DODATOK Č. 4 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: Mgr. Ctibor Koštál, riaditeľ Magistrátu hlavného mesta SR Bratislavy, v súlade s aktuálne platným a účinným Podpisovým poriadkom Objednávateľa
(ďalej len ako „Objednávateľ" v príslušnom gramatickom tvare)

a

Poskytovateľ

Názov: ParkDots s.r.o.
Sídlo: Pribinova 40, Bratislava 811 09
IČO: 55477232
DIČ: 2122004291
IČ DPH: SK2122004291
IBAN: SK93 1100 0000 0029 4315 1102
Zastúpený: Mgr. Martin Budaj, konateľ
(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 13.9.2021 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. Predmetná Zmluva bola upravená vzájomnou dohodou Zmluvných strán na základe Dodatku č.1 k Zmluve zo dňa 15.03.2022 (č. MAGTS2200139) a Dodatku č.2 k Zmluve zo dňa 23.12.2022 (č.MAGTS2200479), Dodatku č. 3 z 28.08.2023 (č.MAGTS2300239) nakoľko počas vzájomnej spolupráce Zmluvných strán v kontexte legislatívno-technického, ako aj vecného, vystali viaceré otázky vyžadujúce si právnu úpravu zmluvného vzťahu a zároveň bol uplatnený čl. XII Zmluvy - Zmenové konanie. Aj v Novom období, definovanom v súlade so Zmluvou, budú doplnené a upravené nové práva a povinnosti Zmluvných strán, ktoré budú súčasťou novej právnej a vecnej 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 v znení neskorších predpisov (ďalej len „Nová zmluva"), a to s poukazom najmä na prijatie Všeobecne záväzného nariadenia hlavného mesta Slovenskej republiky Bratislava č. 6/2023 o dočasnom parkovaní motorových vozidiel z 25.mája 2023 (ďalej ako „VZN 6/2023"), ďalšie legislatívne úpravy vyžadujúce si precizovanie textácie jednotlivých ustanovení Zmluvy, zvýšenie nárokov na kybernetickú bezpečnosť používateľov mobilných Aplikácií, ako aj vzhľadom na celkový technologický progres vo sfére mobilných aplikácií.

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 tejto Zmluvy.

V súlade s vyššie uvedeným, s cieľom aktualizovať a zosúladiť znenie Zmluvy, jej príloh s novým verejným návrhom 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, v znení jej všetkých dodatkov, a v súlade s VZN 6/2023, Zmluvné strany uzatvárajú tento Dodatok.

Článok I
Predmet dodatku

1. Zmluvné strany sa dohodli, že Preambula Zmluvy sa mení v celom rozsahu a nahrádza ju nové znenie nasledovne:

a) Nové znenie Preambuly:

„ Preambula

Objednávateľ je prevádzkovateľom parkovacích miest na území Objednávateľa. Objednávateľ Všeobecne záväzným nariadením č. 6/2023 o dočasnom parkovaní motorových vozidiel (ďalej ako „VZN 6/2023 a/alebo „VZN") ustanovil úseky miestnych ciest 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 v súlade s VZN 6/2023 umožňuje vykonávanie úhrady za parkovací lístok, okrem iného, aj 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 v oblasti predaja a distribúcie parkovacích oprávnení (parkovacích lístkov) pre svojich obyvateľov, ako aj návštevníkov jeho územia, na najvyššej možnej úrovni podporuje otvorenú súťaž pre všetkých poskytovateľov služieb súvisiacich s predajom a distribúciou parkovacích oprávnení, ktorá má potenciál zabezpečiť a kontinuálne udržať požadovanú kvalitu poskytovaných služieb. Poskytovateľ má záujem poskytnúť mobilnú aplikáciu na úhradu parkovacích lístkov, umožniť jej bezplatné stiahnutie a užívanie každej osobe, ktorá o to prejaví záujem. Poskytovateľ poskytuje predmetnú službu za odplatu.

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 a splní všetky technické, administratívne, bezpečnostné a Zmluvou a jej prílohami inak definované kritériá a požiadavky. Objednávateľ sprostredkuje obyvateľom a návštevníkom územia Objednávateľa v rovnakej miere informácie o každom Poskytovateľovi mobilnej aplikácie, ktorý uzatvoril túto Zmluvu na webovej stránke „Bratislavský parkovací asistent" – www.paas.sk, a odkazom na túto webovú stránku, umiestneným na vyhradených miestach, najmä na informačných tabuliach jednotlivých parkovacích zón definovaných VZN. Poskytovateľ berie na vedomie, že Objednávateľ má záujem poskytnúť i vlastnú mestskú mobilnú aplikáciu na úhradu parkovacích lístkov, ktorú vytvorí a sprístupní obyvateľom a návštevníkom svojho územia, a to najneskôr do konca 2. kvartálu r. 2024, a ktorú bude prezentovať v rovnakej miere ako mobilnú aplikáciu Poskytovateľa na vyššie uvedenej webovom stránke. Poskytovateľ zároveň berie na vedomie, že Objednávateľ je oprávnený prezentovať vlastnú mobilnú aplikáciu na úhradu parkovacích lístkov aj na vlastných komunikačných a prezentačných kanáloch (ako napr. webová stránka, sociálne siete) Objednávateľa.

Prijatím verejného návrhu na uzavretie zmluvy každý Poskytovateľ potvrdí, že spĺňa všetky podmienky definované Zmluvou a jej prílohami, ako aj 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. 1 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 ciest určené na dočasné parkovanie motorových vozidiel určené všeobecne záväzným nariadením Objednávateľa pričom ku dňu uzavretia tejto Zmluvy ide o VZN, 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 alebo v Prevádzkovom poriadku;
„**Prevádzkový poriadok**" znamená prevádzkový poriadok Objednávateľa, zverejnený na webovom sídle Objednávateľa a/alebo na webovej stránke „Bratislavský parkovací asistent" – www.paas.sk, ktorý upravuje niektoré podmienky prevádzky Aplikácie a môže obsahovať zoznam Parkovacích miest neuvedených vo VZN a upraviť výšku Parkovného za Parkovacie miesta neuvedené vo VZN; Prevádzkový poriadok môže Objednávateľ jednostranne meniť; v prípade rozporu medzi Prevádzkovým poriadkom a touto Zmluvou vrátane jej príloh má prednosť táto Zmluva;

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. 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) Za pôvodné znenie čl. 7.4.4 Zmluvy sa vkladajú nové body 7.4.5 a 7.4.6 v nasledovnom znení:

„7.4.5 zabezpečí aby boli v Aplikácii prístupné a prostredníctvom Aplikácie pred realizáciou úhrady Parkovného Zákazníkom preukázateľne poskytnuté všetky právne relevantné informácie o právnom základe poskytovania služieb Poskytovateľom, a to tak aby bolo zrejmé, že Parkovné je uhrádzané v mene a na účet Objednávateľa;

7.4.6 zabezpečí aby boli v Aplikácii prístupné a pred realizáciou úhrady Parkovného Zákazníkom poskytnuté všetky potrebné informácie v oblasti spracúvania osobných údajov vrátane postavenia Objednávateľa a Poskytovateľa pri spracúvaní osobných údajov;"

b) Pôvodné označenie čl. 7.4.5 a čl. 7.4.6 sa mení na označenie čl. 7.4.7 a čl. 7.4.8.

5. Zmluvné strany sa dohodli, že čl. 10 Dôverné informácie a ochrana osobných údajov sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 10.6 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným znením:

„10.6 Zmluvné strany ako aj ich zástupcovia berú na vedomie, že zo strany Poskytovateľa bude pri výkone činností podľa tejto Zmluvy dochádzať k spracúvaniu osobných údajov osôb v postavení dotknutých osôb v zmysle 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 ochrany osobných údajov) v platnom znení (ďalej len ako „Nariadenie GDPR") a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení (ďalej len ako „Zákon o ochrane osobných údajov"). Poskytovateľ spracúva osobné údaje dotknutých osôb v mene Objednávateľa ako prevádzkovateľa osobných údajov, a teda má postavenie sprostredkovateľa. Konkrétne podmienky spracúvania osobných údajov a všetky relevantné skutočnosti Zmluvné strany definujú v osobitnej zmluve o spracúvaní osobných údajov, ktorú sú povinné na tento účel uzatvoriť a zaväzujú sa k jej uzatvoreniu pristúpiť spoločne s touto Zmluvou. Poskytovateľ sa zaväzuje pri plnení tejto Zmluvy plniť všetky povinnosti, ktoré mu vyplývajú z Právneho poriadku vo vzťahu k ochrane osobných údajov. Pri spracúvaní osobných údajov Zákazníkov zabezpečí Poskytovateľ splnenie všetkých povinností sprostredkovateľa voči dotknutým osobám podľa Právneho poriadku vo vzťahu k ochrane osobných údaj."

b) Pôvodné znenie čl. 10.9 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným znením:

„10.9 Pravidlá a podmienky spracúvania osobných údajov Poskytovateľom sú predmetom samostatnej zmluvy uzatvorenej medzi Objednávateľom a Poskytovateľom, ktorá tvorí Prílohu č. 10 k tejto Zmluve."

