Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)

Ponuka

Verejný obstarávateľ:	**Národné centrum zdravotníckych informácií**
Sídlo/ adresa doručenia:	Lazaretská 26, Bratislava - mestská časť Staré Mesto 811 09
Kontaktná osoba:	Katarína Grejták Bednáriková
	E-mail: [redacted]
Identifikácia uchádzača	
Názov:	**DATALAN, a.s.**
Sídlo:	Krasovského 14, 851 01 Bratislava
Autor/Vyhotovil:	Ing. Dušan Polóny
Lehota na predkladanie ponúk:	22/08/2022 do 10:00
Lehota viazanosti ponuky:	28/02/2023
Stupeň dôvernosti:	Verejné ☐ Interné ☐ Chránené ☒ Vysoko chránené ☐

Schválila dňa 19/08/2022

[redacted]

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

Zoznam dokladov:

Čestne vyhlasujeme, že pre účely elektronickej komunikácie k tejto zákazke budeme využívať naše konto s užívateľským menom vo@datalan.sk [redacted][1] na portáli https://josephine.proebiz.com. Berieme na vedomie, že dokumenty sa považujú za doručené ich odoslaním do nášho konta s užívateľským menom vo@datalan.sk [redacted]* na portáli https://josephine.proebiz.com, pričom kontrola konta je na našej zodpovednosti.

Čestne vyhlasujeme, že predkladáme jedinú ponuku. Doklady uvedené v ponuke sú pravdivé, nie sú pozmenené a sú skutočné. Zoznam súborov a dokladov, ktorý sme vyššie uviedli je z našej strany vyjadrený kompletne a úplne.

V Bratislave, dňa 19.08.2022

[redacted]

[1] *Doplní uchádzač*

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

1 PONUKA

Národné centrum zdravotníckych informácií
Lazaretská 26
811 09 Bratislava

Predloženie ponuky

Vážený verejný obstarávateľ,

na základe Oznámenia o vyhlásení verejného obstarávania na predmet zákazky s názvom „Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)" vyhlásenej vo Vestníku verejného obstarávania č. 138/2022 dňa 16.06.2022 pod zn. 29600 - MSS, Vám predkladáme ponuku do verejnej súťaže.

V ponuke sa vyskytujú, resp. môžu vyskytovať názvy firiem a produktov, ktoré môžu byť chránené patentovými a autorskými právami alebo môžu byť registrovanými obchodnými značkami podľa príslušných ustanovení právneho poriadku Slovenskej republiky.

S pozdravom

V Bratislave, dňa 19.08.2022 ....

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

2 IDENTIFIKAČNÉ ÚDAJE

Obchodné meno:	DATALAN, a. s.
Právna forma:	akciová spoločnosť
Zápis:	v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/B
Sídlo:	Krasovského 14, 851 01 Bratislava – mestská časť Petržalka Slovenská republika
Štatutárny orgán:	predstavenstvo Ing. Marek Paščák, predseda predstavenstva Ing. Dušan Gavura, člen predstavenstva Ing. Zuzana Škodová Prochotská, člen predstavenstva Ing. Viktor Mikulášek, člen predstavenstva
Veľkosť podniku podľa odporúčania Komisie 2003/361/ES:	Stredný
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
Bankové spojenie:	Tatra banka, a.s., Hodžovo námestie 3, 811 06 Bratislava IBAN SK87 1100 0000 0026 2710 6780
Telefón:	+421 2 5025 7111
Fax:	+421 2 5025 7700
Web:	www.datalan.sk
E-mail:	vo@datalan.sk

Kontaktná osoba na doručovanie: Meno a priezvisko: Ing. Dušan Polóny

V Bratislave, dňa 19.08.2022

Príloha č. 3.1: Identifikačné údaje uchádzača

Obchodné meno alebo názov uchádzača *úplné oficiálne obchodné meno alebo názov uchádzača*	**DATALAN, a.s.**
Názov skupiny dodávateľov *vyplňte v prípade, ak je uchádzač členom skupiny dodávateľov, ktorá predkladá ponuku*	-neuplatňuje sa
Sídlo alebo miesto podnikania uchádzača *úplná adresa sídla alebo miesta podnikania uchádzača*	**Krasovského 14, 851 01 Bratislava**
IČO	**35 810 734**
Právna forma	**Akciová spoločnosť**
Zápis uchádzača v Obchodnom registri *označenie Obchodného registra alebo inej evidencie, do ktorej je uchádzač zapísaný podľa právneho poriadku štátu, ktorým sa spravuje, a číslo zápisu alebo údaj o zápise do tohto registra alebo evidencie*	**Obchodný register Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B**
Štát *názov štátu, podľa právneho poriadku ktorého bol uchádzač založený*	**Slovenská republika**
Zápis uchádzača v Zozname hospodárskych subjektov *označenie záznamu v Zozname hospodárskych subjektov (reg. č.) alebo inej evidencie, do ktorého je uchádzač zapísaný podľa právneho poriadku štátu, ktorým sa spravuje, a číslo zápisu alebo údaj o zápise do tohto registra alebo evidencie*	**Zápis č.: 2019/10-PO-F1458** **platný do 22.10.2022**

Zápis uchádzača v registri partnerov verejného sektora *označenie záznamu v Registri partnerov verejného sektora, do ktorej je uchádzač zapísaný a číslo zápisu alebo údaj o zápise do tohto registra alebo evidencie*	**Zapísaný vl. č. 7784**
Údaj o veľkosti spoločnosti *(mikropodnik, malý alebo stredný podnik)*	Áno □ ~~Nie □~~
Uchádzač predkladá ponuku samostatne:	Áno □ ~~Nie □~~ Ak nie, identifikácia členov skupiny dodávateľov: ---

Zoznam osôb oprávnených konať v mene uchádzača

meno a priezvisko	štátna príslušnosť
Ing. Marek Paščák	**SR**
Ing. Dušan Gavura	**SR**
Ing. Viktor Mikulášek	**SR**
Ing. Zuzana Škodová Prochotská	**SR**

Kontaktné údaje uchádzača
pre potreby komunikácie s uchádzačom

Meno a priezvisko kontaktnej osoby	**Ing. Dušan Polóny**
Telefón	
E-mail	

Oprávnená osoba k podpisu zmluvy

Meno a priezvisko oprávnenej osoby	**Ing. Zuzana Škodová Prochotská**
Funkcia	**člen predstavenstva**

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

3 DOKLAD O ZLOŽENÍ ZÁBEZPEKY

- bude predložený elektronicky

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

4 NÁVRH NA PLNENIE KRITÉRIÍ

Uchádzač / ~~skupina dodávateľov~~	**DATALAN, A.S.** **KRASOVSKÉHO 14** **851 01 BRATISLAVA** **IČO: 35 810 734**
Kritérium na vyhodnotenie ponúk	NAJNIŽŠIA CENA
Je uchádzač platiteľom DPH?[2]	ÁNO / ~~NIE~~

V tabuľke uchádzač doplní návrh na plnenie kritéria určeného na vyhodnotenie ponúk:

	Navrhovaná cena v Eur bez DPH	DPH	Navrhovaná cena v Eur s DPH
Celková cena za predmet zákazky	**14 234 145,00**	**2 846 829,00**	**17 080 974,00**

V Bratislave, dňa 19.08.2022

[2] nehodiace sa preškrtnúť

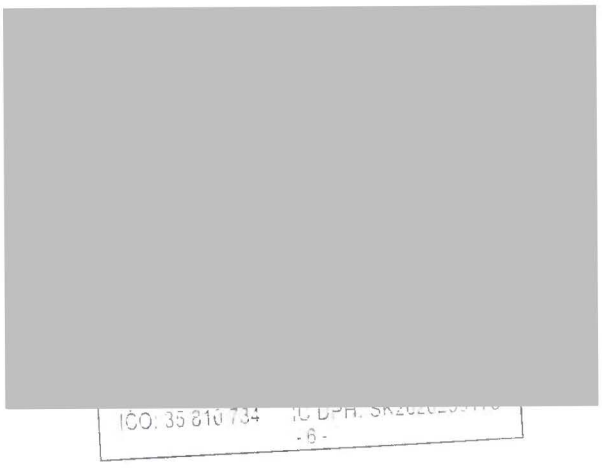
DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

5 VYHLÁSENIE UCHÁDZAČA

Dolu podpísaná Ing. Zuzana Škodová Prochotská, člen predstavenstva spoločnosti DATALAN, a.s., týmto čestne vyhlasuje, že:

- všetky predložené doklady a údaje uvedené v ponuke sú pravdivé a úplné;
- ponuku sme vyhotovili vlastnými zdrojmi, t.j. nevyužili sme služby tretích osôb na jej prípravu;
- spoločnosť DATALAN, a.s. nie je členom skupiny dodávateľov, ktorá predkladá ponuku v rámci predmetného verejného obstarávania;
- spoločnosť DATALAN, a.s. súhlasí s podmienkami určenými verejným obstarávateľom;
- spoločnosť DATALAN, a.s. sa nepokúsila neoprávnene ovplyvniť postup verejného obstarávania;
- spoločnosť DATALAN, a.s. sa nepokúsila získať dôverné informácie, ktoré by jej poskytli neoprávnenú výhodu;
- spoločnosť DATALAN, a.s. neuzavrela v danom verejnom obstarávaní s iným hospodárskym subjektom dohodu narúšajúcu hospodársku súťaž;
- u spoločnosti DATALAN, a.s. neexistujú protichodné záujmy, ktoré môžu nepriaznivo ovplyvniť plnenie zákazky;

V Bratislave, dňa 19.08.2022



IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

6 DOKLADY PREUKAZUJÚCE SPLNENIE PODMIENOK ÚČASTI

6.1. Osobné postavenie

-preukazujeme formulárom JED

Čestné vyhlásenie

Dolu podpísaný Ing. Zuzana Škodová Prochotská, člen predstavenstva spoločnosti DATALAN, a.s., týmto čestne vyhlasuje, že spoločnosť DATALAN, a.s.

a) je zapísaná v Zozname hospodárskych subjektov vedenom Úradom pre verejné obstarávanie pod reg. č. 2019/10-PO-F1458 s platnosťou zápisu do 22. 10. 2022, t.j. spĺňa podmienky účasti týkajúce sa osobného postavenia, ktoré sú stanovené v § 32 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO"); uvedenú skutočnosť si verejný obstarávateľ môže v zmysle § 152 ods. 4 ZVO overiť prostredníctvom Úradu pre verejné obstarávanie;

b) nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v Slovenskej republike alebo miesta podnikania,

c) sa nedopustila v predchádzajúcich troch rokoch od vyhlásenia alebo preukázateľného začatia verejného obstarávania závažného porušenia povinností v oblasti ochrany životného prostredia, sociálneho práva alebo pracovného práva podľa osobitných predpisov, za ktoré mu bola právoplatne uložená sankcia, ktoré dokáže verejný obstarávateľ preukázať,

d) sa nedopustila v predchádzajúcich troch rokoch od vyhlásenia alebo preukázateľného začatia verejného obstarávania závažného porušenia profesijných povinností, ktoré dokáže verejný obstarávateľ preukázať.

V Bratislave, dňa 19.08.2022

IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

6.2. Ekonomické a finančné postavenie

-preukazujeme formulárom JED

6.3. Technická spôsobilosť alebo odborná spôsobilosť

-preukazujeme formulárom JED

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

JEDNOTNÝ EURÓPSKY DOKUMENT – FORMULÁR v.1.00

Časť I : Informácie týkajúce sa postupu verejného obstarávania a verejného obstarávateľa alebo obstarávateľa

V prípade postupov verejného obstarávania, v ktorých bola výzva na súťaž uverejnená v *Úradnom vestníku Európskej únie*, sa informácie požadované v časti I zobrazia automaticky za predpokladu, že na vytvorenie a vyplnenie jednotného európskeho dokumentu pre obstarávanie sa použije elektronická služba jednotného európskeho dokumentu pre obstarávanie[1]. Referenčné číslo príslušného oznámenia[2] uverejneného v Úradnom vestníku Európskej únie :

Ú. v. EÚ S číslo [2022/S 114], dátum [15.06.2022], strana [ ]
Číslo oznámenia v Ú. v. EÚ S : 2022/S 114-321736
Ak v *Úradnom vestníku Európskej únie* nebola uverejnená žiadna výzva na súťaž, verejný obstarávateľ alebo obstarávateľ musí vyplniť informácie umožňujúce jednoznačnú identifikáciu postupu verejného obstarávania.

V prípade, keď nie je potrebné uverejnenie oznámenia v *Úradnom vestníku Európskej únie*, uveďte ďalšie informácie umožňujúce jednoznačnú identifikáciu postupu verejného obstarávania (napr. odkaz na uverejnenie na vnútroštátnej úrovni). [29600 - MSS, Vestník č. 138/2022 zo dňa 16.06.2022]

INFORMÁCIE O POSTUPE VEREJNÉHO OBSTARÁVANIA

Informácie požadované v časti I sa zobrazia automaticky za predpokladu, že na vytvorenie a vyplnenie jednotného európskeho dokumentu pre obstarávanie sa použije spomínaná elektronická služba jednotného európskeho dokumentu pre obstarávanie. Ak sa tieto informácie nezobrazia automaticky, musí ich vyplniť hospodársky subjekt.

Identifikácia obstarávateľa[3]	**Odpoveď:**
Názov:	**Národné centrum zdravotníckych informácií** Vnútroštátne identifikačné číslo: 00165387 Lazaretská 26, 81109 Bratislava - mestská časť Staré Mesto Kód NUTS: SK010 Slovensko Email:
O aké obstarávanie ide?	**Odpoveď:**
Názov alebo skrátený opis obstarávania[4]	Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)
Evidenčné číslo spisu, ktoré pridelil verejný obstarávateľ alebo obstarávateľ (ak sa uplatňuje)[5]:	Referenčné číslo: NCZI-RISEZ-2022-VS

[1] Útvary Komisie bezplatne sprístupnia elektronickú službu jednotného európskeho dokumentu pre obstarávanie verejným obstarávateľom, obstarávateľom, hospodárskym subjektom, poskytovateľom elektronických služieb a iným zainteresovaným stranám.

[2] V prípade **verejných obstarávateľov**: buď **predbežné oznámenie** používané ako prostriedok vyzvania na súťaž, **alebo oznámenie o vyhlásení verejného obstarávania**. V prípade **obstarávateľov** : **pravidelné informatívne oznámenie** používané ako prostriedok výzvy na súťaž, **oznámenie o vyhlásení verejného obstarávania alebo oznámenia o existencii kvalifikačného systému.**

[3] *Informácie, ktoré majú byť prevzaté z oddielu I bod I.1 príslušného oznámenia*, v prípade spoločného obstarávania uveďte mená všetkých zúčastnených obstarávateľov.

[4] Pozri body II.1.1 a II.1.3 príslušného oznámenia.

[5] Pozri bod II.1.1 príslušného oznámenia.

Všetky ostatné informácie vo všetkých oddieloch jednotného európskeho dokumentu pre obstarávanie vypĺňa hospodársky subjekt.

Časť II : Informácie týkajúce sa hospodárskeho subjektu

A : INFORMÁCIE O HOSPODÁRSKOM SUBJEKTE

Identifikácia:	**Odpoveď:**
Názov :	[DATALAN, a.s.]
Identifikačné číslo pre DPH, ak sa uplatňuje: Ak sa identifikačné číslo pre DPH neuplatňuje, uveďte ich národné identifikačné číslo, ak sa vyžaduje a je uplatniteľné.	[SK2020259175] [ ]
Poštová adresa:	[Krasovského 14, Bratislava - mestská časť Petržalka 851 01]
Kontaktné osoby[6]: Telefón: E-mail: Internetová adresa (webová adresa)(ak je k dispozícii):	[Ing. Dušan Polóny] [www.datalan.sk]
Všeobecné informácie:	**Odpoveď:**
Je hospodársky subjekt mikropodnik[7], malý alebo stredný podnik?	☑ Áno ☐ Nie
Len v prípade, ak je obstarávanie vyhradené[8]: je hospodársky subjekt chránená pracovná dielňa, „sociálny podnik“[9] alebo zabezpečí plnenie zákazky v rámci programov chránených pracovných miest? **Ak áno,** aký je zodpovedajúci percentuálny podiel zdravotne postihnutých alebo znevýhodnených pracovníkov? Ak sa to vyžaduje, uveďte, do ktorej kategórie alebo kategórií zdravotne postihnutých alebo znevýhodnených pracovníkov patria príslušní zamestnanci?	☐ Áno ☑ Nie [.....] [.....]
V príslušných prípadoch: je hospodársky subjekt zapísaný v úradnom zozname schválených hospodárskych subjektov alebo má rovnocenné osvedčenie (napríklad v rámci národného (pred)kvalifikačného systému)?	☑ Áno ☐ Nie ☐ Neuplatňuje sa

[6] Poskytnutie informácie o kontaktných osobách toľkokrát, koľkokrát je to potrebné.

[7] Porovnaj odporúčanie Komisie zo 6. mája 2003 týkajúce sa definície mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36). Táto informácia sa vyžaduje len na štatistické účely. **Mikropodniky:** podniky, ktoré **zamestnávajú menej než 10 osôb** a ktorých ročný obrat a/alebo celková ročná súvaha **neprekračuje 2 milióny EUR.**
Malé podniky: podniky, ktoré **zamestnávajú menej ako 50 osôb** a ktorých ročný obrat a/alebo celková ročná súvaha **neprekračuje 10 miliónov EUR.**

Ak áno: **Odpovedzte na zvyšné časti tohto oddielu, oddielu B a v príslušnom prípade oddielu C tejto časti, v prípade potreby vyplňte časť V a v každom prípade vyplňte a podpíšte časť VI.** a) Uveďte názov zoznamu alebo osvedčenia a v príslušnom prípade príslušné číslo zápisu alebo osvedčenia: b) Ak je osvedčenie o zápise alebo osvedčenie k dispozícii v elektronickom formáte, uveďte: c) Uveďte odkazy, na ktorých je založený zápis alebo osvedčenie a v príslušnom prípade klasifikáciu získanú v úradnom zozname[10]: d) Vzťahuje sa zápis alebo osvedčenie na všetky požadované podmienky účasti?	a) [Zoznam hospodárskych subjektov, č. zápisu: 2019/10-PO-F1458 Obchodný register Okresného súdu Bratislava I, odd.: Sa, vl. č. 2704/B] b) (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [https://www.orsr.sk/vypis.asp?ID=31720&SID=2&P=0] c) [https://www.uvo.gov.sk/zoznam-hospodarskych-subjektov/detail/63?page=1&limit=20&sort=nazov&sort-dir=ASC&ext=0&ico=35810734&nazov=&obec=&registracneCislo=] d) ☐ Áno ☑ Nie
Ak nie: **Vyplňte navyše aj chýbajúce informácie v časti IV, oddiely A, B, C alebo D, a to podľa potreby** **Len ak sa to vyžaduje v príslušnom oznámení alebo súťažných podkladoch:**	d) ☐ Áno ☐ Nie

---

Stredné podniky: podniky, ktoré nie sú mikropodnikmi ani malými podnikmi a ktoré **zamestnávajú menej ako 250 osôb** a ktorých **ročný obrat nepresahuje 50 miliónov EUR a/alebo celková ročná súvaha nepresahuje 43 miliónov EUR.**

[8] Pozri oznámenie o ponuke, bod III. 1.5.

[9] To znamená, že jeho hlavným cieľom je sociálna a profesionálna integrácia zdravotne postihnutých alebo znevýhodnených osôb.

[10] Ak existujú odkazy a klasifikácie, tak sú uvedené v osvedčení.

d) Bude môcť hospodársky subjekt poskytnúť **osvedčenie**, pokiaľ ide o platbu príspevkov na sociálne zabezpečenie a daní, alebo informácie, ktoré verejnému obstarávateľovi alebo obstarávateľovi umožnia získať toto osvedčenie priamo prostredníctvom prístupu do vnútroštátnej databázy v ktoromkoľvek členskom štáte, ktorá je k dispozícii bezplatne? Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	(webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....][.....]
Forma účasti:	***Odpoveď:***
Zúčastňuje sa hospodársky subjekt na postupe obstarávania spoločne s inými subjektmi[11]?	☐ Áno ☑ Nie

Ak áno, zaistite, aby príslušné ostatné subjekty poskytli osobitný formulár JED pre obstarávanie.	
Ak áno: a) Uveďte úlohu hospodárskeho subjektu v rámci skupiny (vedúci subjekt, subjekt zodpovedný za osobitné úlohy...): b) Uveďte iné hospodárske subjekty, ktoré sa zúčastňujú na postupe obstarávania spoločne: c) V prípade potreby názov zúčastnenej skupiny:	a) [.....] b) [.....] c) [.....]
Časti	**Odpoveď:**
Ak je to uplatniteľné, oznámenie častí, o ktoré sa hospodársky subjekt chce uchádzať:	[ ]

[11] Najmä ako súčasť skupiny, konzorcia, spoločného podniku alebo podobne.

B : INFORMÁCIE O ZÁSTUPCOCH HOSPODÁRSKEHO SUBJEKTU

V príslušnom prípade uveďte meno a adresu osoby oprávnenej zastupovať hospodársky subjekt na účely tohto postupu obstarávania:

Zastúpenie, ak existuje:	***Odpoveď:***
Celé meno; Doplnené dátumom a miestom narodenia, ak sa vyžadujú:	[Ing. Zuzana Škodová Prochotská] [.....]
Pozícia/zastupujúci:	[člen predstavenstva]
Poštová adresa:	[Krasovského 14,Bratislava - mestská časť Petržalka 851 01]
Telefón:	
E-mail:	
Ak je to potrebné, uveďte potrebné informácie o zastúpení (jeho formu, rozsah, účel...):	[.....]

C : INFORMÁCIE O VYUŽÍVANÍ KAPACÍT INÝCH SUBJEKTOV

Dôvera:	**Odpoveď:**
Využíva hospodársky subjekt kapacity iných subjektov, aby mohol splniť podmienky účasti stanovené v časti IV a prípadne kritéria a pravidlá stanovené ďalej v časti V?	☑ Áno ☐ Nie

Ak áno, predložte samostatný formulár jednotného európskeho dokumentu pre obstarávanie, v ktorom budú uvedené informácie požadované v **oddiele A a B tejto časti a časti III pre každý z** príslušných subjektov, riadne vyplnený a s podpisom príslušných subjektov. Upozorňujeme, že tento formulár by mal zahŕňať aj technikov alebo technické orgány, ktoré priamo nepatria k podniku hospodárskeho subjektu, najmä tých, ktorí zodpovedajú za kontrolu kvality, a v prípade verejných zákaziek na práce by mal zahŕňať technikov alebo technické orgány, na ktoré sa môže hospodársky subjekt obrátiť so žiadosťou o vykonanie práce. Pokiaľ je to relevantné pre špecifickú kapacitu alebo kapacity, ktoré hospodársky subjekt využíva, uveďte informácie v časti IV a V pre každý z príslušných subjektov[12].

[12] Napríklad technické orgány zapojené do kontroly kvality: Časť IV oddiel C bod 3.

D : INFORMÁCIE TÝKAJÚCE SA SUBDODÁVATEĽOV, KTORÝCH KAPACITY HOSPODÁRSKY SUBJEKT NEVYUŽÍVA

(Tento oddiel sa vyplní len vtedy, ak tieto informácie vyslovene vyžaduje verejný obstarávateľ alebo obstarávateľ).

Subdodávatelia:	**Odpoveď:**
Má hospodársky subjekt v úmysle zadať niektorú časť zákazky tretím stranám?	☑ Áno ☐ Nie Ak **áno a pokiaľ sú známe,** uveďte zoznam navrhovaných subdodávateľov: TEMPEST a.s. Krasovského 14 Bratislava - mestská časť Petržalka 851 01 IČO: 31 326 650

Ak verejný obstarávateľ alebo obstarávateľ vyslovene požaduje tieto informácie okrem informácií v tomto oddiele, uveďte informácie požadované v oddieloch A a B tejto časti a časti III pre každého (pre každú z kategórií) z príslušných subdodávateľov.

