ZM/2024/0490

Číslo zmluvy:

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 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
(ďalej len „**Zmluva KB**")

medzi zmluvnými stranami:

Prevádzkovateľ základnej služby:

Názov:	**Národná diaľničná spoločnosť, a. s.**
Sídlo:	Dúbravská cesta 14, 841 04 Bratislava, Slovenská republika
IČO:	35 919 001
DIČ:	202 193 7775
IČ DPH:	SK2021937775
V mene ktorého koná:	Ing. Filip Macháček, predseda predstavenstva a generálny riaditeľ Ing. Peter Braška, MBA Člen predstavenstva
Registrácia:	Akciová spoločnosť zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel Sa, vložka č. 3518/B
Bankové spojenie (názov banky):	Štátna pokladnica
IBAN:	SK95 8180 0000 0070 0069 4593
SWIFT kód:	SPSRSKBA

(ďalej len „**Prevádzkovateľ základnej služby**" alebo aj „**NDS**")

a

Dodávateľ :

Názov:	**Alanata a.s.**
Sídlo:	Krasovského 14, 851 01 Bratislava – mestská časť Petržalka
IČO:	54629331
DIČ:	2121747573
IČ DPH:	SK2121747573
V mene ktorého koná:	Ing. Andrej Bališ, člen predstavenstva
Registrácia:	Spoločnosť je zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel: Sa, vložka č.: 7425/B
Bankové spojenie (názov banky):	Tatra banka a.s.
IBAN:	SK 1611 0000 0000 2947 1299 73
SWIFT kód:	TATRSKBX

(ďalej len „**Dodávateľ**")

(Prevádzkovateľ základnej služby a Dodávateľ spolu ďalej len „**zmluvné strany**")

Článok I.
ÚVODNÉ USTANOVENIA

1. **Národná diaľničná spoločnosť, a. s.** je Prevádzkovateľom základnej služby podľa ustanovenia § 3 písmena m) v spojení s písm. l) bod 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**ZoKB**").

2. Dodávateľ uzatvára s Prevádzkovateľom základnej služby Zmluvu o podpore prevádzky, údržbe a rozvoji informačného systému (ďalej len „**hlavná zmluva**"), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v ZoKB pre Prevádzkovateľa základnej služby (ďalej aj ako „**hlavný zmluvný vzťah**"). Konkrétny rozsah činností Dodávateľa je identifikovaný v hlavnej zmluve.

3. Plnenie povinností podľa tejto Zmluvy KB sa vyžaduje počas celej doby trvania hlavného zmluvného vzťahu medzi Dodávateľom a Prevádzkovateľom základnej služby, pričom táto Zmluva KB trvá najneskôr dovtedy, pokiaľ bude trvať hlavný zmluvný vzťah medzi Dodávateľom a Prevádzkovateľom základnej služby.

4. V súlade s ustanovením § 19 ods. 2 ZoKB je Prevádzkovateľ základnej služby povinný pri uzatvorení zmluvy s Dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre Prevádzkovateľa základnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti hlavnej zmluvy.

Článok II.
ZÁKLADNÉ POJMY

1. Na účely tejto Zmluvy KB sa rozumie:

   a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

   b) kybernetickým priestorom globálny, dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

   c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

   d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

   e) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,

   f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

   g) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

   h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,

j) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

   i. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,

   ii. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,

   iii. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo

   iv. ohrozenie bezpečnosti informácií,

k) základnou službou služba, ktorá je zaradená v zozname základných služieb a

   i. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 ZoKB,

   ii. je informačným systémom verejnej správy, alebo

   iii. je prvkom kritickej infraštruktúry,

l) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k) tohto bodu Zmluvy KB,

m) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 ZoKB,

n) manažér informačnej a kybernetickej bezpečnosti (ďalej len „**MIKB**") je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej a kybernetickej bezpečnosti a ďalších smerniciach Prevádzkovateľa základnej služby. Ide najmä o kontrolné činnosti, riešenie kybernetických bezpečnostných incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,

o) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

Článok III.
PREDMET ZMLUVY

1. V zmysle § 19 ods. 2 ZoKB a s ohľadom na hlavnú zmluvu, je predmetom tejto Zmluvy KB úprava práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti hlavnej zmluvy.

2. Prevádzkovateľ základnej služby je povinný v zmysle § 19 ods. 2 ZoKB uzatvoriť s Dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Obsah zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností definuje a ustanovuje § 9 ods. 2 Vyhlášky č. 362/2018 Z.z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej aj „**Vyhláška NBÚ**").

3. V rámci tejto Zmluvy KB je potrebné stanoviť základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov Prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov Prevádzkovateľa základnej služby a minimalizovať vplyv kybernetických bezpečnostných

incidentov na kontinuitu prevádzkovania základnej služby zo strany Prevádzkovateľa základnej služby (ďalej len „**ciele**"), a to aj v spolupráci s Dodávateľom.

4. Prevádzkovateľ základnej služby a Dodávateľ pri riešení incidentov podľa článku VI., bod 1 tejto Zmluvy KB a implementácií reaktívnych opatrení podľa článku VI., bod 2 tejto Zmluvy KB a ochranných opatrení podľa článku VI., bod 6 tejto Zmluvy KB budú postupovať podľa usmernení vládnej jednotky pre riešenie počítačových incidentov, so zreteľom na oznámenia a varovania špecifikované na web stránkach www.csirt.gov.sk, www.nbu.gov.sk, www.sk-cert.sk.