6. Zmluvné strany sa dohodli, že Čl. 11 Doručovanie sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 11.6 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

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

7. Zmluvné strany sa dohodli, že Čl. 12 Zmenové konanie sa mení a dopĺňa nasledovne:

a) Pôvodné znenie čl. 12.2 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„12.2 Objednávateľ je oprávnený, najneskôr v lehote do 30 (tridsať) kalendárnych dní pred uplynutím doby trvania tejto Zmluvy, vypracovať a doručiť Poskytovateľovi návrh dodatku k tejto Zmluve, ktorým sa úprava vzájomných práv a povinností podľa tejto Zmluvy zosúladí s úpravou verejného návrhu na uzavretie zmluvy na Nové obdobie podľa bodu 12.1 tejto Zmluvy. Pre vylúčenie pochybností platí, že doručenie návrh dodatku k tejto Zmluve podľa tohto článku Zmluvy je možné zachovať aj elektronickou formou."

b) Pôvodné znenie čl. 12.3 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným novým znením:

„12.3 V prípade, ak Poskytovateľ návrh dodatku neprijme do 10 (desiatich) kalendárnych dní po doručení návrhu dodatku od Objednávateľa, Zmluva zanikne uplynutím doby jej trvania podľa bodu 14.1 tejto Zmluvy. Poskytovateľ je oprávnený záujem prijatia alebo neprijatia návrhu dodatku oznámiť pred

uplynutím lehoty uvedenej v prvej vete elektronickou formou s cieľom zvýšiť efektivitu komunikácie medzi Zmluvnými stranami."

8. 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 uzatvára na dobu určitú do 31.12.2024."

9. Zmluvné strany sa dohodli, že Čl. 15 Záverečné ustanovenia sa mení a dopĺňa nasledovne:

   a) Pôvodné znenie čl. 15.1 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným 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, nie však skôr ako 1.1.2024."

   b) Pôvodné znenie čl. 15.2 Zmluvy sa v celom rozsahu mení a nahrádza nasledovným znením:

   „15.2 Táto Zmluva je vyhotovená v 3 (troch) rovnopisoch, z ktorých má každý právnu silu originálu, z ktorých Objednávateľ obdrží po 2 (dvoch) rovnopisoch, a Poskytovateľ 1 (jeden) rovnopis."

10. Zmluvné strany sa dohodli, že Príloha č. 1, Príloha č. 6 , Príloha č. 7, Príloha č. 8, Príloha č. 9 sa dopĺňa a mení v celom rozsahu. K Zmluve sa dopĺňa nová Príloha č. 10: Zmluva o spracúvaní osobných údajov. Samotná textácia jednotlivých príloh podľa nižšie uvedeného je súčasťou tohto Dodatku:

Príloha č. 1:	Technické a funkčné požiadavky (verzia 2024)
Príloha č. 6:	ParkSysAPI (2024)
Príloha č. 7:	Model odmeňovania (2024)
Príloha č. 8:	Zmluva o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností (verzia 2024)
Príloha č. 9:	Vyhlásenie k splneniu Technických a funkčných požiadaviek(verzia 2024)
Príloha č. 10:	Zmluva o spracúvaní osobných údajov

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 2024)
Príloha č. 6:	ParkSysAPI (2024)
Príloha č. 7:	Model odmeňovania (2024)
Príloha č. 8:	Zmluva o zabezpečení plnenia bezpečnostných opatrení, notifikačných povinností (verzia 2024)
Príloha č. 9:	Vyhlásenie k splneniu Technických a funkčných požiadaviek (verzia 2024)
Príloha č. 10:	Zmluva o spracúvaní osobných údajov

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 2024.
5. Tento Dodatok je vyhotovený v 3 (slovom: troch) vyhotoveniach s platnosťou originálu, z ktorých 2 (slovom: dva) obdrží Objednávateľ a 1 (slovom: jeden) obdrží Poskytovateľ.

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.

12. 12. 2023

V Bratislave, dňa: 8.12.2023
Poskytovateľ:

Mgr. Ctibor Koštál,
riaditeľ Magistrátu hlavného mesta SR Bratislava

Mgr. Martin Budaj
konateľ

ZMLUVA O ZABEZPEČENÍ PLNENIA BEZPEČNOSTNÝCH OPATRENÍ A NOTIFIKAČNÝCH POVINNOSTÍ

uzatvorená v zmysle § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, (ďalej len ako „**Zmluva**")
medzi týmito zmluvnými stranami:

Prevádzkovateľ:

Názov:	**Hlavné mesto Slovenskej republiky Bratislava**
Sídlo:	Primaciálne námestie č. 1, 814 99 Bratislava, Slovenská republika
IČO:	00 603 481
DIČ:	2020372596
IČ DPH:	SK2020372596
Štatutárny orgán:	Ing. arch. Matúš Vallo, primátor
Zastúpený:	Mgr. Ctibor Koštál, riaditeľ magistrátu v súlade s aktuálne platným a účinným Podpisovým poriadkom Prevádzkovateľa

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

a

Dodávateľ:

Obchodné meno:	**ParkDots, s.r.o.**
Sídlo:	Pribinova 40, 81109 Bratislava
IČO:	55 477 232
Údaj o konajúcej osobe:	Mgr. Martin Budaj, konateľ

(ďalej len ako „**Dodávateľ**" v príslušnom gramatickom tvare)
(Prevádzkovateľ a Poskytovateľ ďalej spolu len ako „**Zmluvné strany**" alebo jednotlivo ako „**Zmluvná strana**" v príslušnom gramatickom 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. l) 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 aktuálne platnej a účinnej Zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania, uzatvorenej s Prevádzkovateľom v zmysle Verejného návrhu na uzatvorenie zmluvy o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania zverejneného na webovom sídle Prevádzkovateľa pre Nové obdobie (ďalej len „**Základný kontrakt**").

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.

Ak nie je uvedené inak, pojmy používané v tejto Zmluve majú význam im priradený v Zákone o kybernetickej bezpečnosti, jeho vykonávacích predpisoch.

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. 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 (ďalej len „**Ciele**").
3. Súčasťou záväzkov Dodávateľa podľa tejto Zmluvy je povinnosť Dodávateľa prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti 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.
4. 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.
5. Na základe tejto Zmluvy sa tiež Dodávateľ zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve tak, aby boli naplnené jej Ciele.
6. 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.
7. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto Zmluvy po celú dobu trvania Základného kontraktu.

Článok II.
Prevencia kybernetických bezpečnostných incidentov

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

posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov;

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

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

Článok III.
Reaktivita pri hlásení Incidentov

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

Článok IV.
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. 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 V.
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, zároveň určuje dané osobu ako kontaktné body pre technickú podporu, riadenie informačnej bezpečnosti a vedenie projektu:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	Email
Mgr. Martin Slyško	Projektový manažér	Zodpovednosť za realizáciu projektu	+421 903 509 574	martin.slysko@gmail.com
Mgr. Matej Evin	Manažér kybernetickej bezpečnosti	Riadenie informačnej bezpečnosti	+421 903 508 405	matej.evin@bratisiava.sk
Mgr. Matej Evin	Manažér kybernetickej bezpečnosti	Zodpovedná osoba na úseku ochrany osobných údajov	+421 903 508 405	matej.evin@bratislava.sk
Ing. Martin Hrčka	Referent prevádzky parkovacej politiky	Technická podpora	+421 902 972 368	martin.hrcka@bratislava.sk

4. Dodávateľ určí kontaktnú osobu pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti a/alebo iné osoby pre účely naplnenia predmetu Zmluvy v rámci Prílohy č. 3 tejto Zmluvy.
5. Zmenu kontaktných osôb na úseku kybernetickej bezpečnosti môže každá Zmluvná strana zrealizovať tak, že oznámi novú kontaktnú osobu druhej Zmluvnej strane v písomnej forme.

Článok VI.
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,

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 VII.
Spoločné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto Zmluvy v súlade so Zákonom o kybernetickej bezpečnosti, a inými zákonnými úpravami, vykonávacími predpismi (najmä Vyhláškou č.362 Národného bezpečnostného úradu z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení), 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 VIII.
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, vzniká Prevádzkovateľovi nárok na náhradu takejto ujmy voči Dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie.

Článok IX.
Rozsah, spôsob a možnosti vykonávania kontrolných činností a auditu kybernetickej bezpečnosti 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, 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 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 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 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 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 X.
Záverečné ustanovenia

1. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi udelí, poskytne, prevedie alebo na Prevádzkovateľa postúpi všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu s Prevádzkovateľom založeného touto Zmluvou po dobu dohodnutú v trvaní päť rokov po ukončení zmluvného vzťahu.
2. Dodávateľ sa zaväzuje, že po ukončení zmluvného vzťahu s Prevádzkovateľom na základe tejto Zmluvy Prevádzkovateľovi vráti, prevedie a podľa pokynov Prevádzkovateľa prípadne aj zničí všetky informácie a osobné údaje vrátane ich kópií, ku ktorým mal Dodávateľ počas trvania zmluvného vzťahu prístup.
3. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto Zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na plnenie predmetu tejto Zmluvy.
4. Dodávateľ bez predchádzajúceho písomného súhlasu Prevádzkovateľa nemá právo previesť práva a povinnosti vyplývajúce z tejto Zmluvy na tretiu osobu.
5. Táto Zmluva predstavuje úplnú dohodu Zmluvných strán týkajúcu sa predmetu tejto Zmluvy a nahrádza v celom rozsahu akékoľvek predchádzajúce dohody či návrhy uvádzané v korešpondencii či na rokovaniach, či už ústne alebo písomné, ku ktorým došlo pred uzatvorením tejto Zmluvy a ktoré jej uzatvorením zanikajú.
6. Táto Zmluva sa riadi právom Slovenskej republiky. Právne vzťahy neupravené touto Zmluvou sa spravujú príslušnými ustanoveniami Obchodného zákonníka a ostatnými všeobecne záväznými právnymi predpismi. Na riešenie sporov z tejto zmluvy sú príslušné všeobecné súdy Slovenskej republiky.
7. Zmluva je vyhotovená v troch vyhotoveniach, ktoré majú povahu originálu, jedno vyhotovenie obdrží Dodávateľ, dve vyhotovenia obdrží Prevádzkovateľ.
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 platnosti a účinnosti Základného kontraktu.
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 Bratislave, dňa 19. 12. 2023

za Prevádzkovateľa:

Mgr. Ctibor Kostal,
riaditeľ Magistrátu
hlavného mesta SR Bratislava

V Bratislave dňa 8.12.2023

za Dodávateľa:

Mgr. Martin Budaj
konateľ

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 Dodávateľa základnej služby v zmysle Základného kontraktu
Príloha č. 4 - Zoznam schválených Subdodávateľov

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

D. Riadenie prístupov

1. Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy.
2. Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy.
3. Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok.

4. Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.
5. Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.
6. Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.
7. Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.
8. Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá 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 formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy.
14. Implementácia centrálnej správy identít (IDM).
15. Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.
16. Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov.
17. Implementácia, vynucovanie prístupových rolí v informačných technológiách verejnej správy.
18. Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov.

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

1. V zmluve so Subdodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií verejnej správy.
3. Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú najmenej záväzok:
   a) plnenia určených požiadaviek a kritérií pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti pri dodávke predmetu zmluvy,
   b) ochrany informácií, ku ktorým je poskytnutý prístup,
   c) oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti a ďalších opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti špecifických na plnenie predmetu Základného kontraktu a tejto Zmluvy,
   d) riadenia a monitorovania prístupov do informačných technológií verejnej správy vrátane spôsobu a mechanizmu,
   e) možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
   f) oznámenia všetkých bezpečnostných rizík, nedostatkov alebo 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 alebo prechodu k inému Subdodávateľovi.

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

F. Bezpečnosť pri prevádzke informačných systémov a sietí

1. Na účinnú prevenciu pred stratou dát u Dodávateľa sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru.
2. Dodávateľ vypracuje a dodržiava politiku zálohovania, ktorá definuje požiadavky Prevádzkovateľa na zálohovanie vrátane doby uchovávania, testovania záloh, ako aj opatrenia na ochranu záložných médií.
3. Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.
4. Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.
5. Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.
6. Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.
7. Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.
8. Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú.
9. Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.

10. Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.
11. Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.
12. V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.
13. Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:
    a) operačné systémy,
    b) virtualizačné prostredia,
    c) aplikačný softvér,
    d) pracovné stanice,
    e) sieťové zariadenia, vrátane bezpečnostných zariadení,
    f) databázové prostredia.
14. Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.
15. Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

G. Hodnotenie zraniteľností a bezpečnostné aktualizácie

Nastavenie automatickej aktualizácie operačného systému a aplikácií.

1. Dodávateľ zavedie pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.
2. Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.
3. Vykonávanie hodnotenie 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 funkcionalita.

12. Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.
13. Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.

H. Ochrana proti škodlivému kódu

1. Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.
2. V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.
3. Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na
   a) používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
   b) škodlivé emailové prílohy a odkazy,
   c) podozrivé a škodlivé webové stránky a odkazy,
   d) externú a internú sieťovú komunikáciu u Dodávateľa vrátane webových sídiel,
   e) prenos súborov z externých sietí.
4. Vytvorenie procesu alebo postupu na prenos súborov z externých 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 implementuje technológiu detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.
18. Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.
19. Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.

J. Akvizícia, vývoj a údržba informačných technológií verejnej správy

1. Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
2. Pri vytváraní nových alebo úprave existujúcich informačných 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 opatrení 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 technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované.
3. Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:
   a) úspešné a neúspešné autorizačné udalosti,
   b) úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
   c) úspešné a neúspešné prístupy k log súborom,
   d) úspešné a neúspešné prístupy k systémovým zdrojom,
   e) vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
   f) zmeny v prístupových oprávneniach,
   g) aktivácia a deaktivácia bezpečnostných mechanizmov,
   h) spustenie a zastavenie procesov,
   i) konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
   j) spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
   k) významné aktivity v sieťovej komunikácii,
   l) požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
   m) IP adresy pridelené prostredníctvom služby DHCP.
4. Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:
   a) čas a dátum udalosti,
   b) identifikácia používateľa,
   c) identifikácia zariadenia,
   d) informácia týkajúca sa udalosti,
   e) indikácia úspešnosti, alebo zlyhania operácie,
   f) pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port.
5. Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.
6. Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.
7. Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.
8. Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja.
9. Dodávateľ vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy.
10. Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
11. Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.
12. Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.
13. Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.
14. Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.
15. Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

L. Fyzická bezpečnosť a bezpečnosť prostredia

1. Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

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

M. Riešenie kybernetických bezpečnostných incidentov

1. Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe.
2. Dodávateľ má na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov.
3. Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.
4. S interným riadiacim aktom, najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy.
5. Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto.
6. Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.
7. Proces odborného posúdenia a analýzy oznámení realizuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT.
8. Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.

9. Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy.
10. Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov.
11. Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní.
12. Dodávateľ má vytvorené plány na riešenie kybernetických bezpečnostných incidentov.

N. Kryptografické opatrenia

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

1. Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
2. Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä
   a) elektronických dokumentov,
   b) dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
   c) emailovej komunikácie prostredníctvom PGP alebo S/MIME,
   d) komunikačných kanálov na výmenu nešifrovaných dát,
   e) centrálnych úložísk,
   f) záloh.
3. Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä
   a) princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
   b) definovanie požadovanej úrovne ochrany a štandardy šifrovania,
   c) roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
   d) riadenie šifrovacích kľúčov.
4. Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.
5. Dodávateľ pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.

O. Kontinuita prevádzky informačných technológií verejnej správy

1. Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.
2. Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.
3. Plán kontinuity prevádzky obsahuje najmä:
   a) roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
   b) možné vplyvy na prevádzku informačných technológií verejnej správy,
   c) časový rámec obnovy,
   d) identifikáciu zdrojov potrebných na obnovu prevádzky,
   e) identifikáciu zamestnancov potrebných na obnovu prevádzky,
   f) identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
   g) identifikáciu priestorov potrebných na obnovu prevádzky,
   h) stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),

i) identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
j) spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
k) konkrétne havarijné procedúry slúžiace na obnovu prevádzky.

4. Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.

P. Audit a kontrolné činnosti

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

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

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou základnej služby	Telefónny kontakt	Email
Zdeno Kupec	Produkt. manažér	Zodpovednosť za realizáciu projektu	02/ 49 239 048	support@parkdots.com
Juraj Novotný	Security manažér	Kontaktná osoba pre komunikáciu s Prevádzkovateľom na úseku kybernetickej bezpečnosti	02/ 49 239 048	support@parkdots.com
Juraj Novotný	Security manažér	Riadenie informačnej bezpečnosti	02/ 49 239 048	support@parkdots.com
Viktor Róža	Manažér prevádzky	Technická podpora	02/ 49 239 048	support@parkdots.com

PRÍLOHA 4
Zoznam schválených Subdodávateľov

Obchodné meno	Sídlo	IČO	Rozsah činností v zmysle Základného kontraktu

ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

uzatvorená podľa ustanovenia § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v aktuálnom znení čl. 28 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 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 údajov) (ďalej len **„Nariadenie GDPR"**) a § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len **„Zákon o ochrane osobných údajov"**)

(ďalej len „Zmluva")

medzi

(1) **Názov:** **Hlavné mesto Slovenskej republiky Bratislava**
Sídlo: Primaciálne námestie 1, 814 99 Bratislava
IČO: 00 603 481
DIČ: 2020372596
IČ DPH: SK2020372596
zastúpené: JUDr. Rastislav Šorl, riaditeľ sekcie právnych služieb, v súlade s aktuálne platným a účinným Podpisovým poriadkom Prevádzkovateľa
(ďalej len „**HMB**" alebo „**Prevádzkovateľ**")

a

(2) **Obchodné meno:** **ParkDots s.r.o.**
Sídlo: Pribinova 40, Bratislava 811 09
IČO: 55477232
Údaj o konajúcej osobe: Mgr. Martin Budaj, konateľ
(ďalej len „**Sprostredkovateľ**")
(HMB a Sprostredkovateľ ďalej spoločne aj ako **„Zmluvné strany"** alebo jednotlivo **„Zmluvná strana**")

Preambula

1. Zmluvné strany uzatvorili Zmluvu o zabezpečení služby platobného systému prostredníctvom mobilnej aplikácie pre úhradu dočasného parkovania (ďalej len **„Základný kontrakt"**), predmetom ktorej je záväzok Sprostredkovateľa vytvoriť mobilnú aplikáciu na zabezpečenie bezproblémovej, časovo a administratívnej efektívnej úhrady parkovného zákazníkmi Prevádzkovateľa a kontroly úhrady parkovného na základe integrácie aplikácie do systému ParkSys.
2. V súvislosti s plnením v zmysle Základného kontraktu dochádza k spracúvaniu osobných údajov zo strany Sprostredkovateľa a preto sa Zmluvné strany v súlade s Nariadením GDPR a Zákonom o ochrane osobných údajov dohodli na uzatvorení tejto osobitnej Zmluvy, v ktorej upravia vzájomné práva a povinnosti týkajúce sa ochrany a spracúvania osobných údajov.
3. HMB je v pozícii "prevádzkovateľa" v zmysle čl. 4 ods. 7 Nariadenia GDPR pokiaľ ide o akýkoľvek druh informácií bližšie uvedených v tejto Zmluve, týkajúcich sa identifikovaných alebo identifikovateľných osôb definovaných v čl. 4 ods. 1 Nariadenia GDPR (ďalej aj len "**osobné údaje**") a voči nemu je zaviazaný Sprostredkovateľ v zmysle čl. 4 ods. 8 Nariadenia GDPR počas plnenia tejto Zmluvy, ktorý spracúva osobné údaje dotknutých osôb v mene HMB ako Prevádzkovateľa.
4. Po ukončení spracúvania údajov zo strany Sprostredkovateľa pre HMB, nezanikajú povinnosti Sprostredkovateľa na zabezpečenie ochrany osobných údajov, povinnosť mlčanlivosti, ani povinnosti vzťahujúce sa na ukončenie spracúvania údajov zo strany Sprostredkovateľa, ako aj nároky HMB z dôvodu porušenia týchto povinností.

