväzuje zmluvné strany okamihom, keď je podpísaná oboma zmluvnými stranami.
11. Osoby konajúce za zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, prejav ich vôle je slobodný a vážny, určitý a zrozumiteľný a je plne v súlade s obsahom tejto zmluvy, zmluvná voľnosť zmluvných strán nie je obmedzená, Zmluvu si pred jej podpisom prečítali, tejto v celom rozsahu porozumeli a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.

V _____, dňa _____ V Bratislave, dňa 21.1.2022

za Prevádzkovateľa za Dodávateľa

Príloha č. 1 – Rozsah činností Dodávateľa v zmysle Základného kontraktu
Príloha č. 2 – Špecifikácia a rozsah bezpečnostných opatrení
Príloha č. 3 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa v zmysle Základného kontraktu
Príloha č. 4 - Zoznam schválených Subdodávateľov
Príloha č. 5 - Špecifikácia spracúvania osobných údajov

Tabuľka 2: Modelované očakávané počty a objemy transakcií, s prislúchajúcou odmenou (rok 2022)

Predmet	Počet	Hodnota (eur)	Odmena (eur)
Bezplatné transakcie	2 011 539	0	10 058
Platené transakcie	1 669 078	2 778 092	194 466
SPOLU	**3 680 617**	**2 778 092**	**204 524**

Tabuľka 3: Minimálna tarifikácia a minimálna výška parkovného

Predmet	Hodnota	*Po zľave pre plne elektrické vozidlá (50 %)*	*Po zľave pre ZTP (90 %)*
Minimálna tarifikácia v minútach	30 min. a následne po minúte	-	-
Minimálna hodnota transakcie v tarifnom pásme D (0,50 eur/hodina)	0,25 eur	*0,125 eur*	*0,025 eur*
Minimálna hodnota transakcie v tarifnom pásme C (1,00 eur/hodina)	0,50 eur	*0,25 eur*	*0,05 eur*
Minimálna hodnota transakcie v tarifnom pásme B (1,50 eur/hodina)	0,75 eur	*0,375 eur*	*0,075 eur*
Minimálna hodnota transakcie v tarifnom pásme A (2,00 eur/hodina)	1,00 eur	*0,50 eur*	*0,01 eur*

Príloha č. 1: Technické a funkčné požiadavky

ID	Typ Rq	Popis požiadavky	Priebeh kontroly	Spôsob kontroly zo strany MHBA	Spôsob preukázania zo strany Aplikanta	Akceptačné konanie
RQMPA-001	technicke	Požaduje sa aplikácia distribuovaná minimálne v Google Play a Apple App Store. Ku dňu Skúšok aplikácie musia byť podporované oficiálne podporované verzie operačných systémov Android a iOS.	Akceptácia/priebežne	Inštalácia aplikácií z Google Play a AppStore na mobilný telefón	Aplikant pošle linky na stiahnutie aplikácie z Google Play a AppStore	pred uzavretím zmluvy **priebežne na základe incidentov**
RQMPA-002	technicke	Systém bude online komunikovať s ParkSys najmä pre dotiahnutie údajov o existujúcom používateľovi ParkSys a zapisovaním parkovacích transakcií. Každá transakcia zapísaná do ParkSys bude obsahovať identifikáciu aplikácie a zariadenia, z ktorého bola poslaná.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše napinenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-003	technicke	Aplikácia bude zabezpečená minimálne v zmysle OWASP Top 10.	Akceptácia/priebežne	Aktuálny protokol skúšok	Požiadanie o aktuálny protokol **počas prevádzky**	
RQMPA-004	technicke	Aplikácia bude schopná zabezpečiť počet transakcii v zmysle očakávaných objemov podľa Prílohy č. 7 Zmluvy.	Akceptácia/priebežne	Výskyt incidentov	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	pred uzavretím zmluvy **priebežne na základe incidentov**
RQMPA-005	technicke	Systém bude prevádzkovaný 24x7, bude mať Dostupnosť (parameter "D") 99,1% Incidenty A (kritický): RT: 60 minút, FT: 8 hodín B (závažný): RT: 2 hodina, FT: 4 kalendárne dni C (nezávažný): RT: 1 kalendárny deň, FT: 14 kalendárnych dní. Plánované odstávky po dohode s Objednávateľom sú možné iba v So-Ne vo večerných hodinách . Najdlhší plánovaný výpadok je do max 5 hodín.	Akceptácia/priebežne	Priebežná kontrola Príloha č.5 – Mesačný výkaz prevádzky.xlsx	Dodávka priebežne počas prevázky	
RQMPA-006		Aplikácia a zvyšok komunikácie (emaily, notifikácie) budú minimálne v slovenskom a anglickom jazyku.		Kontrola language files a priebežná kontrola aplikácie a komunikácie	Poskytnutie tzv. language files, resp. prekladov všetkých prvkov aplikácie a komunikácie v SJ a AJ.	**priebežne na základe incidentov**
RQMPA-007	Funkcne	Používatelia aplikácie (MPA), krorí chcú využívať benefity parkovacích kariet (RPK, a pod.) musia mať vytvorený účet v danej aplikácií a účet musí obsahovať dvojfaktorovo overený. Každá zmena základných kontaktných a prihlasovacích údajov (e-maii adresy a/alebo mobilného tei. čísia) musí byť (rovnako ako pri iniciálnom zadaní) dvojfaktoro overená (s unikátnym časovo obmedzeným PIN, ktorý je nutné pre schválenie pridania/zmeny zadať v aplikácií). Aplikácia musí po dobu posledných 12 mesiacov uchovávať traksakčné logy aplikačného účtu v súvislosti s využívaním parkovania v HMBA a tieto aj s minimálne hore uvedenými identifikátormi účtu v prípade potreby poskytovať HMBA pre účely kontroly a vybavovania reklamácií. Používateľ aplikácie pre je samotným prvým použitím musí vyjadriť súhlas s obchodnými podmienkami a prevádzkovým poriadkom parkovania HMBA.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-008	Funkcne	Aplikácia umožní Zákazníkom získavať informácie o zozname parkovacích plôch v okolí vo forme interaktívnej mapy s časmi a cenami za parkovanie. Predvolený je parkovací úsek, v ktorej sa zariadenie reálne nachádza (GPS lokalizácia). Zákazník môže zmeniť parkovací úsek aj manuálne zadaním kódu úseku. ~~Mapa bude obsahovať aj umiestnenie parkomatov a predajných partnerov v okolí.~~	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-009	Funkcne	Aplikácia umožní minimálne: (1) využiť aplikáciu ako digitálny parkovací kotúč (pre bezplatné i platené parkovacie miesta s časovo obmedzeným parkovaním) (2) manuálne ukončenie vopred nastaveného parkovania v skoršom ako nastavenom čase s úhradou prostredníctvom následnej platby /postpaid/	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmiuve	**priebežne na základe incidentov**
RQMPA-010	Funkcne	Aplikácia bude notifikovať Zákazníka o udalostiach, najmä ohľadom blížiaceho sa ukončenia parkovacieho lístka, napr. formou push notifikácie.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**