Článok IV.
PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam bezpečnostných opatrení Prevádzkovateľa základnej služby a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 tejto Zmluvy KB.
2. Dodávateľ sa zaväzuje riadiť sa stanovenými bezpečnostnými opatreniami v tejto Zmluve KB.
3. Dodávateľ je povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby (Príloha č. 2 tejto Zmluvy KB), ktoré sa týkajú poskytovania služby podľa hlavnej zmluvy a poskytovania služby podľa hlavnej zmluvy, s ktorými ho Prevádzkovateľ základnej služby preukázateľne písomne oboznámil, a to v rozsahu v akom súvisia s prevádzkovaním základnej služby Prevádzkovateľom základnej služby, a zároveň v akom ich je možné aplikovať na služby uvedené v článku I. bod 2 tejto Zmluvy KB.
4. Dodávateľ je zároveň povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby písomne oboznámi do 10 (desiatich) dní odo dňa nadobudnutia účinnosti tejto Zmluvy KB v znení Usmernenia pre tretie strany (ďalej len „**Usmernenie**") uvedeného v prílohe č. 2 Zmluvy o KB. Po oboznámení podľa predchádzajúcej vety, osoby poverené Dodávateľom, podpíšu čestné prehlásenie o tom, že sa oboznámili s vybranými bezpečnostnými politikami Prevádzkovateľa základnej služby a že s nimi súhlasia.
5. Dodávateľ berie na vedomie, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby. Prevádzkovateľ základnej služby sa zaväzuje o takýchto plánovaných zmenách Dodávateľa informovať najneskôr 30 (tridsať) dní pred ich implementovaním.
6. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve KB tak, aby boli naplnené ciele tejto Zmluvy KB. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto Zmluvy KB.
7. Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto Zmluvy KB, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto Zmluvy KB pre identifikáciu prípadne pre opravu poruchy/incidentu a zabezpečenie bezpečnej prevádzky IS.
8. Prevádzkovateľ základnej služby a Dodávateľ sa dohodli, že Dodávateľ je oprávnený podľa vlastného uváženia a na vlastnú zodpovednosť zapojiť ďalšieho zmluvného partnera (ďalej len „**subdodávateľ**") úplne alebo čiastočne zabezpečujúceho alebo akýmkoľvek spôsobom sa podieľajúceho na službách pre Prevádzkovateľa základnej služby namiesto Dodávateľa alebo

spolu s Dodávateľom. Dodávateľ sa zaväzuje, že nezapojí ďalšieho subdodávateľa predtým, než dostane písomný súhlas Prevádzkovateľa základnej služby.

9. Zoznam subdodávateľov tvorí prílohu č. 3 tejto Zmluvy KB. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Dodávateľa uvedené v tejto Zmluve KB. Dodávateľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa.

10. Pre vylúčenie akýchkoľvek pochybností sa Dodávateľ zaväzuje plniť podmienky tejto Zmluvy KB vrátane podmienok budúcej legislatívy Európskej Únie transponovanej do legislatívy Slovenskej republiky počas účinnosti tejto Zmluvy KB, hlavne no nie výlučne Smernice o bezpečnosti sietí a informácií NIS 2 (Smernica Európskeho parlamentu a rady (EÚ) 2022/2555 zo 14. decembra 2022), pokiaľ sa na neho budú vzťahovať. Prípadné úpravy a doplnenia činností KB budú zmluvné strany riešiť na základe analýzy rizík.

11. Dodávateľ sa zaväzuje, počas trvania hlavnej zmluvy, najneskôr do troch (3) dní od zmeny údajov, Prevádzkovateľovi základnej služby odovzdať v zalepenej zapečatenej obálke všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče príp. overovacie kľúče,. Zoznamy budú v tlačenej alebo elektronickej forme, ku každému prístupu bude uvedené okrem identifikácie prístupu aj meno prideleného, pracovné zaradenie, kontakt (mobil/e-mail), užívateľské meno, heslo. Prevádzkovateľ základnej služby sa zaväzuje, že dané údaje budú uložené na bezpečnom mieste u MIKB, a budú využité výhradne v krízovej situácii po písomnom informovaní Dodávateľa Prevádzkovateľom základnej služby.

12. Dodávateľ sa zaväzuje, po skončení trvania hlavnej zmluvy, najneskôr do troch (3) dní Prevádzkovateľovi základnej služby odovzdať všetky prihlasovacie údaje (administrátorské užívateľské meno a heslo) do príslušného informačného systému na ich správu, prístupové licenčné kľúče, overovacie kľúče, prístupové master kódy do všetkých technických objektov a HW zariadení, pridelené prístupové karty, zariadenia s RFID čipom, kľúče od miestností vo vlastníctve NDS, ako aj všetky ďalšie súvisiace prístupy pre zabezpečenie funkčného a bezproblémového prevzatia systémov a zachovania kontinuity činnosti.

Článok V.
POŽADOVANÝ ROZSAH ČINNOSTÍ DODÁVATEĽA

1. Dodávateľ je povinný v rámci zabezpečenia bezpečného fungovania základnej služby Prevádzkovateľa základnej služby a predchádzaniu kybernetickým bezpečnostným incidentom, ktoré by mohli mať potenciálne nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby v súvislosti s poskytovaním služby podľa hlavnej zmluvy (ďalej len „**incidenty**" v príslušnom gramatickom tvare):

   a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,

   b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy KB alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby,

   c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,

   d) sledovať hrozby, dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,

   e) predchádzať vzniku incidentov,

f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,

g) prijímať od Prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,

h) spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby.

2. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa Zmluvy KB v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na odôvodnené požiadanie povinný predložiť Prevádzkovateľovi základnej služby na nahliadnutie.

3. Dodávateľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 v aktuálne platnej verzii (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby a v prílohe č. 2 tejto Zmluvy KB, ktoré je potrebné vykonať v súvislosti so službami poskytovanými Dodávateľom na základe hlavnej zmluvy, zohľadňujúc charakter a rozsah poskytovaných služieb.

4. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia najmenej v oblastiach podľa § 20 ods. 3 písm. d), g), h), i), k) a m) ZoKB v rozsahu podľa § 8, § 11 až § 13, § 15 a § 17 Vyhlášky NBÚ, špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby, ktoré je potrebné vykonať v súvislosti so službami poskytovanými Dodávateľom na základe hlavnej zmluvy, zohľadňujúc charakter a rozsah poskytovaných služieb.

5. Dodávateľ je povinný prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby a Prílohe č. 2 tejto Zmluvy KB, ktoré je potrebné vykonať v súvislosti so službami poskytovanými Dodávateľom na základe hlavnej zmluvy, zohľadňujúc charakter a rozsah poskytovaných služieb.

6. Dodávateľ je povinný písomne informovať Prevádzkovateľa základnej služby o každej jemu preukázateľne známej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľ alebo o všetkých jemu preukázateľne známych skutočnostiach, majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti; tým nie sú dotknuté povinnosti a zodpovednosť Prevádzkovateľa základnej služby v zmysle ZoKB, osobitných predpisov a/alebo ich vykonávacích predpisov.

7. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov a zamestnancov subdodávateľov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto Zmluvy KB a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1 tejto Zmluvy KB. Dodávateľ je povinný bezodkladne písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Dodávateľ je povinný zaviazať povinnosťou mlčanlivosti podľa ZoKB osoby, ktoré sa budú podieľať na plnení podľa tohto bodu Zmluvy KB.

Článok VI.
POSTUP PRI RIEŠENÍ KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý kybernetický bezpečnostný incident, ako aj všetky ďalšie informácie požadované Prevádzkovateľom základnej služby na plnenie jeho povinností vplývajúcich zo ZoKB a informácie majúce vplyv na Zmluvu KB ako aj hlavnú zmluvu Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov. Ak do okamihu hlásenia

kybernetického bezpečnostného incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Dodávateľ sa po detekcii kybernetického bezpečnostného incidentu zaväzuje riešiť kybernetické bezpečnostné incidenty najmä odozvou alebo inou reakciou na kybernetický bezpečnostný incident, ohraničením kybernetického bezpečnostného incidentu a jeho dopadov, nápravou následkov kybernetického bezpečnostného incidentu, asistenciou pri riešení kybernetického bezpečnostného incidentu na mieste, reakciou na kybernetický bezpečnostný incident a podporou reakcií na kybernetický bezpečnostný incident (ďalej len „**reaktívne opatrenie**"). Pri riešení kybernetických bezpečnostných incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a ďalším ústredným orgánom alebo iným orgánom štátnej správy určeným v § 4 ZoKB jednať, a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy KB alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.

3. Dodávateľ sa zaväzuje v čase detekcie kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby, ktoré je potrebné vykonať v súvislosti so službami poskytovanými Dodávateľom na základe hlavnej zmluvy, zohľadňujúc charakter a rozsah poskytovaných služieb..

4. Dodávateľ sa zaväzuje bezodkladne, ale najneskôr do 24 (dvadsaťštyri) hodín po detekcii kybernetického bezpečnostného incidentu oznámiť Prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s kybernetickým bezpečnostným incidentom mohlo dôjsť k spáchaniu trestného činu.

5. Dodávateľ sa zaväzuje bezodkladne, najneskôr však do 24 (dvadsaťštyri) hodín po nasadení reaktívnych opatrení v zmysle bodu 2 tohto článku Zmluvy KB, oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia v súlade § 27 ods. 4 ZoKB vo formulári, ktorého vzor tvorí prílohu č. 3 tejto Zmluvy KB.

6. Po vyriešení kybernetického bezpečnostného incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického bezpečnostného incidentu (ďalej len „**ochranné opatrenia**") na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.

7. Po schválení ochranného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu, najneskôr však v lehote vyplývajúcej z opatrení schválených príslušným odborom gestora IS, vykonať. Po vykonaní ochranného opatrenia Dodávateľom, je Dodávateľ povinný za prítomnosti MIKB Prevádzkovateľa základnej služby preveriť jeho efektívnu účinnosť. Zmluvné strany sa dohodli, že účinnosť ochranných opatrení bude podmienená výkonom simulovaných útokov, pričom záver takýchto simulovaných útokov bude vyhodnotený na základe protokolu o efektívnom účinku ochranného opatrenia za Prevádzkovateľa základnej služby signovanom MIKB a za Dodávateľa signovanom osobou.

Článok VII.
ZÁVÄZOK MLČANLIVOSTI

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením hlavnej zmluvy a tejto Zmluvy KB, 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. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Dodávateľovi.

2. Dodávateľ sa v rovnakom rozsahu zaväzuje zaviazať povinnosťou mlčanlivosti aj všetky ním poverené osoby, ktoré budú zúčastnené na predmete plnenia tejto Zmluvy KB (t. j. jeho zamestnanci, subdodávatelia a ich zamestnanci). Dodávateľ je povinný na požiadanie preukázať Prevádzkovateľovi základnej služby splnenie tejto povinnosti. Povinnosť mlčanlivosti trvá aj po zániku ich pracovno-právneho vzťahu alebo obchodného vzťahu. Povinnosť zachovávať mlčanlivosť podľa tohto článku Zmluvy KB trvá aj po skončení tejto Zmluvy KB resp. hlavnej zmluvy. Mlčanlivosť sa vzťahuje na všetkých zástupcov Dodávateľa ako aj jeho Subdodávateľov.

3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje ZoKB.

4. Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa ZoKB nie je dotknutá povinnosť mlčanlivosti alebo zachovania obchodného tajomstva podľa osobitných predpisov.