Článok I.
Predmet Zmluvy

1. Na základe tejto Zmluvy a za podmienok v nej uvedených HMB ako Prevádzkovateľ v súlade s článkom 28 Nariadenia GDPR poveruje Sprostredkovateľa spracúvaním osobných údajov, s ktorými príde do styku v súvislosti s realizáciou Základného kontraktu v mene HMB. Predmetom tejto Zmluvy je taktiež určenie vzájomných práv a povinností pri spracúvaní osobných údajov v súlade s Nariadením GDPR a Zákonom o ochrane osobných údajov a úprava ďalších vzájomných práv a povinností Zmluvných strán.

2. Prevádzkovateľ touto Zmluvou poveruje Sprostredkovateľa spracúvaním osobných údajov dotknutých osôb v mene Prevádzkovateľa za podmienok stanovených v tejto Zmluve.
3. Prevádzkovateľ vyhlasuje, že pri výbere Sprostredkovateľa postupoval v súlade s Nariadením GDPR a Zákonom o ochrane osobných údajov a poveruje Sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných bezpečnostných opatrení tak, aby sa zabezpečila ochrana práv dotknutej osoby.
4. Sprostredkovateľ poverenie podľa bodu 2. tohto Článku Zmluvy prijíma a zaväzuje sa vykonávať spracúvanie osobných údajov dotknutých osôb v mene Prevádzkovateľa v rozsahu a spôsobom podľa Základného kontraktu a v zmysle tejto Zmluvy a v zmysle pokynov Prevádzkovateľa tak, aby spracúvanie osobných údajov spĺňalo požiadavky Nariadenia GDPR a aby bola zabezpečená ochrana práv dotknutých osôb.

Článok II.
Predmet a podmienky spracúvania osobných údajov

1. Predmetom spracúvania na základe tejto Zmluvy sú osobné údaje dotknutých osôb, ktorými sú: zákazníci Prevádzkovateľa (ďalej len „**Dotknuté osoby**").
2. **Účelom** spracúvania osobných údajov Dotknutých osôb je zabezpečenie bezproblémovej, časovo a administratívne efektívnej úhrady parkovného zákazníkmi Prevádzkovateľa prostredníctvom Dodávateľom vytvorenej a prevádzkovanej aplikácie a kontrola týchto úhrad integráciou aplikácie do systému ParkSys.
3. Sprostredkovateľ je oprávnený vykonávať **nasledovné spracovateľské operácie s osobnými údajmi** Dotknutých osôb automatizovanými a/alebo neautomatizovanými prostriedkami: získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, opakované spracúvanie, zmenu, vyhľadávanie, prehliadanie, preskupovanie, využívanie, uchovávanie, blokovanie, vymazanie, poskytovanie, sprístupňovanie, publikovanie a akékoľvek iné činnosti, ktoré sú nevyhnutné na splnenie účelu spracúvania osobných údajov len za podmienok uvedených v Základom kontrakte a v tejto Zmluve.
4. Osobné údaje Dotknutých osôb budú Sprostredkovateľovi poskytované prostredníctvom aplikácie na úhradu parkovného, v ktorej Dotknuté osoby vyplnia príslušné osobné údaje.
5. Na účely podľa tejto Zmluvy budú spracúvané osobné údaje Dotknutých osôb, pričom pôjde **najmä o nasledovné typy alebo kategórie osobných údajov**:
   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)
6. **Doba spracúvania:** Sprostredkovateľ je oprávnený spracúvať osobné údaje Dotknutých osôb po dobu trvania Základného kontraktu alebo tejto Zmluvy, nie však dlhšie ako po dobu, po ktorú je v každom jednotlivom prípade Dotknutej osoby oprávnený spracúvať osobné údaje Prevádzkovateľ.
7. Sprostredkovateľ spracúva osobné údaje Dotknutých osôb podľa pokynov Prevádzkovateľa iba vtedy, ak:
   a) platnosť a/alebo účinnosť Základného kontraktu nebola ukončená a spracovanie je nevyhnutné pre dokončenie poskytovania služieb v zmysle Základného kontraktu,
   b) táto Zmluva nebola ukončená alebo
   c) oprávnenie na spracovanie osobných údajov podľa tejto Zmluvy alebo jej časti nebolo Prevádzkovateľom odobraté.

8. Sprostredkovateľ spracúva osobné údaje Žiadateľov vždy len v rozsahu potrebnom na vykonávanie činností podľa tejto Zmluvy a Základného kontraktu a musí dodržať princíp minimalizácie údajov podľa čl. 5 ods. 1 písm. c) Nariadenia GDPR. Sprostredkovateľ zabezpečí najmä to, aby sa osobné údaje Žiadateľov ako dotknutých osôb a vlastné údaje Sprostredkovateľa alebo údaje klientov Sprostredkovateľa spracúvali samostatne a oddelene.
9. Sprostredkovateľ je povinný preukázateľne zdokladovať spracovanie osobných údajov podľa ustanovení Nariadenia GDPR a Zákona o ochrane osobných údajov. Sprostredkovateľ najmä vedie záznamy o spracovateľských činnostiach podľa požiadaviek čl. 30 ods. 2 Nariadenia GDPR. Spracovanie osobných údajov bude monitorovať osoba, ktorá bola poverená takýmto monitorovaním u Sprostredkovateľa.
10. Sprostredkovateľ potvrdzuje a vyhlasuje, že prijal technické a organizačné opatrenia umožňujúce Prevádzkovateľovi zabezpečiť práva Dotknutých osôb, najmä právo na informácie (čl. 13 a 14 Nariadenia GDPR), právo prístupu (čl. 15 Nariadenia GDPR), právo na opravu a vymazanie (čl. 16 a 17 Nariadenia GDPR), právo na obmedzenie spracovania (čl. 18 Nariadenia GDPR) a právo prenosu údajov (čl. 20 Nariadenia GDPR)

v rámci legislatívnych lehôt. Sprostredkovateľ poskytne na požiadanie Prevádzkovateľovi informácie potrebné na tento účel.

11. Sprostredkovateľ vyhlasuje, že zaviedol primerané preventívne opatrenia, najmä podľa ustanovení čl. 32 Nariadenia GDPR, a to za účelom zamedziť akúkoľvek neoprávnenú dispozíciu s osobnými údajmi, vrátane neoprávnenému sprístupneniu tretím osobám a dispozíciu spôsobom, ktorý by bol iným spôsobom v rozpore s Nariadením GDPR. Ďalej Sprostredkovateľ potvrdzuje, že disponuje primeranými zárukami, že príslušné technické a organizačné opatrenia boli vykonané podľa tejto Zmluvy tak, aby bolo spracovanie v súlade s požiadavkami Nariadenia GDPR a ochrana práv Dotknutých osôb bola zabezpečená.

Článok III.
Zodpovednosť a zadávanie pokynov

1. Prevádzkovateľ zapojil Sprostredkovateľa do spracúvania osobných údajov za účelom vykonávania činností špecifikovaných v Základnom kontrakte a súvisiacich s vykonávaním činností v jej zmysle.
2. Zmluvné strany sa dohodli, že znenie Základného kontraktu a tejto Zmluvy sa považujú za zdokumentované pokyny Prevádzkovateľa voči Sprostredkovateľovi vo vzťahu k spracúvaniu osobných údajov. Prevádzkovateľ môže zadať Sprostredkovateľovi aj ďalšie pokyny o povahe, rozsahu a spôsobe spracúvania osobných údajov, ako aj o bezpečnostných opatreniach, ktoré je Sprostredkovateľ povinný podniknúť. Rozsah činností podliehajúcich pokynom je uvedený v Základnom kontrakte. Pokyny Prevádzkovateľa sú určené výlučne na dosiahnutie ochrany osobných údajov v súlade s Nariadením GDPR, Zákonom o ochrane osobných údajov a ostatnými všeobecne záväznými právnymi predpismi, pričom pokynom Prevádzkovateľa nemôže dochádzať k zmene predmetu Základného kontraktu. Sprostredkovateľ je oprávnený vykonať spracúvanie osobných údajov výlučne v rozsahu podľa pokynov Prevádzkovateľa.
3. Prístup k údajom a oprávnenie spracúvať osobné údaje sú obmedzené len na rozsah vyžadovaný na riadne plnenie jednotlivých povinností Sprostredkovateľa vyplývajúcich zo Základného kontraktu. Ak zo Základného kontraktu nevyplýva inak, je zakázané vytvárať kópie alebo duplikáty údajov bez vedomia a súhlasu Prevádzkovateľa.
4. Pokyny Prevádzkovateľa týkajúce sa spracúvania osobných údajov musia byť udelené v písomnej forme, pričom na tento účel sa za písomnú formu považuje aj elektronická komunikácia v podobe e-mailovej správy. Vo výnimočných prípadoch, ktoré neznesú odklad, môže Prevádzkovateľ zadávať pokyny aj ústne.
5. Ak podľa názoru Sprostredkovateľa Prevádzkovateľov pokyn porušuje ustanovenia právnych predpisov týkajúcich sa ochrany osobných údajov, Sprostredkovateľ je povinný o tejto skutočnosti bezodkladne, najneskôr do dvadsať štyri (24) hodín, od okamihu, keď sa o tejto skutočnosti dozvedel, písomne informovať Prevádzkovateľa. Povinnosť splniť pokyn tým nie je dotknutá. Zodpovednosť za porušenie právnych predpisov o ochrane údajov, ku ktorému došlo plnením pokynu Prevádzkovateľa, na splnení ktorého Prevádzkovateľ trval napriek upozorneniu Sprostredkovateľa v zmysle prvej vety tohto bodu , nesie Prevádzkovateľ. Právo Prevádzkovateľa na zadávanie pokynov a kontrolu podľa Zmluvy môže vykonať aj osoba poverená Prevádzkovateľom.
6. Sprostredkovateľ spracúva údaje len na základe zdokumentovaných pokynov Prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii s výnimkou prípadov, keď si to vyžadujú všeobecne záväzné právne predpisy; v takom prípade Sprostredkovateľ oznámi Prevádzkovateľovi túto právnu požiadavku pred spracúvaním, pokiaľ sa takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu.
7. Zmeny podmienok spracúvania osobných údajov sú možné len na základe písomnej dohody medzi Prevádzkovateľom a Sprostredkovateľom; tým nie je dotknuté právo Prevádzkovateľa ukladať Sprostredkovateľovi pokyny týkajúce sa spracúvania osobných údajov.

