DODATOK Č. 2 K ZMLUVE O ZABEZPEČENÍ SLUŽBY PLATOBNÉHO SYSTÉMU PROSTREDNÍCTOM MOBILNEJ APLIKÁCIE PRE ÚHRADU DOČASNÉHO PARKOVANIA

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

(ďalej ako „**Dodatok**")
medzi zmluvnými stranami:

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:	SK88 7500 0000 0002 2504 7483
Zastúpený:	Ing. arch Matúš Vallo, primátor

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

a

Poskytovateľ

Názov:	Bmove Slovakia s.r.o.
Sídlo:	Hodžovo námestie 1A, 811 06 Bratislava
IČO:	54 155 029
DIČ:	2121589976
IČ DPH:	SK2121589976
IBAN:	SK26 0900 0000 0051 8480 1437
Zastúpený:	Johann Breiteneder

(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

Zmluvné strany uzatvorili dňa 11.11.21 Zmluvu o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania (ďalej len ako „**Zmluva**") v súlade s Verejným návrhom na uzatvorenie Zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania podľa § 276 zákona č. 513/1991 zb. Obchodný zákonník zo dňa 20. júla 2021, v znení zmeny zo dňa 1.10.2021. Počas vzájomnej spolupráce medzi Zmluvnými stranami, v zmysle legislatívno-technického, ako aj vecného, v kontexte uplatňovania jednotlivých práv a povinností vyplývajúcich zo Zmluvy, vystali na základe praxe určité oblasti práv a povinností, ktoré budú doplnené a upravené aj v Novom období, a teda budú súčasťou novej právnej úpravy verejného návrhu na uzavretie Zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania podľa § 276 zákona č. 513/1991 zb. Obchodný zákonník, ako aj súčasťou tohto Dodatku. V zmysle čl. XII, ods.12.2 Zmluvy, je Objednávateľ oprávnený, najneskôr v lehote do 30 (tridsať) kalendárnych dní pred uplynutím doby trvania 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 Zmluvy.
V súlade s vyššie uvedeným a na základe vzájomnej spolupráce medzi Zmluvnými stranami, a vzájomných pozitívnych skúseností získaných pri zabezpečovaní časovo a administratívne efektívnej úhrady Parkovného prostredníctvom Aplikácie ako jedného z platobných kanálov na úhradu Parkovného v súlade so Zmluvou, a znením Dodatku č. 1 a Všeobecne záväzným nariadením č. 10/2021 o dočasnom parkovaní motorových vozidiel, ako úplným znením Všeobecne záväzného nariadenia hlavného mesta Slovenskej republiky Bratislavy č. 8/2019 o dočasnom parkovaní motorových vozidiel, ako vyplýva zo zmien vykonaných všeobecne záväzným nariadením hlavného mesta Slovenskej republiky Bratislavy č. 12/2020 a zo zmien a doplnení vykonaných všeobecne záväzným nariadením hlavného mesta Slovenskej republiky Bratislavy č. 9/2021 (ďalej ako „**VZN 10/2021**"), Zmluvné strany uzatvárajú tento Dodatok.

Článok I
Predmet dodatku

1. Zmluvné strany sa dohodli, že Preambula Zmluvy sa mení v celom rozsahu nasledovne:

   a) Nové znenie Preambula:

„ **Preambula**

Objednávateľ je prevádzkovateľom parkovacích miest na území Objednávateľa. Objednávateľ všeobecne záväzným nariadením č. 10/2021 o dočasnom parkovaní motorových vozidiel, ako úplné znenie všeobecne záväzného nariadenia hlavného mesta Slovenskej republiky Bratislavy č. 8/2019 o dočasnom parkovaní motorových vozidiel, ako vyplýva zo zmien vykonaných všeobecne záväzným nariadením hlavného mesta Slovenskej republiky Bratislavy č. 12/2020 a zo zmien a doplnení vykonaných všeobecne záväzným nariadením hlavného mesta Slovenskej republiky Bratislavy č. 9/2021 (ďalej ako „VZN 10/2021"), 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 10/2021 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 má právo umožniť 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."

2. Zmluvné strany sa dohodli, že Čl. I Definícia pojmov sa mení a dopĺňa nasledovne v týchto častiach:

   a) Pôvodné znenie vybraných pojmov sa v celom rozsahu mení a nahrádza nasledovným novým znením:
   „**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 10/2021 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 10/2021 (§ 4 VZN 10/2021) alebo v Prevádzkovom poriadku;

„**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 10/2021 a upraviť výšku Parkovného za Parkovacie miesta neuvedené vo VZN 0/2021; Prevádzkový poriadok môže Objednávateľ jednostranne meniť; v prípade rozporu medzi Prevádzkovým poriadkom a touto Zmluvou vrátane jej Príloh má prednosť táto Zmluva;"

b) Pôvodné znenie Definícia pojmov sa mení a dopĺňa nasledovne o tieto pojmy:

„**UX dizajn - User experience/zážitok**" – znamená používateľský dizajn a postupy v rámci Aplikácie, ktoré rešpektujú potreby Zákazníka v rámci Aplikácie, a zároveň zabezpečujú naplnenie jednotlivých cieľov Zmluvných strán, najmä bezproblémovú, časovo a administratívne efektívnu úhradu Parkovného pomocou samotnej Aplikácie, ktorá ako výsledný produkt, musí byť intuitívna a jej zmyslom je pomoc Zákazníkom za každých okolností nájsť čo hľadajú;

„**UX test**" – znamená test zo strany Objednávateľa alebo ním poverenej tretej osoby v rámci Aplikácie, ktorého výsledkom je analýza User experience/zážitku Zákazníka z používania Aplikácie v praxi.

3. Zmluvné strany sa dohodli, že Čl. 2 Úvodné ustanovenia a vyhlásenia strán sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 2.1 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„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 10/2021. Objednávateľ zavedením systému platieb Parkovného cez mobilné aplikácie Objednávateľom sleduje zvýšenie komfortu služieb pre Zákazníkov."

4. Zmluvné strany sa dohodli, že Čl.7 Práva a povinnosti pri Prevádzkovaní Aplikácie sa mení a dopĺňa nasledovne:

a) Pôvodné znenie sa mení a dopĺňa o nový čl.7.4.6 Zmluvy:

„Poskytovateľ sa zaväzuje, že:

7.4.6 umožní vykonať Objednávateľovi alebo ním poverenej tretej osobe vykonanie UX testu, t.j. testu na UX dizajn – User experience/zážitok, v rámci Fázy prevádzkovania Aplikácie, ako aj Fázy akceptácie Aplikácie, a to kedykoľvek počas trvania Zmluvy, a zároveň poskytne maximálnu súčinnosť pre riadne a včasné vykonanie UX testu. V prípade negatívneho výsledku vyplývajúceho z UX testu alebo v prípade zjavných nedostatkov vyplývajúcich z výsledkov UX testu je Poskytovateľ povinný tieto negatíva a/alebo zjavné nedostatky vyplývajúce z analýzy výsledkov UX testu odstrániť do 30 (slovom: tridsať) pracovných dní od doručenia výzvy zo strany Objednávateľa."

5. Zmluvné strany sa dohodli, že Čl. 8 Zodpovednosť za vady Aplikácie sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 8.10 až 8.13 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

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

a) 30 (tridsať) minút od identifikácie Kritického incidentu,
b) 60 (šesťdesiat) minút od identifikácie Závažného incidentu,

c) 24 (dvadsaťštyri) hodín od identifikácie Nekritického incidentu.

Doba reakcie na Incident sa začína rátať od momentu detegovania Incidentu v zmysle bodu 8.8 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: mpa@bratislava.sk.

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

a) 4 (štyri) hodiny v prípade Kritického incidentu,
b) 96 (deväťdesiatšesť) hodín v prípade Závažného incidentu,
c) 240 (dvestoštyridsať) hodín 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: mpa@bratislava.sk Priebeh každého Incidentu spolu s popisom príčin vzniku Incidentu a spôsobu jeho vyriešenia zaznamená Poskytovateľ v Mesačnom výkaze prevádzky."

b) Pôvodné znenie čl. 8.15 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„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) 4 (štyri) sankčné body za každé porušenie vo vzťahu ku Kritickému incidentu,
b) 2 (dva) sankčné body za každé porušenie vo vzťahu k Závažnému Incidentu,
c) 1 (jeden) sankčný bod 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 kalendárny mesiac dosiahne 8 (osem) bodov, vznikne Objednávateľovi právo odstúpiť od Zmluvy."

6. Zmluvné strany sa dohodli, že Čl. 14 Trvanie Zmluvy sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 14.1 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„14.1 Zmluva sa zatvára na dobu určitú do 31.12.2023."

7. Zmluvné strany sa dohodli, že Čl. 15 Trvanie Zmluvy sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 15.1 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„15. 1 Zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv v zmysle § 47a ods. 1 zák. č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov v spojení s § 5a zák. č. 211/2000 Z. z. zákona o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov."