Článok VIII.
POVINNOSTI PO SKONČENÍ ZMLUVY

1. Po ukončení tejto Zmluvy KB je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto Zmluvy KB prístup, resp. podľa písomného pokynu Prevádzkovateľa základnej služby zabezpečí preukázateľné zničenie akýchkoľvek nosičov elektronickej informácie certifikovanou organizáciu, a doložením protokolu s podpismi oprávnených osôb Dodávateľa a objednávateľa.

2. Zmluvné strany berú na vedomie, že predmetom plnenia hlavnej zmluvy môže byť autorské dielo podľa zákona č. 185/2015 Z. z. Autorský zákon v platnom znení, ktorého súčasťou môže byť:

   a) softvér, ktorý bol vytvorený Dodávateľom predovšetkým pre podmienky a potreby Prevádzkovateľa základnej služby;

   b) softvér Dodávateľa, ktorý má všeobecný charakter;

   c) softvér tretích osôb; alebo

   d) Open Source softvér, ktorý je podriadený príslušnej licencii slobodného softvéru.

3. Zmluvné strany berú ďalej na vedomie, že predmetom plnenia hlavnej zmluvy môže byť aj vytvorenie alebo poskytnutie iných predmetov duševného vlastníctva, ako sú napr. technická a užívateľská dokumentácia, prevádzkový manuál, návrh riešenia k Softvéru alebo k Balíkovému softvéru alebo konkrétne digitálne dizajny, vrátane grafického užívateľského rozhrania (GUI), jednotlivých ikon či symbolov, prípadne konkrétne know-how Dodávateľa.

4. S ohľadom na body 1, 2 a 3 tohto článku Zmluvy KB, zmluvné strany berú na vedomie, že Dodávateľ je v zmysle § 9 ods. 2 písm. p) Vyhlášky NBÚ povinný po zániku hlavnej zmluvy umožniť Prevádzkovateľovi základnej služby zabezpečiť kontinuitu prevádzkovanej základnej služby vo vzťahu k službám, ktoré priamo súvisia s prevádzkou tejto základnej služby v rámci sietí a informačných systémov Prevádzkovateľa základnej služby.

5. Ustanovenie bodov 1 až 3 tohto článku Zmluvy KB sa uplatňuje pre dodávku autorského diela v opačnom prípade sa neaplikuje.

Článok IX.
ZODPOVEDNOSŤ ZA ŠKODU

1. Zmluvná strana zodpovedá za škodu preukázateľne a výlučne spôsobenú zavineným porušením povinnosti zmluvnej strany stanovenej ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvou KB.

2. V prípade, ak v dôsledku porušenia ZoKB alebo preukázateľného porušenia povinností vyplývajúcich z tejto Zmluvy KB na strane Dodávateľa alebo jeho subdodávateľov vznikne Prevádzkovateľovi základnej služby ujma alebo finančná sankcia, Dodávateľ zodpovedá za spôsobenú škodu podľa ustanovení ZoKB. V prípade sankcie uloženej Národným bezpečnostným úradom, túto znáša v plnom rozsahu Dodávateľ.

3. V prípade, že zmluvná strana poruší svoju povinnosť, ktorá jej vyplýva zo ZoKB, jeho vykonávacích predpisov ako aj ostatnou platnou legislatívou alebo Zmluvy KB (ďalej ako „**porušujúca zmluvná strana**") a v dôsledku tohto konania alebo opomenutia konania porušujúcej zmluvnej strany preukázateľne dôjde k vzniku škody na strane druhej zmluvnej strany (ďalej ako „**poškodená zmluvná strana**"), zaväzuje sa porušujúca zmluvná strana túto škodu vzniknutú poškodenej zmluvnej strane nahradiť.

4. Vznik zodpovednosti porušujúcej zmluvnej strany za škodu vzniknutú poškodenej zmluvnej strane je však podmienená povinnosťou poškodenej zmluvnej strany preukázať porušujúcej zmluvnej strane existenciu príčinnej súvislosti medzi porušením povinnosti podľa Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy na strane porušujúcej zmluvnej strany a vznikom škody. Príčinná súvislosť je okrem iného daná aj vtedy, ak porušujúca zmluvná strana nesplnila svoju všeobecnú preventívnu povinnosť počínať si tak, aby nedochádzalo ku vzniku škôd. Počínaním podľa predchádzajúcej vety sa rozumie najmä akýkoľvek postup zmluvnej strany, na ktorý je v zmysle Zmluvy KB alebo ZoKB, jeho vykonávacích predpisov ako aj ostatnej platnej legislatívy oprávnená a prostredníctvom ktorého mohlo byť vzniku škody zabránené.

5. V prípade preukázania existencie príčinnej súvislosti podľa tohto článku Zmluvy KB je porušujúca zmluvná strana povinná uhradiť poškodenej zmluvnej strane vzniknutú škodu, a to v lehote do 10 (desať) dní odo dňa doručenia písomnej výzvy porušujúcej zmluvnej strane na adresu uvedenú v záhlaví tejto Zmluvy KB. V prípade potreby vzniknutú škodu posúdi nezávislá tretia strana, ktorú zabezpečí Prevádzkovateľ základnej služby.

6. Zánikom tejto Zmluvy KB nie sú dotknuté tie ustanovenia, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zániku tejto Zmluvy KB a záväzky na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy KB.

Článok X.
KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Dodávateľ sa zaväzuje komunikovať pri plnení povinností podľa tejto Zmluvy KB s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, t.j. v zmysle komunikačnej matice, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií (napr. PGP šifrovanie).

2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.

3. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy KB.

4. Kontaktné osoby podľa prílohy č. 1 tejto Zmluvy KB môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto Zmluve KB. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia Zmluvy KB o doručovaní.