Časť III: Dôvody na vylúčenie

A: DÔVODY TÝKAJÚCE SA ODSÚDENIA ZA TRESTNÝ ČIN

V článku 57 ods. 1 smernice 2014/24/EÚ sa stanovujú tieto dôvody vylúčenia:

1. Účasť v zločineckej organizácii[13];
2. Korupcia[14];
3. Podvod[15];
4. Teroristické trestné činy alebo trestné činy spojené s teroristickými činnosťami[16];
5. Pranie špinavých peňazí a financovanie terorizmu[17];
6. Detská práca a iné formy obchodovania s ľuďmi[18];

Dôvody týkajúce sa odsúdení za trestný čin podľa vnútroštátnych ustanovení vykonávajúcich dôvody uvedené v článku 57 ods. 1 smernice:	**Odpoveď:**
Bol **samotný hospodársky subjekt** alebo **osoba,** ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, **konečným rozsudkom odsúdený** z jedného z uvedených dôvodov rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje?	☐ Áno ☑ Nie Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte: (webovú adresu, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....][19]

[13] Ako sa vymedzuje v článku 2 rámcového rozhodnutia Rady 2008/841/SVV z 24. októbra 2008 o boji proti organizovanému zločinu (Ú. v. EÚ L 300, 11.11.2008, s. 42).

[14] Ako sa vymedzuje v článku 3 Dohovoru o boji proti korupcii úradníkov Európskych spoločenstiev alebo úradníkov členských štátov Európskej únie (Ú. v. ES C 195, 25.6.1997, s. 1), a v článku 2 ods. 1 rámcového rozhodnutia Rady 2003/568/SVV z 22. júla 2003 o boji proti korupcii v súkromnom sektore (Ú. v. EÚ L 192, 31.7.2003, s. 54). Tento dôvod na vylúčenie zahŕňa aj korupciu v zmysle vnútroštátnych právnych predpisov verejného obstarávateľa (obstarávateľa) alebo hospodárskeho subjektu.

[15] V zmysle článku 1 Dohovoru o ochrane finančných záujmov Európskych spoločenstiev (Ú. v. ES C 316, 27.11.1995, s. 48).

[16] Ako sú vymedzené v článkoch 1 a 3 rámcového rozhodnutia Rady z 13. júna 2002 o boji proti terorizmu (Ú. v. ES L 164, 22.6.2002, s. 3). Tento dôvod na vylúčenie zahŕňa aj podnecovanie alebo napomáhanie alebo navádzanie alebo pokus o spáchanie trestného činu v súlade s článkom 4 uvedeného rámcového rozhodnutia.

[17] Ako sa vymedzuje v článku 1 smernice Európskeho parlamentu a Rady 2005/60/ES z 26. októbra 2005 o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu (Ú. v. EÚ L 309, 25.11.2005, s. 15).

[18] Ako sa vymedzuje v článku 2 smernice Európskeho parlamentu a Rady 2011/36/EÚ z 5. apríla 2011 o prevencii obchodovania s ľuďmi a boji proti nemu a o ochrane obetí obchodovania, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/629/SVV (Ú. v. EÚ L 101, 15.4.2011, s. 1).

[19] Zopakujte toľkokrát, koľkokrát je potrebné.

Ak áno, uveďte[20]: a) dátum odsúdenia, uveďte, o ktoré body 1 až 6 ide a dôvod odsúdenia, b) totožnosť osoby, ktorá bola usvedčená; c) **pokiaľ sa stanovuje priamo v rozsudku:**	a) dátum:[ ], bod/body: [ ], dôvody: [ ] b) [.....] c) dĺžku obdobia vylúčenia. [.....] a príslušný bod/body [ ] Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte: (webovú adresu, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....][21]
V prípade odsúdenia prijal hospodársky subjekt opatrenia, aby sa preukázala jeho spoľahlivosť napriek existencii relevantného dôvodu na vylúčenie[22] („samo očistenie“)?	☐ Áno ☐ Nie
Ak áno, opíšte prijaté opatrenia[23]:	[.....]

[20] Zopakujte toľkokrát, koľkokrát je potrebné.
[21] Zopakujte toľkokrát, koľkokrát je potrebné.
[22] V súlade s vnútroštátnymi ustanoveniami, ktorými sa vykonáva článok 57 ods. 6 smernice 2014/24/EÚ.
[23] Vysvetlenie by so zreteľom na povahu spáchaných trestných činov (presné, opakované a systematické...) malo ukazovať primeranosť prijatých opatrení.

B: DÔVODY TÝKAJÚCE SA PLATBY DANÍ ALEBO PRÍSPEVKOV NA SOCIÁLNE ZABEZPEČENIE

Platby daní alebo príspevkov na sociálne zabezpečenie:	**Odpoveď:**	
Splnil hospodársky subjekt všetky **svoje povinnosti týkajúce sa platby daní alebo príspevkov na sociálne zabezpečenie,** a to v krajine, v ktorej sídli, ako aj v členskom štáte verejného obstarávateľa alebo obstarávateľa, ak ide o inú krajinu, ako je krajina sídla?	☑ Áno ☐ Nie	
	Dane	**Príspevky na sociálne zabezpečenie**
Ak nie, uveďte: a) Krajinu alebo príslušný členský štát b) Príslušnú sumu c) Spôsob stanovenia tohto porušenia povinností	a) [.....] b) [.....]	a) [.....] b) [.....]
1. Prostredníctvom súdneho alebo administratívneho **rozhodnutia:**	c1) ☐ Áno ☐ Nie	c1) ☐ Áno ☐ Nie
- Je rozhodnutie konečné a záväzné?	☐ Áno ☐ Nie	☐ Áno ☐ Nie
- Uveďte dátum odsudzujúceho rozsudku a rozhodnutia.	- [.....]	- [.....]
- V prípade odsúdenia, **pokiaľ sa stanovuje priamo v rozsudku,** aj dĺžku obdobia vylúčenia:	- [.....]	- [.....]
2. **Inými prostriedkami?** Spresnite:	c2) [.....]	c2) [.....]
d) Splnil hospodársky subjekt svoje povinnosti tým, že zaplatil alebo uzavrel záväznú dohodu s cieľom zaplatiť splatné dane alebo príspevky na sociálne zabezpečenie vrátane akýchkoľvek prípadných vzniknutých úrokov alebo sankcií?	☐ Áno ☐ Nie **Ak áno,** uveďte podrobnosti: [.....]	☐ Áno ☐ Nie **Ak áno,** uveďte podrobnosti: [.....]
Ak príslušné dokumenty týkajúce sa platby daní alebo príspevkov sociálneho zabezpečenia sú dostupné v elektronickom formáte, uveďte:	(webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu)[24]: [.....][.....][.....]	

[24] Zopakujte toľkokrát, koľkokrát je potrebné.

C: DÔVODY TÝKAJÚCE SA KONKURZU, KONFLIKTU ZÁUJMOV ALEBO ODBORNÉHO POCHYBENIA[25]

Upozorňujeme, že na účely tohto obstarávania mohli byť niektoré z nasledujúcich dôvodov na vylúčenie presnejšie vymedzené vo vnútroštátnom práve, v príslušnom alebo súťažných podkladoch. Vo vnútroštátnych právnych predpisoch sa preto môže napríklad ustanoviť, že pojem „závažné odborné pochybenie" sa môže vzťahovať na niekoľko rôznych foriem správania.

Informácie týkajúce sa prípadného konkurzu, konfliktu záujmov alebo profesionálneho pochybenia	**Odpoveď:**
Porušil hospodársky subjekt, **podľa jeho vedomostí, svoje povinnosti** v oblasti **environmentálneho, sociálneho a pracovného práva[26]?**	☐ Áno ☑ Nie
	Ak áno, prijal hospodársky subjekt opatrenia, aby sa preukázala jeho spoľahlivosť napriek existencii dôvodu na vylúčenie („samo očistenie")? Áno ☐ Nie ☐ **Ak prijal opatrenia,** opíšte prijaté opatrenia: [.....]
Nachádza sa hospodársky subjekt v niektorej z týchto situácií: a) **úpadok,** alebo b) **konkurz** alebo likvidácia, alebo c) prebieha **vyrovnávacie konanie** alebo d) je v akejkoľvek podobnej situácii vyplývajúcej z podobného konania podľa vnútroštátnych zákonov a iných právnych predpisov[27] alebo e) jeho aktíva spravuje likvidátor alebo súd alebo f) jeho podnikateľské činnosti sú pozastavené?	☐ Áno ☑ Nie
Ak áno: - Uveďte podrobné informácie: - Uveďte dôvody, prečo je hospodársky subjekt napriek tomu schopný plniť zákazku, pričom sa zohľadnia platné vnútroštátne pravidlá a opatrenia týkajúce sa pokračovania podnikateľskej činnosti za týchto okolností[28]?	- [.....] - [.....]
Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	(webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

[25] Pozri článok 57 ods. 4 smernice 2014/24/EÚ.

[26] Ako je uvedené na účely tohto obstarávania vo vnútroštátnom práve, v príslušnom oznámení alebo v súťažných podkladoch alebo v článku 18 ods. 2 smernice 2014/24/EÚ.

[27] Pozri vnútroštátne právo, príslušné oznámenie alebo súťažné podklady.

[28] Tieto informácie sa nemusia uviesť, ak vylúčenie hospodárskych subjektov v jednom z prípadov uvedených pod písmenami a) až f) je **povinné** podľa platného vnútroštátneho práva **bez možnosti výnimky**, keď je však hospodársky subjekt schopný realizovať zákazku.

Dopustil sa hospodársky subjekt **závažného odborného pochybenia**[29]**?** Ak áno, uveďte podrobnejšie informácie:	☐ Áno ☑ Nie [.....]
	Ak áno, prijal hospodársky subjekt samočistiace opatrenia? ☐ Áno ☐ Nie **Ak prijal opatrenia,** opíšte prijaté opatrenia: [.....]
Uzatvoril hospodársky subjekt **dohody** s inými hospodárskymi subjektmi s **cieľom narušiť hospodársku súťaž?** **Ak áno,** uveďte podrobnejšie informácie:	☐ Áno ☑ Nie [.....]
	Ak áno, prijal hospodársky subjekt samočistiace opatrenia? Áno ☐ Nie ☐ **Ak prijal opatrenia,** opíšte prijaté opatrenia: [.....]
Vie hospodársky subjekt o akomkoľvek **konflikte záujmov**[30] z dôvodu jeho účasti na postupe obstarávania? **Ak áno,** uveďte podrobnejšie informácie:	☐ Áno ☑ Nie [.....]
Poskytoval hospodársky subjekt alebo podnik súvisiaci s hospodárskym subjektom **poradenstvo** verejnému obstarávateľovi alebo obstarávateľovi alebo bol iným spôsobom **zapojený do prípravy** postupu obstarávania? **Ak áno,** uveďte podrobnejšie informácie:	☐ Áno ☑ Nie [.....]
Stalo sa hospodárskemu subjektu, že predchádzajúca verejná zákazka, predchádzajúca verejná zákazka s obstarávateľom alebo predchádzajúca koncesná zmluva bola **ukončená predčasne,** alebo že došlo k škode alebo iným porovnateľným sankciám v súvislosti s touto predchádzajúcou zákazkou? **Ak áno,** uveďte podrobnejšie informácie:	☐ Áno ☑ Nie [.....]
	Ak áno, prijal hospodársky subjekt samočistiace opatrenia? ☐ Áno ☐ Nie **Ak prijal opatrenia,** opíšte prijaté opatrenia: [.....]

[29] V prípade potreby pozri definície vo vnútroštátnom práve, príslušnom oznámení alebo v súťažných podkladoch.

[30] Ako sa uvádza vo vnútroštátnom práve, príslušnom oznámení alebo v súťažných podkladoch.

Môže hospodársky subjekt potvrdiť, že: a) nie je vinný zo závažného **skreslenia** pri predkladaní informácií vyžadovaných na overenie neexistencie dôvodov na vylúčenie alebo splnenia podmienok účasti; b) **nezadržal** takéto informácie; c) môže bezodkladne predložiť podporné dokumenty požadované verejným obstarávateľom alebo obstarávateľom a d) nenáležite neovplyvňoval rozhodovací proces verejného obstarávateľa s cieľom získať dôverné informácie, ktoré môžu poskytnúť nenáležité výhody v rámci postupu verejného obstarávania, alebo z nedbalosti neposkytol zavádzajúce informácie, ktoré môžu mať podstatný vplyv na rozhodnutia týkajúce sa vylúčenia, výberu alebo zadania zákazky?	☑ Áno ☐ Nie

D: INÉ DÔVODY NA VYLÚČENIE, KTORÉ MÔŽU BYŤ STANOVENÉ VO VNÚTROŠTÁTNYCH PRÁVNYCH PREDPISOCH ČLENSKÉHO ŠTÁTU VEREJNÉHO OBSTARÁVATEĽA ALEBO OBSTARÁVATEĽA

Čisto vnútroštátne dôvody vylúčenia	**Odpoveď:**
Uplatňujú sa **čisto vnútroštátne dôvody vylúčenia,** ktoré sú špecifikované v príslušnom oznámení alebo súťažných podkladoch? Ak je dokumentácia požadovaná v príslušnom oznámení alebo v súťažných podkladoch dostupná v elektronickom formáte, uveďte:	☐ Áno ☑ Nie (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....][31]
V prípade, že sa uplatňujú len čisto vnútroštátne dôvody vylúčenia, prijal hospodársky subjekt samočistiace opatrenia? **Ak ich prijal,** opíšte prijaté opatrenia:	☐ Áno ☐ Nie [.....]

[31] Zopakujte toľkokrát, koľkokrát je to potrebné.

Časť IV : Podmienky účasti

V súvislosti s podmienkami účasti (oddiel α alebo oddiely A až D tejto časti) hospodársky subjekt vyhlasuje, že :

α: GLOBÁLNY ÚDAJ PRE VŠETKY PODMIENKY ÚČASTI

Hospodársky subjekt by mal toto políčko vyplniť iba v prípade, ak verejný obstarávateľ alebo obstarávateľ uviedol v príslušnom oznámení alebo súťažných podkladoch uvedených v oznámení, že hospodársky subjekt môže vyplniť len oddiel α časti IV bez toho, aby musel vyplniť iné oddiely časti IV:

Splnenie všetkých podmienok účasti	**Odpoveď**
Spĺňa požadované podmienky účasti:	☑ Áno ☐ Nie

A: VHODNOSŤ

Hospodársky subjekt by mal poskytnúť informácie len vtedy, keď verejný obstarávateľ alebo obstarávateľ v príslušnom oznámení alebo v súťažných podkladoch uvedených v oznámení vyžadoval tieto podmienky účasti.

Vhodnosť	**Odpoveď**
1. **Je zapísaný v príslušných profesijných alebo obchodných registroch** vedených v členskom štáte, v ktorom má hospodársky subjekt sídlo[32]: Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	áno (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): Zoznam hospodárskych subjektov, č. zápisu: 2019/10-PO-F1458 Obchodný register Okresného súdu Bratislava I, odd.: Sa, vl. č. 2704/B (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [https://www.orsr.sk/vypis.asp?ID=31720&SID=2&P=0] [https://www.uvo.gov.sk/zoznam-hospodarskych-subjektov/detail/63?page=1&limit=20&sort=nazov&sort-dir=ASC&ext=0&ico=35810734&nazov=&obec=&registracneCislo=]
2. **V prípade zákaziek na poskytnutie služieb:** je osobitné povolenie	☐ Áno ☐ Nie Ak áno, spresnite, o ktoré povolenie alebo členstvo ide a uveďte, či

[32] Ako sa uvádza v prílohe XI k smernici 2014/24/EÚ; ***na hospodárske subjekty z určitých členských štátov sa môže vzťahovať povinnosť dodržiavať iné požiadavky stanovené v uvedenej prílohe.***

alebo členstvo v konkrétnej organizácii potrebné na to, aby bolo možné poskytovať príslušné služby v krajine usadenia hospodárskeho subjektu? Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	ich hospodársky subjekt má: [.....] ☐ Áno ☐ Nie (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

B: EKONOMICKÉ A FINANČNÉ POSTAVENIE

Hospodársky subjekt by mal poskytnúť informácie len vtedy, keď verejný obstarávateľ alebo obstarávateľ v príslušnom oznámení alebo v súťažných podkladoch uvedených v oznámení vyžadoval tieto podmienky účasti.

Ekonomické a finančné postavenie	**Odpoveď:**
1.a) **Ročný obrat** („všeobecný“) hospodárskeho subjektu za niekoľko finančných rokov vyžadovaný v príslušnom oznámení alebo v súťažných podkladoch je takýto: **A/alebo** 1.b) **Priemerný ročný obrat hospodárskeho subjektu za niekoľko rokov vyžadovaný v príslušnom oznámení alebo súťažných podkladoch je takýto[33]:** Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	(webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu):
2.a) Ročný („osobitný“) **obrat hospodárskeho subjektu v oblasti činnosti, na ktorú sa vzťahuje zmluva** a ktorá je špecifikovaná v príslušnom oznámení alebo súťažných podkladoch pre požadovaný počet finančných rokov je takýto: **A/alebo** 2.b) **Priemerný ročný obrat hospodárskeho subjektu v danej oblasti za niekoľko rokov vyžadovaný v príslušnom oznámení alebo súťažných podkladoch je takýto[34]:** Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	rok: [.....] obrat: [.....] [...] mena rok: [.....] obrat: [.....] [...] mena rok: [.....] obrat: [.....] [...] mena (počet rokov, priemerný obrat): [.....] obrat: [.....] [...] mena (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]
3. V prípade, že informácie týkajúce sa obratu (všeobecné alebo osobitné) nie sú k dispozícii za celé požadované obdobie, uveďte dátum, ku ktorému bol hospodársky subjekt zriadený alebo keď začal vykonávať svoju činnosť:	[.....]
4. Pokiaľ ide o **finančné ukazovatele[35]** uvedené v príslušnom oznámení alebo v súťažných podkladoch, hospodársky subjekt vyhlasuje, že skutočná hodnota pre požadovaný ukazovateľ je takáto: Ak je príslušná dokumentácia dostupná	(určenie požadovaného pomeru – pomer medzi x a y[36] – a hodnota): [.....],[.....][37] (webová adresa, vydávajúci orgán alebo subjekt,

[33] Len v prípade, ak je to povolené v príslušnom oznámení alebo v súťažných podkladoch.
[34] Len v prípade, ak je to povolené v príslušnom oznámení alebo v súťažných podkladoch.
[35] Napr. pomer medzi aktívami a pasívami.
[36] Napr. pomer medzi aktívami a pasívami.
[37] Zopakujte toľkokrát, koľkokrát je to potrebné.

v elektronickom formáte, uveďte:	presný odkaz na dokumentáciu): [.....][.....][.....]
5. Poistená suma **poistenia náhrady škôd vyplývajúcich z podnikateľského rizika** hospodárskeho subjektu je takáto: Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	[.....],[.....] mena (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]
6. Pokiaľ ide o **prípadné iné hospodárske alebo finančné požiadavky,** ktoré by mohli byť stanovené v príslušnom oznámení alebo súťažných podkladoch, hospodársky subjekt vyhlasuje, že: Ak je príslušná dokumentácia, ktorá **by mohla** byť stanovená v príslušnom oznámení alebo súťažných podkladoch, dostupná v elektronickom formáte, uveďte:	 (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

C: TECHNICKÁ A ODBORNÁ SPÔSOBILOSŤ

Hospodársky subjekt by mal poskytnúť informácie len vtedy, keď verejný obstarávateľ alebo obstarávateľ v príslušnom oznámení alebo súťažných podkladoch uvedených v oznámení vyžadoval tieto podmienky účasti.

Technická a odborná spôsobilosť	**Odpoveď:**
1.a) *Len v prípade verejných zákaziek na uskutočnenie stavebných prác:* Počas referenčného obdobia[38] hospodársky subjekt **vykonal tieto stavebné práce konkrétneho typu:** Ak je príslušná dokumentácia týkajúca sa uspokojivého vykonania a výsledkov najdôležitejších stavebných prác dostupná elektronicky, uveďte:	Počet rokov (toto obdobie je stanovené v príslušnom oznámení alebo súťažných podkladoch): [.....] Stavebné práce : [.....] webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

1.b) *Len v prípade **verejných zákaziek na dodanie tovaru a verejných zákaziek na poskytnutie služieb:*** Počas referenčného obdobia[39], hospodársky subjekt **doručil tieto hlavné zásielky stanoveného typu alebo poskytol tieto hlavné služby stanoveného typu:** Pri zostavovaní zoznamu, uveďte výšku súm, dátumy	Počet rokov (toto obdobie je stanovené v príslušnom oznámení alebo súťažných podkladoch): [.....]

[38] Verejní obstarávatelia môžu **vyžadovať** až päť rokov a **umožniť** skúsenosti z obdobia **viac** ako päť rokov.
[39] Verejní obstarávatelia môžu **požadovať** až tri rokov a **umožniť** skúsenosti z obdobia **viac** ako tri rokov.

a príjemcov, či už verejných alebo súkromných[40]:	
2. Hospodársky subjekt môže požiadať týchto technikov alebo technické orgány[41], najmä tých, ktorí sú zodpovední za kontrolu kvality: V prípade verejných zákaziek na uskutočnenie stavebných prác hospodársky subjekt bude môcť využiť týchto technikov alebo technické orgány na vykonanie práce:	[.....] [.....]
3. Hospodársky subjekt využíva tieto **technické zariadenia a opatrenia na zabezpečenie kvality a** jeho **výskumné zariadenia** sú:	.
4. Hospodársky subjekt bude môcť pri plnení zákazky uplatňovať tento systém **riadenia dodávateľského reťazca** a sledovací systém:	[.....]
5. **V prípade zložitých výrobkov alebo služieb, ktoré majú byť dodané alebo poskytnuté, alebo výnimočne v prípade výrobkov alebo služieb, ktoré sú požadované na osobitný účel:** Hospodársky subjekt **umožní** vykonanie **kontrol**[42] **výrobných kapacít** alebo **technickej spôsobilosti** hospodárskeho subjektu a v prípade potreby **študijných a výskumných prostriedkov,** ktoré má k dispozícii, a **kvality kontrolných opatrení.**	☐ Áno ☐ Nie
6. Tieto subjekty musia mať takéto **vzdelanie a odbornú kvalifikáciu:** a) Samotný poskytovateľ služieb alebo zhotoviteľ, **a/alebo** (v závislosti od požiadaviek uvedených v príslušnom oznámení alebo súťažných podkladoch) b) jeho riadiaci pracovníci:	a) [.....] b) [.....]
7. Hospodársky subjekt bude pri plnení zákazky schopný uplatňovať tieto **opatrenia environmentálneho riadenia:**	

[40] Inými slovami, **všetci** príjemcovia by mali byť uvedení v zozname a tento zoznam by mal obsahovať verejných aj súkromných klientov pre príslušné dodávky tovaru alebo príslušné služby.

[41] V prípade technikov alebo technických orgánov, ktoré priamo nepatria k podniku hospodárskeho subjektu, ale ktorých kapacity hospodársky subjekt využíva, ako sa stanovuje v časti II, oddiel C, sa musia vyplniť samostatné formuláre jednotného európskeho dokumentu pre obstarávanie.

[42] Kontrolu má vykonávať verejný obstarávateľ alebo v prípade, že verejný obstarávateľ vyjadrí súhlas, v jeho mene príslušný úradný orgán štátu, v ktorom je poskytovateľ služieb alebo dodávateľ usadený.

8. **Ročný priemerný počet zamestnancov** hospodárskeho subjektu a počet riadiacich pracovníkov za posledné tri roky sú takéto:	Rok, ročný priemerný počet zamestnancov: [.....],[.....], [.....],[.....], [.....],[.....], Rok, počet riadiacich pracovníkov: [.....],[.....], [.....],[.....], [.....],[.....],
9. Tieto **nástroje, strojové alebo technické vybavenie** bude mať hospodársky subjekt k dispozícii na realizáciu zákazky:	[.....]
10. Hospodársky subjekt **má v úmysle prípadne zadať subdodávateľom**[43] túto **časť (t. j. percento) zákazky:**	[30%]
11. V prípade **verejných zákaziek na dodanie tovaru:** Hospodársky subjekt poskytne požadované vzorky, opisy alebo fotografie tovaru, ktorý sa má dodať, ku ktorým nemusia byť priložené osvedčenia o pravosti. V náležitosti prípadných hospodárskych subjektov okrem toho vyhlasuje, že bude poskytovať požadované osvedčenie o pravosti. Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	☐ Áno ☐ Nie ☐ Áno ☐ Nie webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]
12. V prípade **verejných zákaziek na dodanie tovaru:** Môže hospodársky subjekt predložiť požadované **osvedčenia** vydané oficiálnymi **ústavmi alebo agentúrami na kontrolu kvality,** ktoré majú priznanú právomoc vydávať potvrdenia o zhode výrobkov, ktorá je jasne určená odkazmi na technické špecifikácie alebo normy, ktoré sú stanovené v príslušnom oznámení alebo v súťažných podkladoch? **Ak nie,** vysvetlite prečo a uveďte, ktoré iné dôkazné prostriedky možno poskytnúť. Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	☐ Áno ☐ Nie [.....] webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

[43] Upozorňujeme, že ak hospodársky subjekt **rozhodol**, že časť zákazky zadá subdodávateľom, a využíva kapacity subdodávateľa, aby splnil túto časť, potom za týchto subdodávateľov vyplňte samostatný jednotný európsky dokument pre obstarávanie, pozri časť II, oddiel C.

