Zmluva na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky
uzavretá podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

(ďalej len „zmluva")

Článok I.
Zmluvné strany

1.1. Objednávateľ:

Názov:	Sociálna poisťovňa
Sídlo:	Ul. 29 augusta 8 a 10, 813 63 Bratislava
IČO:	30 807 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK4081800000007000164314
SWIFT:	SPSRSKBA
Zastúpený:	Ing. Michal Tariška, generálny riaditeľ Sociálnej poisťovne

(ďalej len „objednávateľ")

1.2. Poskytovateľ:

Obchodné meno:	DATALAN, a.s.
Sídlo:	Krasovského 14, 851 01Bratislava
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
Bankové spojenie:	
Číslo účtu:	
Zastúpený:	Ing. Juraj Zelko - Člen predstavenstva
Registrovaný v:	Obchodný register Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 2704/B

(ďalej len „poskytovateľ")
(ďalej spolu len „zmluvné strany")

Zmluvné strany sa v súlade s § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov dohodli na uzavretí tejto zmluvy na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky (ďalej len „zmluva"). Podkladom na uzatvorenie tejto zmluvy je ponuka poskytovateľa predložená objednávateľovi vo verejnom obstarávaní.

Článok II.
Predmet zmluvy

2.1. Predmetom tejto zmluvy je úprava práv a povinností zmluvných strán pri zabezpečovaní pozáručného servisu, údržby a opráv výpočtovej techniky objednávateľa bližšie špecifikovanej v prílohe č. 1 tejto zmluvy – Zoznam zariadení (ďalej aj len ako „zariadenia"), vrátane dodávky a montáže spotrebného materiálu a náhradných dielov, likvidácie nefunkčného dielu zariadenia a posúdenia technického stavu zariadenia (ďalej spolu aj len ako „servisné služby").

2.2. Objednávateľ sa zaväzuje uhradiť poskytovateľovi za riadne poskytnuté/ vykonané servisné služby cenu vo výške a za podmienok uvedených v čl. IV. a V. a v prílohe č. 2 tejto zmluvy.

Článok III.
Spôsob, miesto a čas plnenia predmetu zmluvy

3.1. Poskytovateľ bude poskytovať servisné služby na základe požiadaviek objednávateľa, v ktorých bude identifikovaný typ zariadenia, na ktorom majú byť vykonávané servisné služby spolu s popisom problému, ktorý je potrebné odstrániť.

3.2. Miestom plnenia sú priestory objednávateľa na adrese: Sociálna poisťovňa, ústredie, ul. 29. augusta č. 8, 813 63 Bratislava.

3.3. Objednávateľ nahlási poskytovateľovi potrebu poskytnutia servisnej služby elektronicky, na adresu poskytovateľa spservis@datalan.sk. Na základe požiadavky vznesenej zo strany objednávateľa, poskytovateľ vykoná potrebnú diagnostiku zariadenia na mieste plnenia.

3.4. Ak sa zmluvné strany nedohodnú inak, poskytovateľ je povinný vykonať servisnú službu v mieste plnenia najneskôr do 24 hodín od nahlásenia potreby poskytnutia servisnej služby objednávateľom.

3.5. Ak nie je možné z dôvodu povahy poruchy servisné služby poskytnúť v mieste plnenia podľa bodu 3.3. a 3.4. tohto článku, poskytovateľ je oprávnený zariadenie previezť do vlastnej prevádzky a najneskôr do 30 dní vrátiť zariadenie späť na miesto plnenia a uviesť ho do plnohodnotnej prevádzky, pričom počas trvania doby opravy poskytne náhradné zariadenie porovnateľnej kvality a pri zachovaní minimálne takej funkčnosti, akú poskytovalo pôvodné zariadenie, ak sa zmluvné strany nedohodnú inak. Odovzdanie a prevzatie zariadenia zmluvné strany potvrdia podpisom preberacieho protokolu. Z dôvodu právnej istoty zmluvné strany výslovne uvádzajú, že preprava zariadenia z miesta plnenia do prevádzky poskytovateľa a späť na miesto plnenia je zahrnutá v cene za poskytovanie servisných služieb.

