Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 a 3 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z.z. (ďalej len „**Zmluva**“) medzi

1. **Názov:** **Národná agentúra pre sieťové a elektronické služby**
   So sídlom: Kollárova 8, 917 02 Trnava
   Pracovisko: Trnavská cesta 100/II, 821 01 Bratislava
   IČO: 42 156 424
   Banka: Štátna pokladnica
   IBAN: SK63 8180 0000 0070 0062 0770
   Zastúpená: Ing. Peter Ďurica, generálny riaditeľ
   Kontakt:

   (ďalej len „Objednávateľ“)

a

2. **Názov:** **SWAN, a.s.**
   So sídlom: Landererova 12, 811 09 Bratislava
   IČO: 47 258 314
   Banka: Tatra banka, a.s.
   Číslo účtu: SK21 1100 0000 0026 2072 6338
   Zastúpený: Ing. Juraj Ondriš, predseda predstavenstva
   Ing. Michal Rybovič, podpredseda predstavenstva
   Ing. Miroslav Strečanský, člen predstavenstva

   Kontakt:

   (ďalej len „Dodávateľ“)

   Objednávateľ a Dodávateľ spolu ďalej ako „Zmluvné strany“ a každý samostatne ako „Zmluvná strana“.

Článok 1
Úvodné ustanovenia

1. Zmluvné strany uzatvárajú túto Zmluvu za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na

Zmluvu o poskytnutí verejných služieb uzatvorenej medzi Zmluvnými stranami dňa 27.10.2016 v znení jej dodatkov (ďalej len „Zmluva o poskytnutí verejných služieb“).

2. Objednávateľ je prevádzkovateľom základnej služby v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z. (ďalej ako „zákon o kybernetickej bezpečnosti“).

3. Dodávateľ je právnická osoba, ktorá na základe Zmluvy o poskytnutí verejných služieb poskytuje Objednávateľovi elektronické komunikačné služby a ku ktorému je sieť základnej služby Objednávateľa pripojená podľa §19, odseku 3 zákona o kybernetickej bezpečnosti. .

4. Dodávateľ prehlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tejto Zmluvy.

5. Dodávateľ sa zaväzuje vykonávať všetky činnosti definované v tejto Zmluve v súlade s platnými právnymi predpismi.

Článok 2
Definície pojmov

1. **Bezpečnostné opatrenia**: sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Článok 3
Predmet zmluvy

1. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Objednávateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na tretie strany v zmysle § 19 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 (ďalej len „vyhláška NBÚ“).

2. Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia Zmluvou o poskytnutí verejných služieb, vyhláškou NBÚ alebo inými právnymi predpismi vydanými v súlade so zákonom o kybernetickej bezpečnosti a zákonom o kybernetickej bezpečnosti.

3. Miestom plnenia tejto Zmluvy sú najmä pracovisko alebo sídlo Objednávateľa, pracovisko alebo sídlo Dodávateľa, alebo pracoviská a sídla subdodávateľov v zmysle Zmluvy o poskytnutí verejných služieb. V prípade zmeny alebo doplnenia sídla alebo pracoviska zo strany Zmluvných strán, vykonajú tak Zmluvné strany oznamom zaslaným e-mailom na kontaktné osoby uvedené v záhlaví tejto Zmluvy najneskôr do 30 dní od vykonania tejto zmeny.

4. Rozsah činností, ktoré Dodávateľ vykonáva pre Objednávateľa (ďalej aj ako „Služby"), je definovaný predovšetkým v Zmluve o poskytnutí verejných služieb a v zákone č. 95/20109 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov , zákone č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov a zákone č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

5. Bezpečnostné opatrenia a notifikačné povinnosti sa Dodávateľ zaväzuje plniť od okamihu nadobudnutia účinnosti tejto Zmluvy až do skončenia platnosti Zmluvy o poskytnutí verejných služieb, pokiaľ z právnych predpisov uvedených v tejto Zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti Zmluvy o poskytnutí verejných služieb.

Článok 4
Práva a povinnosti Dodávateľa

1. Všeobecné požiadavky

1.1 Dodávateľ sa zaväzuje pri poskytovaní služby oboznámiť sa a dodržiavať bezpečnostné politiky predložené Objednávateľom, a to predovšetkým Bezpečnostnú politiku informačných systémov č. 14/2017 zo dňa 31.07.2017.

1.2 Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi v prostredí Dodávateľa.

1.3 Dodávateľ sa zaväzuje bezodkladne informovať Objednávateľa o každom podozrení na kybernetický bezpečnostný incident a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti poskytovaných služieb.

1.4 Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Objednávateľom pri zabezpečovaní požiadaviek kladených na

Objednávateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky NBÚ, a to zaslaním mailu na kontakt Objednávateľa uvedený v záhlaví tejto Zmluvy.