D: SYSTÉMY ZABEZPEČENIA KVALITY A NORMY ENVIRONMENTÁLNEHO MANAŽÉRSTVA

Hospodársky subjekt by mal poskytovať informácie len vtedy, ak verejný obstarávateľ alebo obstarávateľ v príslušnom oznámení alebo súťažných podkladoch uvedených v oznámení vyžaduje systém zabezpečenia kvality a/alebo normy environmentálneho manažérstva.

Systém zabezpečenia kvality a normy environmentálneho manažérstva	**Odpoveď:**
Bude môcť hospodársky subjekt predložiť **osvedčenia** vydané nezávislými orgánmi, v ktorých sa potvrdzuje, že hospodársky subjekt spĺňa požadované **normy zabezpečenia kvality** vrátane prístupu pre osoby so zdravotným postihnutím? **Ak nie,** vysvetlite prečo a uveďte, ktoré iné dôkazné prostriedky týkajúce sa systému zabezpečenia kvality možno poskytnúť: Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	☐ Áno ☐ Nie [.....][.....] webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]
Bude môcť hospodársky subjekt predložiť **osvedčenia** vydané nezávislými orgánmi, v ktorých sa potvrdzuje, že hospodársky subjekt spĺňa požadované **systémy alebo normy environmentálneho manažérstva?** **Ak nie,** vysvetlite prečo a uveďte, ktoré iné dôkazné prostriedky týkajúce sa **systémov alebo noriem environmentálneho manažérstva** možno poskytnúť: Ak je príslušná dokumentácia dostupná v elektronickom formáte, uveďte:	☐ Áno ☐ Nie [.....][.....] webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....]

Časť V: Zníženie počtu kvalifikovaných záujemcov

Hospodársky subjekt by mal poskytnúť informácie len vtedy, ak verejný obstarávateľ alebo obstarávateľ stanovil objektívne a nediskriminačné kritéria alebo pravidlá, ktoré sa budú uplatňovať s cieľom obmedziť počet záujemcov, ktorí sa vyzvú na predloženie ponuky alebo na vedenie dialógu. Tieto informácie, ktoré sa môžu doplniť požiadavkami týkajúcimi sa (druhov) osvedčenia alebo foriem listinných dôkazov, ktoré je potrebné predložiť, ak existujú, sú stanovené v príslušnom oznámení alebo v súťažných podkladoch uvedených v oznámení. **Len v prípade užších súťaží, súťažných konaní s rokovaním, súťažných dialógov a inovatívnych partnerstiev:**

Hospodársky subjekt vyhlasuje, že:

Zníženie počtov	Odpoveď:
Spĺňa objektívne a nediskriminačné kritéria alebo pravidlá, ktoré sa budú uplatňovať s cieľom obmedziť počet záujemcov, a to týmto spôsobom:	[.....]
V prípade, ak sa vyžadujú určité osvedčenia alebo ostatné formy listinných dôkazov, pri **každom** uveďte, či má hospodársky subjekt požadované dokumenty:	☐ Áno ☐ Nie [45]
Ak sú niektoré z týchto osvedčení alebo foriem listinných dôkazov k dispozícii v elektronickom formáte[44], uveďte pre každý z nich:	webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu): [.....][.....][.....][46]

[44] Jasne uveďte, ktorej položky sa odpoveď týka.
[45] Zopakujte toľkokrát, koľkokrát je to potrebné.
[46] Zopakujte toľkokrát, koľkokrát je to potrebné.

Časť VI: Záverečné vyhlásenia

Podpísaný/podpísaní vyhlasuje/ú, že informácie uvedené v častiach II – V sú pravdivé a správne a, že boli uvedené pri plnom vedomí následkov závažného skresľovania skutočností.

Podpísaný/podpísaní vyhlasuje/ú, že na požiadanie okamžite predloží/ia uvedené osvedčenia a ostatné formy listinných dôkazov, okrem prípadov, keď:

a) *verejný obstarávateľ alebo obstarávateľ má možnosť získať sprievodnú dokumentáciu priamo na základe prístupu do vnútroštátnej databázy v ktoromkoľvek členskom štáte, ktorá je dostupná bezplatne*[47]*, alebo*
b) *najneskôr do 18. októbra 2018*[48] *bude mať verejný obstarávateľ alebo obstarávateľ príslušnú dokumentáciu k dispozícii.*

Ja/my, dolupodpísaný/dolupodpísaní, formálne súhlasím/súhlasíme, aby [Národné centrum zdravotníckych informácií, IČO: 00165387, Lazaretská 26, 81109 Bratislava - mestská časť Staré Mesto] získala prístup k podporným dokumentom obsahujúcim informácie, ktoré som/sme poskytol/poskytli v tomto jednotnom európskom dokumente pre obstarávanie na účely verejnej súťaže vyhlásenej v Úradnom vestníku Európskej únie číslo 2022/S 114-321736 zo dňa 15.06.2022 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod zn. 29600 – MSS s názvom: Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS).

Dátum, miesto a, ak sa to vyžaduje alebo je to potrebné, podpis:

V Bratislave, 19.08.2022

[redacted]

[47] Pod podmienkou, že hospodársky subjekt poskytol potrebné informácie *(webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu), ktoré umožňujú verejnému obstarávateľovi alebo obstarávateľovi, aby tak urobili. V prípade potreby to musí byť sprevádzané príslušným súhlasom s takýmto prístupom.*

[48] V závislosti od vnútroštátneho vykonávania článku 59 ods. 5 druhého pododseku smernice 2014/24/EÚ.

Čestné vyhlásenie o subdodávateľoch

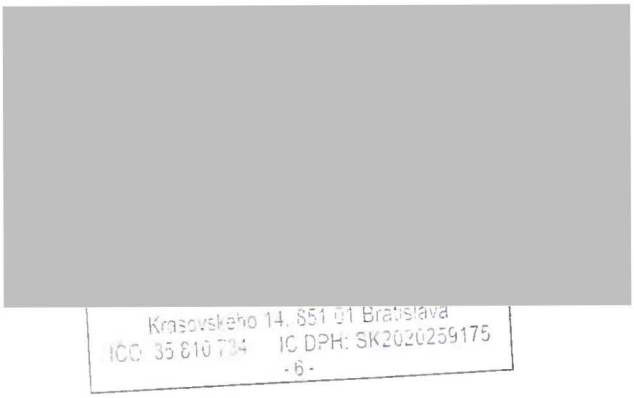
Dolu podpísaná Ing. Zuzana Škodová Prochotská, člen predstavenstva spoločnosti DATALAN, a.s., týmto vyhlasuje, že

plnenie časti predmetu zákazky máme v úmysle zabezpečovať prostredníctvom nasledujúcich subdodávateľov:

TEMPEST a.s.
Krasovského 14
Bratislava - mestská časť Petržalka 851 01
IČO: 31 326 650

Podiel plnenia: 30 %

V Bratislave, dňa 19.08.2022



DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

7 DOKLADY INÉ OSOBY

TEMPEST a.s.
Krasovského 14
Bratislava - mestská časť Petržalka 851 01
IČO: 31 326 650

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

Jednotný európsky dokument pre obstarávanie (JED)

Časť I: Informácie týkajúce sa postupu verejného obstarávania a verejného obstarávateľa alebo obstarávateľa

Informácie o uverejnení

Číslo oznámenia v Úradnom vestníku S:

2022/S 114-321736

Národný vestník

29600 - MSS

Ak výzva na súťaž nebola zverejnená v Úradnom vestníku Európskej únie alebo ak ju nie je potrebné vo vestníku zverejniť, verejný obstarávateľ alebo obstarávateľ musí vyplniť údaje umožňujúce jednoznačnú identifikáciu postupu verejného obstarávania (napr. odkaz na uverejnenie na vnútroštátnej úrovni).

Identifikácia obstarávateľa

Úradný názov:

Národné centrum zdravotníckych informácií Vnútroštátne identifikačné číslo: 00165387 Lazaretská 26, 81109 Bratislava - mestská časť Staré Mesto Kód NUTS: SK010 Slovensko Email: Katarina.GrejtakBednarikova@nczisk.sk

Krajina:

Slovensko

Informácie o postupe verejného obstarávania

Druh postupu:

Verejná súťaž

Názov:

Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)

Stručný opis:

Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)

Referenčné číslo spisu, ktoré pridelil verejný obstarávateľ alebo obstarávateľ (ak existuje):

NCZI-RISEZ-2022-VS

Časť II: Informácie týkajúce sa hospodárskeho subjektu

A: Informácie o hospodárskom subjekte

Názov:

TEMPEST a.s.

Ulica a číslo:

Krasovského 14

PSČ:

85101 - mestská časť Petržlka

Mesto:

Bratislava

Krajina:

Slovensko

Internetová adresa (webová adresa) (ak je k dispozícii):

www.tempest.sk

E-mail:

Telefón:

Kontaktná osoba alebo osoby:

Ing. Andrej Bališ, člen predstavenstva, Peter Vyboch Manager

Identifikačné číslo pre DPH, ak sa uplatňuje:

SK2020327716

Ak sa identifikačné číslo pre DPH neuplatňuje, uveďte iné národné identifikačné číslo, ak sa vyžaduje a je uplatniteľné

-

Hospodársky subjekt je mikropodnik, malý podnik alebo stredný podnik?

○Áno

●Nie

Len v prípade, ak je verejné obstarávanie vyhradené: je hospodársky subjekt chránená pracovná dielňa, „sociálny podnik“ alebo zabezpečí plnenie zákazky v rámci programov chránených pracovných miest?

○Áno

●Nie

V príslušných prípadoch: je hospodársky subjekt zapísaný v úradnom zozname schválených hospodárskych subjektov alebo má rovnocenné osvedčenie (napríklad v rámci národného (pred)kvalifikačného systému)?

●Áno

○Nie

- Odpovedzte na zvyšné časti tohto oddielu, oddielu B a v príslušnom prípade oddielu C tejto časti, v prípade potreby vyplňte časť V a v každom prípade vyplňte a podpíšte časť VI.

a) V príslušnom prípade uveďte príslušné číslo zápisu alebo osvedčenia:

2019/10-PO-D1498

b) Ak je osvedčenie o zápise alebo osvedčenie k dispozícii v elektronickom formáte, uveďte:

https://www.uvo.gov.sk/zoznam-hospodarskych-subjektov/detail/153?page=1&limit=20&sort=nazov&sort-dir=ASC&ext=0&ico=31326650&nazov=&obec=&registracneCislo=

c) Uveďte odkazy, na ktorých je založený zápis alebo osvedčenie, a v príslušnom prípade klasifikáciu získanú v úradnom zozname:

https://www.uvo.gov.sk/zoznam-hospodarskych-subjektov/detail/153?page=1&limit=20&sort=nazov&sort-dir=ASC&ext=0&ico=31326650&nazov=&obec=&registracneCislo=

d) Vzťahuje sa zápis alebo osvedčenie na všetky požadované podmienky účasti?

○Áno

●Nie

Zúčastňuje sa hospodársky subjekt na postupe obstarávania spoločne s inými subjektmi?

○Áno

●Nie

V prípade potreby označenie série(-ií), pre ktoré chce hospodársky subjekt predložiť ponuky:

-

B: Informácie o zástupcoch hospodárskeho subjektu #1

- V príslušnom prípade uveďte meno (-á) a adresu (-y) osoby (osôb) oprávnenej zastupovať hospodársky subjekt na účely tohto postupu obstarávania:

Meno
Andrej
Priezvisko
Bališ
Dátum narodenia
Miesto narodenia
Ulica a číslo:
PSČ:
Mesto:
Krajina:
Slovensko
E-mail:
Telefón:
Pozícia/zastupujúci:
člen predstavenstva
Ak je to potrebné, uveďte podrobné informácie o zastúpení (jeho forma, rozsah, účel...):
-

C: Informácie o využívaní kapacít iných subjektov

Využíva hospodársky subjekt kapacity iných subjektov, aby mohol splniť podmienky účasti stanovené v časti IV a prípadne kritériá a pravidlá stanovené ďalej v časti V?
○Áno
●Nie

D: Informácie týkajúce sa subdodávateľov, ktorých kapacity hospodársky subjekt nevyužíva

- (Tento oddiel sa vyplní len vtedy, ak verejný obstarávateľ alebo obstarávateľ tieto informácie výslovne vyžaduje).

Má hospodársky subjekt v úmysle zadať niektorú časť zákazky tretím stranám?

○Áno

●Nie

- Ak verejný obstarávateľ alebo obstarávateľ výslovne požiada o tieto informácie okrem informácií podľa časti I, uveďte informácie požadované v oddiele A a B tejto časti a časti III pre každého z príslušných subdodávateľov (kategóriu subdodávateľov).

Časť III: Dôvody na vylúčenie

A: Dôvody týkajúce sa odsúdení za trestný čin

V článku 57 ods. 1 smernice 2014/24/EÚ sa stanovujú tieto dôvody vylúčenia

Účasť v zločineckej organizácii

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za účasť v zločineckej organizácii konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje? V zmysle článku 2 rámcového rozhodnutia Rady 2008/841/SVV z 24. októbra 2008 o boji proti organizovanému zločinu (Ú. v. EÚ L 300, 11.11.2008, s. 42).

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Korupcia

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať,

prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za korupciu konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje?
V zmysle článku 3 Dohovoru o boji proti korupcii úradníkov Európskych spoločenstiev alebo úradníkov členských štátov Európskej únie, Ú. v. ES C 195, 25.6.1997, s. 1 a článku 2 ods. 1 rámcového rozhodnutia Rady 2003/568/SVV z 22. júla 2003 o boji proti korupcii v súkromnom sektore (Ú. v. EÚ L 192, 31.7.2003, s. 54). Tento dôvod na vylúčenie zahŕňa aj korupciu v zmysle vnútroštátnych právnych predpisov verejného obstarávateľa (obstarávateľa) alebo hospodárskeho subjektu.

Vaša odpoveď?
○Áno
●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?
○Áno
●Nie

Podvod

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za podvod konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje?
V zmysle článku 1 Dohovoru o ochrane finančných záujmov Európskych spoločenstiev (Ú. v. ES C 316, 27.11.1995, s. 48).

Vaša odpoveď?
○Áno
●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?
○Áno
●Nie

Teroristické trestné činy alebo trestné činy spojené s teroristickými činnosťami

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za teroristické trestné činy alebo trestné činy spojené s teroristickými činnosťami konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje? V zmysle článkov 1 a 3 rámcového rozhodnutia Rady z 13. júna 2002 o boji proti terorizmu (Ú. v. ES L 164, 22.6.2002, s. 3). Tento dôvod na vylúčenie zahŕňa aj podnecovanie alebo napomáhanie alebo navádzanie alebo pokus o spáchanie trestného činu v súlade s článkom 4 uvedeného rámcového rozhodnutia.

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Pranie špinavých peňazí alebo financovanie terorizmu

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za pranie špinavých peňazí alebo financovanie terorizmu konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje? V zmysle článku 1 smernice Európskeho parlamentu a Rady 2005/60/ES z 26. októbra 2005 o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu (Ú. v. EÚ L 309, 25.11.2005, s. 15).

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Detská práca a iné formy obchodovania s ľuďmi

Bol samotný hospodársky subjekt alebo osoba, ktorá je členom jeho správneho, riadiaceho alebo kontrolného orgánu alebo ktorá v ňom má právomoc zastupovať, prijímať rozhodnutia alebo vykonávať v ňom kontrolu, odsúdený za detskú prácu a iné formy obchodovania s ľuďmi konečným rozsudkom vyneseným najviac pred piatimi rokmi, alebo v prípade ktorého sa lehota vylúčenia stanovená priamo v rozsudku naďalej uplatňuje? V zmysle článku 2 smernice Európskeho parlamentu a Rady 2011/36/EÚ z 5. apríla 2011 o prevencii obchodovania s ľuďmi a boji proti nemu a o ochrane obetí obchodovania, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/629/SVV (Ú. v. EÚ L 101, 15.4.2011, s. 1).

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

B: Dôvody týkajúce sa platby daní alebo príspevkov na sociálne zabezpečenie

V článku 57 ods. 2 smernice 2014/24/EÚ sa stanovujú tieto dôvody vylúčenia

Platba daní

Porušil hospodársky subjekt svoje povinnosti týkajúce sa platby daní v krajine, v ktorej má sídlo, a v členskom štáte verejného obstarávateľa alebo obstarávateľa, ak je iná ako krajina sídla?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Platba príspevkov na sociálne zabezpečenie

Porušil hospodársky subjekt svoje povinnosti týkajúce sa platby príspevkov na sociálne zabezpečenie v krajine, v ktorej má sídlo, a v členskom štáte verejného obstarávateľa alebo obstarávateľa, ak je iná ako krajina sídla?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

C: Dôvody týkajúce sa konkurzu, konfliktu záujmov alebo odborného pochybenia

V článku 57 ods. 4 smernice 2014/24/EÚ sa stanovujú tieto dôvody vylúčenia

Porušenie povinností v oblasti environmentálneho práva

Porušil hospodársky subjekt, podľa svojich vedomostí, svoje povinnosti v oblasti environmentálneho práva? Ako je uvedené na účely tohto obstarávania vo vnútroštátnom práve, v príslušnom oznámení alebo v súťažných podkladoch alebo v článku 18 ods. 2 smernice 2014/24/EÚ.

Vaša odpoveď?

○Áno

●Nie

Porušenie povinností v oblasti sociálneho práva

Porušil hospodársky subjekt, podľa svojich vedomostí, svoje povinnosti v oblasti sociálneho práva? Ako je uvedené na účely tohto obstarávania vo vnútroštátnom práve, v príslušnom oznámení alebo v súťažných podkladoch alebo v článku 18 ods. 2 smernice 2014/24/EÚ.

Vaša odpoveď?

○Áno

●Nie

Porušenie povinností v oblasti pracovného práva

Porušil hospodársky subjekt, podľa svojich vedomostí, svoje povinnosti v oblasti pracovného práva? Ako je uvedené na účely tohto obstarávania vo vnútroštátnom práve, v príslušnom oznámení alebo v súťažných podkladoch alebo v článku 18 ods. 2 smernice 2014/24/EÚ.

Vaša odpoveď?

○Áno

●Nie

Úpadok

Je hospodársky subjekt v úpadku?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Konkurz

Je hospodársky subjekt v konkurze alebo v likvidácii?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Vyrovnávacie konanie

Je hospodársky subjekt vo vyrovnávacom konaní?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Podobná situácia ako úpadok podľa vnútroštátneho práva

Je hospodársky subjekt v akejkoľvek podobnej situácii ako úpadok vyplývajúcej z podobného konania podľa vnútroštátnych zákonov a iných právnych predpisov?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Aktíva spravované likvidátorom

Spravuje aktíva hospodárskeho subjektu likvidátor alebo súd?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Pozastavené podnikateľské činnosti

Sú podnikateľské činnosti hospodárskeho subjektu pozastavené?

Vaša odpoveď?

○Áno

●Nie

Sú tieto informácie dostupné bezplatne pre orgány z databázy členského štátu EÚ?

○Áno

●Nie

Dohody s inými hospodárskymi subjektmi s cieľom narušiť hospodársku súťaž

Uzatvoril hospodársky subjekt dohody s inými hospodárskymi subjektmi s cieľom narušiť hospodársku súťaž?

Vaša odpoveď?

○Áno

●Nie

Dopustenie sa závažného odborného pochybenia

Dopustil sa hospodársky subjekt závažného odborného pochybenia? V prípade potreby pozri definície vo vnútroštátnom práve, príslušnom oznámení alebo v súťažných podkladoch.

Vaša odpoveď?

○Áno

●Nie

Konflikt záujmov z dôvodu účasti na postupe obstarávania

Vie hospodársky subjekt o akomkoľvek konflikte záujmov, ako sa uvádza vo vnútroštátnych právnych predpisoch, príslušnom oznámení alebo súťažných podkladoch, vzhľadom na svoju účasť na postupe obstarávania?

Vaša odpoveď?

○Áno

●Nie

Priama alebo nepriama účasť na príprave tohto postupu obstarávania

Poskytoval hospodársky subjekt alebo podnik súvisiaci s hospodárskym subjektom poradenstvo verejnému obstarávateľovi alebo obstarávateľovi alebo bol iným spôsobom zapojený do prípravy postupu obstarávania?

Vaša odpoveď?

○Áno

●Nie

Predčasné ukončenie zmluvy, škody alebo iné porovnateľné sankcie

Stalo sa hospodárskemu subjektu, že predchádzajúca verejná zákazka, predchádzajúca verejná zákazka s obstarávateľom alebo predchádzajúca koncesná zmluva bola ukončená predčasne, alebo že došlo k škode alebo iným porovnateľným sankciám v súvislosti s touto predchádzajúcou zákazkou?

Vaša odpoveď?

○Áno

●Nie

Skreslenie informácií, zadržanie informácií, neschopnosť predložiť požadované dokumenty a získanie dôverných informácií o tomto postupe

Nachádza sa hospodársky subjekt v jednej z týchto situácií?:

a) je vinný zo závažného skreslenia pri predkladaní informácií vyžadovaných na overenie neexistencie dôvodov na vylúčenie alebo splnenia podmienok účasti,

b) zadržal takéto informácie,

c) nebol schopný bezodkladne predložiť podporné dokumenty požadované verejným obstarávateľom alebo obstarávateľom a

d) nenáležite ovplyvňoval rozhodovací proces verejného obstarávateľa alebo obstarávateľa s cieľom získať dôverné informácie, ktoré mu môžu poskytnúť nenáležité výhody v rámci postupu verejného obstarávania, alebo z nedbalosti neposkytol zavádzajúce informácie, ktoré môžu mať podstatný vplyv na rozhodnutia týkajúce sa vylúčenia, výberu alebo zadania zákazky?

Vaša odpoveď?

○Áno

●Nie

Časť IV: Podmienky účasti

α: Globálny údaj pre všetky podmienky účasti

V súvislosti s podmienkami účasti hospodársky subjekt vyhlasuje, že

Spĺňa všetky požadované podmienky účasti

Vaša odpoveď?

●Áno

○Nie

Koniec

Časť VI: Záverečné vyhlásenia

Podpísaný(podpísaní) vyhlasuje(-ú), že informácie uvedené v častiach II – V sú pravdivé a správne a že boli uvedené pri plnom vedomí následkov závažného skresľovania skutočností.

Podpísaný(podpísaní) vyhlasuje(-ú), že na požiadanie okamžite predloží(-ia) uvedené osvedčenia a ostatné formy listinných dôkazov, okrem prípadov, keď:

a) verejný obstarávateľ alebo obstarávateľ má možnosť získať sprievodnú dokumentáciu priamo na základe prístupu do vnútroštátnej databázy v ktoromkoľvek členskom štáte, ktorá je dostupná bezplatne [pod podmienkou, že hospodársky subjekt poskytol potrebné informácie (webová adresa, vydávajúci orgán alebo subjekt, presný odkaz na dokumentáciu), ktoré umožňujú verejnému obstarávateľovi alebo obstarávateľovi, aby tak urobili. V prípade potreby to musí byť sprevádzané príslušným súhlasom s takýmto prístupom], alebo

b) najneskôr do 18. októbra 2018 (v závislosti od vnútroštátnej implementácie článku 59 ods. 5 druhého pododseku smernice 2014/24/EÚ) bude mať verejný obstarávateľ alebo obstarávateľ príslušnú dokumentáciu k dispozícii.

Ja(my), dolupodpísaný(dolupodpísaní) formálne súhlasím(-e), aby [identifikujte verejného obstarávateľa alebo obstarávateľa, ako je stanovený v časti I oddiele A] získal prístup k podporným dokumentom obsahujúcim informácie, ktoré som(sme) poskytol(poskytli) v [identifikujte príslušnú časť/oddiel/ body] tohto jednotného európskeho dokumentu pre obstarávanie na účely [identifikujte postup obstarávania: (opis zhrnutia, odkaz na uverejnenie v Úradnom vestníku Európskej únie, referenčné číslo)].