3.6. Riadne poskytnutie servisnej služby potvrdí objednávateľ poskytovateľovi podpisom servisného listu. V prípade, že poskytnutá servisná služba má vady (t. j. ak nie je poskytnutá podľa podmienok tejto zmluvy a požiadaviek objednávateľa), objednávateľ má právo odmietnuť podpísať servisný list a uviesť v ňom dôvody (teda označiť vady servisnej služby) a poskytovateľ je povinný tieto vady odstrániť spôsobom podľa článku VII tejto zmluvy.

Článok IV. Cena

4.1. Cena za predmet zmluvy poskytovaný na základe tejto zmluvy je stanovená v zmysle zákona Národnej rady Slovenskej republiky č. 18/1996 Z. z. o cenách a vyhlášky Ministerstva financií Slovenskej republiky č. 87/1996 Z. z., ktorou sa vykonáva zákon o cenách v znení neskorších predpisov dohodou zmluvných strán vo výške 23 000,00 € (slovom Dvadsaťtritisíc eur) bez DPH mesačne.

4.2. Celková cena za predmet zmluvy je stanovená v sume 69 000,00 € bez DPH a 82 800,00 € s DPH.

4.3. Mesačný paušál v zmysle bodu 4.1. tejto zmluvy pokrýva všetky a akékoľvek náklady poskytovateľa v rámci poskytovania servisných služieb podľa tejto zmluvy v danom kalendárnom mesiaci, a to bez ohľadu na množstvo prác, ktoré bude potrebné v danom mesiaci vykonať. Pre zamedzenie pochybností, zmluvné strany výslovne uvádzajú, že poskytovateľ nemá právo požadovať zvýšenie mesačného paušálu, resp. akékoľvek náklady nad mesačný paušál v prípade zvýšenej prácnosti v danom mesiaci poskytovania služieb podľa tejto zmluvy.

Článok V.
Platobné podmienky

5.1. Úhrada ceny za poskytovateľom poskytnuté servisné služby v zmysle tejto zmluvy bude realizovaná formou bezhotovostného platobného styku, bez poskytnutia preddavku. Dohodnutú cenu vrátane DPH bude objednávateľ uhrádzať poskytovateľovi na základe predložených faktúr s 30 dňovou lehotou splatnosti odo dňa ich doručenia objednávateľovi.

5.2. Poskytovateľ je oprávnený faktúry vystavovať vždy k poslednému dňu mesiaca, v ktorom boli servisné služby poskytnuté.

5.3. Všetky ceny v tejto zmluve sú uvádzané bez DPH a budú objednávateľovi fakturované zvýšené o zákonom stanovené percento DPH.

5.4. Faktúry vystavené poskytovateľom musia obsahovať náležitosti daňového dokladu podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov. Prílohou každej faktúry bude servisný list podpísaný oprávnenými zástupcami zmluvných strán. Za správne vyhotovenie faktúry zodpovedá v plnom rozsahu poskytovateľ.

5.5. V prípade, že faktúra nebude obsahovať náležitosti daňového dokladu alebo prílohu v zmysle bodu 5.4. tohto článku zmluvy, alebo bude obsahovať iné zrejmé nesprávnosti, vady v písaní alebo počítaní, objednávateľ má právo vrátiť ju poskytovateľovi v lehote splatnosti na doplnenie alebo prepracovanie s uvedením nedostatkov, ktoré sa majú odstrániť. V takom prípade sa ukončí pôvodná lehota splatnosti a nová 30 dňová lehota splatnosti začne plynúť doručením doplnenej, opravenej, resp. novej faktúry objednávateľovi.

5.6. Poskytovateľ sa zaväzuje vystavenú faktúru zaslať listinne poštou a súčasne v textovo čitateľnom súbore vo formáte PDF elektronicky na e-mailovú adresu objednávateľa faktury@socpoist.sk, a to bezodkladne po jej vystavení. Takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. Poskytovateľ vyhlasuje, že obsah faktúry poslanej poštou sa bude zhodovať s faktúrou poslanou v elektronickej podobe na e-mailovú adresu objednávateľa. Miestom doručenia faktúry v listinnej forme je Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava.