8. Zmluvné strany sa dohodli, že Príloha č. 8: Zmluva o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností a ochrany osobných údajov sa dopĺňa a mení v nasledovnom rozsahu - Príloha č. 8: Zmluva o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností a ochrany osobných údajov (verzia 2023):

   a) Pôvodné znenie Prílohy č. 8 o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností a ochrany osobných údajov sa mení a dopĺňa v čl. VI, ods. 3 nasledovne:

      „3. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti:

meno a priezvisko:	Mgr. Martin Slyško
funkcia/pracovná pozícia	projektový manažér
telefónne číslo:	+421 903 509 574
e-mailová adresa:	mpa@bratislava.sk“

   b) Pôvodné znenie Prílohy č. 8 o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností a ochrany osobných údajov sa mení a dopĺňa v čl. VII, ods. 4 nasledovne:

      „4. Prevádzkovateľ určuje nasledovné kontaktné osoby pre komunikáciu s Dodávateľom na úseku ochrany osobných údajov:

meno a priezvisko:	Mgr. Martin Slyško
funkcia/pracovná pozícia	projektový manažér
telefónne číslo:	+421 903 509 574
e-mailová adresa:	mpa@bratislava.sk“

9. Zmluvné strany sa dohodli, že Príloha č. 1, Príloha č.2, a Príloha č. 9 sa dopĺňa a mení v celom rozsahu. Samotná textácia jednotlivých príloh podľa nižšie uvedených je súčasťou tohto Dodatku:

   - „Príloha č. 1: Technické a funkčné požiadavky (verzia 2023)“
   - „Príloha č. 2: Podmienky oprávnenosti a spôsob ich preukázania (verzia 2023)“
   - „Príloha č. 9: Vyhlásenie k splneniu Technických a funkčných požiadaviek (verzia 2023)“

Článok II
Záverečné ustanovenia

1. Tento Dodatok je neoddeliteľnou súčasťou Zmluvy.
2. Tie ustanovenia Zmluvy, ktoré nie sú týmto Dodatkom dotknuté ostávajú v platnosti bez zmeny.
3. Neoddeliteľnou súčasťou a prílohou tohto Dodatku, sú nasledujúce prílohy, ktoré tvoria i neoddeliteľnú súčasť samotnej Zmluvy:
   - „Príloha č. 1: Technické a funkčné požiadavky (verzia 2023)“
   - „Príloha č. 2: Podmienky oprávnenosti a spôsob ich preukázania (verzia 2023)“
   - „Príloha č. 9: Vyhlásenie k splneniu Technických a funkčných požiadaviek (verzia 2023)“
4. Tento Dodatok nadobúda platnosť dňom jeho podpísania zmluvnými stranami. Tento Dodatok nadobúda účinnosť deň nasledujúci po dni jeho zverejnenia v Centrálnom registri zmlúv v súlade § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov v spojení s § 47a Občianskeho zákonníka, nie však skôr ako 1.januára 2023.
5. Tento Dodatok je vyhotovený v 4 (slovom: štyroch) vyhotoveniach s platnosťou originálu, z ktorých 2 (slovom: dva) obdrží Objednávateľ a 2 (slovom: dva) obdrží Zhotoviteľ.
6. Zmluvné strany vyhlasujú, že sú spôsobilé na právne úkony, ich vôľa je slobodná a vážna, prejav vôle je dostatočne zrozumiteľný a určitý, zmluvná voľnosť ~~nie je obmedzená a právny úkon je urobený~~ v predpísanej forme. Zmluvné strany si tento dodatok prečítali a bez výhrad súhlasia s jeho ustanoveniami.

Bmc va Slovakia s.r.o.

TO SK R BRATISLAV

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 nlektorých 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 „**Zmiuva**")
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: Bmove Slovakia s.r.o
sídla: Hodžovo námestie 1A 811 06 Bratislava - mestská časť Staré Mesto
IČO: 54 155 029
DIČ: 2121589976
IČ DPH: SK2121589976
údaj o zápise v OR: Okresný súd Bratsilava I, Vložka čislo: 156231/B
údaj o konajúcej osobe: Johann Breiteneder, Schwarzenbergplatz 5 Top 7/1, Viedeň 1030, Rakúska republika
(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 11.XI.2021 (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 či. 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) siedovať 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 vpiyv 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 vpiyv 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/aiebo tejto Zmluvy a/aiebo 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. **<u>Dodávateľ je povinný bezodkladne oznámiť Prevádzkovateľovi každú zmenu v personálnom obsadení pracovných rolí Dodávateľa.</u>**
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 presiahnutla 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 činností 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 povinností 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 Sietí 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 informácií. 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:	Mgr. Martin Slyško
funkcia/pracovná pozícia	projektový manažér
telefónne číslo:	+421 903 509 574
e-mallová adresa:	mpa@bratislava.sk

   Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti:

meno a priezvisko:	Michael Gasparik
funkcia/pracovná pozícia	Head of IT
telefónne číslo:	+43 664 85 97 559
e-mallová adresa:	m.Gasparik@b-i-p.com

4. 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 povinností 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:	Mgr. Martin Slyško
funkcia/pracovná pozícia	projektový manažér
telefónne číslo:	+421 903 509 574
e-mailová adresa:	mpa@bratislava.sk

Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku ochrany osobných údajov:

meno a priezvisko:	Milan Hruška
funkcia/pracovná pozícia	Operations manager
telefónne číslo:	+421 911 499 315
e-mailová adresa:	m.hruska@b-i-p.com

meno a priezvisko:	Valentina Bichler
funkcia/pracovná pozícia	Area manager
telefónne číslo:	+43 664 859 7580
e-mailová adresa:	v.bichler@b-i-p.com

5. 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 povinností 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 ním 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 čl 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 _____

za Prevádzkovateľa

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

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 aplikáciu 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 aplikácie 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 prostredníctvom 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 sietí,
      - 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 povinnosti 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 poiitiky a systému správy hesiei, ktorá umožní 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 technológií 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 technológií verejnej správy a automatické zaznamenávanie prístupu používateľa.
13. Vedenie formaiizovanej 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, odsúhiasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup aiebo 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 aiebo zraniteľností 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 aiebo prechodu k inému Subdodávateľovi.
5. Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vpiyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a impiementované 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 pravideiného 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 zraniteľností 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 technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností 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 funkcionaiita.
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 sietí, 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 impiementuje 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 technológií 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 sietí 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 technológií 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 opatreni najmä bezpečnostne dôležitých prvkov aplikácií, 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 udalostí 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 technológii 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 aiebo 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 aiebo 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 aiebo 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 aiebo 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 impiementuje 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 pián 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 pián, 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
Milan Hruška Valentina Bichler	Operations manager Area manager	Zodpovednosť za realizáciu projektu	+421 911 499 315 +43 664 859 7580	m.hruska@b-i-p.com v.bichler@b-i-p.com
Michael Gasparik	Head of IT	Riadenie informačnej bezpečnosti	+43 664 85 97 559	m.gasparik@b-i-p.com
Milan Hruška Valentina Bichler	Operations manager Area manager	Zodpovedná osoba na úseku ochrany osobných údajov	+421 911 499 315 +43 664 859 7580	m.hruska@b-i-p.com v.bichler@b-i-p.com
Michael Gasparik	Head of IT	Riadenie informačnej bezpečnosti	+43 664 85 97 559	m.gasparik@b-i-p.com

PRÍLOHA 4
Zoznam schválených Subdodávateľov

Obchodné meno	Sídlo	IČO	Rozsah činností v zmysle Základného kontraktu
Infoart d.o.o.	Lastovska 23, HR-10000 Zagreb	VAT number: HR88255578438	Poskytovateľ služieb v oblasti vývoja softvéru a infraštruktúry
Paydo Services d.o.o.	Trg Petra Preradovica 6, HR-10000 Zagreb	VAT number: HR60162542127	Poskytovateľ IT služby / IT servis

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 čl. 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:
_____, 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:

1.	Poskytovateľ, ani jeho štatutárny orgán, ani člen štatutárneho orgánu ani člen dozorného orgánu, ani prokurista nebol právoplatne odsúdený za trestný čin korupcie, trestný čin poškodzovania finančných záujmov Európskych spoločenstiev, trestný čin legalizácie príjmu z trestnej činnosti, trestný čin založenia, zosnovania a podporovania zločineckej skupiny, trestný čin založenia, zosnovania alebo podporovania teroristickej skupiny, trestný čin terorizmu a niektorých foriem účasti na terorizme, trestný čin obchodovania s ľuďmi, trestný čin, ktorého skutková podstata súvisí s podnikaním alebo trestný čin 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 (napr. výpis z OR SR, iný príslušný doklad).
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

[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.

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

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

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

ID	Typ Rq	Popis požiadavky	Spôsob naplnenia požiadavky (vyplní Poskytovateľ)
RQMPA-001	Technické	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.	Do obchodu Apple App Store aj obchodu Google Play bude nahraná aplikácia
RQMPA-002	Technické	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.	Backend integrácia do API ParkSys splni požiadavku.
RQMPA-003	Technické	Aplikácia bude zabezpečená minimálne v zmysle OWASP Top 10.	Áno
RQMPA-004	Technické	Aplikácia bude schopná zabezpečiť počet transakcií v zmysle očakávaných objemov podľa Prílohy č. 7 Zmluvy.	Áno
RQMPA-005	Technické	Systém bude prevádzkovaný 24x7, bude mať Dostupnosť (parameter "D") 99,1% Incidenty A (kritický): RT: 30 minút, FT: 4 hodiny B (závažný): RT: 60 minút, FT: 96 hodín C (nezávažný): RT: 24 hodín, FT: 240 hodín Plánované odstávky po dohode s Objednávateľom sú možné iba v So-Ne vo večerných hodinách . Najdlhší plánovaný výpadok je do max 5 hodín.	Áno
RQMPA-006		Aplikácia a zvyšok komunikácie (emaily, notifikácie) budú minimálne v slovenskom a anglickom jazyku.	Áno
RQMPA-007	Funkčné	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.	Áno
RQMPA-008	Funkčné	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.	Áno
RQMPA-009	Funkčné	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/	Áno
RQMPA-010	Funkčné	Aplikácia bude notifikovať Zákazníka o udalostiach, najmä ohľadom blížiaceho sa ukončenia parkovacieho lístka, napr. formou push notifikácie.	Áno