Dátum, miesto a, ak sa to vyžaduje alebo je to potrebné, podpis(-y):

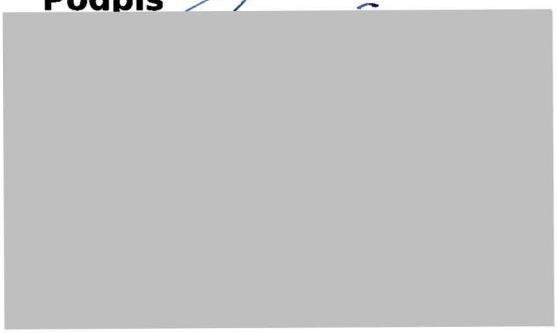
Dátum

19-08-2022

Miesto

Bratislava

Podpis



Zmluva

na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti

na plnenie zákazky:

„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"

uzavretá v zmysle § 34 ods. 3 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO")

- ďalej len „zmluva"

Článok I.
Zmluvné strany

Uchádzač: DATALAN, a.s.
Sídlo: Krasovského 14, Bratislava – mestská časť Petržalka 851 01
Štatutárny orgán: Ing. Zuzana Škodová Prochotská, člen predstavenstva
Bankové spojenie: Tatra banka, a.s.
Číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
IČO: 35 810 734
DIČ: 2020259175
IČ DPH: SK2020259175
Právna forma: akciová spoločnosť zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B
(ďalej len „uchádzač")

Poskytovateľ: TEMPEST a.s.
Sídlo: Krasovského 14, Bratislava - mestská časť Petržalka 851 01
Štatutárny orgán: Ing. Andrej Bališ, člen predstavenstva
Bankové spojenie: Tatra banka
IBAN: SK13 1100 0000 0026 2004 1080
IČO: 31 326 650
DIČ: 2020327716
IČ DPH: SK 2020327716
Právna forma: spoločnosť s ručením obmedzeným zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 3771/B
(ďalej len „poskytovateľ")

- ďalej tiež uchádzač a poskytovateľ spolu ako „zmluvné strany"

Článok II.
Úvodné ustanovenia

1. **Uchádzač** má záujem o účasť vo verejnej súťaži na predmet zákazky: „Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)" verejného obstarávateľa: Národné centrum zdravotníckych informácií, IČO: 00165387, Lazaretská 26, 81109 Bratislava - mestská časť Staré Mesto, Slovensko (ďalej len „verejný obstarávateľ"), ktorá bola vyhlásená vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod značkou 29600-MSS (ďalej len „oznámenie o vyhlásení VO"); ďalej len „verejné obstarávanie", a za tým účelom predloží, resp. predložil verejnému obstarávateľovi ponuku.
2. **Poskytovateľ** je osoba, ktorá bez ohľadu na právny vzťah k uchádzačovi poskytuje uchádzačovi technické a odborné kapacity na preukázanie technickej alebo odbornej spôsobilosti uchádzača pre zákazku špecifikovanú v bode 1 tohto článku zmluvy, k čomu sa touto zmluvou za podmienok v nej dohodnutých zaväzuje.
3. **Technickými a odbornými kapacitami** sa rozumie poskytnutie dokladov podľa časti A.2 Súťažných podkladov, časť 3. Technická a odborná spôsobilosť

- bod 1) Referencie podľa § 34 ods. 1 písm. a) ZVO:
  zoznam poskytnutých služieb za predchádzajúcich päť rokov od vyhlásenia verejného obstarávania s uvedením cien, lehôt dodania a odberateľov; dokladom je referencia, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ podľa zákona o verejnom obstarávaní v rozsahu:
  - podbod 1.1. písm. a)
  realizácia zákaziek poskytnutých služieb rovnakého alebo typovo podobného charakteru a zložitosti ako je predmet zákazky **pre Dielo**, a to preukázaním poskytnutia služieb v kumulatívnej hodnote minimálne 2.750.000,00 EUR bez DPH, pričom hodnota aspoň jednej zákazky musí byť v minimálnom objeme 1.000.000,00 EUR bez DPH/zákazka
  - podbod 1.1. písm. b)
  realizácia zákaziek poskytnutých služieb rovnakého alebo typovo podobného charakteru a zložitosti ako je predmet zákazky **pre služby SLA k Dielu,** a to preukázaním uskutočnenia služieb v kumulatívnej hodnote minimálne 5.000.000,00 EUR bez DPH, pričom hodnota aspoň jednej zákazky musí byť v minimálnom objeme 2.500.000,00 EUR bez DPH/zákazka

- bod 2) Kľúčoví experti podľa § 34 ods. 1 písm. g) ZVO:

Kľúčový expert č. 4 – Hlavný architekt pre novú architektúru
- minimálne päť rokov odbornej praxe v oblasti návrhu architektúry riešenia informačných technológií;
- minimálne dve profesionálne praktické skúsenosti v oblasti informačných systémov alebo návrhu architektúry riešenia informačných systémov v kontajnerizovanej podobe architektúry
- platný certifikát pre oblasť návrhu architektúry IT TOGAF úrovne Certified (Level 2) alebo ekvivalentný vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

Kľúčový expert č. 9 – Hlavný databázový špecialista pre novú architektúru
- minimálne päť rokov odbornej praxe v oblasti tvorby databáz
- skúsenosti s migráciou dát
- minimálne dve profesionálne praktické skúsenosti v oblasti tvorby a migrácie dát komplexných databázových systémov v kontajnerizovanej podobe

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

Kľúčový expert č. 10 – Špecialista pre oblasť integrácie
- minimálne päť rokov odbornej praxe v oblasti návrhu a implementácie integračných rozhraní informačných systémov
- minimálne päť rokov odbornej praxe v oblasti návrhu a implementácie extract, transform load (ETL) alebo v oblasti dátovej kvality;
- minimálne dve profesionálne praktické skúsenosti v oblasti analýzy, návrhu, implementácie a modelovania integračných rozhraní IS a ETL alebo v oblasti dátovej kvality, pričom každá z uvedených profesionálnych praktických skúseností bola (či už v oblasti analýzy, návrhu, implementácie a modelovania integračných rozhraní IS a ETL alebo v oblasti dátovej kvality) v cloud native prostredí (Kubernetes/Openshift/Rancher alebo ekvivalent)

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

Kľúčový expert č. 12 – Špecialista pre oblasť biznis procesov
- minimálne päť rokov odbornej praxe v oblasti návrhu a automatizácie biznis procesov;
- minimálne dve preukázateľné profesionálne praktické skúsenosti v oblasti redizajnu a automatizácie biznis procesov

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

Kľúčový expert č. 13 – Špecialista pre oblasť platformy orchestrácie kontajnerov
- minimálne 3 roky odbornej praxe v oblasti využívania platformy orchestrácie kontajnerov;
- minimálne dve preukázateľné praktické skúsenosti s využívaním orchestračnej platformy pre kontajnery

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

Kľúčový expert č. 14 – Špecialista pre oblasť prevádzky informačných technológií
- minimálne 5 rokov odbornej praxe v oblasti riadenia procesov IT služieb alebo v oblasti riadenia projektov v oblasti prevádzky informačných technológií,
- minimálne dve preukázateľné praktické skúsenosti v oblasti prevádzky informačných technológií;
- platný certifikát v oblasti riadenia IT služieb napr. ITIL Practitioner alebo ekvivalentný vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou

preukáže predložením dokladov podľa bodu 2.2. časti 3. v A.2. Súťažných podkladov;

(ďalej tiež „oprávnenia").

Článok III.
Účel zmluvy

1. Účelom tejto zmluvy je preukázanie technickej alebo odbornej spôsobilosti uchádzača v rámci zákazky špecifikovanej v článku II. bod 1 tejto zmluvy oprávneniami poskytovateľa.
2. Zmluvné strany uzatvárajú túto zmluvu podľa § 34 ods. 3 ZVO, na základe ktorého uchádzač môže na preukázanie technickej alebo odbornej spôsobilosti využiť technické a odborné kapacity inej osoby, bez ohľadu na ich právny vzťah. Uchádzač sa rozhodol v chýbajúcom rozsahu využiť oprávnenia

poskytovateľa a poskytovateľ sa uchádzačovi touto zmluvou zaväzuje, že oprávnenia mu poskytne počas celého trvania zmluvného vzťahu s verejným obstarávateľom. Poskytovateľ týmto dáva súhlas a uchádzač prehlasuje, že pri plnení zmluvy s verejným obstarávateľom bude skutočne používať kapacity poskytovateľa poskytnuté na základe tejto zmluvy.

3. Poskytovateľ oprávnení spĺňa podmienky účasti spôsobom a v rozsahu uvedenom v súťažných podkladoch /v oznámení o vyhlásení VO v znení ich vysvetľovania a doplnenia, podľa § 34 ods. 1 písm. a) a g) ZVO v rozsahu podľa článku II. bod 3. tejto Zmluvy viažuce sa k predmetu zákazky špecifikovanej v článku II. bod 1. tejto zmluvy.
4. Účelom tejto zmluvy je tiež potvrdenie zmluvných strán, že poskytovateľ spĺňa podmienky účasti podľa § 32 ods. 1 ZVO, neexistujú u neho dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až h) a ods. 7 ZVO a má oprávnenie dodávať tovar a poskytovať službu vo vzťahu k tej časti predmetu zákazky, na ktorú boli kapacity uchádzačovi poskytnuté. Poskytovateľ zároveň vyhlasuje, že je registrovaný v Registri partnerov verejného sektora.

Článok IV.
Spoločné a záverečné ustanovenia

1. Táto zmluva nadobúda platnosť a účinnosť v deň, v ktorom bude podpísaná oboma zmluvnými stranami.
2. Túto zmluvu je možné meniť len písomne, dodatkami k zmluve podpísanými oprávnenými osobami oboch zmluvných strán. Akceptačná lehota na prijatie návrhu dodatku k tejto zmluve je 15 (slovom: pätnásť) dní odo dňa jeho doručenia príslušnej zmluvnej strane ako adresátovi.
3. Zmluvné strany sa dohodli, že návrhy dodatkov k tejto zmluve, ako aj ostatnú korešpondenciu týkajúcu sa tejto zmluvy, si budú doručovať do podateľne v sídle tej zmluvnej strany, ktorá je adresátom.
4. Táto zmluva je vyhotovená v troch rovnopisoch, z ktorých každá zmluvná strana dostane jeden rovnopis a jeden rovnopis sa predloží verejnému obstarávateľovi.
5. Táto zmluva zaniká bez potreby akéhokoľvek ďalšieho písomného právneho úkonu v deň, kedy bude uchádzačovi doručené oznámenie verejného obstarávateľa o neúspechu vo verejnom obstarávaní na zákazku špecifikovanú v článku II. bod 1 tejto zmluvy (ďalej len „oznámenie o neúspechu"), za podmienky, že uchádzač neuplatní žiaden z revíznych postupov v zmysle ZVO alebo v prípade zrušenia verejného obstarávania zo strany verejného obstarávateľa (ďalej len „oznámenie o zrušení").
6. Na účel uvedený v bode 5 tohto článku sa uchádzač zaväzuje poskytovateľovi písomne alebo elektronicky formou e-mailu oznámiť, že neuspel vo verejnom obstarávaní na zákazku špecifikovanú v článku II. bod 1 tejto zmluvy a že nevyužil, prípadne v ZVO stanovenej lehote nemieni využiť žiaden z revíznych postupov v zmysle ZVO. Uchádzač skutočnosti uvedené v tomto bode oznámi poskytovateľovi do 10 (slovom: desiatich) dní odo dňa doručenia oznámenia o neúspechu alebo oznámenia o zrušení.
7. Poskytovateľ podpisom tejto zmluvy potvrdzuje, že si je vedomý svojej povinnosti poskytnúť oprávnenia uchádzačovi v rozsahu, po dobu a spôsobom podľa tejto zmluvy.

8. Zmluvné strany prehlasujú, že si túto zmluvu pred jej podpisom prečítali, že je prejavom ich slobodnej a určitej vôle, že sú si vedomí záväzkov z nej vyplývajúcich a že súhlasia s jej použitím na účely ponuky na zákazku špecifikovanú v článku II. bod 1 tejto zmluvy. Iné ako verejným obstarávateľom dovolené použitie tejto zmluvy je možné len s písomným súhlasom zmluvných strán.

Za uchádzača:

V Bratislave, dňa: 19.8.2022

[redacted]

Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

Za poskytovateľa:

V Bratislave, dňa: 19.8.2022

[redacted]

Ing. Andrej Bališ
člen predstavenstva
TEMPEST a.s.

8 ČESTNÉ VYHLÁSENIE O SÚHLASE A AKCEPTOVANÍ ZÁVÄZNÝCH NÁVRHOV ZMLÚV

Uchádzač/~~skupina dodávateľov~~:

DATALAN, a.s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734

Čestné vyhlásenie

Dolu podpísaný zástupca uchádzača týmto čestne vyhlasujem, že súhlasím so zmluvnými podmienkami verejnej súťaže uvedenými v časti *B.2 Obchodné podmienky* týchto súťažných podkladov na poskytnutie predmetu zákazky s názvom **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"**, vyhlásenej verejným obstarávateľom **Národné centrum zdravotníckych informácií**, so sídlom Lazaretská 26, 811 09 Bratislava, v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS.

Uvedené požiadavky verejného obstarávateľa akceptujeme a v prípade nášho úspechu v tomto verejnom obstarávaní ich zapracujeme do návrhu zmluvy.

V nadväznosti na bod 5. časti A.3 súťažných podkladov sa v prípade úspešnosti zaväzujem minimálne po dobu účinnosti Zmluvy o dielo zamestnávať 3 osoby so zmenenou pracovnou schopnosťou.

V Bratislave, dňa 19.08.2022

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

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 medzi

Prevádzkovateľom základnej služby:

Názov:	**Národné centrum zdravotníckych informácií**
Sídlo:	Lazaretská 26, 811 09 Bratislava 1
IČO:	00165387
DIČ:	2020830119
IČ DPH:	.....
zapísaným:	.....
v mene ktorého koná :	.....
kontaktná osoba:	.....
e-mail kontaktnej osoby:	.....

(ďalej aj len ako „**Prevádzkovateľ**")

a

Dodávateľom:

Obchodné meno:	**DATALAN, a.s.**
Sídlo:	Krasovského 14, Bratislava - mestská časť Petržalka 851 01
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
zapísaným:	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B.
v mene ktorého koná:	Ing. Zuzana Škodová Prochotská, člen predstavenstva
kontaktná osoba:	Ing. Dušan Polóny
e-mail kontaktnej osoby:	

(ďalej aj len ako „**Dodávateľ**")
(Prevádzkovateľ a Dodávateľ spolu ďalej aj len ako „**zmluvné strany**")

Článok I.
Úvodné ustanovenia a vyhlásenia

1. Prevádzkovateľ ako objednávateľ uzavrel s Dodávateľom ako zhotoviteľom **Zmluvu o dielo na dodávku informačného systému** (ďalej aj len ako „**dodávateľská zmluva**").

2. Prevádzkovateľ je podľa § 3 písm. m) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o kybernetickej bezpečnosti**") prevádzkovateľom základnej služby podľa § 3 písm. l) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej

bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

3. Za účelom plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a § 8 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 OBO**"), zmluvné strany uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**zmluva**"); pred uzatvorením tejto zmluvy sa vykonala analýza rizík.

4. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na dodávateľskú zmluvu, na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi služby (činnosti), ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

5. Vzhľadom na aktuálny stav architektúry IS ezdravie [článok 1. bod 1.1 písm. l) dodávateľskej zmluvy], ktorý nezohľadňuje všetky požiadavky podľa aktuálne platnej legislatívy, sa zmluvné strany dohodli, že vo vzťahu k Časti RISEZ bez redizajnu podľa článku 1. bodu 1.1 písm. e) dodávateľskej zmluvy a pre Doplnok ezdravie podľa článku 1. bodu 1.1 písm. k) dodávateľskej zmluvy je Dodávateľ povinný plniť opatrenia a povinnosti podľa tejto zmluvy primerane; pre účely tohto bodu zmluvy sa pod pojmom „primerane" rozumie plnenie opatrení a povinností Dodávateľa uvedených v tejto zmluve v maximálnej možnej miere a rozsahu.

Článok II.
Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na dodávateľskú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa (s ktorými priamo súvisí výkon činností Dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa.

2. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, ako aj bezpečnostná udalosť:
   a) ktorú zistí alebo o ktorej sa dozvie Dodávateľ,
   b) ktorá sa týka informačných systémov alebo sietí vo vzťahu, ku ktorým Dodávateľ poskytuje výkon činností podľa dodávateľskej zmluvy,
   c) a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti príp. integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa.

Článok III.
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať platné bezpečnostné politiky Prevádzkovateľa, Prevádzkovateľom vydané bezpečnostné smernice a štandardy, ktorými bol Dodávateľ preukázateľne oboznámený (ďalej aj len ako „**bezpečnostná politika**"), a požiadavky na bezpečnosť definované zákonom o kybernetickej bezpečnosti, vyhláškou OBO, zákonom č.

95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v platnom znení, ako aj ostatnými všeobecne záväznými právnymi predpismi platnými v čase plnenia tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve. Dodávateľ vyhlasuje, že sa pred podpisom tejto zmluvy oboznámil s platnou bezpečnostnou politikou Prevádzkovateľa a vyjadruje s ňou súhlas.

2. Dodávateľ súhlasí s bezpečnostnou politikou Prevádzkovateľa a s tým, že bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcich sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať najmenej bezpečnostné opatrenia Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami Prevádzkovateľa.

4. Dodávateľ súhlasí s tým, že bezpečnostné opatrenia Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov Prevádzkovateľa, pričom nie je potrebné uzatvoriť dodatok k zmluve. Dodávateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené bezpečnostné opatrenia Prevádzkovateľa od okamihu, v ktorom ho s nimi Prevádzkovateľ preukázateľne oboznámi.

5. Dodávateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti počas celej doby trvania tejto zmluvy, pokiaľ zo všeobecne záväzných právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.

6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi.

8. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy v oblastiach podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v rozsahu podľa vyhlášky OBO a v rozsahu špecifikovanom v bezpečnostnej politike Prevádzkovateľa.

9. Zoznam zamestnancov Dodávateľa, subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí budú mať prístup k informáciám Prevádzkovateľa (ďalej len „**Zoznam osôb**“) tvorí **Prílohu č. 3** tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v Zozname osôb podľa tohto bodu bezodkladne na e-mailovú adresu kontaktnej osoby Prevádzkovateľa.

10. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy.

11. Dodávateľ môže zapojiť do poskytovania služieb na základe dodávateľskej zmluvy ďalšieho dodávateľa (subdodávateľ), ak mu to vyplýva z ustanovení dodávateľskej zmluvy počas doby jej platnosti a účinnosti.

12. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

13. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nzcisk.sk.

14. Dodávateľ sa zaväzuje poskytnúť Prevádzkovateľovi bezodkladne všetky podklady, informácie a súčinnosť nevyhnutnú k tomu, aby si Prevádzkovateľ mohol riadne a včas plniť všetky povinnosti podľa zákona o kybernetickej bezpečnosti a vyhlášky OBO.

15. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany" v zmysle zákona o kybernetickej bezpečnosti.

16. Poskytovateľ vykonáva len činnosti, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy, tejto zmluvy, všeobecne záväzných právnych predpisov alebo na základe požiadavky Prevádzkovateľa. Na výkon týchto činností môže poveriť Poskytovateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v **Prílohe č. 3**.

Článok IV.
Okolnosti plnenia zmluvy

1. Výklad pojmov používaných v tejto zmluve sa nesmie dostať do rozporu s významom, ktorý im je priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou záväzkov podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa podľa dodávateľskej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania dodávateľskej zmluvy.

4. 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 plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa dodávateľskej zmluvy a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Článok V.
Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

1. Dodávateľ je povinný v rámci prevencie pred kybernetickými incidentmi:

   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Dodávateľa nebolo možné ohroziť siete a informačné systémy Prevádzkovateľa,

   b) preukázateľne vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k dátam alebo informáciám Prevádzkovateľa,

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

   d) sledovať hrozby, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,

   e) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Dodávateľa,

   f) v prípade vzniku kybernetických incidentov v prostredí Dodávateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,

   g) prijímať od Prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,

   h) zasielať Prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a

   i) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Prevádzkovateľa.

Článok VI.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, ktorý je uvedený v **Prílohe č. 2,** vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „**Reakčné opatrenia**"), a to ako na výzvu Prevádzkovateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.

3. Dodávateľ pri reakciách na incidenty spolupracuje s Prevádzkovateľom, Národným bezpečnostným úradom a inými príslušnými orgánmi a za týmto účelom im poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami, ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

4. Dodávateľ pri riešení a reakcii na kybernetický incident postupuje v súlade so všeobecne záväznými právnymi predpismi, touto zmluvou, ako aj svojimi internými procedúrami a

postupmi tak, aby bol kybernetický incident a jeho dôsledky odstránené v čo najkratšom možnom čase.

5. Dodávateľ je povinný oznámiť Prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.

6. Dodávateľ je povinný v čase kybernetického incidentu, ktorý mal dopad na Prevádzkovateľa, zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho Prevádzkovateľovi.

7. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.

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

9. Po schválení ochranného opatrenia Prevádzkovateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť Prevádzkovateľovi.

10. Dodávateľ je povinný informovať Prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nczisk.sk.

Článok VII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy na výkon činností a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. 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. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.

3. Dodávateľ je povinný chrániť všetky informácie, ku ktorým má prístup na základe dodávateľskej zmluvy, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa oboznámil v dôsledku vlastnej činnosti s tým, že všetci dotknutí zamestnanci Dodávateľa, jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých Dodávateľ poskytuje služby podľa dodávateľskej zmluvy (ďalej len „**tretia osoba**“) sú povinní zaviazať sa k zachovávaniu mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

4. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba, a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

5. Dodávateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Zozname osôb zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je Dodávateľ povinný preukázať Prevádzkovateľovi u každej z týchto osôb.

6. Ak táto zmluva neustanovuje inak a nevylučuje to všeobecne záväzný právny predpis, zmluvné strany sa pri ochrane dôverných informácií a zachovávaní mlčanlivosti spravujú ustanoveniami článku 12. dodávateľskej zmluvy. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok VIII.
Audit kybernetickej bezpečnosti

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. Výdavky Prevádzkovateľa spojené s vykonaním auditu znáša Prevádzkovateľ.

2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote šesťdesiat (60) kalendárnych dní.

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

5. Dodávateľ je pri audite povinný spolupracovať s Prevádzkovateľom a sprístupniť priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, umožniť osobám určených Prevádzkovateľom voľný vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto zmluvy.

6. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa a ďalším osobám, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

7. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a/alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie. Preukázanie skutočností uvedených v predchádzajúcej vete môže Dodávateľ realizovať napr. prostredníctvom predloženia relevantných certifikátov, poučení, prezenčných listín a inej dokumentácie.

8. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej desať (10) pracovných dní vopred svoj zámer vykonať u Dodávateľa audit.

9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje zodpovednosti Dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

10. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

11. Prevádzkovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené 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 boli v súlade s týmto bodom, 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 osoby určené Objednávateľom 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 IX.
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenia kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania a riešenia kybernetických incidentov a dokumentovania školení svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy) a na žiadosť Prevádzkovateľa mu predložiť túto dokumentáciu.

4. V prípade, ak Dodávateľ plní dodávateľskú zmluvu prostredníctvom svojich subdodávateľov, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby Prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.

5. Všetky informácie, ktoré majú vplyv na plnenie tejto zmluvy sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na e-mailové adresy kontaktných osôb uvedené v záhlaví tejto zmluvy a súčasne na e-mailovú adresu: csirt@nczisk.sk.

6. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť Prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, Dodávateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO a za dôsledky a škodu vzniknutú Prevádzkovateľovi alebo akejkoľvek tretej osobe v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu. Prevádzkovateľ má voči Dodávateľovi nárok na náhradu preukázateľnej škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.

7. V prípade porušenia povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, je Dodávateľ povinný Prevádzkovateľovi zaplatiť zmluvnú pokutu vo výške 15 000,- EUR (slovom: pätnásťtisíc eur); nárok Prevádzkovateľa na náhradu škody v plnej výške, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením povinností Dodávateľa, tým nie sú dotknuté.