RQMPA-011 Funkcne	Aplikácia umožní držiteľom parkovacích kariet zobrazenie a čepanie zostávajúceho kreditu Bonusovej parkovacej karty v zmysle VZN. ParkSys poskytuje interface na jednotný cenník pre danú EČV, parkovací úsek, a po zadaní ďalších povinných parametrov (čas od-do) včítane výšky zostatkového kreditu. Postpaid: Používateľ si nastaví očakávanú dĺžku parkovania. Zobrazí sa mu očakávaná cena za parkovné, a to vrátane započítania zostávajúceho kreditu Bonusovej parkovacej karty (zníženie ceny ak je nárok). Po ukončení parkovania (skoršom manuálnom alebo po dosiahnutí pôvodne nastaveného, príp. predĺženého času) sa v transakcií zohľadní aj kredit Bonusovej parkovacej karty. Ak je prepaid: Používateľ si nastaví očakávanú dĺžku parkovania. Zobrazí sa mu očakávaná cena za parkovné, a to vrátane započítania zostávajúceho kreditu Bonusovej parkovacej karty (zníženie ceny ak je nárok). Potvrdí kúpenie parkovacieho lístka a odráta využitý kredit z Bonusovej parkovacej karty. Výpočet: Počet nastavených minút parkovania - počet zostávajúcich minút/kreditu Bonusovej parkovacej karty = výsledný čas parkovania (ak je výsledný čas v rozmedzí 1 sekunda až 30 minút je použitá minimálna transakcia; ak je hodnota nižšia alebo rovná 0 ide o bezplatnú transakciu, ak je viac ako 30 minút platí minútová tarifikácia po 30 min.). Jednotlivé aplikácie môžu mať vlastné "krokovanie" pridávania minút pri nastavení času (viď nižšie). Čerpanie kreditov BPK v zmysle aktuálneho prevádzkového poriadku - aktuálne s krokom 1 min. Čerpanie bežnej tarify v zmysle aktuálneho prevádzkového poriadku - aktuálne minimálna dĺžka transakcie 30 min., krok predĺženia 15 min. (tj predlžovanie v násobkoch 15min)	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-012 Funkcne	Aplikácia umožní držiteľom parkovacích kariet zadávania parkovania pre svoje návštevy (Návštevnícka parkovacia karta) v zmysle VZN voči aktuálnemu kreditu na NPK. ParkSys poskytuje interface na jednotný cenník pre danú EČV, parkovací úsek, a po zadaní ďalších povinných parametrov (čas od-do) včítane výšky zostatkového kreditu. Aplikácia zašle číslo NPK (jednoznacny identifikator NPK, ktory obdrzi pouzivatei pri registracii v ParkSys a može si ho uložiť do aplikácie), ID parkovacieho úseku a čas parkovania (od-do). ParkSys vráti zostatok kreditu, cenu hodinového parkovania a 100 % zľavu z nej, maximalnu dobu statia v danom úseku. Čerpanie kreditov z NPK v zmysle aktuálneho prevádzkového poriadku - aktuálne s krokom 1 min.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-013 Funkcne	Účet používateľa poskytuje prehľad o stave účtu: história transakcii, zakúpených aktívnych aj historických produktov, registrované vozidlá. Aplikácia môže umožniť parkovanie aj neregistrovaným používateľom, rozumej tu používateľom bez účtu, avšak v tomto prípade neregistrovaný používateľ platí plné sumy za parkovné bez prípadných zliav a benefitov vyplývajúcich z VZN.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-014 Funkcne	Podklady pre zóny/oblasti a tarify budú jednoducho importovateľné do systému (zo systému ArcGis).	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-015 Funkcne	Aplikácia musí vedieť posiať parametre parkovania (kód úseku, EČV, zľavy/karty, začiatok a koniec parkovania...) cez API podľa popisu/dokumentácie, algoritmus výpočtu ceny za parkovné aj so zľavami bude na strane ParkSys a dodá aplikácii správne info na základe paramterov.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše napinenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-016 Funkcne	Aplikácia bude pre HMBA vytvárať zúčtovaci report o všetkých parkovacích transakciách vrátane informácii o platbách na mesačnej báze.	Akceptácia/priebežne	Priebežne Príloha č.4 – Výkaz parkovné.xlsx	Dodávka priebežne počas prevázky	
RQMPA-017 Funkcne	Poskytovateľ bude umožňovať ľahko prístupné a komunikované odoslanie spätnej väzby (in-app, alebo externe). Poskytovateľ sprístupni v režime read-only interný workflow riešenia feedbacku a na požiadanie vyexportuje evidované requesty.	Akceptácia/priebežne	Popis riešenia, prístup do IS pre request management priebežne reporty feedbackou akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-018 Funkcne	Aplikácia bude na platbu využívať svoju platobnú bránu na vlastné náklady a riziko.	Akceptácia	Akceptačné testy a kontrola zmluvy o poskytovaní služieb platobnej brány	Aplikant doloží úradný preklad zmiuvy o platobnej bráne pri pristúpení k zmluve (s cenzurovaným údajom o výške poplatkov za transakcie)	**pred uzavretím zmluvy priebežne na základe incidentov**
RQMPA-019 Funkcne	Vystavovanie daňového dokladu v mene HMBA. Aplikácia umožní prístup k týmto daňovým dokladom.	Akceptácia/priebežne	Doloženie vzoru daňového dokladu	Aplikant popíše naplnenie požiadavky a doloží presný vzor daňového dokladu	**priebežne na základe incídentov**
RQMPA-020 Funkcne	Aplikácia komunikuje používateľovi a zreteľne rozlišuje príčinu prípadných chýb. Rozlišuje tieto tri kategórie chýb: 1. **interná chyba aplikácie** napr: Neúplné dáta -Nekompletné údaje: chýba EČV, zvolený úsek parkovania 2. **Interná chyba aplikácie - mobilného zariadenia** - napr. Nepodarilo sa získať pozíciu GPS, Aplikácia nemá pripojenie do internetu 3. **Externá chyba parkovacej služby** - chýbajúce dáta napr. Parkovacia služba HMBA je vypnutá alebo nedostupná.	Akceptácia/priebežne	Akceptačné testy	Aplikant pri pristúpení k zmluve dodá zoznam zobrazovaných chybových hlášok v daných kategóriach	**priebežne na základe incidentov**