RQMPA-011 Funkčné	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 - minimálna dĺžka transakcie 30 min., minimálny krok predĺženia 1 min., max krok predĺženia 15 min.	Áno
RQMPA-012 Funkčné	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, maximalnu dobu statia v danom úseku. Čerpanie kreditov z NPK v zmysle aktuálneho prevádzkového poriadku - aktuálne s krokom 1 min.	Áno
RQMPA-013 Funkčné	Účet používateľa poskytuje prehľad o stave účtu: história transakcii, zakúpených aktívnych aj historických produktov, registrované vozidlá.	Áno
RQMPA-014 Funkčné	Podklady pre zóny/oblasti a tarify budú jednoducho importovateľné do systému (zo systému ArcGis).	Áno, bude sa o to strať systém Bmove a tím
RQMPA-015 Funkčné	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.	Áno
RQMPA-016 Funkčné	Aplikácia bude pre HMBA vytvárať zúčtovací report o všetkých parkovacích transakciách vrátane informácií o platbách na mesačnej báze.	Áno
RQMPA-017 Funkčné	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.	Áno, prostredníctvom emialu na lístok Jira
RQMPA-018 Funkčné	Aplikácia bude na platbu využívať svoju platobnú bránu na vlastné náklady a riziko.	Áno
RQMPA-019 Funkčné	Vystavovanie daňového dokladu v mene HMBA. Aplikácia umožní prístup k týmto daňovým dokladom.	Áno
RQMPA-020 Funkčné	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.	Áno

RQMPA-021 Funkčné	Všetky MPA podporujúce systém PAAS musia reagovať na nové zmeny v systéme ParkSys, ktoré súvisia aj s integráciou na Pricing API 2.0. Povinnosťou každého Poskytovateľa bude integrácia na Pricing API 2.0 podľa technickej špecifikácie, ktorú vopred poskytne Objednávateľ. Doba reakcie na predmetné zmeny: a) Pri menšej zmene ako napríklad zmena týkajúca sa pridania/zmeny premennej v endpointoch je lehota implementácie 10 dní. b) Pri funkčnej zmene, ktorá bude zavedená za účelom zvýšenia komfortu používateľa alebo bezpečnosti je lehota implementácie 20 dní.	Áno
RQMPA-022 Funkčné	Pokiaľ Aplikácia zobrazuje zoznam parkovacích kariet prináležiacich k EČV, expirované parkovacie karty je potrebné odstrániť a/alebo poskytnúť Zákazníkovi možnosť aby si ich odstránil v Aplikácii sám.	Áno
RQMPA-023 Funkčné	Poskytovateľ je povinný zobrazovať v Aplikácii aktuálne geo dáta. V priebehu r. 2023 bude potrebné naintegrovať sa na Geoportál (Rest API), odkiaľ sa budú sťahovať aktualizované dáta na základe oznámenia.	Áno
RQMPA-024 Funkčné	Príprava na potenciálnu zmenu zabezpečenia bonusových kariet, v prípade vyskytnutia ich zneužití - v takom prípade na základe pokynu je potrebné zapracovať overovanie bonusovej karty podľa Zákazníckeho emailu v Aplikácii, alebo cez zadanie čísla kreditnej karty (ako to funguje v prípade návštevníckej parkovacej karty). Ak existuje pre dané EČV bonusová karta, vždy ju posielať do endpointu na charging/ticket endpointy (ako nepovinný parameter).	Áno

Príloha č. 1: Technické a funkčné požiadavky

ID	Typ Rq	Popis požiadavky	Priebeh kontroiy	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 naplnenie 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 transakcií 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: 30 minút, FT: 4 hodiny B (závažný): RT: 60 hodina, FT: 96 hodín C (nezávažný): RT: 24 hodín, FT: 240 hodín 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-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.	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 zmluve	**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 piatí 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 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, 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 aplikácií správne info na základe paramterov.	Akceptácia/priebežne	Akceptačné testy	Aplikant popíše naplnenie danej požiadavky pri pristúpení k zmluve	**priebežne na základe incidentov**
RQMPA-016 Funkcne	Aplikácia bude pre HMBA vytvárať zúčtovací report o všetkých parkovacích transakciách vrátane informácií o platbách na mesačnej báze.	Akceptácia/priebežne	Priebežne Príloha č.4 – Výkaz parkovné.xisx	Dodávka priebežne počas prevázky	
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.	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 zmluvy 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 incidentov**
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 - mobiiného 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 hiášok v daných kategóriach	**priebežne na základe incidentov**