Článok XI.
SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB v súlade so ZoKB a jeho vykonávacími predpismi ostatnej platnej legislatívy, 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 sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto Zmluvy KB na zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.
4. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto Zmluvy KB bezodkladne od účinnosti hlavnej zmluvy a odo dňa prebratia diela k plneniu predmetu hlavnej zmluvy, pokiaľ to nie je v tejto Zmluve KB alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
5. V prípade, ak Dodávateľ plní Zmluvu KB prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Dodávateľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy KB aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy KB. Dodávateľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto Zmluvy KB aj u týchto subdodávateľov.
6. Akékoľvek oznámenia zmluvných strán podľa tejto Zmluvy KB realizované formou e-mailu sa považujú za doručené druhej zmluvnej strane nasledujúci pracovný deň po dni, kedy bolo odosielateľovi preukázateľne odoslané potvrdenie o doručení e-mailu adresátovi bez ohľadu na to, či došlo k prečítaniu správy na strane adresáta, s tým, že v prípade detekcie kybernetického bezpečnostného incidentu a povinností Dodávateľa spojených s jeho hlásením Prevádzkovateľovi základnej služby je podmienené aj odoslaním SMS MIKB podľa ustanovenia článku VI bod 2 Zmluvy KB.
7. Komunikácia, majúca vplyv na zmenu alebo zánik tejto Zmluvy KB bude uskutočnená písomnou formou. Písomné podanie sa považuje za riadne uskutočnené, ak bolo podané na poštovú prepravu alebo doručené osobne na adresu sídla druhej zmluvnej strany uvedenú v záhlaví Zmluvy KB, prípadne na inú adresu písomne oznámenú druhou zmluvnou stranou.
8. Ak sa podanie odoslané prostredníctvom pošty vráti odosielateľovi späť s vyznačením adresát neznámy alebo adresát neprevzal v odbernej lehote, bude sa podanie považovať za doručené v deň jeho vrátenia odosielateľovi, a to bez ohľadu na to, či sa s podaním zmluvná strana oboznámila alebo nie, ak nie je doručenie podania preukázané skôr.

9. Ak zmluvná strana bezdôvodne odoprie prijať doručovanú písomnosť, považuje sa písomnosť za doručenú dňom, keď prijatie písomnosti bolo odopreté.

10. Podanie odoslané prostredníctvom pošty sa adresuje vždy na adresu zmluvných strán uvedenú v záhlaví tejto zmluvy alebo na adresu, ktorú zmluvná strana oznámi písomne podľa tejto Zmluvy KB druhej zmluvnej strane. Odoslanie podania odosielajúca strana preukáže predložením podacieho lístku, a v prípade použitia fikcie doručenia uvedenej v bode 9 tohto článku tejto Zmluvy KB aj podaním, ktoré sa vrátilo späť odosielateľovi s vyznačením adresát neznámy alebo adresát neprevzal v odbernej lehote.

11. Podanie, ktoré zmluvné strany doručujú osobne sa považuje za riadne doručené v deň, ktorý zmluvná strana prevezme podanie a tento dátum vyznačí na origináli podania, na ktorom bude vyznačený dátum doručenia podania a podpis osoby, ktorá podanie prevzala.

12. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 (piatich) pracovných dní po tom, čo k takejto zmene dôjde.

Článok XII.

VYŠŠIA MOC

1. Vyššia moc znamená mimoriadnu udalosť alebo okolnosť, ktorú nemohla žiadna zo zmluvných strán pred uzatvorením Zmluvy KB predvídať, ktorá je mimo kontroly ktorejkoľvek zo zmluvných strán a nebola spôsobená úmyselne alebo z nedbanlivosti konaním alebo opomenutím ktorejkoľvek zmluvnej strany a ktorá podstatným spôsobom sťažuje alebo znemožňuje plnenie povinností podľa Zmluvy KB ktoroukoľvek zo zmluvných strán. Takýmito udalosťami alebo okolnosťami sú najmä živelné pohromy alebo prírodné katastrofy. Výslovne sa stanovuje, že vyššou mocou nie je štrajk personálu Dodávateľa ani hospodárske pomery zmluvných strán.

2. Ak niektorej zo zmluvných strán bráni alebo bude brániť v plnení niektorej jej povinnosti podľa Zmluvy KB vyššia moc, potom písomne oznámi druhej zmluvnej strane udalosť alebo okolnosti, ktoré predstavujú vyššiu moc, uvedie povinnosti, v ktorých plnení jej vyššia moc bráni alebo bude brániť a predpokladané trvanie takej okolnosti predstavujúcej vyššiu moc. Oznámenie musí byť urobené bezodkladne, najneskôr však v lehote 15 (pätnásť) dní potom, čo sa zmluvná strana dozvedela alebo sa pri vynaložení riadnej odbornej starostlivosti mala a mohla dozvedieť o príslušnej udalosti alebo okolnostiach predstavujúcich dôvod vyššej moci. Ak je to možné, pri vynaložení riadnej odbornej starostlivosti, musí uvedené oznámenie obsahovať návrh opatrení vedúcich k zmierneniu alebo vylúčeniu dôsledkov okolností predstavujúcich vyššiu moc. V ostatných prípadoch bude oznámenie obsahovať iba najbližší možný termín, do ktorého môže byť návrh opatrenia poskytnutý pri vynaložení primeraného úsilia. Ak návrh opatrenia druhá zmluvná strana schváli, na čo má lehotu 15 (pätnásť) dní, postupuje zmluvná strana dotknutá vyššou mocou podľa neho až do ukončenia okolností vyššej moci.

3. Po uskutočnení tohto oznámenia príslušnou zmluvnou stranou, nebude táto zmluvná strana zodpovedná za príslušné porušenia povinností po dobu, dokiaľ jej vyššia moc bráni alebo bude brániť v ich plnení.