Článok VI.
Práva a povinnosti zmluvných strán

6.1. Objednávateľ je povinný:

6.1.1. umožniť poskytovateľovi prístup do miesta plnenia podľa čl. III. bod 3.2. tejto zmluvy a k jednotlivým zariadeniam, na ktorých je vykonávaná objednaná servisná služba;

6.1.2. spolupracovať s poskytovateľom, najmä poskytnúť mu potrebnú súčinnosť, úplné, pravdivé a včasné informácie potrebné pre riadne poskytovanie servisných služieb;

6.1.3. v dohodnutom termíne, resp. na vyzvanie poskytovateľa riadne poskytnutú servisnú službu prevziať. Objednávateľ prevezme riadne a včas vykonané servisné služby podpísaním servisného listu, vyplneného a podpísaného zodpovedným zamestnancom poskytovateľa.

6.2. Poskytovateľ je povinný:

6.2.1. poskytovať servisné služby na svoje náklady a na svoje nebezpečenstvo v lehote podľa čl. III. bod 3.4. a 3.5. tejto zmluvy;

6.2.2. pri poskytovaní servisných služieb dodržiavať príslušné STN, predpisy požiarnej ochrany, bezpečnosti a ochrany zdravia pri práci a hygienické predpisy a postupovať v súlade s ustanoveniami zmluvy a s odbornou starostlivosťou tak, aby bol dosiahnutý požadovaný výsledok;

6.3. Poskytovateľ sa zaväzuje, že zaviaže povinnosťou mlčanlivosti svojich zamestnancov a všetky osoby, ktoré sa pri plnení záväzkov z tejto zmluvy môžu oboznámiť alebo prísť do styku s akýmikoľvek informáciami objednávateľa, vrátane osobných údajov v súlade s § 79 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Splnenie povinnosti v zmysle predchádzajúcej vety je poskytovateľ povinný kedykoľvek na výzvu objednávateľa preukázať.

6.4. Zmluvné strany sa výslovne dohodli, že poskytovateľ nie je oprávnený bez predchádzajúceho písomného súhlasu objednávateľa postúpiť na tretiu osobu a ani založiť akékoľvek svoje pohľadávky vzniknuté na základe alebo v súvislosti s touto zmluvou alebo plnením záväzkov na základe tejto zmluvy.

Článok VII.
Záručná doba, kvalita a zodpovednosť za vady

7.1. Na vykonané servisné služby poskytovateľ poskytuje objednávateľovi záruku v trvaní dvanásť (12) mesiacov od podpísania servisného listu oprávnenými zástupcami zmluvných strán podľa bodu 3.5. tejto zmluvy. Ak sa v lehote podľa predchádzajúcej vety vyskytnú na poskytnutých servisných službách vady, objednávateľ má právo na ich bezplatné odstránenie poskytovateľom. Vady plnenia objednávateľ nahlasuje bez zbytočného odkladu od ich zistenia. Poskytovateľ je povinný zistenú vadu odstrániť do 24 hodín odo dňa jej nahlásenia.

7.2. V prípade nenastúpenia poskytovateľa na poskytnutie servisnej služby alebo odstránenia vady poskytnutej servisnej služby najneskôr 10 dní od nahlásenia požiadavky objednávateľa je objednávateľ oprávnený zabezpečiť odstránenie vady treťou osobou na náklady poskytovateľa.

Článok VIII.
Zmluvné sankcie a náhrada škody

8.1. V prípade omeškania objednávateľa s úhradou riadne doručenej faktúry, má poskytovateľ právo v súlade s § 369a zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov účtovať objednávateľovi úrok z omeškania vo výške podľa nariadenia vlády SR č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v platnom znení.

8.2. V prípade omeškania poskytovateľa s vykonaním servisných služieb v lehote podľa čl. III. bod 3.4 zmluvy a v prípade omeškania poskytovateľa s odstránením vád podľa bodu 7.1. zmluvy, má objednávateľ právo účtovať poskytovateľovi zmluvnú pokutu vo výške 50,- Eur za každý, aj začatý deň omeškania za každú jednu nahlásenú požiadavku na servisnú službu, alebo za každú jednu vadu, zvlášť. Objednávateľ je oprávnený požadovať od poskytovateľa popri zmluvnej pokute aj náhradu škody spôsobenej porušením zabezpečovanej povinnosti, a to v plnej výške.

8.3. Zmluvná pokuta, úrok z omeškania a náhrada škody sú splatné do 30 dní odo dňa doručenia osobitnej faktúry na ich uhradenie povinnej zmluvnej strane.