RQMPA-021 Funkcne	Všetky MPA podporujúce systém PAAS musia reagovať na nové zmeny v systéme ParkSys, ktoré súvisia aj s integráciou na Pricing API 2.0. Povinnosťou každého Poskytovateľa bude integrácia na Pricing API 2.0 podľa technickej špecifikácie, ktorú vopred poskytne Objednávateľ. Doba reakcie na predmetné zmeny: a) Pri menšej zmene ako napríklad zmena týkajúca sa pridania/zmeny premennej v endpointoch je lehota implementácie 10 dní. b) Pri funkčnej zmene, ktorá bude zavedená za účelom zvýšenia komfortu používateľa alebo bezpečnosti je lehota implementácie 20 dní.	Akceptácia/priebežne	Akceptačné testy	Aplikant/Poskytovateľ popíše naplnenie danej požiadavky pri pristúpení k zmluve/v požadovanej lehote	**pred uzavretím zmluvy** **priebežne na základe incidentov**
RQMPA-022 Funkcne	Pokiaľ Aplikácia zobrazuje zoznam parkovacích kariet prináležiacich k EČV, expirované parkovacie karty je potrebné odstrániť a/aiebo poskytnúť Zákazníkovi možnosť aby si ich odstránil v Aplikácii sám.				
RQMPA-023 Funkcne	Poskytovateľ je povinný zobrazovať v Aplikácii aktuálne geo dáta. V priebehu r. 2023 bude potrebné naintegrovať sa na Geoportál (Rest API), odkiaľ sa budú sťahovať aktualizované dáta na základe oznámenia.	Akceptácia/priebežne	Akceptačné testy	Aplikant/Poskytovateľ popíše naplnenie danej požiadavky pri pristúpení k zmiuve/v požadovanej lehote	**pred uzavretím zmluvy** **priebežne na základe incidentov**
RQMPA-024 Funkcne	Príprava na potenciálnu zmenu zabezpečenia bonusových kariet, v prípade vyskytnutia ich zneužití - v takom prípade na zákiade pokynu je potrebné zapracovať overovanie bonusovej karty podľa Zákazníckeho emailu v Aplikácii, alebo cez zadanie čísla kreditnej karty (ako to funguje v prípade návštevníckej parkovacej karty). Ak existuje pre dané EČV bonusová karta, vždy ju posielať do endpointu na charging/ticket endpointy (ako nepovinný parameter).				

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

#	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. zostaok 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 poskyntutých language files.	Language files (min. SK, EN) použité v aplikácií 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 dvojfoktorovom 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, či 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 premiestnlť 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, či 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 transakcií je po uplynutí času (z max. časového obmedzenia) v daný deň EČV 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 zákazníka	Cieľom je notifikovanie používateľa o blížiacej expirácií a expirácií parkovacieho lístka alebo digitálneho parkovacieho kotúča, príp. 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 (transakcle).	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 histórií 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 histórií 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.
RQMPA-021	Integrácia na Pricing API 2.0	Cieľom je preveriť funkčnosť integrácie na aktualizovanú Pricing API 2.0, a zakomponovanie nových funkcionalít, ktoré prinesie	Testovacie scenáre budú špecifikované v období dokončenia Pricing API 2.0	MPA pre všetky typy používateľov	Korektný výpočet ceny a spoplatneného času, správny chod nových funkcionalít
RQMPA-022	Vymazanie/možnosť vymazania expirovaných parkovacích kariet	Cieľom je preveriť či sa expirované parkovacie karty z aplikácie automaticky odstraňujú, prípadne má užívateľ možnosť odstrániť si ich sám	Používateľ sa naviguje do sekcie "parkovacie karty/oprávnenia", expirované karty nie sú viac zobrazené, prípadne sú expirované karty vyznačené ako už neplatné, a používateľ má k dispozícii ľahko pochopiteľný spôsob na ich odstránenie	MPA s používateľom ParkSys s RPK a/alebo APK a/alebo BPK a/alebo NPK	Expirované karty sú odstránené alebo používateľ ich vie odstrániť sám
RQMPA-023	Integrácia na Geoportál	Cieľom je preveriť funkčnosť integrácie na Geoportál	MPA je schopná sťahovať zmeny v GIS dátach a zakomponovať ich do mapy. Testovacie scenáre budú špecifikované v období dokončenia Geoportálu	MPA pre všetky typy používateľov	MPA sťahuje posledné zmeny v GIS dátach z Geoporálu
RQMPA-024	V prípade potreby na pokyn HMBA, zabezpečiť bonusové karty	Cieľom je preveriť funkčnosť zabezpečenia bonusových kariet	Bonusová karta je overená	MPA s používateľom ParkSys s BPK	Bonusová karta je zabezpečená, len jej držiteľ ju vie použiť

Číslo dožiadania : el-306510/2022/B

VÝPIS Z OBCHODNÉHO REGISTRA
Okresného súdu Bratislava I

Oddiel: **Sro**
Vložka číslo: 156231/B

I. Obchodné meno

Bmove Slovakia s.r.o.