1.5 Dodávateľ sa zaväzuje hlásiť všetky informácie, ktoré majú vplyv na túto Zmluvu zaslaním mailu na kontakt Objednávateľa uvedený v záhlaví tejto Zmluvy.

1.6 Dodávateľ sa zaväzuje prijať a dodržiavať opatrenia definované v čl. 4, bod 2 až 5 tejto Zmluvy, alebo opatrenia s porovnateľným účinkom.

2. Bezpečnostné požiadavky

2.1 Pre oblasť technických zraniteľností systémov a zariadení realizuje Dodávateľ opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi a ktoré toto poskytovanie služieb Objednávateľovi ovplyvňujú, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

2.1.1 Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb.
2.1.2 Zavedenie a prevádzka nástroja alebo mechanizmu určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí, ak sú súčasťou poskytovaných služieb
2.1.3 Využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2.2 Pre oblasť riadenia bezpečnosti sietí a informačných systémov realizuje Dodávateľ opatrenia podľa § 10 vyhlášky NBÚ, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

2.2.1 Riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Objednávateľa ktoré využíva pri poskytovaní služieb Objednávateľovi, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom.

2.2.2 Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.

2.2.3 Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.

2.2.4 Sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete.

2.2.5 Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.

2.2.6 Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.

2.2.7 Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.

2.2.8 Zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou.

2.2.9 Blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje.

2.2.10 Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.

2.2.11 Zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.

2.2.12 Implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.

2.2.13 Smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu.

2.2.14 Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.

2.2.15 Vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

2.3 Pre oblasť riadenia prístupov realizuje Dodávateľ opatrenia podľa § 12 vyhlášky NBÚ, napríklad prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

2.3.1 Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.

2.3.2 Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb Objednávateľa, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.

2.3.3 Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu.

2.3.4 Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.

2.3.5 Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.

2.3.6 Využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy).

2.3.7 Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.

2.3.8 Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

2.4 Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Dodávateľ opatrenia podľa § 14 vyhlášky NBÚ, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na poskytovanie Služieb Objednávateľovi. To zahŕňa napríklad prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľným účinkom:

2.4.1 Oboznámenie sa s postupmi Objednávateľa pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči Objednávateľovi.

2.4.2 Monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Objednávateľovi,

2.4.3 Detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.,

2.4.4 Zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.

2.4.5 Riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Objednávateľa,

2.4.6 Vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Objednávateľom.

2.5 Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Dodávateľ opatrenia podľa § 15 vyhlášky NBÚ

v rozsahu potrebnom pre poskytovanie služieb v zmysle Zmluvy o poskytnutí verejných služieb.

3. Personálne opatrenia

3.1 Dodávateľ vykonáva len činnosti, ktoré vyplývajú zo Zmluvy o poskytnutí verejných služieb alebo z právnych predpisov uvedených v tejto Zmluve alebo ich vykonával na základe písomnej požiadavky od Objednávateľa. Na výkon týchto činností môže poveriť Dodávateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam Dodávateľ poskytne Objednávateľovi po podpise tejto Zmluvy.

3.2 Akákoľvek zmena v personálnom obsadení pracovných rolí musí byť Objednávateľovi oznámená vopred. Oznámenie zabezpečí Dodávateľ elektronickou poštou na kontakt Objednávateľa uvedený v záhlaví tejto Zmluvy.

3.3 Každá osoba, ktorá sa bude podieľať na výkone činností pre Objednávateľa musí podpísať vyjadrenie o zachovaní mlčanlivosti v zmysle § 12 ods. 1 zákona o kybernetickej bezpečnosti. Vyjadrenie o zachovaní mlčanlivosti uchováva Objednávateľ.

4. Výkon kontrolných činností a auditu

4.1 Dodávateľ je povinný poskytnúť Objednávateľovi informácie potrebné na preukázanie splnenia povinností vyplývajúcich z tejto Zmluvy, zákona o kybernetickej bezpečnosti a vyhlášky NBÚ.

4.2 Dodávateľ je povinný poskytnúť Objednávateľovi súčinnosť v rámci auditu prijatých bezpečnostných opatrení a kontroly zo strany Objednávateľa, národnej jednotky CSIRT, vládnej jednotky CSIRT alebo subjektu, ktorého na vykonanie auditu poveril Objednávateľ.

4.3 Zmluvné strany sa dohodli, že Objednávateľ je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu
- 4.3.1 pravidelne raz za kalendárny rok;
- 4.3.2 v prípade podozrenia z porušenia tejto Zmluvy alebo zákona;
- 4.3.3 v prípade nedodržania bezpečnostných opatrení;
- 4.3.4 v prípade žiadosti dozorného orgánu podľa zákona.

4.4 Objednávateľ informuje o termíne vykonania auditu alebo kontroly Dodávateľa oznámením zaslaným elektronickou poštou na kontakt uvedený v záhlaví tejto Zmluvy, a to minimálne 7 dní pred vykonaním auditu alebo kontroly. Dodávateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby

sa audit alebo kontrola uskutočnili najneskôr do 14 dní odo dňa zaslania oznámenia. Pokiaľ Dodávateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí. Náklady na vykonanie auditu znáša Objednávateľ.