Článok IV.
Technické a organizačné opatrenia

1. Sprostredkovateľ sa zaväzuje nastaviť svoju internú organizáciu v súlade so Základným kontaktom a touto Zmluvou tak, aby splnil príslušné požiadavky na ochranu osobných údajov. Sprostredkovateľ sa zaväzuje, že prostredníctvom technických a organizačných opatrení, ktoré zodpovedajú súčasnému stavu techniky, zabezpečí primeranú úroveň bezpečnosti vykonávaných spracovateľských činností a systémov, v ktorých dochádza k spracúvaniu osobných údajov, a to najmä ich neustálu dôvernosť, integritu, dostupnosť

a odolnosť. Sprostredkovateľ vyhlasuje, že súčasný stav ním využívanej techniky využíva implementované zdokonalené postupy, zariadenia a prevádzkové metódy, ktoré podľa prevládajúceho názoru vedúcich expertov, dosahujú zákonom požadované ciele v oblasti ochrany údajov a ich bezpečnosti. Postupy, zariadenia a prevádzkové metódy alebo podobné postupy sa musia osvedčiť v praxi alebo by mali byť – pokiaľ sa tak ešte nestalo – ideálne aj úspešne otestované v prevádzke.

2. Sprostredkovateľ musí zabezpečiť, aby jeho zamestnanci dodržiavali všetky právne predpisy o ochrane osobných údajov pri spracúvaní osobných údajov a pri výkone príslušných práv a povinností Sprostredkovateľa podľa tejto Zmluvy.
3. Sprostredkovateľ sa zaväzuje zabezpečiť, aby jeho zamestnanci spracúvali osobné údaje v súlade so zdokumentovanými pokynmi Prevádzkovateľa.
4. Sprostredkovateľ berie na vedomie, že Prevádzkovateľ podľa svojho výlučného vlastného uváženia priebežne vyhodnocuje spracúvanie osobných údajov zamýšľané touto Zmluvou voči právnym predpisom o ochrane osobných údajov, pričom Sprostredkovateľ na základe upozornení zo strany Prevádzkovateľa musí bezodkladne vyriešiť všetky nezrovnalosti s ochranou osobných údajov, vrátane ich zabezpečenia, identifikované Prevádzkovateľom ako porušenie alebo možné porušenie právnych predpisov o ochrane osobných údajov alebo povinností Sprostredkovateľa podľa tejto Zmluvy.
5. Sprostredkovateľ sa zaväzuje zaistiť, aby spracúvanie a prístup k osobným údajom boli vždy striktne obmedzené na zamestnancov, ktorí potrebujú vykonávať spracúvanie predmetných osobných údajov, či mať k nim prístup, a to prísne na účely výkonu činností v rozsahu povinností takejto osoby voči Sprostredkovateľovi (ďalej len „**Oprávnení zamestnanci**").
6. Sprostredkovateľ sa zaväzuje zabezpečiť, aby všetci Oprávnení zamestnanci:
   a) uzatvorili s Sprostredkovateľom príslušnú dohodu o mlčanlivosti, alebo boli iným spôsobom viazaní povinnosťou mlčanlivosti vo vzťahu k osobným údajom, a to pred prístupom k osobným údajom;
   b) boli písomne oboznámení s dôvernou povahou osobných údajov;
   c) preukázateľne absolvovali a priebežne ďalej podstupovali zodpovedajúce a pravidelné školenie o právnych predpisoch o ochrane údajov.
7. Sprostredkovateľ s ohľadom na povahu spracúvania osobných údajov, ktoré má k dispozícii, musí sám napomáhať a tiež zabezpečiť, aby jeho zamestnanci napomáhali Prevádzkovateľovi pri plnení jeho povinností podľa právnych predpisov o ochrane osobných údajov, čo znamená aj pomoc pri posúdeniach vplyvu na ochranu osobných údajov a pri predbežných konzultáciách vykonávaných Prevádzkovateľom v súlade s právnymi predpismi o ochrane osobných údajov.
8. Ak v súvislosti s prebiehajúcim správnym, trestným alebo iným konaním bola zo strany príslušného orgánu verejnej moci uložená Sprostredkovateľovi povinnosť sprístupniť spracúvané osobné údaje, alebo ak mu takáto povinnosť vyplynula zo všeobecne záväzného predpisu, alebo ak bezpečnosť alebo dôvernosť spracúvaných osobných údajov je ohrozená inými udalosťami či krokmi tretích strán, Sprostredkovateľ o tom bezodkladne informuje Prevádzkovateľa.
9. Sprostredkovateľ je povinný pravidelne testovať, posudzovať a hodnotiť účinnosť zavedených technických a organizačných opatrení. V tejto súvislosti je Sprostredkovateľ povinný zohľadniť náklady na implementáciu, povahu, rozsah a účel spracúvania a meniacu sa pravdepodobnosť a závažnosť rizík v súvislosti s právami a slobodami fyzických osôb v zmysle čl. 32 ods. 1 Nariadenia GDPR. Na zabezpečenie súladu je Sprostredkovateľ povinný dodržiavať dohodnuté technické a organizačné opatrenia podľa **Prílohy č. 1** tejto Zmluvy.
10. Pre technologický pokrok a vývoj legislatívy môže byť nutné prispôsobiť zavedené technické a organizačné opatrenia. Sprostredkovateľ je povinný zaviesť postup na pravidelnú kontrolu, posúdenie a vyhodnotenie efektívnosti technických a organizačných opatrení a zaručiť tak ochranu práv dotknutých osôb. Pri prispôsobení sa technologickému pokroku môže Sprostredkovateľ zaviesť vhodné alternatívne technické a organizačné opatrenia. V takom prípade nesmie byť príslušná úroveň bezpečnosti nižšia než pri pôvodných opatreniach.
11. Potrebné prispôsobenie technických a organizačných opatrení zmeneným alebo novým legislatívnym požiadavkám musí Sprostredkovateľ vykonať najneskôr do momentu, keď takéto požiadavky nadobudnú platnosť a účinnosť, pokiaľ sa Zmluvné strany nedohodnú inak. Všetky prispôsobenia musí Sprostredkovateľ zdokumentovať a písomne oznámiť Prevádzkovateľovi bezodkladne po tom, ako zistil potrebu upraviť technické a organizačné opatrenia.
12. Náklady na prispôsobenie technických a organizačných opatrení znáša Sprostredkovateľ.
13. Ak Prevádzkovateľ vydá pokyn na zmenu technických a organizačných opatrení, Sprostredkovateľ je povinný prispôsobiť technické a organizačné opatrenia danému pokynu.

14. Sprostredkovateľ vyhlasuje, že je plne schopný zaistiť technické a organizačné zabezpečenie ochrany osobných údajov a prijal také opatrenia, aby nemohlo dôjsť k neoprávnenému alebo náhodnému prístupu k osobným údajom, neoprávneným prenosom, k ich inému neoprávnenému spracúvaniu, alebo k inému zneužitiu, a to počas doby ich spracúvania, tak aj po jej ukončení.

Článok V.
Oprava, obmedzenie, vymazanie a odovzdanie osobných údajov

1. Sprostredkovateľ nesmie opraviť osobné údaje, vymazať osobné údaje ani obmedziť spracúvanie osobných údajov, pokiaľ Základný kontrakt, táto Zmluva, pokyn Prevádzkovateľa alebo všeobecne záväzné právne predpisy neurčujú inak.
2. V súlade s pokynom Prevádzkovateľa alebo požiadavkou na výmaz údajov ako aj po ukončení spracúvania údajov musí Sprostredkovateľ (i) odovzdať Prevádzkovateľovi všetky dokumenty, výsledky spracúvania a databázy týkajúce sa zmluvného vzťahu s Prevádzkovateľom alebo (ii) tieto zlikvidovať v súlade s požiadavkami na ochranu osobných údajov, a to podľa rozhodnutia Prevádzkovateľa o tom, ktorý z postupov sa má aplikovať. Pokiaľ všeobecne záväzné právne predpisy vyžadujú dlhšiu lehotu uchovávania alebo bol voči Sprostredkovateľovi v súvislosti so Základným kontraktom alebo touto Zmluvou zo strany Prevádzkovateľa uplatnený právny nárok (napr. nárok zo zodpovednosti za škodu) a Sprostredkovateľ osobné údaje potrebuje na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov, Sprostredkovateľ zabezpečí, aby boli osobné údaje ďalej uchovávané, a to len v nevyhnutnom rozsahu a po nevyhnutnú dobu.
3. Splnenie povinností uvedených v článku V bodoch 1 až 2 tejto Zmluvy musí Sprostredkovateľ Prevádzkovateľovi na požiadanie písomne potvrdiť najneskôr v lehote pätnásť (15) dní od doručenia požiadavky Prevádzkovateľa formou Likvidačného protokolu, ktorého vzor tvorí **Prílohu č. 3** tejto Zmluvy.
4. Zmluvné strany sú povinné plniť zákonné povinnosti týkajúce sa archivácie a uchovávania registratúrnych záznamov.
5. Sprostredkovateľ uchováva dokumentáciu slúžiacu na overenie riadneho spracúvania osobných údajov podľa zadania (napr. interné smernice týkajúce sa spracúvania osobných údajov, pokyny udelené Prevádzkovateľom, záznamy o likvidácii údajov) aj po ukončení Zmluvy v súlade s príslušnými lehotami uchovávania alebo túto dokumentáciu odovzdá Prevádzkovateľovi.
6. Ak Základný kontrakt určuje iné podmienky opravy, obmedzenia, vymazania alebo odovzdania osobných údajov, resp. súvisiacej dokumentácie, majú takéto ustanovenia prednosť pred ustanoveniami tohto článku Zmluvy.