#	Požiadavka	Názov testovacieho scenára	Cieľ	Popis scenára	Vstup	Výstup	Poznámka
	RQMPA-001	Inštalácia aplikácií z AppStore a Google Play	Cieľom je zistiť, či je aplikácia verejne prístupná a bezplatná na Google Play a AppStore a či je možné ju nainštalovať a spustí sa.	Preklik z poskutnutých URL priamo z mobilných telefónov s podporovaným OS a inštalácia aplikácií z Google Play/AppStore.	Aplikant poskytne URL na stiahnutie aplikácie z Google Play a AppStore.	Úspešné zobrazenie aplikácie v katalógu aplikácií (Google Play/AppStore), úspešná inštalácia aplikácie a úspečné spustenie aplikácie.	
	RQMPA-002	Zápis transakcie do MoPO	Cieľom je zistiť správny zápis údajov do MoPO a čítanie potrebných údajov ako napr. zostatok bonusových hodín pre používateľa ParkSys	MPA má konektivitu na ParkSys Používateľ s kontom aj v ParkSys si zobrazí zostatkový kredit vyplývajúci z parkovacích kariet. Používateľ zadá a následne ukončí parkovaciu transakciu.	MPA s používateľom ParkSys s RPK a/alebo APK a/alebo BPK a/alebo NPK, ktorý si pozrie zostatkový kredit z BPK a NPK ako aj zakúpi parkovací lístok.	Správne zaevidovaná transakcia (vrátane napr. zľavy z parkovného vďaka kreditu) v MoPO so všetkými vyžadovanými údajmi po zaevidovaní začiatku parkovania i po jeho ukončení.	
	RQMPA-006	Jazyková kontrola	Cieľom je zistiť, či aplikácia komunikuje po slovensky a po anglicky.	Kontrola poskytnutých language files.	Language files (min. SK, EN) použité v aplikácii a emailových a iných notifikáciach.	Korektné preklady.	
	RQMPA-007	Vytvorenie používateľského konta MPA s overením e-mailovej adresy a/alebo tel. čísla	Cieľom je preveriť vytvorenie, zaregistrovanie nového používateľa v MPA.	1. Vytvorenie nového účtu v MPA s povinným zadaním e-mailovej adresy a/alebo mobilného tel. čísla, viazaného k účtu. 2. Zadaná e-mail adresa a/alebo mobilné tel. číslo bude akceptované a účet aktívny pre použitie v HMBA až po jeho dvojfaktorovom overení. 3. Pred prvým použitím je vyžadovaný súhlas s obchodnými podmienkami a prevádzkovým poriadkom parkovania HMBA. 4. Na používateľskom účte sa vykoná zmena e-mailovej adresy a/alebo mobilného telefónneho čísla a bude akceptovaná až po jej dvojfaktorovom overení.	MPA pre všetky typy používateľov	Vytvorený nový účet, overený e-mail a/alebo mobilné telefónne číslo viažuce sa k účtu. Zmena e-mailu a/alebo mobilného tel. čísla akceptovaná až po dvojfaktorovom overení. Nemožnosť zadať parkovaciu transakciu na novou účte s nepotvrdeným oboznámením sa s obchodnými podmienkami a prevádzkovým poriadkom parkovania HMBA.	
	RQMPA-008	Preverenie identifikácie správnej zóny podľa lokality používateľa.	Preverenie funkčnosti, čí aplikácia podľa GPS zariadenia správne identifikuje a predvolí aktuálnu parkovaciu zónu, zobrazí ceny a čas parkovania a dovolí korekciu zóny (napr. manuálne zadať kód zóny a/alebo premiestniť pozíciu na mape). Aplikácia dovoľuje prehľadávať zóny so zobrazením parametrov parkovania.	MPA v oblasti výberu zóny zobrazí správnu zónu podľa aktuálnehop GPS zariadenia s cenami a časom a parkovania a poskytuje GUI na prehľadávania ďalších zón a informácií ku nim. Aplikácia tiež umožňuje manuálne zadanie kódu zóny a/alebo premiestnenie pozície na mape.	MPA pre všetky typy používateľov	Správe určená zóna podľa aktuálnej lokality zariadenia, možnosť prehľadávania susedných zón, možnosť posunu pozície na mape do inej zóny a/alebo manuálne zadanie kódu zóny, všetky zóny majú zobrazené korektné údaje o časoch a cenách za parkovanie.	