8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

9. Po ukončení tejto zmluvy je Dodávateľ povinný podľa pokynu Prevádzkovateľa vrátiť alebo previesť na Prevádzkovateľa všetky údaje a informácie, ku ktorým mal počas trvania tejto zmluvy prístup, ako aj údaje a informácie získané v súvislosti s plnením tejto zmluvy, resp. tieto údaje a informácie zničiť, 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 Prevádzkovateľa.

10. Dodávateľ bezodkladne po ukončení tejto zmluvy, najneskôr však do troch (3) dní, predloží Prevádzkovateľovi sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré priamo alebo nepriamo súvisia s povinnosťami vyplývajúcich z tejto zmluvy, zo zákona o kybernetickej bezpečnosti alebo z osobitného všeobecne záväzného právneho predpisu v oblasti kybernetickej bezpečnosti a ktoré sa týkajú Prevádzkovateľa. Prevádzkovateľ na základe sumarizácie podľa predchádzajúcej vety písomne informuje Dodávateľa o tom, ktoré podklady a informácie má Dodávateľ vrátiť Prevádzkovateľovi, previesť na Prevádzkovateľa a ktoré má zničiť. Dodávateľ je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do piatich (5) dní odo dňa, kedy Prevádzkovateľ informoval Dodávateľa o spôsobe naloženia s týmito podkladmi a informáciami.

11. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby, ktoré musia byť účinné najmenej po dobu piatich (5) rokov po ukončení tejto zmluvy, ak z dodávateľskej zmluvy nevyplýva dlhšia doba trvania dodávateľom udelených (poskytnutých) licencií, práv a/alebo súhlasov. Ustanovenia

o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľskej zmluve, nie sú týmto dotknuté.

Článok X.
Záverečné ustanovenia

1. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky, nie však skôr ako dňom nadobudnutia účinnosti dodávateľskej zmluvy.

2. Táto zmluva sa uzatvára na dobu určitú, a to do skončenia platnosti a účinnosti dodávateľskej zmluvy.

3. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve. Odstúpenie od tejto zmluvy je možné vykonať v písomnej forme, pričom odstúpenie od zmluvy musí byť riadne doručené druhej zmluvnej strane. V prípade platného odstúpenia od tejto zmluvy sa zmluva považuje na zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strane.

4. Prevádzkovateľ je oprávnený odstúpiť od tejto zmluvy v prípade, ak Dodávateľ poruší akúkoľvek povinnosť alebo záväzok plynúci mu z tejto zmluvy.

5. Prevádzkovateľ je oprávnený vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou tri (3) mesiace. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená výpoveď Dodávateľovi.

6. Ukončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem práv a povinností, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.

7. Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Prevádzkovateľom a Dodávateľom je zákonnou povinnosťou Prevádzkovateľa. Z uvedeného dôvodu je Prevádzkovateľ v prípade skončenia platnosti tejto Zmluvy oprávnený bez ďalšieho odstúpiť od dodávateľskej zmluvy uzatvorenej s Dodávateľom.

8. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

9. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd Slovenskej republiky.

10. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve, ak táto zmluva neustanovuje inak.

11. Kontaktné osoby zmluvných strán a ich kontaktné údaje môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu alebo kontaktné druhej zmluvnej strane v písomnej forme, pričom nie je potrebné uzatvoriť dodatok k zmluve. Rovnako je oprávnený postupovať Prevádzkovateľ pri zmene spôsobu hlásenia bezpečnostného incidentu uvedeného v **Prílohe č. 2** tejto zmluvy.

12. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane 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 neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu neplatných alebo nevykonateľných ustanovení.

13. Neoddeliteľnou súčasťou tejto zmluvy je:
Príloha č. 1 – Špecifikácia a rozsah bezpečnostných opatrení
Príloha č. 2 – Spôsob hlásenia bezpečnostného incidentu
Príloha č. 3 – Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa.

14. Táto zmluva sa vyhotovuje v štyroch (4) rovnopisoch, po dvoch (2) pre každú zmluvnú stranu.

15. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa .....

V Bratislave, dňa 19.08.2022

Za Prevádzkovateľa:

.....
Mgr. Peter Lukáč, PhD.
generálny riaditeľ
Národné centrum zdravotníckych informácií

Za Dodávateľa:

[redacted]

Ing. Zuzana Škodová Prochotská
člen predstavenstva
DATALAN, a.s.

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

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

B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

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

C. Personálna bezpečnosť

1. Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.
2. Dodávateľ zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
3. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
4. Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí:
    a. vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
    b. zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
    c. zrušenie prístupových práv v informačných systémoch verejnej správy,
    d. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
5. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
6. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.
7. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn 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 (6) 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 (6) 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 (2) 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, integračného, predprodukčného a produkčného 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 (6) 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 e-mailové 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 (6) 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 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.

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. e-mailovej 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 č. 2 Spôsob hlásenia bezpečnostného incidentu

1) Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v záhlaví tejto zmluvy.

2) Pri nahlasovaní incidentu je potrebné uviesť, že sa jedná o bezpečnostný incident v zmysle tejto zmluvy a tiež kontaktnú osobu, s ktorou je možné komunikovať za účelom získania dodatočných informácií súvisiacich s procesom analýzy a riešenia bezpečnostného incidentu.

3) Samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom Prevádzkovateľa – „Riadenie bezpečnostných incidentov".

Príloha č. 3 Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa

Prevádzkovateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		
		príp. ďalšie procesy uviesť		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		
		príp. ďalšie procesy uviesť		

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 medzi

Prevádzkovateľom základnej služby:

Názov:	**Národné centrum zdravotníckych informácií**
Sídlo:	Lazaretská 26, 811 09 Bratislava 1
IČO:	00165387
DIČ:	2020830119
IČ DPH:	.....
zapísaným:	.....
v mene ktorého koná :	.....
kontaktná osoba:	.....
e-mail kontaktnej osoby:	.....

(ďalej aj len ako „**Prevádzkovateľ**")

a

Dodávateľom:

Obchodné meno:	**DATALAN, a.s.**
Sídlo:	Krasovského 14, Bratislava - mestská časť Petržalka 851 01
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
zapísaným:	Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B.
v mene ktorého koná:	Ing. Zuzana Škodová Prochotská, člen predstavenstva
kontaktná osoba:	Ing. Dušan Polóny
e-mail kontaktnej osoby:	

(ďalej aj len ako „**Dodávateľ**")
(Prevádzkovateľ a Dodávateľ spolu ďalej aj len ako „**zmluvné strany**")

Článok I.
Úvodné ustanovenia a vyhlásenia

1. Prevádzkovateľ ako objednávateľ uzavrel s Dodávateľom ako zhotoviteľom **Zmluvu o podpore prevádzky, údržbe a rozvoji informačného systému** (ďalej aj len ako „**dodávateľská zmluva**").

2. Prevádzkovateľ je podľa § 3 písm. m) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o kybernetickej bezpečnosti**") prevádzkovateľom základnej služby podľa § 3 písm. l) zákona o kybernetickej bezpečnosti. Dodávateľ je s poukazom na § 19 ods. 2 zákona o kybernetickej

bezpečnosti dodávateľom služieb, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

3. Za účelom plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a § 8 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 OBO**"), zmluvné strany uzatvárajú túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**zmluva**"); pred uzatvorením tejto zmluvy sa vykonala analýza rizík.

4. Zmluvné strany uzatvárajú túto zmluvu v nadväznosti na dodávateľskú zmluvu, na základe ktorej Dodávateľ bude poskytovať Prevádzkovateľovi služby (činnosti), ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov pre Prevádzkovateľa ako prevádzkovateľa základnej služby.

5. Vzhľadom na aktuálny stav architektúry IS ezdravie [článok 1. bod 1.1 písm. j) dodávateľskej zmluvy], ktorý nezohľadňuje všetky požiadavky podľa aktuálne platnej legislatívy, sa zmluvné strany dohodli, že pri poskytovaní služieb podľa dodávateľskej zmluvy vo vzťahu k IS ezdravie [článok 1. bod 1.1 písm. j) dodávateľskej zmluvy] a k časti (komponentom) Systému bez Redizajnu [článok 1. bod 1.1 písm. oo) v spojení s písm. uu) dodávateľskej zmluvy] je Dodávateľ povinný plniť opatrenia a povinnosti podľa tejto zmluvy primerane; pre účely tohto bodu zmluvy sa pod pojmom „primerane" rozumie plnenie opatrení a povinností Dodávateľa uvedených v tejto zmluve v maximálnej možnej miere a rozsahu.

Článok II.
Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán a ich práv a povinností pri plnení bezpečnostných opatrení a notifikačných povinností realizovaných v nadväznosti na dodávateľskú zmluvu, a to s cieľom zabezpečiť kybernetickú bezpečnosť v súvislosti s prevádzkou sietí a informačných systémov Prevádzkovateľa (s ktorými priamo súvisí výkon činností Dodávateľa na základe dodávateľskej zmluvy) počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť Prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania služieb, sietí a informačných systémov Prevádzkovateľa.

2. Pre účely tejto zmluvy sa za kybernetický incident považuje kybernetický bezpečnostný incident podľa zákona o kybernetickej bezpečnosti, ako aj bezpečnostná udalosť:
   a) ktorú zistí alebo o ktorej sa dozvie Dodávateľ,
   b) ktorá sa týka informačných systémov alebo sietí vo vzťahu, ku ktorým Dodávateľ poskytuje výkon činností podľa dodávateľskej zmluvy,
   c) a ktorej následkom došlo alebo s najväčšou pravdepodobnosťou môže dôjsť k takému narušeniu kybernetickej bezpečnosti príp. integrity alebo dostupnosti služby Prevádzkovateľa, alebo k narušeniu dôvernosti prenášaných dát, k nemožnosti poskytovania služby Prevádzkovateľa alebo k zníženiu kvality poskytovanej služby Prevádzkovateľa.

Článok III.
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje dodržiavať platné bezpečnostné politiky Prevádzkovateľa, Prevádzkovateľom vydané bezpečnostné smernice a štandardy, ktorými bol Dodávateľ preukázateľne oboznámený (ďalej aj len ako „**bezpečnostná politika**"), a požiadavky na

bezpečnosť definované zákonom o kybernetickej bezpečnosti, vyhláškou OBO, zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v platnom znení, ako aj ostatnými všeobecne záväznými právnymi predpismi platnými v čase plnenia tejto zmluvy a bezpečnostné požiadavky uvedené v tejto zmluve. Dodávateľ vyhlasuje, že sa pred podpisom tejto zmluvy oboznámil s platnou bezpečnostnou politikou Prevádzkovateľa a vyjadruje s ňou súhlas.

2. Dodávateľ súhlasí s bezpečnostnou politikou Prevádzkovateľa a s tým, že bezpečnostná politika Prevádzkovateľa sa môže priebežne meniť a dopĺňať tak, aby zodpovedala aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa a aktuálnym hrozbám dotýkajúcich sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa. Prevádzkovateľ je povinný bezodkladne oboznámiť Dodávateľa s aktualizovanou bezpečnostnou politikou s dôrazom na zmeny v nej uvedené, pričom Dodávateľ následne preukázateľne potvrdí akceptáciu zmien bezpečnostnej politiky.

3. Dodávateľ sa zaväzuje prijímať a dodržiavať najmenej bezpečnostné opatrenia Prevádzkovateľa, ktoré tvoria **Prílohu č. 1** k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými opatreniami Prevádzkovateľa.

4. Dodávateľ súhlasí s tým, že bezpečnostné opatrenia Prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným požiadavkám, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov Prevádzkovateľa, pričom nie je potrebné uzatvoriť dodatok k zmluve. Dodávateľ sa zaväzuje dodržiavať takto zmenené alebo doplnené bezpečnostné opatrenia Prevádzkovateľa od okamihu, v ktorom ho s nimi Prevádzkovateľ preukázateľne oboznámi.

5. Dodávateľ je povinný plniť bezpečnostné opatrenia a notifikačné povinnosti v oblasti kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti počas celej doby trvania tejto zmluvy, pokiaľ zo všeobecne záväzných právnych predpisov uvedených v tejto zmluve nevyplývajú určité povinnosti pre Dodávateľa aj po skončení platnosti a účinnosti tejto zmluvy alebo dodávateľskej zmluvy.

6. Dodávateľ sa zaväzuje chrániť všetky informácie poskytnuté Prevádzkovateľom, najmä chrániť ich integritu, dostupnosť a dôvernosť pri ich spracovaní a nakladaní s nimi.

7. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna, priebežne aktualizovaná a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi.

8. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy v oblastiach podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v rozsahu podľa vyhlášky OBO a v rozsahu špecifikovanom v bezpečnostnej politike Prevádzkovateľa.

9. Zoznam zamestnancov Dodávateľa, subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa tejto zmluvy a ktorí budú mať prístup k informáciám Prevádzkovateľa (ďalej len „**Zoznam osôb**“) tvorí **Prílohu č. 3** tejto zmluvy. Dodávateľ je povinný oznámiť Prevádzkovateľovi každú zmenu v Zozname osôb podľa tohto bodu bezodkladne na e-mailovú adresu kontaktnej osoby Prevádzkovateľa.

10. Dodávateľ je povinný písomne informovať Prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom na účely plnenia tejto zmluvy.

11. Dodávateľ môže zapojiť do poskytovania služieb na základe dodávateľskej zmluvy ďalšieho dodávateľa (subdodávateľ), ak mu to vyplýva z ustanovení dodávateľskej zmluvy počas doby jej platnosti a účinnosti.

12. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu Dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

13. Dodávateľ sa zaväzuje hlásiť všetky potrebné informácie požadované Prevádzkovateľom pri zabezpečovaní požiadaviek kladených na Prevádzkovateľa podľa zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nzcisk.sk.

14. Dodávateľ sa zaväzuje poskytnúť Prevádzkovateľovi bezodkladne všetky podklady, informácie a súčinnosť nevyhnutnú k tomu, aby si Prevádzkovateľ mohol riadne a včas plniť všetky povinnosti podľa zákona o kybernetickej bezpečnosti a vyhlášky OBO.

15. Dodávateľ sa zaväzuje zaistiť pri poskytovaní služieb Prevádzkovateľovi dodržiavanie bezpečnostných požiadaviek, ktoré sú kladené na „tretie strany" v zmysle zákona o kybernetickej bezpečnosti.

16. Poskytovateľ vykonáva len činnosti, ktoré vyplývajú z podstaty služieb poskytovaných na základe dodávateľskej zmluvy, tejto zmluvy, všeobecne záväzných právnych predpisov alebo na základe požiadavky Prevádzkovateľa. Na výkon týchto činností môže poveriť Poskytovateľ len konkrétne osoby v rámci pracovných rolí, ktorých zoznam je uvedený v **Prílohe č. 3**.

Článok IV.
Okolnosti plnenia zmluvy

1. Výklad pojmov používaných v tejto zmluve sa nesmie dostať do rozporu s významom, ktorý im je priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou záväzkov podľa tejto zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto zmluvy.

3. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany Dodávateľa pre Prevádzkovateľa podľa dodávateľskej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania dodávateľskej zmluvy.

4. 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 plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Dodávateľovi podľa dodávateľskej zmluvy a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Článok V.
Všeobecné bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

1. Dodávateľ je povinný v rámci prevencie pred kybernetickými incidentmi:

   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby cez siete a informačné systémy Dodávateľa nebolo možné ohroziť siete a informačné systémy Prevádzkovateľa,

   b) preukázateľne vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k dátam alebo informáciám Prevádzkovateľa,

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

   d) sledovať hrozby, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,

   e) predchádzať vzniku kybernetických incidentov implementovaním najmä bezpečnostných opatrení v prostredí Dodávateľa,

   f) v prípade vzniku kybernetických incidentov v prostredí Dodávateľa, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,

   g) prijímať od Prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy resp. kybernetickú bezpečnosť Prevádzkovateľa,

   h) zasielať Prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a

   i) spolupracovať s Prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti Prevádzkovateľa.

Článok VI.
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident Prevádzkovateľovi spôsobom určeným Prevádzkovateľom, ktorý je uvedený v **Prílohe č. 2,** vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, Dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Najčastejšími spôsobmi riešenia incidentov, ktoré Dodávateľ využíva, sú odozva, označenie incidentov a ich účinkov, náprava nepriaznivých dopadov incidentov a iné vhodné činnosti spojené s nápravou incidentov (ďalej len „**Reakčné opatrenia**"), a to ako na výzvu Prevádzkovateľa, tak aj bez jeho výzvy, ak sa o incidente dozvie.

3. Dodávateľ pri reakciách na incidenty spolupracuje s Prevádzkovateľom, Národným bezpečnostným úradom a inými príslušnými orgánmi a za týmto účelom im poskytuje súčinnosť a zdieľa všetky získané informácie, ktoré nie sú dôvernými informáciami, ktoré by mohli mať vplyv na implementáciu Reakčných opatrení v budúcnosti.

4. Dodávateľ pri riešení a reakcii na kybernetický incident postupuje v súlade so všeobecne záväznými právnymi predpismi, touto zmluvou, ako aj svojimi internými procedúrami a postupmi tak, aby bol kybernetický incident a jeho dôsledky odstránené v čo najkratšom možnom čase.

5. Dodávateľ je povinný oznámiť Prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.

6. Dodávateľ je povinný v čase kybernetického incidentu, ktorý mal dopad na Prevádzkovateľa, zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho Prevádzkovateľovi.

7. Dodávateľ je povinný bezodkladne oznámiť a preukázať Prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.

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

9. Po schválení ochranného opatrenia Prevádzkovateľom je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť Prevádzkovateľovi.

10. Dodávateľ je povinný informovať Prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to zaslaním e-mailu kontaktnej osobe Prevádzkovateľa uvedenú v tejto zmluve a súčasne na e-mailovú adresu: csirt@nczisk.sk.

Článok VII.
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy na výkon činností a tejto zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. 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. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.

3. Dodávateľ je povinný chrániť všetky informácie, ku ktorým má prístup na základe dodávateľskej zmluvy, tejto zmluvy, alebo ktoré mu boli poskytnuté alebo sprístupnené zo strany Prevádzkovateľa alebo osoby spriaznenej s Prevádzkovateľom alebo s ktorými sa oboznámil v dôsledku vlastnej činnosti s tým, že všetci dotknutí zamestnanci Dodávateľa, jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých Dodávateľ poskytuje služby podľa dodávateľskej zmluvy (ďalej len „**tretia osoba**“) sú povinní zaviazať sa k zachovávaniu mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

4. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba, a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

5. Dodávateľ je povinný zabezpečiť, aby sa každá osoba uvedená v Zozname osôb zaviazala zachovávať mlčanlivosť podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti. Tento záväzok mlčanlivosti je Dodávateľ povinný preukázať Prevádzkovateľovi u každej z týchto osôb.

6. Ak táto zmluva neustanovuje inak a nevylučuje to všeobecne záväzný právny predpis, zmluvné strany sa pri ochrane dôverných informácií a zachovávaní mlčanlivosti spravujú ustanoveniami článku 12. dodávateľskej zmluvy. Touto zmluvou nie sú dotknuté ustanovenia o záväzkoch mlčanlivosti podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

Článok VIII.
Audit kybernetickej bezpečnosti

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. Výdavky Prevádzkovateľa spojené s vykonaním auditu znáša Prevádzkovateľ.

2. Dodávateľ sa zaväzuje, že Prevádzkovateľovi umožní kedykoľvek vykonať audit, ktorým si Prevádzkovateľ overí mieru a efektívnosť plnenia povinností Dodávateľom uvedených v bode 1 tohto článku, pričom tento audit bude zameraný najmä na kontrolu technického, technologického a personálneho vybavenia a procesných postupov, ktoré Dodávateľ využíva pri plnení svojich povinností v oblasti kybernetickej bezpečnosti a tiež bude zameraný na overenie nastavenia a efektívnosti procesov a technológií v organizačnej a technickej oblasti Dodávateľa.

3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote šesťdesiat (60) kalendárnych dní.

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

5. Dodávateľ je pri audite povinný spolupracovať s Prevádzkovateľom a sprístupniť priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy, umožniť osobám určených Prevádzkovateľom voľný vstup do svojich priestorov a zabezpečiť im dokumentáciu a technické vybavenie potrebné na plnenie úloh podľa tejto zmluvy.

6. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa a ďalším osobám, ktoré sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

7. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a/alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie. Preukázanie

skutočností uvedených v predchádzajúcej vete môže Dodávateľ realizovať napr. prostredníctvom predloženia relevantných certifikátov, poučení, prezenčných listín a inej dokumentácie.

8. Prevádzkovateľ je povinný oznámiť Dodávateľovi najmenej desať (10) pracovných dní vopred svoj zámer vykonať u Dodávateľa audit.

9. Vykonanie alebo nevykonanie auditu Prevádzkovateľom nezbavuje zodpovednosti Dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

10. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.

11. Prevádzkovateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Prevádzkovateľ a osoby ním určené 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 boli v súlade s týmto bodom, 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 osoby určené Objednávateľom 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 IX.
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenia kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti Prevádzkovateľa tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.

3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania a riešenia kybernetických incidentov a dokumentovania školení svojich zamestnancov a ďalších osôb, ktoré sa budú v mene Dodávateľa podieľať na plnení tejto zmluvy) a na žiadosť Prevádzkovateľa mu predložiť túto dokumentáciu.

4. V prípade, ak Dodávateľ plní dodávateľskú zmluvu prostredníctvom svojich subdodávateľov, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ

je povinný zabezpečiť, aby Prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.

5. Všetky informácie, ktoré majú vplyv na plnenie tejto zmluvy sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na e-mailové adresy kontaktných osôb uvedené v záhlaví tejto zmluvy a súčasne na e-mailovú adresu: csirt@nczisk.sk.

6. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie alebo porušenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť Prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, Dodávateľ zodpovedá v celom rozsahu za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO a za dôsledky a škodu vzniknutú Prevádzkovateľovi alebo akejkoľvek tretej osobe v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu. Prevádzkovateľ má voči Dodávateľovi nárok na náhradu preukázateľnej škody, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov Dodávateľa. Zodpovednosť za škodu sa spravuje príslušnými ustanoveniami Obchodného zákonníka.

7. V prípade porušenia povinnosti alebo záväzku Dodávateľa vyplývajúceho mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky OBO, je Dodávateľ povinný Prevádzkovateľovi zaplatiť zmluvnú pokutu vo výške 15 000,- EUR (slovom: pätnásťtisíc eur); nárok Prevádzkovateľa na náhradu škody v plnej výške, ako aj nárok na náhradu pokút právoplatne uložených orgánmi verejnej moci a iných nákladov (napr. povinnosť Prevádzkovateľa nahradiť tretej osobe nemajetkovú ujmu vyvolanú kybernetickým incidentom), ktoré Prevádzkovateľovi vzniknú v súvislosti s porušením povinností Dodávateľa, tým nie sú dotknuté.

8. Touto zmluvou nie sú dotknuté ustanovenia o sankciách podľa dodávateľskej zmluvy alebo iných zmlúv uzatvorených medzi Prevádzkovateľom a Dodávateľom.

9. Po ukončení tejto zmluvy je Dodávateľ povinný podľa pokynu Prevádzkovateľa vrátiť alebo previesť na Prevádzkovateľa všetky údaje a informácie, ku ktorým mal počas trvania tejto zmluvy prístup, ako aj údaje a informácie získané v súvislosti s plnením tejto zmluvy, resp. tieto údaje a informácie zničiť, 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 Prevádzkovateľa.

10. Dodávateľ bezodkladne po ukončení tejto zmluvy, najneskôr však do troch (3) dní, predloží Prevádzkovateľovi sumarizáciu všetkých podkladov a všetkých informácií zachytených na akomkoľvek druhu nosiča dát, ktoré priamo alebo nepriamo súvisia s povinnosťami vyplývajúcich z tejto zmluvy, zo zákona o kybernetickej bezpečnosti alebo z osobitného všeobecne záväzného právneho predpisu v oblasti kybernetickej bezpečnosti a ktoré sa týkajú Prevádzkovateľa. Prevádzkovateľ na základe sumarizácie podľa predchádzajúcej vety písomne informuje Dodávateľa o tom, ktoré podklady a informácie má Dodávateľ vrátiť Prevádzkovateľovi, previesť na Prevádzkovateľa a ktoré má zničiť. Dodávateľ je povinný splniť si povinnosť podľa predchádzajúcej vety najneskôr do piatich (5) dní odo dňa, kedy Prevádzkovateľ informoval Dodávateľa o spôsobe naloženia s týmito podkladmi a informáciami.

11. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby, ktoré musia byť účinné najmenej po dobu piatich (5) rokov

po ukončení tejto zmluvy, ak z dodávateľskej zmluvy nevyplýva dlhšia doba trvania dodávateľom udelených (poskytnutých) licencií, práv a/alebo súhlasov. Ustanovenia o autorských právach (licenciách) k výsledkom služieb Dodávateľa, ktoré sú obsiahnuté v dodávateľskej zmluve, nie sú týmto dotknuté.

Článok X.
Záverečné ustanovenia

1. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky, nie však skôr ako dňom nadobudnutia účinnosti dodávateľskej zmluvy.

2. Táto zmluva sa uzatvára na dobu určitú, a to do skončenia platnosti a účinnosti dodávateľskej zmluvy.

3. Každá zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade uvedenom vo všeobecne záväznom právnom predpise alebo tejto zmluve. Odstúpenie od tejto zmluvy je možné vykonať v písomnej forme, pričom odstúpenie od zmluvy musí byť riadne doručené druhej zmluvnej strane. V prípade platného odstúpenia od tejto zmluvy sa zmluva považuje na zrušenú momentom doručenia písomného odstúpenia od tejto zmluvy druhej zmluvnej strane.

4. Prevádzkovateľ je oprávnený odstúpiť od tejto zmluvy v prípade, ak Dodávateľ poruší akúkoľvek povinnosť alebo záväzok plynúci mu z tejto zmluvy.

5. Prevádzkovateľ je oprávnený vypovedať túto zmluvu aj bez udania dôvodu s výpovednou lehotou tri (3) mesiace. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená výpoveď Dodávateľovi.

6. Ukončením tejto zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce z tejto zmluvy okrem práv a povinností, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy, ku ktorému dôjde do skončenia tejto zmluvy.

7. Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Prevádzkovateľom a Dodávateľom je zákonnou povinnosťou Prevádzkovateľa. Z uvedeného dôvodu je Prevádzkovateľ v prípade skončenia platnosti tejto Zmluvy oprávnený bez ďalšieho odstúpiť od dodávateľskej zmluvy uzatvorenej s Dodávateľom.

8. Právne vzťahy neupravené touto zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

9. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd Slovenskej republiky.

10. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve, ak táto zmluva neustanovuje inak.

11. Kontaktné osoby zmluvných strán a ich kontaktné údaje môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu alebo kontaktné druhej zmluvnej strane v písomnej forme, pričom nie je potrebné uzatvoriť dodatok k zmluve. Rovnako je oprávnený postupovať

Prevádzkovateľ pri zmene spôsobu hlásenia bezpečnostného incidentu uvedeného v **Prílohe č. 2** tejto zmluvy.

12. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane 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 neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu neplatných alebo nevykonateľných ustanovení.

13. Neoddeliteľnou súčasťou tejto zmluvy je:
Príloha č. 1 – Špecifikácia a rozsah bezpečnostných opatrení
Príloha č. 2 – Spôsob hlásenia bezpečnostného incidentu
Príloha č. 3 – Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa.

14. Táto zmluva sa vyhotovuje v štyroch (4) rovnopisoch, po dvoch (2) pre každú zmluvnú stranu.

15. Zmluvné strany vyhlasujú, že túto zmluvu pred jej podpísaním prečítali, že bola uzatvorené po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave dňa .....

Za Prevádzkovateľa:

.....
Mgr. Peter Lukáč, PhD.
generálny riaditeľ
Národné centrum zdravotníckych informácií

V Bratislave dňa 19.08.2022

Za Dodávateľa:

[redacted]

Ing. Zuzana Škodová Prochotská
člen predstavenstva
DATALAN, a.s.

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

Príloha č. 1 Špecifikácia a rozsah bezpečnostných opatrení

A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

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

B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

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

C. Personálna bezpečnosť

1. Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.
2. Dodávateľ zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.
3. Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
4. Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí:
    a. vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
    b. zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
    c. zrušenie prístupových práv v informačných systémoch verejnej správy,
    d. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.
5. Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.
6. Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.
7. Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn 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 (6) 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 (6) 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 (2) 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, integračného, predprodukčného a produkčného 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 (6) 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 e-mailové 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 (6) 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 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.

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. e-mailovej 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 č. 2 Spôsob hlásenia bezpečnostného incidentu

1) Hlásenie incidentov a následná komunikácia prebieha medzi kontaktnými osobami zmluvných strán uvedených v záhlaví tejto zmluvy.

2) Pri nahlasovaní incidentu je potrebné uviesť, že sa jedná o bezpečnostný incident v zmysle tejto zmluvy a tiež kontaktnú osobu, s ktorou je možné komunikovať za účelom získania dodatočných informácií súvisiacich s procesom analýzy a riešenia bezpečnostného incidentu.

3) Samotný spôsob a forma hlásenia bezpečnostné incidentu sa bude riadiť platným predpisom Prevádzkovateľa – „Riadenie bezpečnostných incidentov".

Príloha č. 3 Zoznam osôb a pracovných rolí Prevádzkovateľa a Dodávateľa

Prevádzkovateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		
		príp. ďalšie procesy uviesť		

Dodávateľ:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou služby	Telefónny kontakt	E-mail
		Zodpovednosť za realizáciu projektu		
		Riadenie informačnej a kybernetickej bezpečnosti		
		Technická podpora pre oblasť bezpečnosti		
		Osoba zodpovedná za SLA		
		príp. ďalšie procesy uviesť		

Zmluva o spracúvaní osobných údajov

uzatvorená v súlade s 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 ako „**Zmluva**“) medzi:

Prevádzkovateľom:	**Národné centrum zdravotníckych informácií**
so sídlom:	Lazaretská 26, 811 09 Bratislava
IČO:	00165387
DIČ:	2020830119
IČ DPH:	nie je platca DPH
v mene ktorého koná:	Mgr. Peter Lukáč, PhD., generálny riaditeľ
e-mail:	nczisk@nczisk.sk

(ďalej aj len „**NCZI**“ a/alebo „**Prevádzkovateľ**“)

a

Sprostredkovateľom:	**DATALAN, a.s.**
so sídlom:	Krasovského 14, Bratislava - mestská časť Petržalka 851 01
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
v mene ktorého koná:	Ing. Zuzana Škodová Prochotská, člen predstavenstva
e-mail:	

(ďalej aj len „**Sprostredkovateľ**“)

(Prevádzkovateľ a Sprostredkovateľ spolu ako „**Zmluvné strany**“ alebo jednotlivo ako „**Zmluvná strana**“)

Článok I
Úvodné ustanovenia

1.1 Prevádzkovateľ ako objednávateľ uzavrel so Sprostredkovateľom ako zhotoviteľom ..... (ďalej aj len ako „**dodávateľská zmluva**“).

1.2 Zmluvné strany sú zodpovedné za riadne dodržiavanie práv a povinností vyplývajúcich z platných právnych predpisov, ktoré upravujú problematiku ochrany a spracovania osobných údajov, a to najmä nariadenie 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 aj ako „**GDPR**“) a zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení iných zákonov v znení neskorších predpisov (ďalej aj ako „**ZOOÚ**“).

1.3 Prevádzkovateľ v rámci výkonu svojej činnosti nakladá s osobnými údajmi v zmysle GDPR a ZOOÚ, pričom vymedzuje účel spracúvania osobných údajov, určuje podmienky ich spracúvania a spracúva tieto osobné údaje vo vlastnom mene.

1.4 Zmluvné strany uzatvárajú túto Zmluvu v súvislosti s poskytovaním služieb Sprostredkovateľom Prevádzkovateľovi na základe dodávateľskej zmluvy (ďalej aj len ako „**služby**").

1.5 GDPR/ZOOÚ vyžadujú, aby vzájomné vzťahy medzi Prevádzkovateľom a Sprostredkovateľom pri spracúvaní osobných údajov boli upravené zmluvou v písomnej alebo elektronickej forme.

Článok II
Predmet zmluvy a povaha spracúvania

2.1 Pri poskytovaní služieb Sprostredkovateľ spracúva osobné údaje v mene Prevádzkovateľa.

2.2 Predmetom tejto Zmluvy je úprava vzájomných práv a povinnosti Zmluvných strán pri spracúvaní osobných údajov dotknutých osôb Sprostredkovateľom v mene Prevádzkovateľa a poverenie Sprostredkovateľa Prevádzkovateľom spracúvaním osobných údajov pri poskytovaní služieb, a to v rozsahu a za podmienok dohodnutých v tejto Zmluve.

2.3 Povaha spracúvania je daná hlavným zmluvným vzťahom medzi Zmluvnými stranami, ktorý je upravený v samostatnej dodávateľskej zmluve. Spracúvanie bude zahŕňať služby .....

2.4 Zmluvné strany berú na vedomie, že žiadne z ustanovení tejto Zmluvy nezbavuje Sprostredkovateľa zodpovednosti za plnenie povinností, ktoré mu priamo vyplývajú z GDPR.

2.5 Spracúvanie osobných údajov Sprostredkovateľom sa uskutočňuje v súvislosti s plnením dodávateľskej zmluvy a Sprostredkovateľ nemá nárok na osobitnú odmenu za plnenie tejto Zmluvy ani na úhradu akýchkoľvek nákladov s tým spojených. Odplata za plnenie povinností Sprostredkovateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených Sprostredkovateľom v súvislosti s plnením povinností Sprostredkovateľom podľa tejto Zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom Sprostredkovateľovi podľa dodávateľskej zmluvy a na žiadne ďalšie peňažné plnenia Sprostredkovateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Článok III
Spracúvanie osobných údajov

3.1 Prevádzkovateľ na základe tejto Zmluvy poveruje Sprostredkovateľa, aby v jeho mene spracúval osobné údaje v rozsahu a za podmienok dohodnutých v tejto Zmluve. Sprostredkovateľ sa zaväzuje vykonávať toto spracúvanie v súlade s touto Zmluvou a GDPR.

3.2 Prevádzkovateľ týmto poveruje Sprostredkovateľa na spracúvanie osobných údajov na účel:

a) .....

3.3 Sprostredkovateľ je poverený spracúvať osobné údaje do vydania pokynu Prevádzkovateľa adresovanému Sprostredkovateľovi o ukončení spracúvania osobných údajov k určitému dňu, najdlhšie však po dobu trvania účinnosti tejto Zmluvy.

3.4 Prevádzkovateľ poveruje Sprostredkovateľa spracúvaním osobných údajov nasledovných dotknutých osôb ..... (ďalej len „**dotknuté osoby**").

3.5 Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb, a to v rozsahu: ..... (ďalej aj len „**osobné údaje**").

3.6 Sprostredkovateľ je v zmysle tejto Zmluvy oprávnený realizovať najmä nasledujúce spracovateľské operácie: získavanie, zhromažďovanie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, prehliadanie, kombinovanie, poskytovanie, prípadne ďalšie spracovateľské operácie nevyhnutné pre splnenie povinností a účelu tejto Zmluvy.

3.7 Sprostredkovateľ nesmie poskytnúť, sprístupniť, zverejniť alebo preniesť osobné údaje, ktoré spracúva na základe tejto Zmluvy bez predchádzajúceho preukázateľného súhlasu Prevádzkovateľa, ak táto Zmluva neustanovuje inak, takúto povinnosť výslovne neustanovuje všeobecne záväzný právny predpis, ktorým je Sprostredkovateľ povinný sa riadiť, alebo Prevádzkovateľ na to neudelil písomný pokyn na základe tejto Zmluvy. Sprostredkovateľ je povinný vopred (pred uskutočnením niektorej zo spracovateľských operácií s osobnými údajmi podľa tohto bodu Zmluvy) oznámiť Prevádzkovateľovi existenciu takéhoto všeobecne záväzného právneho predpisu.

3.8 Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb prostredníctvom automatizovaných a neautomatizovaných prostriedkov, a to vlastnými alebo ním kontrolovanými personálnymi a technologickými kapacitami a IT infraštruktúrou.

3.9 Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb v elektronickej podobe a/alebo v listinnej podobe.

3.10 Sprostredkovateľ je oprávnený komunikovať s dotknutými osobami.

3.11 Sprostredkovateľ berie na vedomie, že v prípade, ak poruší pokyny udelené Prevádzkovateľom alebo ustanovené touto Zmluvou, najmä tým, že v rozpore s pokynmi Prevádzkovateľa vykoná spracovateľské operácie alebo určí účely a prostriedky spracúvania osobných údajov, vo vzťahu k takémuto spracúvaniu sa na neho v zmysle GDPR vzťahujú všetky povinnosti a zodpovednosti ako na samostatného Prevádzkovateľa.

3.12 Kontaktné osoby Prevádzkovateľa a Sprostredkovateľa pre účely plnenia Zmluvy:

- za Prevádzkovateľa: ....., e-mail: .....
- za Sprostredkovateľa: ....., e-mail: .....

Zmluvné strany sa zaväzujú bezodkladne si navzájom oznámiť akúkoľvek zmenu/doplnenie kontaktnej osoby a/alebo jej kontaktných údajov; na takúto zmenu/doplnenie sa nevyžaduje uzatvorenie dodatku k tejto Zmluve.

Článok IV
Vyhlásenie zmluvných strán

4.1 Prevádzkovateľ vyhlasuje, že osobné údaje o dotknutých osobách, ktoré poskytne a/alebo sprístupní Sprostredkovateľovi, či už v podobe elektronickej databázy, ako súčasť aplikácie, alebo iným spôsobom, Prevádzkovateľ získal zákonným spôsobom a v súlade s príslušnými podmienkami GDPR ako aj inými príslušnými právnymi predpismi.

4.2 Prevádzkovateľ vyhlasuje, že pri výbere Sprostredkovateľa postupoval s odbornou starostlivosťou a zohľadnil všetky Sprostredkovateľom poskytnuté záruky, v rámci ktorých Sprostredkovateľ deklaroval prijatie a implementovanie primeraných technických a organizačných opatrení na zabezpečenie a splnenie všetkých zákonných požiadaviek na zabezpečenie ochrany práv a slobôd dotknutých osôb pri spracúvaní ich osobných údajov v informačných systémoch Sprostredkovateľa.

4.3 Sprostredkovateľ vyhlasuje, že disponuje všetkými potrebnými prostriedkami (technickými, organizačnými a pod.) na zabezpečenie ochrany osobných údajov dotknutých osôb a prijme primerané technické a organizačné opatrenia spôsobom a v súlade s príslušnými podmienkami tak, aby spracúvanie osobných údajov dotknutých osôb spĺňalo požiadavky GDPR a ZOOÚ. Sprostredkovateľ prijal bezpečnostné opatrenia podľa čl. 32 GDPR bližšie uvedené v **Prílohe č. 1** tejto Zmluvy a je povinný na vlastné náklady prijať dodatočné opatrenia na žiadosť Prevádzkovateľa, ak sa také dodatočné opatrenia ukážu byť primerané.

4.4 Zmluvné strany sa zaväzujú uchovávať všetky písomné (alebo elektronické) podklady, dokumenty a/alebo akékoľvek iné materiály a dátové nosiče získané od druhej Zmluvnej strany za účelom plnenia tejto Zmluvy obsahujúce osobné údaje na chránených miestach a zabezpečiť ich primeranú ochranu pred náhodným a/alebo nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek nezákonnými spôsobmi spracúvania. Zmluvné strany sa tiež zaväzujú, že všetky databázy, aplikácie a/alebo informačné systémy, v ktorých sa spracúvajú osobné údaje zabezpečia tak, aby bola zaistená kontinuálna dôvernosť, integrita a dostupnosť osobných údajov. Na tento účel Zmluvné strany deklarujú, že prijmú všetky primerané technické, organizačné a personálne opatrenia.

Článok V
Práva a povinnosti Sprostredkovateľa

5.1 Sprostredkovateľ je povinný spracúvať osobné údaje dotknutých osôb v súlade s touto Zmluvou, GDPR, ZOOÚ a ďalších súvisiacich právnych predpisov.

5.2 Sprostredkovateľ spracúva osobné údaje len na základe zdokumentovaných pokynov Prevádzkovateľa, preukázateľne doručených Sprostredkovateľovi, a to aj vtedy, ak ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, okrem prenosu na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Sprostredkovateľ je pri takom prenose povinný oznámiť Prevádzkovateľovi túto požiadavku pred spracúvaním osobných údajov, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, takéto oznámenie nezakazuje z dôvodov verejného záujmu.

5.3 Za zdokumentovaný a preukázateľne doručený pokyn sa považuje aj objednávka inštrukcia Prevádzkovateľa alebo inštrukcia doručená e-mailom na adresu kontaktných osôb uvedených v tejto Zmluve alebo ďalších osôb určených zmluvnými stranami. Sprostredkovateľ zaväzuje sa postupovať výlučne v súlade s pokynmi Prevádzkovateľa a prípadne inými internými predpismi Prevádzkovateľa a/alebo Prevádzkovateľa o ochrane osobných údajov, ktoré Prevádzkovateľ preukázateľne oznámi Sprostredkovateľovi. Medzi pokyny patria aj relevantné ustanovenia dodávateľskej zmluvy.

5.4 V prípade, ak by bol pokyn Prevádzkovateľa rozporný s GDPR alebo jeho splnenie by podľa právneho názoru Sprostredkovateľa mohlo viesť k porušeniu GDPR, je Sprostredkovateľ o možnom rozpore pokynu Prevádzkovateľa povinný informovať Prevádzkovateľa a vyžiadať si potvrdzujúci alebo nový pokyn Prevádzkovateľa.

5.5 Sprostredkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva podľa tejto Zmluvy a zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje (napríklad jeho zamestnanci alebo ďalší sprostredkovatelia) zaviazali, že zachovajú dôvernosť/mlčanlivosť o spracúvaných osobných údajoch Prevádzkovateľa.

5.6 Sprostredkovateľ je povinný prijať primerané technické a organizačné opatrenia, ktorými sa zabezpečí bezpečnosť spracúvania osobných údajov podľa čl. 32 GDPR. Predmetné opatrenia prijaté a zdokumentované Sprostredkovateľom v **Prílohe č. 1** tejto Zmluvy berie Prevádzkovateľ do úvahy a v čase uzatvorenia tejto Zmluvy ich považuje za dostatočné najmä s ohľadom na vyhlásenie Sprostredkovateľa v čase uzatvorenia tejto Zmluvy, že Sprostredkovateľ pri navrhovaní a následnej implementácii bezpečnostných opatrení zohľadnil:

a) všetky relevantné riziká, ktorých uplatnenie by mohlo viesť k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu a sprístupneniu spracúvaných osobných údajov,
b) náklady Sprostredkovateľa na vykonanie týchto bezpečnostných opatrení a
c) aktuálny stav poznania v oblasti informačnej bezpečnosti.

5.7 Prevádzkovateľ je povinný priebežne overovať a prehodnocovať primeranosť a účinnosť zavedených opatrení tak, aby predchádzal porušeniu bezpečnosti, ktoré by viedlo k náhodnému alebo nezákonnému poškodeniu, zničeniu, strate, zmene, zneužitiu, zverejneniu alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim, a to s ohľadom na svoju zodpovednosť podľa čl. 24 GDPR aj prostredníctvom auditov, spolupráce a žiadostí o súčinnosť doručených Sprostredkovateľovi v súlade s touto Zmluvou. V prípade potreby je Prevádzkovateľ najmä s ohľadom na pravdepodobnosť a závažnosť rizík týkajúcich sa spracúvania osobných údajov podľa tejto Zmluvy oprávnený pokynom Sprostredkovateľovi určiť zmeny v aplikovaných bezpečnostných opatreniach alebo doplnenie prijatých bezpečnostných opatrení novými vhodnými technickými a organizačnými opatreniami. To však nezbavuje Sprostredkovateľa jeho povinnosti podľa čl. 32 GDPR, v zmysle ktorej je povinný prijať primerané technické a organizačné opatrenia s ohľadom na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku.

5.8 Sprostredkovateľ je povinný plniť v mene Prevádzkovateľa jeho informačné povinnosti iba odkazovaním na informácie o spracúvaní osobných údajov, ktoré v súlade s čl. 13 a čl. 14 GDPR pripraví Prevádzkovateľ. Ak Prevádzkovateľ neposkytne Sprostredkovateľovi konkrétne informácie podľa predchádzajúcej vety a pokynom nespresní spôsob plnenia informačných povinností v konkrétnej situácii, Sprostredkovateľ je povinný počas získavania osobných údajov v mene Prevádzkovateľa alebo

pri prvom kontakte s dotknutou osobou odkazovať len na všeobecné informácie o ochrane osobných údajov, ktoré budú aktuálne dostupné na webovom sídle Prevádzkovateľa (www.nczisk.sk).

5.9 Sprostredkovateľ je povinný pomáhať Prevádzkovateľovi pri plnení povinnosti Prevádzkovateľa reagovať na žiadosti o výkon práv dotknutej osoby a ďalších povinností Prevádzkovateľa podľa čl. 32 až čl. 36 GDPR s prihliadnutím na povahu spracúvania a informácie dostupné Sprostredkovateľovi.

5.10 Sprostredkovateľ nie je oprávnený sám odpovedať na žiadosti dotknutých osôb a akékoľvek žiadosti dotknutých osôb doručené Sprostredkovateľovi, ktoré sa týkajú Prevádzkovateľa, je Sprostredkovateľ okamžite povinný preposlať Prevádzkovateľovi. Sprostredkovateľ je povinný poskytovať súčinnosť Prevádzkovateľovi aj v prípade akéhokoľvek konania alebo sporu týkajúceho sa alebo súvisiaceho so spracúvaním osobných údajov podľa tejto Zmluvy.

5.11 Sprostredkovateľ je povinný bez zbytočného odkladu informovať Prevádzkovateľa, ak sa domnieva, že pokynom Prevádzkovateľa dochádza k priamemu alebo nepriamo porušovaniu zákona, osobitného predpisu a/alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a ktorá sa týka ochrany osobných údajov.

5.12 Sprostredkovateľ je povinný prijať primerané opatrenia na zabezpečenie toho, aby jeho zamestnanci, poverení spracúvaním osobných údajov dotknutých osôb v zmysle tejto Zmluvy, spracúvali predmetné osobné údaje výlučne a len na základe a v súlade s pokynmi Prevádzkovateľa. Za týmto účelom využije Sprostredkovateľ najmä tieto postupy a metódy:

a) pseudonymizáciu a/alebo šifrovanie osobných údajov,
b) zabezpečenie kontinuálnej dôvernosti, integrity, dostupnosti a odolnosti informačných systémov, v ktorých sa spracúvajú osobné údaje,
c) proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,
d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti prijatých technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov,
e) zabezpečovanie pravidelných školení všetkých osôb poverených spracúvaním osobných údajov.

5.13 Sprostredkovateľ je povinný na písomnú výzvu Prevádzkovateľa uviesť informáciu o tom, aké technické, organizačné a/alebo iné opatrenia boli implementované, a to za účelom kontroly plnenia jeho povinností zo strany Prevádzkovateľa.

5.14 Sprostredkovateľ sa ďalej zaväzuje poskytovať Prevádzkovateľovi súčinnosť, ktorá je potrebná na:

a) zabezpečenie bezpečnosti spracúvania osobných údajov Prevádzkovateľom a/alebo Sprostredkovateľom,
b) oznámenie porušenia ochrany osobných údajov dozornému orgánu a dotknutým osobám,
c) vypracovanie posúdenia rizík pre práva a slobody dotknutých osôb, posúdenia vplyvu na ochranu osobných údajov a predchádzajúcu konzultáciu s dozorným orgánom.

5.15 Sprostredkovateľ sa zaväzuje oznámiť porušenie ochrany osobných údajov Prevádzkovateľovi bez zbytočného odkladu (do 24 hodín) po tom, ako sa Sprostredkovateľ o tomto porušení dozvedel. Sprostredkovateľ sa zaväzuje poskytnúť Prevádzkovateľovi všetky jemu dostupné informácie tak, aby Prevádzkovateľ mohol splniť povinnosti podľa čl. 33 a čl. 34 GDPR. Sprostredkovateľ sa zaväzuje poskytnúť informácie minimálne v rozsahu: opis povahy porušenia ochrany osobných údajov a rozsah porušenia, pravdepodobné následky uvedeného porušenia a všetky príslušné opatrenia prijaté za účelom odstránenia alebo zmiernenia následkov. Ak Sprostredkovateľ zmešká túto lehotu, je povinný uviesť aj dôvod zmeškania lehoty. Oznámenie porušenia ochrany osobných údajov Sprostredkovateľ oznamuje písomne alebo e-mailom (a následne písomne) Prevádzkovateľovi. Sprostredkovateľ nie je oprávnený oznamovať porušenie ochrany osobných údajov týkajúcich sa tejto Zmluvy dozorným orgánom ani dotknutým osobám, ak Prevádzkovateľ s takýmto postupom nevyjadrí súhlas prostredníctvom svojej zodpovednej osoby telefonicky alebo e-mailom.