8.4. Zodpovednosť za škodu spôsobenú v súvislosti s touto zmluvou sa spravuje ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

Článok IX.
Komunikácia zmluvných strán

9.1. Ak v tejto zmluve nie je ustanovené inak, akékoľvek oznámenia, súhlas, schválenia alebo rozhodnutia, vrátane úkonov podľa článku III. tejto zmluvy, vyžadované alebo predpokladané podľa tejto zmluvy a/alebo dokumenty jednej zmluvnej strany adresované druhej zmluvnej strane, musia byť vyhotovené písomne v slovenskom jazyku a podpísané príslušnou zmluvnou stranou, resp. oboma zmluvnými stranami, ak to vyplýva z kontextu danej písomnosti, a doručené druhej zmluvnej strane formou doporučenej zásielky, do elektronickej schránky, prípadne prostredníctvom kuriérskej služby, osobne alebo elektronickou poštou na nasledovné adresy:

Objednávateľ:
Ing.
E-mail: n@socpoist.sk
Telefón+421 9

Poskytovateľ:

E-mail: i@datalan.sk
Telefón+421

9.2. Odosielateľ akejkoľvek písomnej správy môže požadovať písomné potvrdenie príjemcu.

9.3. Každá komunikácia týkajúca sa platnosti alebo účinnosti zmluvy, jej zániku či zmeny musí byť písomná a doručovaná výhradne poštou ako doporučená zásielka, kuriérom alebo osobne.

9.4. Akákoľvek písomnosť doručovaná v súvislosti so zmluvou sa považuje za doručenú druhej zmluvnej strane v prípade doručovania prostredníctvom:

9.4.1. elektronickej pošty (e-mail) dňom, kedy zmluvná strana, ktorá prijala e-mail od odosielajúcej zmluvnej strany potvrdila jeho prijatie odoslaním potvrdzujúceho e-mailu odosielajúcej zmluvnej strane. Prijímajúca zmluvná strana je povinná doručiť odosielajúcej zmluvnej strane potvrdenie o prijatí e-mailu do 24 hodín, pričom po uplynutí uvedenej lehoty je odosielajúca zmluvná strana povinná informovať sa o dôvodoch nepotvrdenia doručenia e-mailu telefonicky, bezdôvodné porušenie povinnosti potvrdiť doručenie e-mailu prijímajúcou stranou má za následok omeškanie prijímajúcej zmluvnej strany;

9.4.2. pošty, kuriérom alebo v prípade osobného doručovania, doručením písomnosti adresátovi s tým, že v prípade doručovania prostredníctvom pošty musí byť písomnosť zaslaná doporučene s doručenkou preukazujúcou doručenie na adresu príslušnej zmluvnej strany. V prípade doručovania inak ako poštou, je možné písomnosť doručovať aj na inom mieste ako na adrese príslušnej zmluvnej strany, ak sa na tomto mieste zmluvná strana v čase doručenia zdržuje. Za deň doručenia písomnosti sa považuje aj deň, v ktorý zmluvná strana, ktorá je adresátom, odoprie doručovanú písomnosť prevziať, alebo tretí deň odo dňa uloženia zásielky na pošte, doručovanej poštou zmluvnej strane, alebo v ktorý je na zásielke, doručovanej poštou zmluvnej strane, preukázateľne zamestnancom pošty vyznačená poznámka, že „adresát sa odsťahoval", „adresát je neznámy" alebo iná poznámka podobného významu, ak sa súčasne takáto poznámka zakladá na pravde.

9.5. Poverení zástupcovia zmluvných strán uvedení v bode 9.1 tohto čl. zmluvy zodpovedajú za koordináciu a organizačné zabezpečenie realizácie tejto zmluvy a môžu za zmluvnú stranu realizovať všetky oznámenia, súhlasy, schválenia alebo rozhodnutia vyžadované alebo predpokladané podľa tejto zmluvy, s výnimkou úkonov podľa čl. X. body 10.2. až 10.4. a 10.9. zmluvy.