II. Sídlo

Názov ulice (Iného verejného priestranstva) a orientačné číslo (príp. súpisné číslo): Hodžovo námestie 1A
Názov obce: Bratislava - mestská časť Staré Mesto
PSČ: 811 06
Štát: Slovenská republika

III. IČO: 54 155 029

IV. Deň zápisu: 27.10.2021

V. Právna forma: Spoločnosť s ručením obmedzeným

VI. Predmet podnikania (činnosti)

1. počítačové služby
2. služby súvisiace s počítačovým spracovaním údajov
3. kúpa tovaru na účely jeho predaja konečnému spotrebiteľovi (maloobchod) alebo iným prevádzkovateľom živnosti (veľkoobchod)
4. sprostredkovateľská činnosť v oblasti obchodu
5. sprostredkovateľská činnosť v oblasti služieb
6. činnosť podnikateľských, organizačných a ekonomických poradcov
7. reklamné a marketingové služby
8. prieskum trhu a verejnej mienky
9. organizovanie športových, kultúrnych a iných spoločenských podujatí
10. vykonávanie mimoškolskej vzdelávacej činnosti
11. faktoring a forfaiting
12. prenájom nehnuteľností spojený s poskytovaním iných než základných služieb spojených s prenájmom
13. prenájom hnuteľných vecí
14. administratívne služby

15. výskum a vývoj v oblasti prírodných, technických, spoločenských a humanitných vied

VII. Štatutárny orgán: konateľ

Meno a priezvisko: Johann Breiteneder
Bydlisko:
Názov ulice (iného verejného priestranstva) a orientačné číslo (príp. súpisné číslo): Schwarzenbergplatz 5 Top 7/1
Názov obce: Viedeň
PSČ: 1030
Štát: Rakúska republika
Dátum narodenia: 15.11.1975
Iný identifikačný údaj: cestovný doklad U5460069

Vznik funkcie: 27.10.2021

Spôsob konania štatutárneho orgánu v mene spoločnosti s ručením obmedzeným: V prípade, ak má spoločnosť jediného konateľa, koná konateľ v mene spoločnosti samostatne. V prípade, ak má spoločnosť viacero konateľov, konajú konatelia v mene spoločnosti aspoň dvaja spoločne. Konateľ podpisuje za spoločnosť tak, že pripojí k napísanému alebo predtlačenému obchodnému menu spoločnosti vlastnoručný podpis.

VIII. Spoločníci

Obchodné meno/názov:
Best in Parking AG
Sídlo:
Názov ulice (iného verejného priestranstva) a orientačné číslo (príp. súpisné číslo): Schwarzenbergplatz 5/7.1
Názov obce: Viedeň
PSČ: 1030
Štát: Rakúska republika
Iné identifikačné číslo: FN533363 h

Výška vkladu: 5 000,000000 EUR (Peňažný vklad)
Rozsah splatenia: 5 000,000000 EUR

IX. Výška základného imania

5 000,000000 EUR

X. Rozsah splatenia základného imania

5 000,000000 EUR

Výpis zo dňa 05.12.2022

Osvedčovacia doložka

edčujem, že tento listinný dokument vznikol zaručenou konverziou z elektronickej do listinnej podoby podľa § 35 ods. 1 písm. a) zákona 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov a Vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 331/2018 Z. z. o zaručenej konverzii.

Údaje o pôvodných elektronických dokumentoch

Pôvodný dokument v elektronickej podobe

Názov dokumentu: Sro_156231_B.pdf

Formát dokumentu: PDF

Hodnota elektronického odtlačku pôvodného elektronického dokumentu

PqVJHyD0GyAdl5cas7ArnYulvQ6s9WiYasINd2gsK89cK7MGo+Mg9XCpC8WEeWFVloQB+FLgo8gRKqeQufkjyw==

Funkcia použitá pre výpočet elektronického odtlačku: SHA-512

Autorizačné prvky pôvodných dokumentov v elektronickej podobe

- ⊙ Dokument obsahuje prostriedky autorizácie alebo časovú pečiatku
- ○ Dokument neobsahuje prostriedky autorizácie alebo časovú pečiatku

Autorizácia pôvodného elektronického dokumentu

Typ autorizácie: Kvalifikovaná elektronická pečať

Stav autorizácie: platná

Čas autorizácie: 05.12.2022 14:49

Čas overenia autorizácie: 05.12.2022 14:50

Miesto autorizácie: Neuvedené

Ďalšie údaje o autorizácii:

Osoba, ktorá autorizáciu vykonala

Identifikátor: Ministerstvo spravodlivosti SR, ICA - 10432139, NTRSK-00166073

Zastupovaná osoba: Žiadna

Mandát: Žiaden

Časová pečiatka pripojená k prostriedku autorizácie

Typ časovej pečiatky: Kvalifikovaná

Stav časovej pečiatky: platná

Čas vystavenia časovej pečiatky: 05.12.2022 14:49

Vydavateľ časovej pečiatky: Time Stamp Authority 6

Čas overenia časovej pečiatky: 05.12.2022 14:50

SLOVENSKÁ POŠTA, a. s. Partizánska 975 99 Banská Bystrica - 1829 -

Autorizované elektronické dokumenty

Názov dokumentu: Sro_156231_B.pdf

Údaje novovzniknutého dokumentu v listinnej forme

Počet listov: 2

Počet neprázdnych strán: 3

Formát papiera novovzniknutého dokumentu

Formát papiera: Formát papiera A4 (210 × 297 mm)

Počet listov: 2

Údaje o zaručenej konverzii

Evidenčné číslo záznamu o zaručenej konverzii: 7346-221205-5883

Dátum a čas vykonania zaručenej konverzie: 05.12.2022 14:50

Zaručenú konverziu vykonal *

IČO: 36631124

Názov právnickej osoby: Slovenská pošta, a.s.,
Partizánska cesta 9, 975 99 Banská Bystrica,
OR OS BB, oddiel Sa, vl. č. 803/S

Meno: Mária

Priezvisko: Poláková

Funkcia alebo pracovné zaradenie: zamestnanec pošty

*) Ak bola zaručená konverzia vykonaná automatizovaným spôsobom, údaje o mene, priezvisku, funkcii a o pracovnom zaradení sa neuvádzajú.

Podpis a pečiatka

SLOVENSKÁ POŠTA, a.s.
Partizánska cesta 9
975 99 Banská Bystrica
- 1829 -

Adsigo

Certificate

Certificate of PCI Compliance

Adsigo AG confirms that Datatrans AG has been assessed and was found to be compliant according to the

PCI Data Security Standard v3.2.1

Datatrans AG

Kreuzbühlstrasse 26, 8008 Zürich, Switzerland

Scope of validation

Internet Payment Processing

Validation Method

Review by QSA, Report on Compliance issued with compliance date May 28, 2022

This certificate is valid only in combination with the Attestation of Compliance document prepared to finalize the assessment. The certificate bearer has committed itself to use the certificate and the certification logo only during the validity period. Note that this certificate does not constitute an endorsement of any kind by the PCI Security Standards Council or any payment card brand.

May 28, 2022

Dr. Stephan Engelke
Chief Operation Officer

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
QUALIFIED PIN ASSESSOR

PCI Security Standards Council
P2PE ASSESSOR

PCI Security Standards Council
SECURE SOFTWARE ASSESSOR

PCI Security Standards Council
3-D SECURE ASSESSOR

CERTIFIKAT · CERTIFICATE · ZERTIFIKAT

ADRIACERT

When excellence matters

Management system of the Company

Infoart d.o.o.

Lastovska 23, 10000 Zagreb, Croatia

has been audited and found to be in accordance with the requirements of the management system standard

ISO/IEC 27001:2013

for the following scope:

Software development and maintenance

Certification issue date: 11.11.2022.
Validity of the certificate: 24.10.2025.
Certificate number: iSMS-00265/Issue 1

The certification was carried out in accordance with ADRIACERT certification procedures for management system certification and is subjected to regular surveillance audits.

IAS ACCREDITED Management Systems Certification Body MSCB-277

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

Zdenko Mondekar MSc.EE.
CEO

All other clarifications related to the scope of certification and application of the management system can be obtained from the organization that issued the certificate: ADRIACERT d.o.o.,Fallerovo šetalište 22, 10 000 Zagreb, Croatia.

To check the validity of the certificate, please send an inquiry to: certifikacija@adriacert.hr

CERTIFIKAT · CERTIFICATE · ZERTIFIKAT

ADRIACERT

When excellence matters

Management system of the Company

Infoart d.o.o.

Lastovska 23, 10000 Zagreb, Croatia

has been audited and found to be in accordance with the requirements of the management system standard

ISO 9001:2015

for the following scope:

Software development and maintenance

Certification issue date: 08.07.2022.
Validity of the certificate: 07.07.2025.
Certificate number: QMS-00248/Issue 1

The certification was carried out in accordance with ADRIACERT certification procedures for management system certification and is subjected to regular surveillance audits.

17021 · HAA
4605
QMS

Zdenko Mondekar MSc EE
CEO

All other clarifications related to the scope of certification and application of the management system can be obtained from the organization that issued the certificate: ADRIACERT d.o.o., Fallerovo šetalište 22, 10000 Zagreb, Croatia.

To check the validity of the certificate, please send an inquiry to: certifikacija@adriacert.hr