5.16 Ak dôjde k porušeniu ochrany osobných údajov u Sprostredkovateľa, je Sprostredkovateľ povinný dané porušenie zdokumentovať v rozsahu podľa čl. 33 ods. 3 a ods. 5 GDPR, pričom predmetnú dokumentáciu poskytne Prevádzkovateľovi bezodkladne. V prípade neskoršieho aktualizovania

predmetnej dokumentácie o porušení ochrany osobných údajov postupuje Sprostredkovateľ primerane ako podľa predchádzajúcej vety.

5.17 Sprostredkovateľ poskytne Prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností v čl. 28 GDPR a umožní audity, ako aj kontroly vykonávané Prevádzkovateľom alebo iným audítorom, ktorého poveril Prevádzkovateľ, a prispieva k nim. Prípadné náklady, ktoré vzniknú s výkonom auditu znáša každá Zmluvná strana v plnej miere výlučne samostatne a nezávisle od druhej Zmluvnej strany bez akýchkoľvek nárokov na kompenzácie takýchto nákladov.

5.18 Sprostredkovateľ bezodkladne informuje Prevádzkovateľa o kontrolách a/alebo konaniach vykonávaných štátnymi orgánmi, najmä, nie však výlučne zo strany Úradu na ochranu osobných údajov Slovenskej republiky u Sprostredkovateľa a/alebo ďalšieho Prevádzkovateľa (subdodávateľa), ako aj o rozhodnutiach a opatreniach prijatých v súvislosti s týmito kontrolami a/alebo konaniami, pokiaľ Sprostredkovateľ má alebo má mať o príslušnej kontrole a/alebo konaní, rozhodnutí alebo opatrení vedomosť a ak sa akýmkoľvek spôsobom dotýkajú spracúvania osobných údajov podľa tejto Zmluvy.

5.19 Sprostredkovateľ nesmie osobné údaje spracúvané na základe tejto Zmluvy spracúvať na svoje vlastné účely. Sprostredkovateľ sa zaväzuje spracúvané osobné údaje nepoužiť v rozpore s oprávnenými záujmami a očakávaniami dotknutých osôb, neohrozovať ani nepoškodzovať ich práva a právom chránené záujmy a svojím konaním nesmie neoprávnene zasahovať do práva na ochranu ich osobnosti a súkromia. Táto Zmluva sa naopak netýka iných osobných údajov, ktoré Sprostredkovateľ získal a spracúva mimo plnenia tejto Zmluvy ako samostatný prevádzkovateľ.

Článok VI
Práva a povinnosti Prevádzkovateľa

6.1 Prevádzkovateľ vyhlasuje, že pri výbere Sprostredkovateľa dbal na odbornú, technickú, organizačnú a personálnu spôsobilosť Sprostredkovateľa a jeho schopnosť poskytnúť dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo zákonné požiadavky a aby sa zabezpečila ochrana práv dotknutých osôb.

6.2 Prevádzkovateľ sa zaväzuje poskytnúť Sprostredkovateľovi súčinnosť nevyhnutne potrebnú na plnenie povinností Sprostredkovateľa v zmysle a v rozsahu tejto Zmluvy a iných právnych predpisov, súvisiacich s ochranou osobných údajov. V prípade, ak Sprostredkovateľ v súvislosti so spracúvaním osobných údajov upozorní Prevádzkovateľa na spracúvanie neúplných, či nesprávnych osobných údajov, prípadne na možné porušenie GDPR, ZOOÚ alebo iných všeobecných alebo osobitných právnych predpisov, je Prevádzkovateľ povinný bez zbytočného odkladu zabezpečiť primeranú nápravu.

6.3 Prevádzkovateľ je oprávnený vykonať audit ochrany osobných údajov a kontrolu plnenia povinnosti Sprostredkovateľa:

a) pravidelne raz za kalendárny rok,
b) v prípade podozrenia z porušovania podmienok tejto Zmluvy, GDPR alebo ZOOÚ,
c) v prípade narušenia bezpečnosti údajov,
d) v prípade žiadosti dotknutej osoby podľa GDPR alebo ZOOÚ.

6.4 Prevádzkovateľ informuje Sprostredkovateľa o termíne vykonania auditu alebo kontroly oznámením zaslaným elektronickou poštou na e-mail uvedený v záhlaví tejto Zmluvy, a to minimálne sedem (7) dní vopred. Sprostredkovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit uskutočnil najneskôr do štrnásť (14) dní odo dňa zaslania oznámenia. Pokiaľ Sprostredkovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí. Audit alebo kontrola sa uskutoční v priestoroch Sprostredkovateľa tak, aby mohol byť naplnený príslušný účel kontroly. Počas auditu alebo kontroly je Sprostredkovateľ povinný zabezpečiť prítomnosť zodpovednej osoby, príp. inej osoby poverenej agendou ochrany osobných údajov a ďalších osôb potrebných pre poskytnutie kompletných informácií o ochrane osobných údajov.

Článok VII

Zapojenie ďalšieho sprostredkovateľa do spracúvania osobných údajov

7.1 Sprostredkovateľ je povinný dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa podľa čl. 28 ods. 2 a ods. 4 GDPR.

7.2 Sprostredkovateľ zodpovedá za všetko spracúvanie osobných údajov ďalšími sprostredkovateľmi ako keby spracúval osobné údaje sám a zaväzuje sa zaviazať ďalších sprostredkovateľov tými istými podmienkami ako sú upravené v tejto Zmluve.

7.3 Sprostredkovateľ prehlasuje, že na spracúvanie osobných údajov podľa tejto Zmluvy použije len nasledovných ďalších sprostredkovateľov, pričom ak by došlo k zmene ďalších sprostredkovateľov, Sprostredkovateľ si vyžiada predchádzajúci súhlas Prevádzkovateľa so zmenou:

Identifikácia ďalšieho sprostredkovateľa	Dôvod zapojenia	Zmluva uzatvorená aj s ohľadom na požiadavky podľa čl. 28 ods. 3 GDPR

7.4 Sprostredkovateľ garantuje Prevádzkovateľovi, že ďalší sprostredkovatelia podľa článku 7 bod 7.3 Zmluvy poskytujú dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky GDPR a aby sa zabezpečila ochrana práv dotknutej osoby.

7.5 Súhlas so zapojením ďalšieho sprostredkovateľa môže vykonať Prevádzkovateľ aj e-mailom.

Článok VIII
Právo na náhradu škody a zodpovednosť

8.1 Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním osobných údajov v rozpore s príslušnými ustanoveniami GDPR, ZOOÚ alebo ak konal nad rámec alebo v rozpore s touto Zmluvou alebo pokynmi Prevádzkovateľa.

8.2 Sprostredkovateľ sa môže zbaviť zodpovednosti v zmysle bodu 8.1 tejto Zmluvy v prípade ak preukáže, že vznik škody nezavinil.

8.3 Pokiaľ Prevádzkovateľ uhradil náhradu škody v plnej výške v súlade s čl. 82 GDPR, má právo žiadať od Sprostredkovateľa tú časť náhrady škody, ktorá zodpovedá jeho podielu zodpovednosti za škodu za podmienok uvedených v bode 8.1 tejto Zmluvy.

Článok IX
Doba trvania zmluvy

9.1 Zmluvné strany uzatvárajú túto Zmluvu na dobu určitú, a to do uplynutia doby platnosti a účinnosti dodávateľskej zmluvy.

9.2 Pred uplynutím dohodnutej doby platnosti tejto Zmluvy, môže táto Zmluva zaniknúť:

a) dohodou zmluvných strán v písomnej forme,
b) výpoveďou,
c) odstúpením od Zmluvy.

9.3 Prevádzkovateľ je oprávnený túto Zmluvu vypovedať bez udania dôvodu s výpovednou lehotou tri (3) mesiace. Výpovedná lehota začína plynúť prvým dňom kalendárneho mesiaca nasledujúceho po mesiaci, v ktorom bola doručená výpoveď Sprostredkovateľovi. Výpoveď musí byť v písomnej forme a doručená Sprostredkovateľovi.

9.4 Prevádzkovateľ je oprávnený od tejto Zmluvy odstúpiť, ak Sprostredkovateľ porušil povinnosti vyplývajúce mu z tejto Zmluvy, GDPR alebo ZOOÚ.

9.5 Sprostredkovateľ je oprávnený odstúpiť od tejto Zmluvy, ak Prevádzkovateľ trvá na spracúvaní osobných údajov dotknutých osôb Sprostredkovateľom podľa pokynov, aj keď ho Sprostredkovateľ bez zbytočného odkladu informoval, že má za to, že sa pokynom Prevádzkovateľa porušuje túto Zmluvu, osobitný právny predpis alebo medzinárodnú zmluvu, ktorou je Slovenská republika viazaná, a ktoré týkajú ochrany osobných údajov.

9.6 Prevádzkovateľ je kedykoľvek oprávnený rozhodnúť o obmedzení spracúvania alebo vymazaní osobných údajov podľa tejto Zmluvy doručením preukázateľného pokynu Sprostredkovateľovi, čím však nie je dotknutá platnosť a účinnosť tejto Zmluvy.

9.7 Po ukončení spracúvania osobných údajov v mene Prevádzkovateľa je Sprostredkovateľ povinný na základe pokynu Prevádzkovateľa všetky osobné údaje vymazať alebo vrátiť Prevádzkovateľovi a vymazať existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov; Sprostredkovateľ je povinný oznámiť Prevádzkovateľovi existenciu takéhoto všeobecne záväzného právneho predpisu.

9.8 Povinnosť mlčanlivosti podľa tejto Zmluvy platí aj po uplynutí jej platnosti a účinnosti, a to bez časového obmedzenia.

9.9 Zmluvné strany berú na vedomie, že uzatvorenie a existencia tejto zmluvy medzi Prevádzkovateľom a Sprostredkovateľom je povinnosťou podľa GDPR a/alebo ZOOÚ. Z uvedeného dôvodu je Prevádzkovateľ v prípade skončenia platnosti tejto Zmluvy oprávnený bez ďalšieho odstúpiť od dodávateľskej zmluvy uzatvorenej so Sprostredkovateľom.

Článok X
Doručovanie a komunikácia

10.1 Na doručovanie pokynov a iných písomnosti potrebných na plnenie tejto Zmluvy sa použijú kontaktné a korešpondenčné údaje uvedené v tejto Zmluve.

10.2 V prípade zmeny adries uvedených v tejto Zmluve sú Zmluvné strany povinné sa o týchto zmenách písomne informovať a následne po písomnom oznámení doručovať všetky podania na poslednú oznámenú adresu na doručovanie.

10.3 Akákoľvek písomnosť doručovaná pri plnení tejto Zmluvy Zmluvnou stranou poštou sa bude považovať za doručenú aj okamihom, keď sa písomnosť vráti odosielajúcej Zmluvnej strane späť s vyznačením „adresát neznámy" alebo „adresát neprevzal v odbernej lehote", a to bez ohľadu na to, či sa s odoslanou písomnosťou Zmluvné strany oboznámili alebo nie.

10.4 E-mail doručený kontaktnej osobe alebo inej osobe Zmluvnej strany sa bude považovať za doručený momentom jeho odoslania druhou Zmluvnou stranou, ak odosielateľ nedostal automatickú informáciu o nedoručení e-mailu.

10.5 Zmluvné strany sú si navzájom povinné poskytovať riadnu súčinnosť potrebnú na dodržiavanie tejto Zmluvy, GDPR a iných všeobecne záväzných právnych predpisov súvisiacich s ochranou osobných údajov alebo bezpečnosťou a ochranou informácií.

10.6 Zmluvné strany sú povinné navzájom otvorene komunikovať akékoľvek otázky a problémy týkajúce sa praktického dodržiavania a plnenia tejto Zmluvy a ochrany osobných údajov, pričom Zmluvné strany komunikujú prostredníctvom kontaktných údajov uvedených v tejto Zmluve, a to vrátane e-mailovej komunikácie. Zmenu kontaktných údajov a osôb sú Zmluvné strany povinné si vzájomne bezodkladne oznámiť.

Článok XI
Spoločné a záverečné ustanovenia

11.1 Táto Zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky, nie však skôr ako dňom nadobudnutia účinnosti dodávateľskej zmluvy.

11.2 Zmluvné strany sa zaväzujú vyvinúť maximálne možné úsilie na odstránenie vzájomných sporov vzniknutých na základe tejto Zmluvy alebo v súvislosti s touto Zmluvou a na ich vyriešenie predovšetkým prostredníctvom vzájomného rokovania a dohody. V prípade, že Zmluvné strany ani po vzájomných rokovania nedospejú k dohode alebo k riešeniu, budú všetky prípadné spory, vznikajúce z tejto Zmluvy a v súvislosti s ňou, rozhodované pred všeobecnými súdmi Slovenskej republiky, určenými podľa platných a účinných právnych predpisov o vecnej a miestnej príslušnosti súdov.

11.3 Túto Zmluvu je možné meniť a dopĺňať iba na základne písomnej dohody Zmluvných strán vo forme jednotlivo očíslovaných dodatkov k tejto Zmluve podpísaných oprávnenými zástupcami obidvoch Zmluvných strán, ak v Zmluve nie uvedené inak. Táto Zmluva je vyhotovená v štyroch (4) rovnopisoch, v dvoch (2) vyhotoveniach pre Prevádzkovateľa a dvoch (2) vyhotoveniach pre Sprostredkovateľa.

11.4 Zmluvné strany prehlasujú, že ich zmluvné prejavy sú dostatočne zrozumiteľné, určité a zmluvnú voľnosť nemajú obmedzenú. Zmluvné strany zároveň vyhlasujú, že túto Zmluvu neuzatvárali v tiesni, za nápadne nevýhodných podmienok, jej text si prečítali, obsahu porozumeli a na znak toho, že obsah dohody zodpovedá ich skutočnej a slobodnej vôli, Zmluvu vlastnoručne podpísali.

11.5 Akékoľvek odkazy na GDPR v tejto Zmluve znamenajú odkazy na významovo obdobné alebo relevantné ustanovenie ZOOÚ, ak by sa mal vzťahovať na dané spracúvanie namiesto alebo popri GDPR, a naopak.

11.6 Neoddeliteľnou súčasťou tejto Zmluvy je nasledovná príloha:

Príloha č. 1: Prijaté bezpečnostné opatrenia Sprostredkovateľa

Za Prevádzkovateľa:

V Bratislave, dňa

Mgr. Peter Lukáč, PhD.
generálny riaditeľ
Národné centrum zdravotníckych informácií

Za Sprostredkovateľa:

V Bratislave, dňa 19.08.2022

[redacted]

Ing. Zuzana Škodová Prochotská
člen predstavenstva
DATALAN, a.s.

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

Príloha č. 1 **Prijaté bezpečnostné opatrenia Sprostredkovateľa**

Technické a organizačné opatrenia prijaté Sprostredkovateľom podľa čl. 32 GDPR:	Áno	Nie
Zabezpečenie chráneného priestoru pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia)	☑	☐
Stála prítomnosť a dohľad povereného príjemcu osobných údajov nad akoukoľvek neoprávnenou osobou (napr. návšteva) počas jej zotrvávania v chránenom priestore Sprostredkovateľa, v ktorom sú spracúvané osobné údaje	☑	☐
Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)	☑	☐
Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí	☑	☐
Šifrová ochrana elektronických súborov s citlivými dátami alebo obsahom pri zasielaní e-mailom alebo odosielaní z databázy cez API	☑	☐
Prístup k informačným systémom len prostredníctvom hesiel	☑	☐
Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov	☑	☐
Používanie legálneho softvéru	☑	☐
Bezpečné vymazanie osobných údajov z dátových nosičov	☑	☐
Zariadenie na likvidáciu dátových nosičov osobných údajov napr. skartovačka	☑	☐
Pravidelná aktualizácia operačného systému a programového aplikačného vybavenia	☑	☐
Bezpečnostná politika ochrany osobných údajov určujúca organizačné postupy s vplyvom na bezpečnosť spracúvania osobných údajov	☑	☐
Interná politika IT bezpečnosti	☑	☐
Interná politika ochrany osobných údajov	☑	☐
Pseudonymizácia a primerané šifrovanie osobných údajov	☑	☐
Proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania	☑	☐
Ochrana pred nevyžiadanou elektronickou poštou (anti-spam)	☑	☐
Firewall	☑	☐
Logovanie a analýza logov	☑	☐
Vytváranie záloh s vopred zvolenou periodicitou	☑	☐

Vzájomné zastupovanie zamestnancov (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru)	☑	☐
Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti	☑	☐
Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých zamestnancov (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)	☑	☐
Pravidlá prístupu k internetu (napr. zamedzenie pripojenia k určitým webovým sídlam)	☑	☐
Test obnovy informačného systému zo zálohy	☑	☐
Test funkcionality dátového nosiča zálohy	☑	☐
Vymedzenie internej zodpovednosti za porušenie GDPR zamestnancami Sprostredkovateľa	☑	☐
Oboznámenie zamestnancov s prijatými internými politikami v oblasti ochrany osobných údajov	☑	☐
Vzdelávanie zamestnancov v oblasti ochrany osobných údajov a IT bezpečnosti	☑	☐
Vedenie zoznamu aktív a jeho aktualizácia	☑	☐
Kontrola vstupu do objektu a chránených priestorov Sprostredkovateľa	☑	☐
Prideľovanie prístupových práv a úrovní prístupu (rolí) zamestnancom	☑	☐
Testovanie nových funkcionalít bez použitia reálne spracúvaných osobných údajov	☑	☐
Správa silných hesiel	☑	☐
Monitorovacie úlohy zodpovednej osoby (DPO)	☑	☐
Monitorovacie úlohy manažéra pre kyber-bezpečnosť	☑	☐
Pravidlá pre zvýšené zabezpečenie API komunikácie (filtrovanie IP adries, autentizácia, fail2ban, blokovanie objemového útoku, rate limmiting)	☑	☐
Vykonanie nezávislého bezpečnostného auditu	☑	☐

9 ČESTNÉ VYHLÁSENIE O NEPRÍTOMNOSTI KONFLIKTU ZÁUJMOV

ČESTNÉ VYHLÁSENIE O NEPRÍTOMNOSTI KONFLIKTU ZÁUJMOV

DATALAN, a.s., Krasovského 14, 851 01 Bratislava, IČO: 35 810 734, spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B., zastúpený Ing. Zuzana Škodová Prochotská, člen predstavenstva ako uchádzač, ktorý predložil ponuku do zadávania zákazky na predmet zákazky **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"** vyhlásenom verejným obstarávateľom Národné centrum zdravotníckych informácií, Lazaretská 26, 811 09 Bratislava oznámením o vyhlásení verejného obstarávania zverejneným v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS

týmto vyhlasujem, že v súvislosti s uvedeným postupom zadávania zákazky:

- som nevyvíjal a nebudem vyvíjať voči žiadnej osobe na strane verejného obstarávateľa, ktorá je alebo by mohla byť zainteresovanou osobou v zmysle ustanovenia § 23 ods. 3 ZVO (ďalej len „zainteresovaná osoba") akékoľvek aktivity, ktoré by mohli viesť k zvýhodneniu nášho postavenia v postupe tohto verejného obstarávania,
- neposkytol som a neposkytnem akejkoľvek čo i len potenciálne zainteresovanej osobe priamo alebo nepriamo akúkoľvek finančnú alebo vecnú výhodu ako motiváciu alebo odmenu súvisiacu so zadaním tejto zákazky,
- budem bezodkladne informovať verejného obstarávateľa o akejkoľvek situácii, ktorá je považovaná za konflikt záujmov alebo ktorá by mohla viesť ku konfliktu záujmov kedykoľvek v priebehu procesu verejného obstarávania,
- poskytnem verejnému obstarávateľovi v postupe tohto verejného obstarávania presné, pravdivé a úplné informácie

V Bratislave, dňa 19.08.2022

.....

Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

10 ČESTNÉ VYHLÁSENIE UCHÁDZAČA O ZHODNOSTI DOKUMENTOV

ČESTNÉ VYHLÁSENIE O ZHODE ELEKTRONICKÝCH DOKUMENTOV S ORIGINÁLNYMI DOKUMENTMI

DATALAN, a.s., Krasovského 14, 851 01 Bratislava, IČO: 35 810 734, spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B., zastúpený Ing. Zuzana Škodová Prochotská, člen predstavenstva ako uchádzač, ktorý predložil ponuku do zadávania zákazky na predmet zákazky **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"** vyhlásenom verejným obstarávateľom Národné centrum zdravotníckych informácií, Lazaretská 26, 811 09 Bratislava oznámením o vyhlásení verejného obstarávania zverejneným v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS

týmto čestne vyhlasujem, že dokumenty predložené elektronicky v ponuke uchádzača, sú zhodné s originálnymi dokumentmi.

V Bratislave, dňa 19.08.2022 ...

Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

11 ZOZNAM DÔVERNÝCH INFORMÁCIÍ

ZOZNAM DÔVERNÝCH INFORMÁCIÍ

DATALAN, a.s., Krasovského 14, 851 01 Bratislava, IČO: 35 810 734, spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č.: 2704/B., zastúpený Ing. Zuzana Škodová Prochotská, člen predstavenstva ako uchádzač, ktorý predložil ponuku do zadávania zákazky na predmet zákazky **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"** vyhlásenom verejným obstarávateľom Národné centrum zdravotníckych informácií, Lazaretská 26, 811 09 Bratislava oznámením o vyhlásení verejného obstarávania zverejneným v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS

týmto vyhlasujem, že predložená ponuka

~~-neobsahuje žiadne dôverné informácie.*~~
~~-obsahuje dôverné informácie, ktoré sú v ponuke označené slovom „DÔVERNÉ".*~~
-obsahuje nasledovné dôverné informácie:*

P. č.	Názov dokumentu	Strana ponuky
1	Vlastný návrh riešenia predmetu zákazky	bod 13. ponuky
2	Stručná sumarizácia navrhovaného riešenia	bod 13. ponuky
3	Štruktúrovaný rozpočet	bod 15. ponuky

V Bratislave, dňa 19.08.2022

.....
Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

12 SÚHLAS SO SPRACOVANÍM OSOBNÝCH ÚDAJOV

Uchádzač/~~skupina dodávateľov~~:
DATALAN, a.s.
Krasovského 14
IČO: 35 810 734

Dolu podpísaný zástupca uchádzača, ktorý predložil ponuku do zadávania zákazky na predmet zákazky s názvom **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"** vyhlásenej verejným obstarávateľom Národné centrum zdravotníckych informácií so sídlom Lazaretská 26, 811 09 Bratislava, Slovenská republika v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS

týmto udeľujem

verejnému obstarávateľovi Národné centrum zdravotníckych informácií so sídlom Lazaretská 26, 811 09 Bratislava, Slovenská republika ako prevádzkovateľovi súhlas na spracúvanie osobných údajov v rozsahu potrebnom na účel vyhodnotenia splnenia podmienok účasti a vyhodnotenia ponúk vo verejnom obstarávaní na vyššie uvedený predmet zákazky.

Účel spracúvania osobných údajov: preukázanie splnenia podmienok účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo verejnom obstarávaní na predmet **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)"**. Právny základ spracúvania: súhlas dotknutej osoby – článok 6 ods. 1 písm. a) nariadenia GDPR.

Prevádzkovateľ bude osobné údaje spracúvať odo dňa ich poskytnutia, najdlhšie na dobu podľa § 39 ods. 3 zákona č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov.

Dotknutá osoba má právo kedykoľvek odvolať tento svoj súhlas, a to rovnakým spôsobom ako ho poskytuje alebo písomne, priamo u prevádzkovateľa podľa toho, ktorý spôsob dotknutej osobe viac vyhovuje. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania vychádzajúceho zo súhlasu pred jeho odvolaním. Ďalšie informácie týkajúce sa spracúvania osobných údajov, ako právo požadovať od prevádzkovateľa prístup k osobným údajom, právo na opravu osobných údajov, právo na výmaz osobných údajov alebo právo na obmedzenie spracúvania osobných údajov a pod. sú dostupné na webovom sídle prevádzkovateľa.