Článok VI.
Výkon práv dotknutých osôb

1. Sprostredkovateľ musí Prevádzkovateľovi oznámiť skutočnú alebo tvrdenú požiadavku dotknutej osoby na uplatnenie jej práv (podanú samotnou dotknutou osobou alebo v jej mene) na emailovú adresu **mojepravo@bratislava.sk** do dvoch (2) pracovných dní od okamihu, kedy ju obdržal od dotknutej osoby, v súlade s právnymi predpismi o ochrane osobných údajov, vrátane akejkoľvek požiadavky o prístup k osobným údajom dotknutej osoby, o opravu akýchkoľvek nepresností v osobných údajoch, o vymazanie osobných údajov, o obmedzenie spracúvania osobných údajov dotknutej osoby alebo o poskytnutie prenosnej kópie osobných údajov alebo jej poskytnutie tretej strane, ďalej v prípade vznesenia námietky proti ľubovoľnému prípadu spracúvania osobných údajov dotknutej osoby, rovnako ako v prípade inej požiadavky, sťažnosti alebo oznámenia zo strany dotknutej osoby, ktoré sa týkajú povinností Prevádzkovateľa podľa právnych predpisov o ochrane osobných údajov (ďalej len „**Požiadavka Dotknutej osoby**"), alebo obdržanie požiadavky, korešpondencie alebo oznámenia (písomné alebo ústne) od dozorného orgánu (ďalej len „**Korešpondencia od dozorného orgánu**").
2. S ohľadom na povahu spracúvania sa Sprostredkovateľ zaväzuje prostredníctvom zodpovedajúcich technických a organizačných opatrení v maximálnej možnej miere napomáhať Prevádzkovateľovi pri plnení jeho povinností v reakcii na:
   a) Požiadavku Dotknutej osoby alebo
   b) Korešpondenciu od dozorného orgánu.

3. Sprostredkovateľ nesmie splniť žiadnu požiadavku dotknutej osoby, ani na ňu reagovať bez toho, že vec najskôr konzultuje s Prevádzkovateľom a získa od neho k danej požiadavke zodpovedajúce pokyny.
4. Sprostredkovateľ sa zaväzuje bez zbytočného odkladu poskytnúť Prevádzkovateľovi všetky podrobnosti ku každej Požiadavke Dotknutej osoby alebo Korešpondencii od dozorného orgánu, a taktiež primerané informácie o okolnostiach ich vzniku, vrátane informácií o príslušných údajoch či ďalších informáciách, ktoré môže Prevádzkovateľ opodstatnene požadovať, pričom Prevádzkovateľ má povolené zverejňovať ich voči svojim odborným poradcom a príslušným dozorným orgánom.
5. Sprostredkovateľ sa zaväzuje poskytovať Prevádzkovateľovi akúkoľvek súčinnosť, aby Prevádzkovateľ mohol vykonať šetrenie a odpovedať na každú takúto Požiadavku Dotknutej osoby alebo Korešpondenciu od dozorného orgánu.

Článok VII.
Ohlasovanie porušenia ochrany údajov

1. Sprostredkovateľ sa zaväzuje upozorniť Prevádzkovateľa bez zbytočného odkladu písomným oznámením zaslaným na e-mailovú adresu **mojepravo@bratislava.sk** na akýkoľvek prípad porušenia zabezpečenia údajov, či skutočne nastal, či existuje podozrenie na porušenie zabezpečenia, hrozí alebo bezmála nastal, a to vždy najneskôr do dvadsať štyri (24) hodín od okamihu, kedy sa o takomto prípade dozvie. Toto upozornenie musí obsahovať:
   a) opis povahy porušenia zabezpečenia osobných údajov, pokiaľ možno vrátane kategórií osobných údajov, počtu dotknutých osôb a kategórií a približného počtu dotknutých záznamov osobných údajov;
   b) meno, priezvisko, pracovné zaradenie a kontaktné údaje kompetentného zamestnanca alebo iné kontaktné miesto, odkiaľ možno získať ďalšie informácie;
   c) špecifikáciu predpokladaných dôsledkov daného porušenia zabezpečenia osobných údajov;
   d) špecifikáciu opatrení prijatých či navrhovaných Sprostredkovateľom pre riešenie daného porušenia zabezpečenia osobných údajov, podľa okolností vrátane opatrení na zmiernenie možných negatívnych následkov.
2. Sprostredkovateľ berie na vedomie a je uzrozumený s tým, že Objednávateľ má povinnosť podať oznámenie príslušným dozorným orgánom do sedemdesiatich dvoch (72) hodín od okamihu, kedy sa o porušení zabezpečenia osobných údajov dozvie, ako i povinnosť upozorniť dotknuté osoby. Sprostredkovateľ je povinný poskytnúť všetku nevyhnutnú súčinnosť a informácie, ktoré môže Prevádzkovateľ opodstatnene požadovať tak, aby mohol riadne vyhodnotiť, prešetriť, zmierniť a napraviť porušenie zabezpečenia osobných údajov a splniť svoje povinnosti vyplývajúce z právnych predpisov v oblasti ochrany osobných údajov. Sprostredkovateľ sám nesmie podávať oznámenia príslušným dozorným orgánom ani upozorňovať dotknuté osoby, pokiaľ na to nezíska predchádzajúci súhlas Prevádzkovateľa.
3. Sprostredkovateľ sa zaväzuje realizovať všetky opatrenia (vrátane opatrení opísaných v článku IV Zmluvy), ktoré sú nevyhnutné pre obnovenie bezpečnosti dotknutých osobných údajov.

Článok VIII.
Subdodávatelia

1. Sprostredkovateľ nesmie zapojiť tretiu stranu na vykonávanie spracúvania osobných údajov (ďalej „**Subdodávateľ**") bez predchádzajúceho výslovného písomného súhlasu Prevádzkovateľa , s výnimkou prípadov, kedy to Sprostredkovateľovi ukladajú platné právne predpisy. V takom prípade musí Sprostredkovateľ o predmetnej zákonnej povinnosti upovedomiť Prevádzkovateľa ešte pred spracúvaním osobných údajov, s výnimkou prípadov, kedy mu zákon nepovoľuje informovať Prevádzkovateľa. Prevádzkovateľ je vždy oprávnený pravidelne kontrolovať Subdodávateľov a kedykoľvek odvolať súhlas udelený podľa prvej vety tohto bodu.
2. Zoznam Subdodávateľov, využívaných Sprostredkovateľom ku dňu účinnosti tejto Zmluvy tvorí **Prílohu č. 2** tejto Zmluvy.
3. Sprostredkovateľ je oprávnený zmeniť Subdodávateľa iba s predchádzajúcim písomným súhlasom Prevádzkovateľa a je povinný Prevádzkovateľovi v žiadosti o poskytnutie predmetného súhlasu oznámiť:
   a) identifikačné údaje Subdodávateľa, vrátane údajov o osobe oprávnenej za neho konať, v rozsahu meno a priezvisko, trvalý pobyt, pracovné zaradenie alebo funkcia,
   b) časť plnenia, ktoré bude plniť Subdodávateľ,
   c) dôvody zmeny Subdodávateľa, ako aj dopady zmeny na Prevádzkovateľa.

4. Prevádzkovateľ sa vyjadrí k navrhovanému Subdodávateľovi do štrnástich (14) dní odo dňa doručenia žiadosti o poskytnutie súhlasu podľa bodu 1. alebo bodu 3. tohto Článku Zmluvy.
5. Prevádzkovateľ nie je povinný s navrhovaným Subdodávateľom vyjadriť súhlas a je oprávnený vylúčiť Subdodávateľa aj bez udania dôvodu.
6. Sprostredkovateľ berie na vedomie, že za plnenie povinností podľa tejto Zmluvy zodpovedá voči Prevádzkovateľovi vždy Sprostredkovateľ, a to bez ohľadu na skutočnosť, či je do spracúvania osobných údajov podľa tejto Zmluvy zapojený Subdodávateľ.
7. Sprostredkovateľ je povinný Prevádzkovateľovi bezodkladne oznámiť akúkoľvek zmenu údajov o Subdodávateľovi, vrátane údajov o osobe oprávnenej za neho konať.
8. Prevádzkovateľ má právo kedykoľvek namietať zapojenie Subdodávateľa do spracúvania údajov. V prípade podľa prvej vety je Sprostredkovateľ povinný okamžite ukončiť zapojenie príslušného Subdodávateľa do procesu spracúvania údajov.