	RQMPA-009	Digitály parkovací kotúč	Cieľom je overiť, čí aplikácia obmedzí nastaviť dĺžku parkovania na max. časové obmedzenie dané dopravným značením (úseky dopravnej regulácie) a to bez ohľadu či ide o platenú alebo neplatenú transakciu.	MPA obmedzí možnosť vytvoriť platenú alebo neplatenú parkovaciu transakciu na základe časového obmedzenia. Časové obmedzenie sa resetuje o polnoci. Pri platenej i neplatenej transakcii ie po uplynutí času (z max. časového obmedzenia) v daný deň ECV evidovaná ako priestupca (neplatný parkovací lístok) a neumožní zaevidovanie ďalšej parkovacej transakcie.	MPA pre všetky typy používateľov na úseku dopravnej regulácie s max. časovým obmedzením (napr. 30 min.).	Možnosť zvoliť dĺžku parkovania v úseku s obmedzenou dĺžkou parkovania. Parkovanie sa zaeviduje príp. zaplatí, (zápis do ParkSysu) ak nebol vyčerpaný čas v daný deň. V prípade že čas parkovania už bol vyčerpaný, MPA neumožní zaevidovanie parkovania.	
	RQMPA-009	Následná platba za parkovanie s vopred nastaveným časom	Cieľom je zaevidovanie parkovania s určeným začiatkom parkovania a vopred nastavenou dĺžkou parkovania s možnosťou ukončenia kedykoľvek pred skončením platnosti parkovacieho lístka s následnou platbou za reálny čas parkovania (postpaid)	MPA vytvorí transakciu na parkovanie so začiatkom parkovania a dĺžkou parkovania (konkrétne nastavená dĺžka, resp. čas ukončenia parkovania). Používateľ má možnosť kedykoľvek ukončiť parkovanie s následným zaplatením za reálny čas parkovania.	MPA pre všetky typy používateľov	Možnosť zvoliť začiatok parkovania, nastaviť dĺžku parkovania na 3 h a 15 min. Zaevidovanie parkovania v ParkSyse. Následné ukončenie parkovania používateľom pred exporáciou parkovacieho lístka. Platba (alebo jej evidencia na strane MPA) najskôr po manuálnom ukončení parkovania.	
	RQMPA-010	Notifikuj zákaznika	Cieľom je notifikovanie používateľa o blížiacej expirácií a expirácii parkovacieho lístka alebo digitálneho parkovacieho kotúča, prip. iných udalostiach súvisiacich s parkovaním.	MPA notifikuje o blížiacom sa konci platnosti parkovania a o automatickom ukončení (vo vopred nastavený čas) parkovania.	MPA pre všetky typy používateľov	Push notifikácia alebo SMS	
	RQMPA-011	Zobraz kredit a zaeviduj zľavu na parkovné z Bonusovej parkovacej karty (BPK)	Cieľom je umožniť držiteľom BPK zobrazenie denného kreditu (limitu/času) a započítanie voľného kreditu (aktuálne 100 % zľava z parkovného) na parkovanie v rámci parkovacej transakcie (zaevidovanie/kúpa parkovacieho lístku) zo zostávajúceho kreditu BPK karty v zmysle VZN.	MPA zobrazí zostávajúci kredit z BPK. Po spustení parkovania vytvorí transakciu v ParkSyse a v prípade prepaid platby zašle MPA do ParkSysu informáciu o zostatkovom bonusovom kredite hneď pri začiatku parkovania (transakcie), v prípade postpaidu po skončení parkovania (transakcie).	MPA s používateľom ParkSys s BPK	Zaevidovanie transakcie v MoPO, zaslanie informácie o znížení kreditu z BPK do ParkSysu	