4. Zmluvnú stranu nezbavuje zodpovednosti za porušenie povinnosti vyššia moc, ktorá nastala až v čase, kedy bola povinná zmluvná strana v omeškaní s plnením jej povinnosti. Účinky vylúčenia zodpovednosti sú obmedzené iba na dobu, dokiaľ trvá vyššia moc.

5. Každá zmluvná strana vždy vyvinie všetko úsilie potrebné k tomu, aby minimalizovala omeškanie pri plnení svojich povinností podľa Zmluvy KB , ktoré vzniklo v dôsledku vyššej moci, najmä plniť návrh opatrenia, ak je tento schválený druhou zmluvnou stranou.

6. Príslušná zmluvná strana oznámi druhej zmluvnej strane okamih ukončenia pôsobenia vyššej

moci v rovnakej lehote ako pri oznámení o jej vzniku podľa bodu 2 tohto článku tejto Zmluvy KB.

7. Ak je z dôvodu okolnosti vylučujúcej zodpovednosť alebo prípadu vyššej moci plnenie Zmluvy KB *jednej zo zmluvných strán ovplyvnené len čiastočne, takáto zmluvná strana zostáva zodpovedná* za plnenie tých záväzkov, ktoré okolnosťou vylučujúcou zodpovednosť alebo vyššou mocou nie sú dotknuté.

8. Ak má niektorý zo subdodávateľov podľa akejkoľvek zmluvy či dohody týkajúcej sa poskytovania služby podľa tejto Zmluvy KB širšie definovaný nárok na omeškanie v dôsledku pôsobenia vyššej moci, okolností vylučujúcich zodpovednosť *alebo iného obdobného právneho inštitútu, než ako* je definovaná vyššia moc podľa tejto Zmluvy KB, takéto širšie definované udalosti alebo okolnosti neospravedlňujú porušenie povinností podľa Zmluvy KB s Dodávateľom ani mu nezakladajú nároky podľa tohto článku Zmluvy KB.

Článok XIII
AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa ako aj u jeho subdodávateľov audit zameraný na overenie plnenia povinností Dodávateľa a subdodávateľov podľa tejto Zmluvy KB a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa a subdodávateľov na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa a subdodávateľov pre plnenie cieľov tejto Zmluvy KB.

2. Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 (tridsiatich) dní od ukončenia auditu. Prevádzkovateľ základnej služby zároveň na základe predloženej záverečnej správy o výsledkoch auditu posudzuje riziká dodávateľských služieb, akvizície a vývoja a údržby informačných systémov podľa § 9 ods. 1 Vyhlášky NBÚ.

3. Prípadné nedostatky zistené auditom sú Dodávateľ a subdodávatelia povinní odstrániť bez zbytočného odkladu. V prípade, že tieto nedostatky nebudú v lehote 60 (šesťdesiat) dní od zistenia na základe auditu odstránené, považuje sa to za podstatné porušenie Zmluvy KB zo strany Dodávateľa.

4. Prevádzkovateľ základnej služby môže audit u Dodávateľa a subdodávateľov realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.

5. Dodávateľ sa zaväzuje za seba ako aj za subdodávateľov pri audite spolupracovať s Prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa *tejto Zmluvy KB, prípadne poskytnúť ďalšiu potrebnú súčinnosť.*

6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa a subdodávateľom, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB.

7. V rámci auditu sú Dodávateľ a subdodávatelia povinní preukázať Prevádzkovateľovi základnej služby súlad s touto Zmluvou KB, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy KB, aktuálne a vysoké bezpečnostné povedomie *svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich* zamestnancov o povinnosti mlčanlivosti podľa tejto Zmluvy KB a aktuálnosť svojej bezpečnostnej dokumentácie.

8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej 15 (pätnásť) pracovných dní vopred svoj zámer realizovať u Dodávateľa alebo jeho subdodávateľov audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto Zmluvy KB. Ak Dodávateľ alebo jeho subdodávateľ neumožní vykonanie auditu, považuje sa to za podstatné porušenie Zmluvy KB a Prevádzkovateľ základnej služby je oprávnený vyvodiť voči Dodávateľa zmluvné sankcie.

9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby v zmysle komunikačnej matice o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.

10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VII. ods. 2, 3 a 4 tejto Zmluvy KB sa uplatňujú primerane.

11. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Dodávateľa alebo jeho subdodávateľov v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa alebo jeho subdodávateľov 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 boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie Prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov Dodávateľa alebo jeho subdodávateľov na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ sa zaväzuje pred vykonaním auditu v priestoroch Dodávateľa alebo jeho subdodávateľov písomne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa alebo jeho subdodávateľov môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ alebo jeho subdodávatelia 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 alebo jeho subdodávateľov.

12. Pre vylúčenie akýchkoľvek pochybností sa Dodávateľ zaväzuje zabezpečiť Prevádzkovateľovi základnej služby vykonanie auditu v zmysle tohto článku tejto Zmluvy KB aj u svojich subdodávateľov.

Článok XIV.
SANKCIE

1. Zmluvné strany sa dohodli, že v prípade porušenia povinnosti v zmysle čl. XIII a prílohy č. 2 Dodávateľa v zmysle tejto zmluvy a jej príloh ; je Prevádzkovateľ základnej služby oprávnený uložiť Dodávateľovi zmluvnú pokutu vo výške 2500 EUR (slovom: dvetisícpäťsto eur) za každý, aj začatí deň trvania porušenia povinnosti, až do vykonania nápravy, a to aj opakovane a za každé jednotlivé porušenie povinnosti samostatne.

2. V prípade, ak Dodávateľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo Zmluvy KB akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. Obchodného zákonníka. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.