9. Sprostredkovateľ musí Subdodávateľa (ak bolo jeho zapojenie prípustné podľa predchádzajúcich bodov tohto článku) vybrať s náležitou starostlivosťou a musí sa pred jeho poverením primeraným spôsobom uistiť, že dokáže plniť povinnosti Sprostredkovateľa vyplývajúce zo Základného kontraktu , tejto Zmluvy a súvisiacich všeobecne záväzných právnych predpisov. Sprostredkovateľ je povinný zaviazať písomnou zmluvou príslušného Subdodávateľa k plneniu povinností podľa tejto Zmluvy v rozsahu, v akom Subdodávateľ má konať za Sprostredkovateľa. Ak Subdodávateľ riadne nesplní svoje povinnosti, Sprostredkovateľ zostáva voči Prevádzkovateľovi plne zodpovedný za takéto konania Subdodávateľa.

Článok IX.
Prenos údajov

1. Spracúvanie údajov bude prebiehať len v členskom štáte Európskej únie (EÚ) alebo v rámci členského štátu Európskeho hospodárskeho priestoru (EHP).
2. Prenos osobných údajov do tretej krajiny si vyžaduje predchádzajúci písomný súhlas Prevádzkovateľa a môže nastať, iba ak boli splnené požiadavky podľa čl. 44 a nasl. Nariadenia GDPR.

Článok X.
Právo na kontrolu

1. Sprostredkovateľ udeľuje Prevádzkovateľovi, a najmä jeho zodpovednej osobe (Data Protection Officer) ako aj tretím stranám povereným Prevádzkovateľom, právo kedykoľvek a bez obštrukcií skontrolovať, či sa spracúvanie údajov vykonáva v súlade s Nariadením GDPR a ďalšími predpismi ochrany osobných údajov, ustanoveniami Základného kontraktu, tejto Zmluvy a pokynmi Prevádzkovateľa.
2. Sprostredkovateľ sa zaväzuje poskytnúť Prevádzkovateľovi v procese podľa tohto Článku podporu v potrebnom rozsahu, a najmä poskytnúť potrebné informácie, vysvetlenia a vykonať všetky potrebné kroky na tento účel. Prevádzkovateľ má právo vykonať vyššie uvedené kontroly s pomocou tretích strán. Prevádzkovateľ oznámi Sprostredkovateľovi výkon kontroly minimálne desať (10) dní vopred. Každá Zmluvná strana znáša svoje vlastné náklady spojené s výkonom kontroly.
3. Kontrola podľa bodu (1) tohto článku sa môže tiež vykonať prostredníctvom:
   a) súladu so schváleným kódexom správania podľa čl. 40 Nariadenia GDPR,
   b) certifikátov podľa čl. 42 Nariadenia GDPR.

Článok XI.
Zodpovednosť za škodu

1. Ak dotknutá osoba úspešne uplatní u jednej zo Zmluvných strán právo na náhradu škody pre porušenie ustanovení Nariadenia GDPR alebo iných predpisov v oblasti ochrany osobných údajov, uplatní sa primerane čl. 82 Nariadenia GDPR, pričom platí najmä nasledovné:
   a) Sprostredkovateľ zodpovedá za škodu spôsobenú porušením povinností obsiahnutých v tejto Zmluve alebo spracúvaním údajov, ak neboli splnené povinnosti, ktoré sa v Nariadení GDPR ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi Prevádzkovateľa ;
   b) Sprostredkovateľ je zbavený zodpovednosti, ak sa preukáže, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila predmetnú škodu;

c) Prevádzkovateľ , Sprostredkovateľ a ďalší Subdodávateľ, ktorý sa zúčastnil na spracúvaní zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada;
d) ak Prevádzkovateľ, Sprostredkovateľ alebo ďalší Subdodávateľ zaplatil náhradu spôsobenej škody v plnej výške, má právo žiadať od ostatných strán zapojených do toho istého spracúvania tú časť náhrady škody, ktorá zodpovedá ich podielu zodpovednosti za škodu.

2. Sprostredkovateľ zodpovedá v súlade s právnymi predpismi za všetky iné škody spôsobené Objednávateľovi z dôvodu nedodržania pokynov Objednávateľa.
3. Sprostredkovateľ nezodpovedá za škodu, ktorá vznikne v dôsledku plnenia pokynu Prevádzkovateľa, ktorý je v rozpore s právnymi predpismi ochrany osobných údajov a Sprostredkovateľ Prevádzkovateľa na túto skutočnosť upozornil v súlade s článkom III bod 5 tejto Zmluvy, pričom Prevádzkovateľ naďalej trval na splnení pokynu.

Článok XII.
Ukončenie spracúvania údajov alebo uplynutie doby spracúvania údajov

1. Prevádzkovateľ má právo bez akejkoľvek penalizácie ukončiť spracúvanie údajov, alebo požadovať úpravu spracúvania údajov tak, aby bolo napravené protiprávne spracúvanie, a to pokiaľ sa niektoré z činností podľa Základného kontraktu opierajú o spracúvanie údajov, ktoré bude podľa platných právnych predpisov kvalifikované ako protiprávne.
2. Prevádzkovateľ má právo bez akejkoľvek sankcie ukončiť spracúvanie údajov, pokiaľ je opodstatnene presvedčený, že Sprostredkovateľ alebo Subdodávateľ neplní svoje povinnosti týkajúce sa spracúvania podľa tejto Zmluvy alebo všeobecne záväžných právnych predpisov.
3. Pri ukončení spracúvania údajov alebo uplynutí doby ich spracúvania musí Sprostredkovateľ podľa voľby Prevádzkovateľa buď:
   a) bezpečne vymazať všetky osobné údaje, vrátane ich kópií tak, aby tieto údaje nemohli byť obnovené ani zrekonštruované, pokiaľ však platné právne predpisy nestanovujú povinnosť archivácie daných osobných údajov, alebo
   b) všetky osobné údaje vrátiť Prevádzkovateľovi za pomoci technických prostriedkov dohodnutých s Prevádzkovateľom a bezpečne vymazať všetky existujúce kópie tak, aby sa nedali obnoviť ani zrekonštruovať, pokiaľ však platné právne predpisy nestanovujú povinnosť archivácie daných osobných údajov.
4. Sprostredkovateľ písomne potvrdí Prevádzkovateľovi, že vykonal úkony stanovené v bode tri (3) tohto článku, a to formou likvidačného protokolu zmysle Prílohy č. 3 tejto Zmluvy.

Článok XIII.
Komunikácia Zmluvných strán

1. Pokiaľ nie je v tejto Zmluve uvedené inak, komunikácia medzi Zmluvnými stranami prebieha všetkými dostupnými komunikačnými prostriedkami, najmä, nie však výlučne, listovou zásielkou, elektronickou správou, telefonicky a osobne.
2. Listovú zásielku je možné doručovať prostredníctvom poštového podniku alebo kuriéra na adresu sídla uvedenú v záhlaví tejto Zmluvy alebo na korešpondenčnú adresu, ak je iná ako adresa sídla. Za doručenú sa považuje každá listová zásielka, ktorá:
   a) bola adresátom prevzatá dňom jej prevzatia,
   b) prevzatie bolo adresátom odmietnuté, dňom, kedy bolo prevzatie odmietnuté,
   c) bola uložená na pobočke poštového podniku uplynutím tretieho dňa od uloženia, aj keď sa adresát s jej obsahom neoboznámil.
3. Za prvé kontaktné osoby boli určené:

   a) za Prevádzkovateľa – Mgr. Martin Slyško, martin.slysko@bratislava.sk

   b) za Sprostredkovateľa – Ing. Marek Líška, liska@parkdots.com

4. Elektronická správa sa považuje za doručenú deň nasledujúci po jej odoslaní na emailovú adresu adresáta podľa tejto Zmluvy a to aj vtedy, ak sa adresát o jej obsahu nedozvedel. Uvedené neplatí, ak je odosielateľovi doručená automatická správa o nemožnosti adresáta oboznámiť sa so správou spolu s uvedením inej kontaktnej osoby.
5. V prípade vyhlásenia mimoriadnej situácie alebo mimoriadnej udalosti v zmysle zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov, alebo v prípade vyhlásenia vojny, vojnového stavu, výnimočného alebo núdzového stavu v zmysle ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov, je možné doručovať tie písomnosti, ktoré môžu mať za následok vznik, zmenu alebo zánik práv a povinností zmluvných strán vyplývajúcich z tejto dohody aj prostredníctvom elektronickej schránky v zmysle zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) (ďalej len ako „zákon o e-Governmente"). Doručovanie písomností zaslaných prostredníctvom elektronickej schránky v zmysle zákona o e-Governmente sa riadi príslušnými ustanoveniami tohto zákona.
6. Zmluvné strany sú povinné minimálne raz denne kontrolovať kontaktné emailové schránky.
7. Zmluvné strany sú povinné bez zbytočného odkladu, najneskôr do 5 (päť) kalendárnych dní od zmeny, oznámiť si navzájom akúkoľvek zmenu kontaktných údajov. Takéto oznámenie je účinné jeho doručením.