	RQMPA-012	Zobraz kredit a zaeviduj zľavu na parkovné z Návštevníckej parkovacej karty (NPK)	Cieľom je umožniť držiteľom NPK zobrazenie ročného kreditu (limitu/času) a započítanie (aktuálne 100 % zľava z parkovného) na parkovanie zo zostávajúceho kreditu NPK v zmysle VZN.	MPA zaeviduje do ParkSysu začiatok a koniec parkovnia, na zvolenom úseku pre manuálne vložené EČV čerpajúc kredit z NPK.	MPA s používateľom ParkSys s NPK	Zaevidovanie transakcie v MoPO, zaslanie informácie o znížení kreditu z NPK do ParkSysu	
	RQMPA-013	Zobraz profil, produkty a vozidlá (prihláseného) používateľa	Cieľom je zobrazenie informácií o prehľade a stave účtu, história transakcií, zakúpených aktívnych aj historických produktov, registrované aktívne vozidlá.	MPA zobrazí informácie o prehľade a stave účtu, história transakcií, zakúpených aktívnych aj historických produktov, registrované aktívne vozidlá	MPA s používateľom ParkSys s RPK a/alebo APK a/alebo BPK a/alebo NPK	Prehľad všetkých transakcií a informácií v MPA	
	RQMPA-014	Importuj zóny a tarify	Cieľom je importovať definované zóny/oblasti a ich vrstvy zo systému ArcGIS mesta	MPA sa v dohodnutých časových intervaloch synchronizuje so systémom ArcGIC a v prípade, že je to potrebné, stiahne si informácie o zónach/oblastiach a tarifách do systému MPA.	Volanie API na synchronizáciu dát z ArcGiS	Prezentácia aktuálnych dát o zónach/oblastiach v aplikácií.	
	RQMPA-015	Vypočítaj cenu parkovného	Cieľom je vypočítať a poskytnúť aktuálnu cenu za parkovné na základe parametrov: úsek parkovania (podľa GPS), čas a dátum parkovania (začiatok a koniec), výška zľavy z ceny parkovného	MPA volá API ParkSys na výpočet ceny parkovného na základe vstupných parametrov. API vráti cenu za parkovné v dohodnutom formáte.	Volanie API na výpočet ceny parkovného	Vypočítaná cena za parkovné	
	RQMPA-017	Odošli spätnú väzbu (prihlásený používateľ)	Cieľom je prezentácia funkčosti zaslania spätnej väzby od autentifikovaného (prihláseného) používateľa MPA.	MPA poskytne používateľovi spôsob odoslania spätnej väzby.	MPA pre všetky typy používateľov	MPA pre všetky typy používateľov	
	RQMPA-018	Platba cez platobnú bránu	Cieľom je overiť či je možné cez aplikáciu zaplatiť za parkovné.	Výber parkovacieho úseku, zadanie času parkoania a EČV, platba.	MPA pre všetky typy používateľov	Úspešná platba za parkovné.	
	RQMPA-019	Vystavovanie a doručovanie daňových dokladov v mene HMBA	Cieľom je preveriť funkčnosť vystavovania a zasielania daňových dokladov v mene HMBA.	Používateľ zaplatí parkovací lístok. Nasleduje aspoň jedna z možností: a. MPA odošle používateľovi e-mail s daňovým dokladom za danú transakciu. b. MPA umožní používateľovi zobraziť si transakciuv histórii transakcií a stiahnúť si k nej daňový doklad.	MPA pre všetky typy používateľov	(a) E-mail s daňovým dokladom a/alebo (b) Transakcia zaevidovaná v histórii transakcií s možnosťou stiahnutia.	
	RQMPA-020	Rozlišovanie chýb	Cieľom je preveriť, či aplikácia správne komunikuje chyby.	Simulácia výpadku Internetu, nekompletných údajov, výpadku na strane ParkSys pri práci s aplikáciou.	MPA pre všetky typy používateľov	Korektné chybové hlášky podľa poskytnutého zoznamu chybových hlášok.	