3. Zmluvné strany sa dohodli, že uplatnením sankcií v zmysle tohto článku Zmluvy KB nie je dotknutý nárok Prevádzkovateľa základnej služby na náhradu škody, ktorá mu vznikla porušením povinností Dodávateľa.

4. Zaplatenie zmluvnej pokuty nezbavuje Dodávateľa povinnosti splniť záväzok zabezpečený zmluvnou pokutou.

Článok XV.
TRVANIE ZMLUVY

1. Táto Zmluva KB sa uzatvára na dobu určitú, a to na dobu trvania hlavnej zmluvy. Táto Zmluva KB môže byť ukončená v prípadoch ustanovených v Zmluve KB alebo na základe zákona.

2. Túto Zmluvu KB nie je možné vypovedať Dodávateľom ani Prevádzkovateľom základnej služby, a je viazaná na účinnosť hlavnej zmluvy.

3. Po zániku tejto Zmluvy KB je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom základnej služby. Licenčné podmienky sú definované hlavnou zmluvou.

Článok XVI.
ZÁVEREČNÉ USTANOVENIA

1. Táto Zmluva KB sa spravuje zákonmi Slovenskej republiky. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.

2. Prípadné spory vyplývajúce z tejto Zmluvy KB budú riešené predovšetkým mimosúdne. Podpisom tejto Zmluvy KB zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto Zmluvy KB sú príslušné súdy Slovenskej republiky.

3. Táto Zmluva KB sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo Zmluvy KB nevyplýva niečo iné.

4. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto Zmluvy KB na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.

5. V prípade, ak niektoré z ustanovení Zmluvy KB je alebo sa stane neúplným, neplatným, neúčinným a/alebo nevykonateľným, nie sú tým dotknuté ostatné ustanovenia Zmluvy KB, pokiaľ z jeho povahy, obsahu alebo okolností, za ktorých bolo dojednané nevyplýva, že ho nie je možné oddeliť od ostatného obsahu Zmluvy KB. Zmluvné strany sa zaväzujú bez zbytočného odkladu nahradiť takéto neúplné, neplatné, neúčinné a/alebo nevykonateľné ustanovenie, takým úplným, platným, účinným a/alebo vykonateľným ustanovením, ktoré svojím obsahom najviac zodpovedá nahrádzanému ustanoveniu.

6. Táto Zmluva KB predstavuje úplnú dohodu zmluvných strán o jej obsahu. Podpisom tejto Zmluvy KB zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto Zmluvy KB a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto Zmluve KB neuvedených, ústnych alebo písomných dojednaní a dohôd.

7. Táto Zmluva KB bola vyhotovená v **(4) štyroch** rovnopisoch, po (2) dvoch pre každú zmluvnú stranu.

8. Zmluvné strany berú na vedomie, že Prevádzkovateľ základnej služby je v zmysle § 2 ods. 1 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 povinnou osobou, a preto je

táto zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.

9. Táto Zmluva KB nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.
10. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
    - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa, **(nezverejňuje sa v CRZ s ohľadom na GDPR)**
    - Príloha č. 2 - Špecifikácia a rozsah bezpečnostných opatrení

      (vyplývajúce z Bezpečnostných smerníc Prevádzkovateľa základnej služby),**(nezverejňuje sa v CRZ)**
    - Príloha č. 3 – Vzor - Záznam o kybernetickom bezpečnostnom incidente
11. Zmluvné strany vyhlasujú, že sú plne *spôsobilé na právne úkony, že ich zmluvná voľnosť nie je* ničím obmedzená, že túto Zmluvu KB neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah Zmluvy KB dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

Objednávateľ:

V Bratislave dňa..... 28. OKT. 2024

Národná diaľničná spoločnosť, a. s,
Ing. Filip Macháček
predseda predstavenstva a generálny riaditeľ

Národná diaľničná spoločnosť, a. s,
Ing. Peter Braška, MBA
člen predstavenstva

Poskytovateľ:

V Bratislave dňa ..... 28. OKT. 2024

Alanata a.s.
Ing. Andrej Bališ,
člen predstavenstva

Príloha č. 1: Zoznam pracovných rolí Prevádzkovateľa základnej služby a Dodávateľa (***nezverejňuje* sa v CRZ s ohľadom na GDPR)**

Prevádzkovateľ základnej služby:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou ZS**	**Telefónny kontakt**	**Email**

Dodávateľ:

Meno a priezvisko	**Rola**	**Proces súvisiaci s prevádzkou ZS**	**Telefónny kontakt**	**Email**

Príloha č. 2 (návrh obsahu)(schválená verzia- NEZVEREJŇUJE SA v CRZ):
Špecifikácia a rozsah bezpečnostných opatrení:

1. **Oblasť technických zraniteľností systémov a zariadení sa zabezpečuje prostredníctvom nasledovných opatrení:**

a) Dodávateľ je povinný pravidelne monitorovať a aktualizovať aplikačnú vrstvu s cieľom odstrániť známe bezpečnostné zraniteľnosti.

b) Dodávateľ sa zaväzuje, že v prípade zistenia kritickej zraniteľnosti, bude táto zraniteľnosť odstránená do 24 hodín od identifikácie. O tejto skutočnosti bude Prevádzkovateľ okamžite informovaný.