9.6. Zmluvné strany sa zaväzujú bezodkladne písomne oznámiť akúkoľvek zmenu svojich kontaktných

údajov uvedených v bode 9.1 tohto čl. zmluvy druhej zmluvnej strane bez potreby uzatvorenia dodatku k tejto zmluve. Pre zamedzenie pochybností zmluvné strany sú oprávnené rovnako kedykoľvek zmeniť aj ich poverených zástupcov uvedených bode 9.1 zmluvy, pričom táto zmena je účinná voči druhej zmluvnej strane ku dňu, kedy jej bolo, doručené písomné oznámenie o zmene povereného zástupcu.

Článok X.
Záverečné ustanovenia

10.1. Táto zmluva sa uzatvára na 3 mesiace odo dňa nadobudnutia jej účinnosti.

10.2. Pred uplynutím dohodnutej doby trvania tejto zmluvy v zmysle predošlého bodu zmluvy je možné tento zmluvný vzťah ukončiť kedykoľvek písomnou dohodou zmluvných strán, výpoveďou za podmienok podľa bodu 10.3. tohto článku zmluvy alebo odstúpením od zmluvy podľa bodu 10.4. tohto článku zmluvy.

10.3. Objednávateľ je oprávnený túto zmluvu vypovedať aj bez udania dôvodu s výpovednou lehotou 1 mesiac, ktorá začína plynúť od prvého dňa kalendárneho mesiaca nasledujúceho po doručení písomnej výpovede druhej zmluvnej strane.

10.4. Ktorákoľvek zmluvná strana je oprávnená odstúpiť od tejto zmluvy v prípade jej podstatného porušenia. Odstúpenie od zmluvy nadobúda účinnosť dňom doručenia písomného oznámenia o odstúpení od zmluvy druhej zmluvnej strane.

10.5. Za podstatné porušenie zmluvy objednávateľom sa považuje omeškanie s úhradou splatnej faktúry o viac ako 60 kalendárnych dní.

10.6. Za podstatné porušenie zmluvy poskytovateľom sa považuje opakované, t. j. viac ako 3x počas trvania tejto zmluvy, riadne nevykonanie servisnej služby v lehote podľa bodu 3.4. a 3.5. tejto zmluvy alebo neodstránenie vady v lehote podľa bodu 7.1. zmluvy.

10.7. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
Príloha č.1 - Zoznam zariadení
Príloha č. 2 – Cenová kalkulácia
Príloha č. 3 - Sprostredkovateľská zmluva
Príloha č. 4 - Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

10.8. V prípade zmeny obchodného mena, názvu, sídla, právnej formy, zástupcov/ štatutárnych orgánov alebo spôsobu ich konania za zmluvnú stranu, bankového spojenia, čísla účtu alebo osoby zodpovednej za realizáciu, oznámi zmluvná strana, ktorej sa niektorá z uvedených zmien týka, písomnou formou túto skutočnosť druhej zmluvnej strane, a to bez zbytočného odkladu, inak povinná zmluvná strana zodpovedá za všetky prípadné škody z toho vyplývajúce alebo náklady, ktoré v tejto súvislosti musela vynaložiť druhá zmluvná strana.

10.9. Zmeny a doplnky tejto zmluvy, s výnimkou podľa bodu 9.6. tohto článku zmluvy, je možné robiť len písomnými očíslovanými dodatkami podpísanými oprávnenými zástupcami oboch zmluvných strán. K návrhu dodatkov tejto zmluvy sa zmluvné strany zaväzujú vyjadriť do 14 dní od doručenia návrhu.

10.10. Zmluvné strany sa zaväzujú riešiť prípadné spory vyplývajúce z tejto zmluvy formou rokovania prostredníctvom svojich poverených zástupcov. V prípade, že sa rokovaním spor nevyrieši, ktorákoľvek zmluvná strana je oprávnená predložiť spor na rozhodnutie príslušnému súdu v Slovenskej republike.

10.11. Práva a povinnosti zmluvných strán touto zmluvou výslovne neupravené sa spravujú právnym poriadkom Slovenskej republiky, predovšetkým príslušnými ustanoveniami zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

10.12. Táto zmluva je vyhotovená v 4 rovnopisoch, z ktorých objednávateľ obdrží dva rovnopisy a poskytovateľ obdrží dva rovnopisy.

10.13. Ak niektoré ustanovenia tejto zmluvy stratili platnosť alebo sú platné len sčasti alebo neskôr stratia platnosť, nie je tým dotknutá platnosť ostatných ustanovení. Na miesto neplatných ustanovení sa použije úprava, ktorá sa čo najviac približuje zmyslu a účelu tejto zmluvy.