Manuál k skúškam aplikácie

Úvod
Objednávateľ je prevádzkovateľom parkovacích miest na území Objednávateľa. Objednávateľ všeobecne záväzným nariadením č. 8/2019 o dočasnom parkovaní motorových vozidiel (ďalej ako „VZN 8/2019") ustanovil úseky miestnych komunikácií na dočasné parkovanie motorových vozidiel na svojom území, určil spôsob zabezpečenia prevádzky parkovacích miest, výšku úhrady za dočasné parkovanie, spôsob jej platenia a spôsob preukázania jej zaplatenia. Objednávateľ umožnil vo VZN 8/2019 vykonávanie úhrady za parkovací lístok prostredníctvom internetového rozhrania, vrátane mobilných aplikácií, ktoré sú bežným a veľmi využívaným platobným nástrojom v oblasti úhrady za dočasné parkovanie v rámci krajín Európskej únie.
Objednávateľ v snahe zabezpečiť poskytovanie kvalitných služieb pre svojich obyvateľov, ako aj návštevníkom na najvyššej možnej úrovni aj v oblasti predaja a distribúcie parkovacích oprávnení (parkovacích lístkov) podporuje otvorenú súťaž pre všetkých poskytovateľov služieb súvisiacich s predajom a distribúciou parkovacích oprávnení, ktorá ako jediná dokáže zabezpečiť a kontinuálne udržať požadovanú úroveň a kvalitu poskytovaných služieb.
Objednávateľ v tejto súvislosti vypracoval tento dokument, ktorým popisuje proces skúšok aplikácie a formálne požiadavky ktoré sú kladené na Poskytovateľa, a ktoré musí zároveň nepretržite spĺňať, aby zostal pripojený k centrálnemu systémom Objednávateľa ako Poskytovateľ.

Východiská
Úhrada Parkovného musí byť vykonaná správne a úplne
Výmena dát s MPA vs ParkSys musí byť technicky a vecne správna
Zákazníkom musí byť jasné, za čo je úhrada vykonaná a aké sú možné zľavy
Dôvera v poskytovanie služby platobného systému nesmie byť ohrozená

Príloha 4: Mesačný výkaz parkovného (formulár)

Vyplní Poskytovateľ:		
Poskytovateľ:	________	
Výkaz za mesiac a rok:	________	
Vytvorené dňa:	________	

Vyplní Objednávateľ:		
Schválené dňa:	________	
Aplikovaný podiel na trhu:	________	%
Celková odmena za kontrolovaný mesiac:	________	EUR
Schválil:	________	
Podpis:	________	