4.5 Audit alebo kontrola sa uskutoční v mieste určenom Objednávateľom, pokiaľ sa Zmluvné strany nedohodnú na inom mieste vykonania auditu.

5. Zapojenie ďalšieho Dodávateľa

5.1 Dodávateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto zmluve.

5.2 Dodávateľ je povinný vopred informovať Objednávateľa o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom elektronickej pošty na kontakt uvedený v záhlaví tejto Zmluvy.

5.3 Dodávateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb Objednávateľovi nového dodávateľa bez predchádzajúceho výslovného písomného súhlasu Objednávateľa.

5.4 Ak Dodávateľ zapojí do vykonávania činností spojených s poskytovaním Služieb Objednávateľovi nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto Zmluve. Zodpovednosť voči Objednávateľovi nesie Dodávateľ, ak nový dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

Článok 5
Zodpovednosť za škodu

1. V prípade, ak Dodávateľ poruší akýkoľvek záväzok vyplývajúci mu z Článku 4 tejto Zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky NBÚ, a tento nesplní ani v lehote 5 pracovných dní odo dňa doručenia výzvy Objednávateľa na jeho splnenie, má Objednávateľ nárok na preukázanú náhradu škody, pokuty alebo iných nákladov, ktoré Objednávateľovi vzniknú v súvislosti s porušením tohto záväzku Dodávateľom, pričom strata ušlého zisku sa nenahrádza.

Článok 6
Podmienky a spôsob ukončenia zmluvy

1. Po ukončení zmluvného vzťahu založeného touto Zmluvou je Dodávateľ povinný na základe rozhodnutia Objednávateľa vrátiť, previesť, alebo zničiť všetky informácie Objednávateľa, ku ktorým mal prístup počas trvania tejto Zmluvy, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane Dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach Objednávateľa.

2. Dodávateľ je povinný po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy ktoré boli predmetom Zmluvy o poskytnutí verejných služieb a sú nevyhnutné na zabezpečenie kontinuity prevádzkovaných služieb na Objednávateľa. Tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu založeného touto Zmluvou po dobu nevyhnutne potrebnú na zabezpečenie kontinuity prevádzkovaných služieb, najviac však 5 rokov.

Článok 7
Spoločné a záverečné ustanovenia

1. Táto Zmluva nadobúda platnosť dňom jej podpísania všetkými Zmluvnými stranami, resp. poslednou zo Zmluvných strán a účinnosť deň nasledujúci po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR. Táto Zmluva je povinne zverejňovaná v Centrálnom registri zmlúv v súlade s § 47a Zb. Občiansky zákonník v znení neskorších predpisov a so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií).

2. Všetky práva a povinnosti vyplývajúce z tejto Zmluvy ako aj vzťahy v tejto Zmluve bližšie neupravené sa riadia príslušnými ustanoveniami Obchodného zákonníka a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky.

3. Zmluvu možno meniť len po vzájomnej dohode Zmluvných strán formou číslovaného dodatku podpísaného všetkými Zmluvnými stranami.

4. Ak ktorékoľvek ustanovenie tejto Zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto Zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.

5. Zmluvné strany sa týmto zaväzujú, že vynaložia všetko úsilie, ktoré je od nich možné spravodlivo požadovať, aby došlo k urovnaniu všetkých sporov, rozporov alebo nárokov vzniknutých medzi nimi na základe tejto Zmluvy a v súvislosti s ňou zmierom. Ak Zmluvné strany nevyriešia akýkoľvek spor zmierom, bude takýto spor predložený na rozhodnutie príslušnému všeobecnému súdu v Slovenskej republike.

6. Táto Zmluva je vyhotovená v 3 (troch) rovnopisoch, z ktorých každý má platnosť originálu, pričom Objednávateľ dostane 2 (dva) rovnopisy a Dodávateľ dostane 1 (jeden) rovnopis.

7. Zmluvné strany týmto vyhlasujú, že si túto Zmluvu prečítali, pričom všetky jej ustanovenia sú im jasné a zrozumiteľné a vyjadrujú slobodnú a vážnu vôľu Zmluvných strán zbavenú akýchkoľvek omylov, na dôkaz čoho pripájajú svoje podpisy.

Za Objednávateľa

V Bratislave dňa .....

.....
Ing. Peter Ďurica
generálny riaditeľ
NASES

Za Dodávateľa

V Bratislave dňa .....

.....
Ing. Juraj Ondriš
predseda predstavenstva
SWAN, a.s.

V Bratislave dňa .....

.....
Ing. Michal Rybovič
podpredseda predstavenstva
SWAN, a.s.

V Bratislave dňa .....

.....
Ing. Miroslav Strečanský
člen predstavenstva
SWAN, a.s.