10.14. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v zmysle § 47a ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov v spojení s § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

10.15. Zmluvné strany vyhlasujú, že túto zmluvu uzatvárajú slobodne a vážne, zmluvná voľnosť zmluvných strán nie je obmedzená, zmluvné prejavy sú určité a zrozumiteľné, zmluvu si prečítali, jej obsahu a právnym účinkom z nej vyplývajúcim porozumeli, zmluva nebola podpísaná v tiesni ani za nápadne nevýhodných podmienok a na znak súhlasu s jej obsahom túto vlastnoručne podpisujú.

V ....., dňa 11-07-2024

za objednávateľa :

Ing. Michal Tariška
generálny riaditeľ Sociálnej poisťovne

V Bratislave, dňa 28 JÚN 2024

za poskytovateľa :

Ing. Juraj Zelko
člen predstavenstva DATALAN, a.s.

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

Príloha č. 1 Zoznam zariadení

ZOZNAM ZARIADENÍ,
ktoré sú predmetom vykonávania pozáručného servisu
Druhy, typy a značky zariadení pre vykonávanie autorizovaného pozáručného servisu

Lokalita	*Výrobca/Typ*	*Serial number*	*Počet*
Bratislava, ústredie Sociálnej poisťovne	*LENOVO ThinkSystem SR850 (Type 7x19)*	*S4ALT070* *S4ALT069* *S4ALT071* *S4ALT123* *S4ALT122* *S4ALT124* *S4ALT068* *S4CDH863* *S4CDH862* *S4CDH857* *S4CDH856* *S4CDH865* *S4CDH869*	*13 ks*
Bratislava, ústredie Sociálnej poisťovne	*HP ProLiant DL 360 Gen9*	*CZJ74506D8* *CZJ74506D9*	*2 ks*
Bratislava, ústredie Sociálnej poisťovne	*HPE ProLiant DL580 Gen9*	*CZJ8350TPX* *CZJ8350TPY* *CZJ7401T2D* *CZJ7401T2F* *CZJ835007T* *CZJ835007V*	*6ks*
Bratislava, ústredie Sociálnej poisťovne	*UPS PowerWat 33300RMX (225kW)*	*3927160259*	*1 ks*
Bratislava, ústredie Sociálnej poisťovne	*Obálkovacia linka KERN 658*	*10001249* *10010658*	*2 ks*
Bratislava, ústredie Sociálnej poisťovne	*Farankovacie stroje a obálkovače Quadient (Neopost) – Typová rada IJ, DS, IS, IM*		*7 ks*

Príloha č. 2 Cenová kalkulácia

Cenník servisných služieb

DATALAN

2 Návrh uchádzača na plnenie kritérií

NÁVRH UCHÁDZAČA NA PLNENIE KRITÉRIÍ

Obchodné meno uchádzača: **DATALAN, a.s.**

Adresa alebo sídlo uchádzača: **Krasovského 14, 851 01 Bratislava**

Predmet zákazky: Pozáručný autorizovaný servis zariadení výpočtovej techniky.

Tabuľka č. 1: Návrh uchádzača na plnenie kritérií na vyhodnotenie ponúk

P.č.	Názov položky	Predpokladané množstvo[2]	Jednotková cena v EUR bez DPH[3]	Celková cena v EUR bez DPH[3]	Výška DPH v EUR	Celková cena v EUR vrátane DPH
1.	Pozáručný autorizovaný servis zariadení výpočtovej techniky.	3	23 000,00	69 000,00	13 800,00	82 800,00
Celková cena za predmet zákazky				69 000,00	13 800,00	82 800,00

Uchádzač do *Tabuľky č. 1: Návrh uchádzača na plnenie kritérií na vyhodnotenie ponúk* uvedie Celkové náklady na realizáciu predmetu zákazky.

V Bratislave dňa 18.06.2024

DATALAN a.s. Krasovského 14, 851 01 Bratislava IČO: 35810734 IČ DPH: SK2020759175

Ing. Jozef [illegible]
Člen predstavenstva

[2] v bode 1 je uvedený predpokladaný počet mesačných paušálov.
[3] v bode 1 sa uvedie cena za mesačný paušál.
[3] v bode 1 sa uvedie súčin predpokladaného množstva a jednotkovej ceny vyjadrenej v EUR bez DPH.