Poskytovateľ (ID)	**Rok**	**Mesiac**	**Timestamp príchod**	**Timestamp odchod**	**Mestská časť (ID)**	**Parkovací úsek (ID)**	**ECV (resp. anonymizované ID)**	**GPS latitude***	**GPS longitude***	**Platená transakcia**	**Úhrada v eur**
(celé číslo)	*(celé číslo)*	*(celé číslo)*	*(timestamp)*	*(timestamp)*	*(celé číslo)*	*(celé číslo)*	*(text)*	*(desatinné číslo)*	*(desatinné číslo)*	*(logická)*	*(desatinné číslo)*

Príloha č. 9: Vyhlásenie k splneniu Technických a funkčných požiadaviek
Poskytovateľ: _____

ID	Typ Rq	Popis požiadavky	Spôsob naplnenia požiadavky (vyplní Poskytovateľ)
RQMPA-001	technicke	Požaduje sa aplikácia distribuovaná v Google Play a Apple App Store. Ku dňu Skúšok aplikácie musia byť podporované oficiálne podporované verzie operačných systémov Android a iOS.	
RQMPA-002	technicke	Systém bude online komunikovať s ParkSys najmä pre dotiahnutie údajov o existujúcom používateľovi ParkSys a zapisovanim parkovacích transakcií. Každá transakcia zapísaná do ParkSys bude obsahovať identifikáciu aplikácie a zariadenia, z ktorého bola poslaná.	
RQMPA-003	technicke	Aplikácia bude zabezpečená minimálne v zmysle OWASP Top 10.	
RQMPA-004	technicke	Aplikácia bude schopná zabezpečiť počet transakcií v zmysle očakávaných objemov podľa Prílohy č. 7 Zmluvy.	
RQMPA-005	technicke	Systém bude prevádzkovaný 24x7, bude mať Dostupnosť (parameter "D") 99,1% Incidenty A (kritický): RT: 60 minút, FT: 8 hodín B (závažný): RT: 2 hodina, FT: 4 kalendárne dni C (nezávažný): RT: 1 kalendárny deň, FT: 14 kalendárnych dní. Plánované odstávky po dohode s Objednávateľom sú možné iba v So-Ne vo večerných hodinách . Najdlhší plánovaný výpadok je do max 5 hodín.	
RQMPA-006		Aplikácia a zvyšok komunikácie (emaily, notifikácie) budú minimálne v slovenskom a anglickom jazyku.	
RQMPA-007	Funkcne	Používatelia aplikácie (MPA), krorí chcú využívať benefity parkovacích kariet (RPK, a pod.) musia mať vytvorený účet v danej aplikácií a účet musí obsahovať dvojfaktorovo overený. Každá zmena základných kontaktných a prihlasovacích údajov (e-mail adresy a/alebo mobilného tel. čísla) musí byť (rovnako ako pri iniciálnom zadaní) dvojfaktoro overená (s unikátnym časovo obmedzeným PIN, ktorý je nutné pre schválenie pridania/zmeny zadať v aplikácií). Aplikácia musí po dobu posledných 12 mesiacov uchovávať traksakčné logy aplikačného účtu v súvislosti s využívaním parkovania v HMBA a tieto aj s minimálne hore uvedenými identifikátormi účtu v prípade potreby poskytovať HMBA pre účely kontroly a vybavovania reklamácií. Používateľ aplikácie pre je samotným prvým použitím musí vyjadriť súhlas s obchodnými podmienkami a prevádzkovým poriadkom parkovania HMBA.	
RQMPA-008	Funkcne	Aplikácia umožní Zákazníkom získavať informácie o zozname parkovacích plôch v okolí vo forme interaktívnej mapy s časmi a cenami za parkovanie. Predvolený je parkovací úsek, v ktorej sa zariadenie reálne nachádza (GPS lokalizácia). Zákazník môže zmeniť parkovací úsek aj manuálne zadaním kódu úseku. Mapa bude obsahovať aj umiestnenie parkomatov a predajných partnerov v okolí.	
RQMPA-009	Funkcne	Aplikácia umožní minimálne: (1) využiť aplikáciu ako digitálny parkovací kotúč (pre bezplatné i platené parkovacie miesta s časovo obmedzeným parkovaním) (2) manuálne ukončenie vopred nastaveného parkovania v skoršom ako nastavenom čase s úhradou prostredníctvom následnej platby /postpaid/	
RQMPA-010	Funkcne	Aplikácia bude notifikovať Zákazníka o udalostiach, najmä ohľadom blížiaceho sa ukončenia parkovacieho lístka, napr. formou push notifikácie.	