2. **Oblasť riadenia prístupov sa zabezpečuje prostredníctvom nasledovných opatrení:**

c) riadenia prístupu používateľov;

d) vymedzenie príslušných zodpovedností používateľov a rolí;

e) *riadenia prístupu k sieťam, čím sa rozumie:*

   i) že každému používateľovi siete a informačného systému sa prideľuje jednoznačný identifikátor na autorizovaný vstup do siete a informačného systému; (NDS požaduje aby dodávateľ a jeho subdodávatelia používali jednoznačné identifikátory s ohľadom na bezpečnosť sieti a riadili sa bezpečnostnou dokumentáciu NDS),

   ii) zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane ich prístupových práv;

   iii) využívanie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroja 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);

   iv) výkon kontroly súladu schválených používateľských účtov a prístupových oprávnení v pravidelných intervaloch, najmenej však na kvartálnej báze a v prípade ich nesúladu následné deaktivovanie, resp. zmazanie;

   v) 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 prevádzkových záznamov o každom prístupe do siete a informačného systému. (Určenú zodpovednú osobu požaduje NDS aj na strane Dodávateľa ako aj na strane NDS)

f) riadenie prístupov osôb k sieti a informačnému systému je 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. Definovanie spôsobu prideľovania a odoberania prístupových práv používateľom definované Prevádzkovateľom základnej služby, vedenie ich formálnej evidencie,

g) *výkon kontroly a poskytnutie súčinnosti Prevádzkovateľovi základnej služby pri kontrole* 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, minimálne raz ročne počas výkonu technického servisu.

h) dodávateľ je povinný implementovať silnú autentifikáciu pre všetky osoby s prístupom do aplikačnej vrstvy, vrátane viacfaktorovej autentifikácie (MFA), za splnenia podmienky, že to daná technológia umožňuje.

i) prístup k citlivým údajom a systémovým zdrojom bude obmedzený len na osoby s príslušnými oprávneniami a bude založený na princípe najmenších právomocí (least privilege).

3. **Oblasť riešenia kybernetických bezpečnostných incidentov (ďalej len „KBI") sa zabezpečuje prostredníctvom nasledovných opatrení:**

a) oboznámenie sa s postupmi Prevádzkovateľa pri riešení KBI a spracovanie interných postupov riešenia KBI, ktoré zahŕňajú minimálne postupy hlásenia KBI voči Prevádzkovateľovi.
b) monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Prevádzkovateľovi.
c) riešenie zistených KBI a zníženie následkov zistených KBI v súčinnosti s Prevádzkovateľa.
d) Súčinnosť pri vyhodnocovaní spôsobov riešenia KBI po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI v súčinnosti s Prevádzkovateľom,
e) hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v prílohe č. 1 tejto Zmluvy a postupom a cez kontakty uvedené v prílohe č. 4 tejto Zmluvy,

4. **Oblasť monitorovanie, testovanie bezpečnosti a bezpečnostné audity sa zabezpečuje prostredníctvom nasledovných opatrení:**

a) služieb prístupných do externých sietí, ak sú súčasťou služieb pre Prevádzkovateľa.

5. **Ďalšie opatrenia:**

a) Dodávateľ zabezpečí šifrovanie všetkých dát prenášaných medzi aplikačnou vrstvou a inými systémami, vrátane interných a externých komunikačných kanálov, pomocou protokolov podporujúcich minimálne TLS 1.2 alebo ekvivalent, za splnenia podmienky, že to daná *technológia umožňuje..*
b) Chránené a prísne chránené aktíva uchovávané v rámci aplikačnej vrstvy budú šifrované pomocou kryptografických algoritmov, ktoré zodpovedajú aktuálnym bezpečnostným štandardom (napr. AES-256).

Príloha č. 3:
Záznam o kybernetickom bezpečnostnom incidente

Záznam o kybernetickom bezpečnostnom incidente					
Názov bezpečnostného incidentu:				Číslo bezpečnostného incidentu:	**(Vyplní NDS)**
Dátum a čas vzniku bezpečnostného incidentu:			Dátum a čas hlásenia bezpečnostného incidentu:		
Bezpečnostný incident nahlásil:				Funkcia a osobné číslo:	
Útvar/úsek/ spoločnosť:		Telefonický kontakt:		Email:	
Bezpečnostný incident zaevidoval:				Funkcia a osobné číslo:	
Dotknutá základná služba(príp. objekt) :					
Dotknuté IS a riadiace systémy:					
Popis incidentu:					
Dotknutý útvar:			Odhadovaný dopad: **(Vyplní NDS)**	Malý ☐ Stredný ☐ Veľký ☐	
Druh bezpečnostného incidentu **(Vyplní NDS)**	Kategória I. ☐ Kategória II. ☐ Kategória III. ☐	Vstup/Spôsob hlásenia:			
Hlásenie incidentu do JISKB NBÚ SR **(Vyplní NDS)**	Číslo: Forma hlásenia (rozhranie JISKB, email): Popis dotknutej základnej služby:				

Popis a vyčíslenie možného dopadu: **(Vyplní NDS)**	
Popis vyšetrovania incidentu: **(Vyplní dodávateľ aj NDS)**	

Kategória bezpečnostného incidentu:	Útok, ☐ Zneužitie, ☐ Odcudzenie , ☐ Zlyhanie ľudského faktora, ☐ Vplyv zmien, ☐ Prerušenie prevádzky IS/SW, ☐ Nesprávna konfigurácia zariadení, ☐ Iné (uviesť):	Typ bezpečnostného incidentu:	Neautorizované činnosti v IKT ☐ Infiltrácia, alebo pokus o zavedenie škodlivého kódu, ☐ Neoprávnený fyzický prístup, ☐ Zneužitie prístupových práv, ☐ Únik informácií, ☐ Neautorizované externé činnosti voči IKT, ☐ Iné (uviesť):

Popis prijatých/navrhovaných opatrení: **(Vyplní dodávateľ aj NDS)**

Opatrenie:	Popis opatrenia:	Útvar/osoba zodpovedná za riešenie:	Termín splnenia:

Poznámky:	
Zoznam príloh:	
Podpisy zodpovedných osôb:	Hlásenie o KBI podal: Hlásenie o KBI prijal: Navrhované opatrenia schválil:

Príloha č. 4:
Komunikačná matica pre riešenie bezpečnostných incidentov