SP číslo zmluvy: 28033-6/2024 - BA

Príloha č. 3 k zmluve

Sprostredkovateľská zmluva

uzatvorená podľa čl. 28 ods. 3 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 osobných údajov) a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Zmluvné strany

Prevádzkovateľ	
Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA
IČO:	308 07 484
DIČ:	2020592332

(ďalej len „**prevádzkovateľ**")

a

Sprostredkovateľ	
Obchodné meno:	**DATALAN, a. s.**
Sídlo:	Krasovského 14, Bratislava – mestská časť Petržalka, PSČ 851 01
Štatutárny orgán:	Ing. Juraj Zelko člen predstavenstva
Bankové spojenie:	[illegible]
IBAN:	
IČO:	35810734
DIČ:	2020259175
IČ DPH:	SK2020259175

Zapísaný v Obchodnom registri Mestského súdu Bratislava III, Oddiel Sa, Vložka číslo 2704/B

(ďalej len „**sprostredkovateľ**")

(spolu ďalej ako „**zmluvné strany**")

Preambula

Zmluvné strany uzatvárajú zmluvný vzťah na základe Zmluvy č. 28033-5/2024 - BA na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

Sprostredkovateľ vystupuje v tejto dohode ako poskytovateľ týchto služieb, pričom nie je vylúčené, že v rámci plnenia predmetu zmluvy sa dostane priamo k spracovaniu osobných údajov dotknutých osôb, aj keď takéto spracovanie nie je predmetom zmluvy. Vzhľadom na vyššie uvedenú možnosť

spracovania osobných údajov prevádzkovateľa sprostredkovateľom, zmluvné strany uzatvárajú podľa čl. 28 ods. 3 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 osobných údajov) (ďalej len „GDPR") a podľa § 34 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „ZOOU") túto sprostredkovateľskú zmluvu (ďalej len „zmluva").

Článok I.
Vymedzenie pojmov

Dotknutá osoba je identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú – dotknutí zamestnanci a klienti Prevádzkovateľa.

Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Prevádzkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.

Sprostredkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Spracúvanie – je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.

Čl. II
Predmet zmluvy

1. Predmetom tejto zmluvy je poverenie sprostredkovateľa na spracovanie osobných údajov dotknutých osôb v mene prevádzkovateľa a podľa pokynov prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre plnenie účelu dohody o poskytovaní služieb.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje po splnení povinností uvedených v tejto zmluve.
3. Účel spracúvania osobných údajov je vymedzený v zákone č. 461/2003 Z. z. o sociálnom poistení, v Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, v Nariadení (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, podľa ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje dotknutých osôb za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje výhradne pre poskytovanie služieb prevádzkovateľovi, a to na základe pokynov prevádzkovateľa podľa podmienok stanovených v tejto zmluve v súlade so všeobecne záväznými právnymi predpismi upravujúcimi ochranu a

spracúvanie osobných údajov. Za pokyny prevádzkovateľa sa považujú pokyny uvedené v tejto zmluve, v dohode o poskytovaní služieb, prípadne iné písomne zdokumentované pokyny alebo požiadavky prevádzkovateľa na poskytnutie služby v zmysle dohody o poskytovaní služieb.

5. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou Zmluvy 28033-5/2024 - BA na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky a to na účel:

   - Účelom spracúvania osobných údajov poskytovateľom je poskytovanie služieb pozáručného autorizovaného servisu zariadení výpočtovej techniky.

6. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu dohody o poskytovaní služieb y o poskytovaní služieb je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétu zákonnú povinnosť ustanovuje dohoda o poskytovaní služieb osobitne a § 78 ods. 3 ZOOU.

Čl. III
Zoznam osobných údajov a okruh dotknutých osôb

1. Zmluva, v rámci plnenia predmetu ktorej je sprostredkovateľ poverený spracúvať osobné údaje dotknutých osôb:
   Zmluva č. 28033-5/2024 – BA na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky.
2. Zoznam osobných údajov, ktoré môžu byť v prípade realizácie predmetu dohody o poskytovaní služieb predmetom spracúvania:
   meno, priezvisko, titul, emailová adresa, telefón.
3. Spracúvané osobné údaje sú povahy:
   Iné osobné údaje v rozsahu bodu 2 tohto článku.
4. Spracúvané osobné údaje sú typu:
   adresné, zamestnanecké, ekonomické, sociálne, elektronické.