RQMPA-011 Funkcne	Aplikácia umožní držiteľom parkovacích kariet zobrazenie a čepanie zostávajúceho kreditu Bonusovej parkovacej karty v zmysie VZN. ParkSys poskytuje interface na jednotný cenník pre danú EČV, parkovací úsek, a po zadaní ďalších povinných parametrov (čas od-do) včítane výšky zostatkového kreditu. Postpaid: Používateľ si nastaví očakávanú dĺžku parkovania. Zobrazí sa mu očakávaná cena za parkovné, a to vrátane započítania zostávajúceho kreditu Bonusovej parkovacej karty (zníženie ceny ak je nárok). Po ukončení parkovania (skoršom manuálnom alebo po dosiahnutí pôvodne nastaveného, príp. predĺženého času) sa v transakcií zohľadní aj kredit Bonusovej parkovacej karty. Ak je prepaid: Používateľ si nastaví očakávanú dĺžku parkovania. Zobrazí sa mu očakávaná cena za parkovné, a to vrátane započítania zostávajúceho kreditu Bonusovej parkovacej karty (zníženie ceny ak je nárok). Potvrdí kúpenie parkovacieho lístka a odráta využitý kredit z Bonusovej parkovacej karty. Výpočet: Počet nastavených minút parkovania - počet zostávajúcich minút/kreditu Bonusovej parkovacej karty = výsledný čas parkovania (ak je výsledný čas v rozmedzí 1 sekunda až 30 minút je použitá minimálna transakcia; ak je hodnota nižšia alebo rovná 0 ide o bezplatnú transakciu, ak je viac ako 30 minút platí minútová tarifikácia po 30 min.). Jednotlivé aplikácie môžu mať vlastné "krokovanie" pridávania minút pri nastavení času (viď nižšie). Čerpanie kreditov BPK v zmysle aktuálneho prevádzkového poriadku - aktuálne s krokom 1 min. Čerpanie bežnej tarify - minimálna dĺžka transakcie 30 min., minimálny krok predĺženia 1 min., max krok predĺženia 15 min.
RQMPA-012 Funkcne	Aplikácia umožní držiteľom parkovacích kariet zadávania parkovania pre svoje návštevy (Návštevnícka parkovacia karta) v zmysle VZN voči aktuálnemu kreditu na NPK. ParkSys poskytuje interface na jednotný cenník pre danú EČV, parkovací úsek, a po zadaní ďalších povinných parametrov (čas od-do) včítane výšky zostatkového kreditu. Aplikácia zašle číslo NPK (jednoznacny identifikator NPK, ktory obdrzi pouzivatel pri registracii v ParkSys a može si ho uložiť do aplikácie), ID parkovacieho úseku a čas parkovania (od-do). ParkSys vráti zostatok kreditu, cenu hodinového parkovania a 100 % zľavu z nej, maximainu dobu statia v danom úseku. Čerpanie kreditov z NPK v zmysle aktuálneho prevádzkového poriadku - aktuálne s krokom 1 min.
RQMPA-013 Funkcne	Účet používateľa poskytuje prehľad o stave účtu: história transakcii, zakúpených aktívnych aj historických produktov, registrované vozidlá.
RQMPA-014 Funkcne	Podklady pre zóny/oblasti a tarify budú jednoducho importovateľné do systému (zo systému ArcGis).
RQMPA-015 Funkcne	Aplikácia musí vedieť poslať parametre parkovania (kód úseku, EČV, zľavy/karty, začiatok a koniec parkovania...) cez API podľa popisu/dokumentácie, algoritmus výpočtu ceny za parkovné aj so zľavami bude na strane ParkSys a dodá aplikácií správne info na základe paramterov.
RQMPA-016 Funkcne	Aplikácia bude pre HMBA vytvárať zúčtovací report o všetkých parkovacích transakciách vrátane informácií o platbách na mesačnej báze.
RQMPA-017 Funkcne	Poskytovateľ bude umožňovať ľahko prístupné a komunikované odoslanie spätnej väzby (in-app, alebo externe). Poskytovateľ sprístupní v režime read-only interný workflow riešenia feedbacku a na požiadanie vyexportuje evidované requesty.
RQMPA-018 Funkcne	Aplikácia bude na platbu využívať svoju platobnú bránu na vlastné náklady a riziko.
RQMPA-019 Funkcne	Vystavovanie daňového dokladu v mene HMBA. Aplikácia umožní prístup k týmto daňovým dokladom.
RQMPA-020 Funkcne	Aplikácia komunikuje používateľovi a zreteľne rozlišuje príčinu prípadných chýb. Rozlišuje tieto tri kategórie chýb: 1. **Interná chyba aplikácie** napr: Neúplné dáta -Nekompletné údaje: chýba EČV, zvolený úsek parkovania 2. **Interná chyba aplikácie - mobilného zariadenia** - napr. Nepodarilo sa získať pozíciu GPS, Aplikácia nemá pripojenie do internetu 3. **Externá chyba parkovacej služby** - chýbajúce dáta napr. Parkovacia služba HMBA je vypnutá alebo nedostupná.