Článok XIV.
Záverečné ustanovenia

1. Táto Zmluva nadobúda platnosť dňom jej podpisu obidvomi Zmluvnými stranami a účinnosť dňom nadobudnutia účinnosti Základného kontraktu.
2. Zmeny alebo doplnenia tejto Zmluvy možno vykonávať len vo forme písomného dodatku podpísaného oboma Zmluvnými stranami.
3. Ak sa niektoré ustanovenie tejto Zmluvy stane neplatným alebo nevykonateľným, nebude to mať vplyv na platnosť alebo vykonateľnosť ostatných ustanovení Zmluvy s výnimkou, ak by tieto ustanovenia nemohli byť oddelené od ostatného obsahu Zmluvy pre povahu Zmluvy, jej obsah alebo okolnosti, za ktorých bola Zmluva uzatvorená. Zmluvné strany sa namiesto neplatného alebo nevykonateľného ustanovenia dohodnú na ustanovení a/alebo vykonajú všetko pre to, aby dosiahli rovnaký výsledok, aký bol zamýšľaný predmetným neplatným alebo nevykonateľným ustanovením.
4. V prípade zmien právnych predpisov ochrany osobných údajov sa Sprostredkovateľ zaväzuje na žiadosť Prevádzkovateľa zabezpečiť včasnú implementáciu opatrení potrebných na riadne plnenie zákonných povinností v oblasti ochrany osobných údajov. Náklady na implementáciu opatrení, ktoré je nevyhnutné vykonať u Sprostredkovateľa znáša Sprostredkovateľ.
5. Táto Zmluva a vzťahy z nej vyplývajúce sa riadia právom Slovenskej republiky a príslušným právom Európskej únie platným v oblasti ochrany osobných údajov.
6. Súčasťou tejto Zmluvy sú nasledujúce prílohy:
   Príloha č. 1: Technické a organizačné opatrenia
   Príloha č. 2: Zoznam aktuálnych subdodávateľov
   Príloha č. 3: Likvidačný protokol – vzor
7. Zmluvné strany vyhlasujú, že si túto Zmluvu prečítali, vzájomne vysvetlili, jej obsahu porozumeli a na znak súhlasu s ňou ju slobodne, vážne, dobrovoľne, s určitosťou vlastnoručne podpísali a sú si plne vedomé následkov z nej vyplývajúcich.

Za Prevádzkovateľa:

JUDr. Rastislav Šorl
riaditeľ sekcie právnych služieb
a v súlade s aktuálne platným a účinným
Podpisovým poriadkom Prevádzkovateľa

Za Sprostredkovateľa:

V Bratislave, dňa 8.12.2023

.....
Mgr. Martin Budaj, konateľ

Príloha č. 1 k Zmluve o spracúvaní osobných údajov – Technické a organizačné opatrenia

TECHNICKÉ A ORGANIZAČNÉ OPATRENIA

1.	**Pseudonymizácia** Aké opatrenia sa prijali na zaručenie pseudonymizácie osobných údajov? Pseudonymizácia znamená spracovanie osobných údajov takým spôsobom, kedy osobné údaje nemožno pripísať konkrétnej dotknutej osobe bez použitia dodatočných informácií za predpokladu, že sa takéto dodatočné informácie uschovávajú oddelene a podliehajú technickým a organizačným opatreniam na zabezpečenie, že osobné údaje nie sú priradené identifikovanej alebo identifikovateľnej osobe.	☐ osobné údaje sú nahradené náhodnými kódmi ☐ maskovanie údajov ☐ iné:
2.	**Šifrovanie** Aké opatrenia sa prijali na zabezpečenie šifrovania osobných údajov? Opatrenie šifrovania transformujú jasný text v závislosti od položky ďalších informácií (známych ako kľúč) do zodpovedajúceho tajného textu (šifrovaný text), ktorý by nemal byť dešifrovaný pre osoby alebo osobami, ktoré nepoznajú kľúč.	☐ použitie typografických nástrojov ☐ Data Hashing ☒ šifrovanie pamäťových médií ☒ šifrovanie komunikácie ☐ iné:
3.	**Schopnosť zabezpečiť dôvernosť** Aké opatrenia sa prijímajú s cieľom natrvalo zaručiť schopnosť dôvernosti údajov? Dôvernosť znamená, že osobné údaje sú chránené pred neoprávneným prístupom.	☐ elektronický systém kontroly prístupu ☐ bezpečnostné dvere a/alebo okná ☐ mreže na oknách a dverách ☐ bezpečnosť v prevádzke, vrátnik/recepcia ☐ systém alarmu ☐ sledovanie priemyselnou kamerou ☐ špeciálna ochrana serverovej miestnosti ☒ individuálne prihlásenia a ochrana heslom ☐ ďalšie prihlásenia pre určité aplikácie ☒ automatické odhlasovanie užívateľov ☒ manažovanie kontroly práv a prístupov ☐ šifrovanie systémov ☒ šifrovanie komunikácie ☒ šifrovanie externých pevných diskov a/alebo notebookov ☒ šifrované vzdialené pripojenia (VPN) ☒ zabezpečená sieť WIFI ☐ iné:
4.	**Schopnosť zabezpečiť integritu** Aké opatrenia sa prijímajú s cieľom natrvalo zaručiť schopnosť integrity údajov? Integrita znamená zabezpečenie správnosti (neporušiteľnosti) údajov a správneho fungovania systémov. Keď sa termín integrita používa	☐ bezpečný vývoj softvéru ☐ postupy bezpečného obstarávania systémov ☒ sieťové firewally ☒ ochrana proti malware ☐ segmentácia počítačovej siete ☐ virtualizácia a vyhradenie spracovateľského prostredia

	v súvislosti s výrazom „dáta" (údaje), znamená, že údaje sú úplné a nezmenené.	☐ sledovanie siete, analýza spracúvania, analýza anomálií ☐ automatická analýza zraniteľnosti ☐ zaznamenávanie udalostí v systéme (logovanie) ☐ iné:
5.	**Schopnosť zabezpečiť dostupnosť** Aké opatrenia sa prijímajú s cieľom natrvalo zaručiť schopnosť dostupnosti údajov? Dostupnosť služieb a informačných systémov, informačných aplikácií a funkcií informačnej siete alebo informácií je zaručená, ak ich môžu používatelia kedykoľvek používať.	☒ postupy zálohovania ☐ zrkadlenie pevných diskov ☒ trvalé napájanie elektronickou energiou ☒ klimatizácia ☒ kontrola proti požiaru, proti vode ☒ správna archivácia ☐ iné:
6.	**Obnova** Aké opatrenia sa prijali na zabezpečenie dostupnosti a prístupnosti osobných údajov včas v prípade bezpečnostného incidentu?	☒ postupy zálohovania ☒ migrované sieťové úložiská dát ☒ záložné kópie dát ☒ geograficky alebo metropolitne oddelené dátové centrá ☐ plán pre núdzové prípady ☐ prevádzkový monitoring ☐ organizácia zastupovania ☐ iné:
7.	**Proces pravidelného testovania** Ako sa zabezpečuje pravidelné prehodnocovanie opatrení na ochranu osobných údajov?	☐ vopred stanovená skúšobná rutina existuje ☒ testovacie správy sú vyhodnocované ☒ návrhy na implementovanie a vylepšenie ☐ iné:
8.	**Pokyn fyzických osôb (zamestnancov)** Ako zabezpečiť, že osobné údaje budú spracovávané iba v súlade s pokynmi Objednávateľa a s príslušnými predpismi na ochranu osobných údajov?	☒ poučenie o povinnostiach pri spracúvaní osobných údajov ☒ pravidlá výkonu kontroly vstupu do objektov a chránených priestorov ☒ vzdelávanie, zvyšovanie povedomia ☒ určenie postupov likvidácie osobných údajov ☒ pravidlá manipulácie s fyzickými nosičmi osobných údajov mimo chránených priestorov ☒ pravidlá používania prenositeľných IT prostriedkov (napr. notebook) ☒ postupy pri údržbe alebo oprave IT prostriedkov ☒ politika čistého stola ☒ postup pri ukončení pracovného pomeru ☒ režim zastupovania oprávnených osôb ☒ režim údržby a upratovania chránených priestorov ☒ vedenie zoznamov aktív a ich aktualizácia ☒ riadenie zmien ☒ postup pri ohlasovaní a riešení bezpečnostných incidentov ☒ organizácia tímu reakcie na bezpečnostné incidenty ☒ definovanie bezpečnostných požiadaviek v zmluvách

		☒ pravidlá výberu dodávateľov a audit služieb ☒ vykonávanie vnútorných politík ochrany osobných údajov ☒ určenie kontaktu a zodpovedného manažéra pre plnenie Zmluvy ☐ iné:

Príloha č. 2
Zoznam aktuálnych subdodávateľov Sprostredkovateľa

Obchodné meno	Sídlo	IČO	Rozsah činností v zmysle Základného kontraktu

Príloha č. 3 k Zmluve o spracúvaní osobných údajov – Likvidačný protokol - vzor

ZÁPIS O LIKVIDÁCII OSOBNÝCH ÚDAJOV

Prevádzkovateľ: **Hlavné mesto Slovenskej republiky Bratislava**
so sídlom: Primaciálne nám. č. 1, 814 99 Bratislava

Sprostredkovateľ: .....
so sídlom: .....
IČO: .....

Právny titul spracúvania: .....
(v znení prípadných neskorších dodatkov)

Dňa ..... bola uskutočnená likvidácia .....[1] nasledujúcich spracúvaných/archivovaných osobných údajov automatizovane/čiastočne automatizovane/manuálne v tomto rozsahu:
Kategórie osobných údajov: .....
Počet osobných údajov na likvidáciu: .....
Zdroj záznamu o osobných údajoch: .....
Miesto likvidácie: .....
Poznámka: .....[2]

Prítomní zástupcovia za Prevádzkovateľa: .....
Prítomní zástupcovia za Sprostredkovateľa: .....
Tento zápis o likvidácii je vyhotovený v 2 vyhotoveniach a každá zo zúčastnených strán obdrží po jednom.

Za Prevádzkovateľa:

V ..... dňa .....

.....

Za Sprostredkovateľa:

V ..... dňa .....

.....

[1] Forma likvidácie – skartovanie, spálenie, znehodnotenie nosiča, vymazanie z informačného systému
[2] Poznámka bližšie špecifikované osobné údaje, ktoré sú predmetom likvidácie, informačné zdroje, verzie informácií a pod.