Som si vedomá/-ý, že poskytnutie osobných údajov, ako aj udelenie súhlasu s ich spracúvaním je dobrovoľné. Súhlas môžem kedykoľvek odvolať zaslaním písomného odvolania súhlasu na adresu prevádzkovateľa. Odvolanie súhlasu je účinné dňom jeho doručenia.

Ako dotknutá osoba vyhlasujem, že poskytnuté osobné údaje sú pravdivé, aktuálne a boli poskytnuté slobodne a potvrdzujem vlastnoručným podpísaním tohto dokumentu, že prevádzkovateľ splnil oznamovaciu povinnosť v súlade s článkom 13 nariadenia GDPR.

V Bratislave, dňa 19.08.2022 ...

Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

13 VLASTNÝ NÁVRH PLNENIA/ TECHNICKÁ ŠPECIFIKÁCIA

Dôverné

a) **Vlastný návrh riešenia/plnenia predmetu zákazky** (podrobný technický popis navrhovaného riešenia) v súlade s požiadavkami špecifikovanými v časti B.1 Opis predmetu zákazky a B.2 Obchodné podmienky dodania predmetu zákazky týchto súťažných podkladov;

b) **Stručná sumarizácia navrhovaného riešenia** vypracovaná podľa Prílohy č. 3.12 týchto súťažných podkladov.

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

DÔVERNÉ

14 VYHLÁSENIE O VYPRACOVANÍ PONUKY

Uchádzač/~~skupina dodávateľov~~:
Obchodné meno DATALAN, a.s.
Adresa spoločnosti Krasovského 14, 851 01 Bratislava
IČO 35 810 734

Čestné vyhlásenie

Dolu podpísaný zástupca uchádzača týmto čestne vyhlasujem, že ponuku na predmet zákazky s názvom **„Rozšírenie portfólia služieb a inovácia služieb elektronického zdravotníctva (VS)“**, vyhlásenej verejným obstarávateľom **Národné centrum zdravotníckych informácií**, so sídlom Lazaretská 26, 811 09 Bratislava, v Úradnom vestníku EÚ zo dňa 15.06.2022 pod číslom 2022/S 114-321736 a vo Vestníku verejného obstarávania č. 138/2022 zo dňa 16.06.2022 pod číslom 29600-MSS som

vypracoval – ~~nevypracoval~~ sám.
(nehodiace sa preškrtnúť)

Identifikačné údaje osoby, ktorej služby alebo podklady som/sme pri vypracovaní ponuky využil:

Meno a priezvisko: -----

Adresa pobytu: -----

Obchodné meno alebo názov spoločnosti: ---

Sídlo alebo miesto podnikania: ---

IČO: ---

V Bratislave, dňa 19.08.2022 .....

Ing. Zuzana Škodová Prochotská
člen predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175
- 6 -

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

15 ŠTRUKTUROVANÝ ROZPOČET

-predložené aj v xls.

Dôverné

DATALAN, a. s., Krasovského 14, 851 01 Bratislava, Tel.: +421 2 50 25 77 77, Fax: +421 2 50 25 77 00, info@datalan.sk, www.datalan.sk
IČO: 35 810 734, IČ DPH: SK2020259175, banka: Tatra banka, a.s., číslo účtu: 2627106780/1100, IBAN: SK87 1100 0000 0026 2710 6780
Spoločnosť je zapísaná v Obchodnom registri Okresného súdu Bratislava 1, oddiel: Sa, vložka č. 2704/b

Názov spoločnosti:	**DATALAN, a.s.**
Sídlo spoločnosti:	**Krasovského 14, 851 01 Bratislava**
IČO spoločnosti:	**35810734**
Platca DPH? ÁNO/NIE	**ÁNO**
Kontaktná osoba (meno, email, telefonický kontakt)	**Ing. Dušan Polóny, mail: dusan_polony@datalan.sk, tel.: +421 907 745 482**

ŠTRUKTÚROVANÝ ROZPOČET ZA VEREJNÉ OBSTARÁVANIE AKO CELOK - ZHRNUTIE

Položka rozpočtu	Jednotková cena v EUR bez DPH	DPH v EUR	Jednotková cena v EUR s DPH	Počet jednotiek	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Dielo RISEZ					5 570 145,00 €	1 114 029,00 €	6 684 174,00 €
Služby podpory prevádzky a údržby (paušálne služby) - ezdravie pred RISEZ	72 000,00 €	14 400,00 €	86 400,00 €	12	864 000,00 €	172 800,00 €	1 036 800,00 €
Služby podpory prevádzky a údržby (paušálne služby) - KISnoRed	18 000,00 €	3 600,00 €	21 600,00 €	60	1 080 000,00 €	216 000,00 €	1 296 000,00 €
Služby podpory prevádzky a údržby (paušálne služby) - KISRed	63 000,00 €	12 600,00 €	75 600,00 €	60	3 780 000,00 €	756 000,00 €	4 536 000,00 €
Služby podpory prevádzky a údržby (paušálne služby) - KIS	9 000,00 €	1 800,00 €	10 800,00 €	60	540 000,00 €	108 000,00 €	648 000,00 €
Objednávková služba RaM					1 200 000,00 €	240 000,00 €	1 440 000,00 €
Objednávkové služby - rozvoj systému	400,00 €	80,00 €	480,00 €	3000	1 200 000,00 €	240 000,00 €	1 440 000,00 €
Celková cena za					**14 234 145,00 €**	**2 846 829,00 €**	**17 080 974,00 €**

Hospodársky subjekt vyplní takto zvýraznené bunky - v tejto záložke len identifikačné údaje, ktoré sa prenesú do ostatných záložiek

V Bratislave, dňa 19.09.2022

[redacted]

Názov spoločnosti:	DATALAN, a.s.
Sídlo spoločnosti:	Krasovského 14, 851 01 Bratislava
IČO spoločnosti:	35810734
Platca DPH? ÁNO/NIE	ÁNO
Kontaktná osoba	Ing. Dušan Polóny, mail: dusan_polony@datalan.sk, tel.: +421 907 745 482

ŠTRUKTÚROVANÝ ROZPOČET ZA DIELO

Rola/Produkt:	Sadzba/1 MD, resp. ks v EUR bez DPH	DPH v EUR	Sadzba/1MD, resp. ks v EUR s DPH	Počet MD*, resp. ks	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Projektový manažér	505,00 €	101,00 €	606,00 €	420,00	212 100,00 €	42 420,00 €	254 520,00 €
IT analytik	505,00 €	101,00 €	606,00 €	3000,00	1 515 000,00 €	303 000,00 €	1 818 000,00 €
IT architekt	505,00 €	101,00 €	606,00 €	567,00	286 335,00 €	57 267,00 €	343 602,00 €
IT programátor/vývojár	505,00 €	101,00 €	606,00 €	3000,00	1 515 000,00 €	303 000,00 €	1 818 000,00 €
IT tester	400,00 €	80,00 €	480,00 €	967,00	386 800,00 €	77 360,00 €	464 160,00 €
Odborník pre IT dohľad/Quality Assurance	505,00 €	101,00 €	606,00 €	186,00	93 930,00 €	18 786,00 €	112 716,00 €
Release manažér	505,00 €	101,00 €	606,00 €	500,00	252 500,00 €	50 500,00 €	303 000,00 €
Špecialista pre bezpečnosť IT	505,00 €	101,00 €	606,00 €	437,00	220 685,00 €	44 137,00 €	264 822,00 €
Špecialista pre infraštruktúry/HW špecialista	505,00 €	101,00 €	606,00 €	626,00	316 130,00 €	63 226,00 €	379 356,00 €
Školiteľ pre IT systémy	400,00 €	80,00 €	480,00 €	60,00	24 000,00 €	4 800,00 €	28 800,00 €
Systémový špecialista	505,00 €	101,00 €	606,00 €	1433,00	723 665,00 €	144 733,00 €	868 398,00 €
Dokumentarista	400,00 €	80,00 €	480,00 €	60,00	24 000,00 €	4 800,00 €	28 800,00 €
Iné (pozícia, ktorú nie je možné zaradiť do vyššie uvedených	- €	- €	- €		- €	- €	- €
Preexistentný SW**	*Presenie sa automaticky sumárna cena vyplnením nasledujúcej tabuľky =>*				- €	- €	- €
Celková cena za dielo					**5 570 145,00 €**	**1 114 029,00 €**	**6 684 174,00 €**

** Pozn.: Verejný obstarávateľ v predloženej žiadosti o nenávratný finančný príspevok počíta s objemom 13 227 človekodní (MD) za časť predmetu zákazky týkajúcu sa dodania diela (riadky 12 - 23 vyššie)*

*** Ak návrh riešenia počíta aj s využitím preexistentného SW, hospodársky subjekt Vyplní aj nasledujúcu tabuľku a skontroluje, či sa súčtový riadok nižšie uvedenej tabuľky preniesol správne do tohto riadku, súčasťou ceny je vyplatenie alikvotnej čiastky licenčného pokrytia z NFP v rozsahu od dodania licencie v súlade s harmonogramom diela do ukončenia realizácie hlavných aktivít diela*

ŠTRUKTÚROVANÝ ROZPOČET ZA DIELO - SW tretích strán - dekompozícia

Produkt:	Jednotková cena v EUR bez DPH	DPH v EUR	Jednotková cena v EUR s DPH	Počet jednotiek	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Preexistentný SW*** *(hospodársky subjekt doplní za každý preexistentný SW samostatný riadok)*	- €	- €	- €		- €	- €	- €
		- €	- €		- €	- €	- €
		- €	- €		- €	- €	- €
Celková cena za Preexistentný SW					**- €**	**- €**	**- €**

**** Ak návrh riešenia počíta aj s využitím preexistentného SW, hospodársky subjekt rozšíri tabuľk*
SW", súčasťou ceny je vyplatenie alikvotnej čiastky licenčného pokrytia z NFP v rozsahu od dodan

Uchádzač vyplní takto zvýraznené bunky

1.

Názov spoločnosti:	DATALAN, a.s.
Sídlo spoločnosti:	Krasovského 14, 851 01 Bratislava
IČO spoločnosti:	35810734
Platca DPH? ÁNO/NIE	ÁNO
Kontaktná osoba	Ing. Dušan Polóny, mail: dusan_polony@datalan.sk, tel.: +421 907 745 482

Služby podpory prevádzky a údržby (paušálne služby) - ezdravie pred RISEZ / KISnoRed							
Názov aktivity	Výška mesačného paušálu v EUR bez DPH	DPH v EUR	Výška mesačného paušálu v EUR s DPH	Max. doba poskytovania služby	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
1. Služby podpory prevádzky a údržby (paušálne služby) - ezdravie pred RISEZ	72 000,00 €	14 400,00 €	86 400,00 €	12	864 000,00 €	172 800,00 €	1 036 800,00 €
2. Služby podpory prevádzky a údržby (paušálne služby) - KISnoRed (časť Systému bez Redizajnu)	18 000,00 €	3 600,00 €	21 600,00 €	60	1 080 000,00 €	216 000,00 €	1 296 000,00 €

Služby podpory prevádzky a údržby (paušálne služby) - KISRed (časť Systému po Redizajne vykonaného v rámci Diela RISEZ)							
Výdavok / Položka	Výška mesačného paušálu v EUR bez DPH	DPH v EUR	Výška mesačného paušálu v EUR s DPH	Max. doba poskytovania služby	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
3. Paušálne služby podľa prílohy č. 1	63 000,00 €	12 600,00 €	75 600,00 €	60	3 780 000,00 €	756 000,00 €	4 536 000,00 €
4. Licenčné poplatky *(ak aplikovateľné)* *Prenesú sa z tabuľky - Licenčné poplatky - dekompozíca*		- €	- €	60	- €	- €	- €
Cena celkom	63 000,00 €	12 600,00 €	75 600,00 €	60	3 780 000,00 €	756 000,00 €	4 536 000,00 €

Služby podpory prevádzky a údržby (paušálne služby) - KIS (Komplexný systém po Redizajne v rámci Diela RISEZ a Redizajne v rámci SLA)							
Výdavok / Položka	Výška mesačného paušálu v EUR bez DPH	DPH v EUR	Výška mesačného paušálu v EUR s DPH	Max. doba poskytovania služby	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
5. Paušálne služby podľa prílohy č. 1	9 000,00 €	1 800,00 €	10 800,00 €	60	540 000,00 €	108 000,00 €	648 000,00 €
6. Licenčné poplatky *(ak aplikovateľné)* *Prenesú sa z tabuľky - Licenčné poplatky - dekompozíca*	- €	- €	- €	60	- €	- €	- €
Cena celkom	9 000,00 €	1 800,00 €	10 800,00 €	60	540 000,00 €	108 000,00 €	648 000,00 €

Licenčné poplatky RISEZ - dekompozícia							
Licenčný poplatok	Jednotková cena v EUR bez DPH	DPH v EUR	Jednotková cena v EUR s DPH	Počet jednotiek	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Preexistentný SW č. 1 *(hospodársky subjekt doplní za každý preexistentný SW)*		- €	- €	60	- €	- €	- €
		- €	- €	60	- €	- €	- €
		- €	- €	60	- €	- €	- €
Cena celkom	- €	- €	- €	60	- €	- €	- €

Licenčné poplatky Redizajn a migrácia - dekompozícia							
Licenčný poplatok	Jednotková cena v EUR bez DPH	DPH v EUR	Jednotková cena v EUR s DPH	Počet jednotiek	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Preexistentný SW č. 1 (hospodársky subjekt doplní za každý preexistentný SW)		- €	- €	60	- €	- €	- €
		- €	- €	60	- €	- €	- €
		- €	- €	60	- €	- €	- €
Cena celkom	- €	- €	- €	60	- €	- €	- €

Uchádzač vyplní takto zvýraznené bunky

V Bratislave, dňa 19.08.2022

[redacted]

1

Názov spoločnosti:	DATALAN, a.s.
Sídlo spoločnosti:	Krasovského 14, 851 01 Bratislava
IČO spoločnosti:	35810734
Platca DPH? ÁNO/NIE	ÁNO
Kontaktná osoba	Ing. Dušan Polóny, mail: dusan_polony@datalan.sk, tel.: +421 907 745 482

ŠTRUKTÚROVANÝ ROZPOČET ZA OBJEDNÁVKOVÚ SLUŽBU
REDIZAJN A MIGRÁCIA NA NOVÚ ARCHITEKTÚRU "KOMPLEXNÉHO SYSTÉMU BEZ REDIZAJNU" ("RaM")

Výdavok / Položka	Jednotková cena za človekodeň/ licencie za vyriešenie objednávky bez DPH (v EUR)	DPH v EUR	Jednotková cena za človekodeň/ licencie za vyriešenie objednávky s DPH (v EUR)	Počet človekodní/ licencií za dobu poskytovania služby*	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Projektový manažér	400,00 €	80,00 €	480,00 €	110,00	44 000,00 €	8 800,00 €	52 800,00 €
IT analytik	400,00 €	80,00 €	480,00 €	800,00	320 000,00 €	64 000,00 €	384 000,00 €
IT architekt	400,00 €	80,00 €	480,00 €	150,00	60 000,00 €	12 000,00 €	72 000,00 €
IT programátor/vývojár	400,00 €	80,00 €	480,00 €	800,00	320 000,00 €	64 000,00 €	384 000,00 €
IT tester	400,00 €	80,00 €	480,00 €	260,00	104 000,00 €	20 800,00 €	124 800,00 €
Odborník pre IT dohľad/Quality Assurance	400,00 €	80,00 €	480,00 €	50,00	20 000,00 €	4 000,00 €	24 000,00 €
Release manažér	400,00 €	80,00 €	480,00 €	120,00	48 000,00 €	9 600,00 €	57 600,00 €
Špecialista pre bezpečnosť IT	400,00 €	80,00 €	480,00 €	120,00	48 000,00 €	9 600,00 €	57 600,00 €
Špecialista pre infraštruktúry/HW špecialista	400,00 €	80,00 €	480,00 €	170,00	68 000,00 €	13 600,00 €	81 600,00 €
Školiteľ pre IT systémy	400,00 €	80,00 €	480,00 €	20,00	8 000,00 €	1 600,00 €	9 600,00 €
Systémový špecialista	400,00 €	80,00 €	480,00 €	360,00	144 000,00 €	28 800,00 €	172 800,00 €
Dokumentarista	400,00 €	80,00 €	480,00 €	40,00	16 000,00 €	3 200,00 €	19 200,00 €
Iné (pozícia, ktorú nie je možné zaradiť do vyššie uvedených		- €	- €		- €	- €	- €
7. Celková cena za Objednávkovú službu RaM bez preexistentného SW					**1 200 000,00 €**	**240 000,00 €**	**1 440 000,00 €**
8. Preexistentný SW** *(ak aplikovateľné)*					- €	- €	- €
Celková cena za za Objednávkovú službu RaM					**1 200 000,00 €**	**240 000,00 €**	**1 440 000,00 €**

*** Ak návrh RaM počíta aj s využitím preexistentného SW , hospodársky subjekt Vyplní aj nasledujúcu tabuľku a skontroluje, či sa súčtový riadok nižšie uvedenej tabuľky preniesol správne do riadku 26*

ŠTRUKTÚROVANÝ ROZPOČET ZA OBJEDNÁVKOVÚ SLUŽBU RaM - SW tretích strán - dekompozícia

Produkt:	Jednotková cena v EUR bez DPH	DPH v EUR	Jednotková cena v EUR s DPH	Počet jednotiek	Cena spolu v EUR bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
Preexistentný SW č. 1*** *(hospodársky subjekt doplní za každý SW samostatný riadok)*		- €	- €		- €	- €	- €
		- €	- €		- €	- €	- €
		- €	- €		- €	- €	- €
Celková cena za SW tretích strán					**- €**	**- €**	**- €**

**** Ak návrh RaM počíta aj s využitím preexistentného SW , hospodársky subjekt rozšíri tabuľku o potrebný počet riadk[redacted] „Preexistentný SW č. 1"*

Uchádzač vyplní takto zvýraznené bunky

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Názov spoločnosti:	**DATALAN, a.s.**
Sídlo spoločnosti:	**Krasovského 14, 851 01 Bratislava**
IČO spoločnosti:	**35810734**
Platca DPH? ÁNO/NIE	**ÁNO**
Kontaktná osoba	**Ing. Dušan Polóny, mail: dusan_polony@datalan.sk, tel.: +421 907 745 482**

ŠTRUKTÚROVANÝ ROZPOČET ZA OBJEDNÁVKOVÉ SLUŽBY - ROZVOJ SYSTÉMU

Výdavok / Položka	Cena za človekodeň za vyriešenie objednávky bez DPH (v EUR)	DPH v EUR	Cena za človekodeň za vyriešenie objednávky s DPH (v EUR)	Počet človekodní za dobu poskytovania služby*	Cena spolu bez DPH	Spolu DPH v EUR	Cena spolu v EUR s DPH
9. Objednávkové služby - rozvoj systému	400,00 €	80,00 €	480,00 €	**3000**	1 200 000,00 €	240 000,00 €	1 440 000,00 €

**Pozn.: počet človekodní za dobu poskytovania objednávkových služieb predstavuje 600 človekodní ročne, t. j. 3000 človekdní za obdobie 5 rokov*

Uchádzač vyplní takto zvýraznené bunky

V Bratislave, dňa 19.08.2022

[redacted]

1.

Etapa	Obsah etapy	% podiel z celkovej ceny za Dielo	Počet ks; MD*	Cena spolu v EUR bez DPH za etapu	Suma DPH	Cena spolu v EUR s DPH za etapu	Fakturačný míľnik (rozmedzie v mesiacoch)**
1. fakturačný míľnik	**Analýza a dizajn**			**0,00**	**0,00**	**0,00**	**T+4**
nákup (v ks):	Nákup preexistentného SW		0	0,00	0,00	0,00	-
2. fakturačný míľnik, z toho:	**Ukončenie: Analýza a dizajn**			**1 490 760,00**	**298 152,00**	**1 788 912,00**	**T+10 až 11**
role (v MD):	Dokumentarista	max. 27% z ceny za Dielo	0,00	0,00	0,00	0,00	-
	IT analytik		1 700,00	858 500,00	171 700,00	1 030 200,00	-
	IT architekt		300,00	151 500,00	30 300,00	181 800,00	-
	IT programátor/vývojár		400,00	202 000,00	40 400,00	242 400,00	-
	IT tester		0,00	0,00	0,00	0,00	-
	Projektový manažér		120,00	60 600,00	12 120,00	72 720,00	-
	Quality Assurance		36,00	18 180,00	3 636,00	21 816,00	-
	Release manažér		0,00	0,00	0,00	0,00	-
	Systémový špecialista		133,00	67 165,00	13 433,00	80 598,00	-
	Školiteľ pre IT systémy		0,00	0,00	0,00	0,00	-
	Špecialista pre bezpečnosť IT		137,00	69 185,00	13 837,00	83 022,00	-
	Špecialista pre infraštruktúry/HW špecialista		126,00	63 630,00	12 726,00	76 356,00	-
3. fakturačný míľnik, z toho:	**Ukončenie: Implementácia a testovanie plus nasadenie DEVD prostredie**			**3 508 875,00**	**701 775,00**	**4 210 650,00**	**T+13 až 14**
role (v MD):	Dokumentarista	max. 77 % z ceny za Dielo	30,00	12 000,00	2 400,00	14 400,00	-
	IT analytik		1 250,00	631 250,00	126 250,00	757 500,00	-
	IT architekt		200,00	101 000,00	20 200,00	121 200,00	-
	IT programátor/vývojár		2 500,00	1 262 500,00	252 500,00	1 515 000,00	-
	IT tester		800,00	320 000,00	64 000,00	384 000,00	-
	Projektový manažér		200,00	101 000,00	20 200,00	121 200,00	-
	Quality Assurance		75,00	37 875,00	7 575,00	45 450,00	-
	Release manažér		400,00	202 000,00	40 400,00	242 400,00	-
	Systémový špecialista		1 200,00	606 000,00	121 200,00	727 200,00	-
	Školiteľ pre IT systémy		20,00	8 000,00	1 600,00	9 600,00	-
	Špecialista pre bezpečnosť IT		200,00	101 000,00	20 200,00	121 200,00	-
	Špecialista pre infraštruktúry/HW špecialista		250,00	126 250,00	25 250,00	151 500,00	-
4. fakturačný míľnik, z toho:	**Ukončenie: Nasadenie DEVO/INT/PREPROD/PROD + migrácia údajov, dokončovacia fáza**			**570 510,00**	**114 102,00**	**684 612,00**	**T+15 až 16**
role (v MD):	Dokumentarista	max. 15 % z ceny za Dielo	30,00	12 000,00	2 400,00	14 400,00	-
	IT analytik		50,00	25 250,00	5 050,00	30 300,00	-
	IT architekt		67,00	33 835,00	6 767,00	40 602,00	-
	IT programátor/vývojár		100,00	50 500,00	10 100,00	60 600,00	-
	IT tester		167,00	66 800,00	13 360,00	80 160,00	-
	Projektový manažér		100,00	50 500,00	10 100,00	60 600,00	-
	Quality Assurance		75,00	37 875,00	7 575,00	45 450,00	-
	Release manažér		100,00	50 500,00	10 100,00	60 600,00	-
	Systémový špecialista		100,00	50 500,00	10 100,00	60 600,00	-
	Školiteľ pre IT systémy		40,00	16 000,00	3 200,00	19 200,00	-
	Špecialista pre bezpečnosť IT		100,00	50 500,00	10 100,00	60 600,00	-
	Špecialista pre infraštruktúry/HW špecialista		250,00	126 250,00	25 250,00	151 500,00	-
Celkový max. počet MD na projekt			**13 227**	**5 570 145,00**	**1 114 029,00**	**6 684 174,00**	-

**jednotlivé časti diela musia byť dodávané a fakturované v termíne rozmedzia, ktorý je jednotne definovaný v časovom harmonograme a fakturačných míľnikoch; písmeno "T" je dátum účinnosti ZoD.	
*MD - človekodeň (man-day)	
	polia označené slabo žltou farbou vypĺňa dodávateľ; role, ktoré v daných etapách neobsadí (nevyužije), napíše do príslušnej bunky číslicu "0"

V Bratislave, dňa 19.08.2022

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175