Čl. IV
Spôsob výkonu a oprávnenia sprostredkovateľa

1. Osobné údaje o dotknutých osobách prevádzkovateľ spracúva v súlade so zákonom o sociálnom poistení, s Nariadením (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, s Nariadením (ES) Európskeho parlamentu a Rady č. 987/2009 za účelom výkonu sociálneho poistenia a vedenia ekonomickej, prevádzkovej, personálnej a mzdovej agendy Sociálnej poisťovne.
2. Na spracúvanie osobných údajov sprostredkovateľom sa v zmysle § 34 ods. 1 ZOOU nevyžaduje súhlas dotknutej osoby.
3. Sprostredkovateľ má v rámci spracúvania osobných údajov podľa tejto zmluvy povolené operácie s osobnými údajmi v rozsahu najmä:
   a) zaznamenávanie
   b) usporadúvanie,
   c) štruktúrovanie,
   d) vyhľadávanie,
   e) prehliadanie,
   f) preskupovanie alebo kombinovanie,
   g) vymazanie alebo likvidácia.

4. Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb po dobu trvania účelu spracúvania, resp. po dobu platnosti a účinnosti dohody o poskytovaní služieb a po dobu platnosti a účinnosti tejto zmluvy.

Čl. V
Vyhlásenie prevádzkovateľa

1. Prevádzkovateľ vyhlasuje, že pri výbere sprostredkovateľa dbal na odbornú, technickú, organizačnú a personálnu spôsobilosť sprostredkovateľa a jeho schopnosť zaručiť ochranu práv dotknutých osôb.
2. Prevádzkovateľ prehlasuje, že
   a) osobné údaje sa spracúvajú na základe primeraného právneho dôvodu v súlade s GDPR a ZOOU,
   b) osobné údaje sa spracúvajú v súlade s jasne definovaným účelom spracúvania,
   c) osobné údaje, ktoré sprostredkovateľ spracúva na základe tejto zmluvy sú aktuálne, úplné a primerané vzhľadom na účel spracúvania.

Čl. VI
Vyhlásenie sprostredkovateľa

1. Sprostredkovateľ vyhlasuje, že pri činnosti spracovania nedochádza k odovzdaniu osobných údajov do tretej krajiny alebo medzinárodnej organizácii ani iným organizáciám v SR, ak prevádzkovateľ neprejavil s takýmto úkonom vopred písomný súhlas.
2. Sprostredkovateľ vyhlasuje, že prijal také opatrenia organizačného a technického rázu, aby nemohlo dôjsť k neoprávnenému alebo náhodnému prístupu k osobným údajom, k ich zmene, zničeniu či strate, neoprávneným prenosom, k ich inému neoprávnenému spracovaniu, ako aj k inému zneužitiu osobných údajov. Sprostredkovateľ je povinný prijať organizačné a technické opatrenia na prevenciu rizík pre práva a slobody fyzických osôb, vyvolaných spracovaním, v maximálnej miere, akú dovoľujú súčasný stav techniky, náklady a ďalšie ovplyvniteľné okolnosti. Táto povinnosť platí aj po ukončení spracovávania osobných údajov ukončením tejto zmluvy až do okamihu protokolárnej úplnej likvidácie osobných údajov.
3. Sprostredkovateľ vyhlasuje, že zabezpečí, aby všetky ním určené oprávnené osoby boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti.

Čl. VII
Povinnosti sprostredkovateľa

1. Sprostredkovateľ sa pri spracúvaní osobných údajov podľa tejto zmluvy zaväzuje najmä:
   a) postupovať s náležitou starostlivosťou a v súlade s GDPR, ZOOU a súvisiacimi všeobecne záväznými právnymi predpismi Slovenskej republiky, dodržiavať povinnosti vyplývajúce z tejto zmluvy a pokynov prevádzkovateľa, a dodržiavať zásady ochrany osobných údajov zverejnené Prevádzkovateľom,
   b) akékoľvek spracúvanie osobných údajov vykonávať len za účelom plnenia predmetu tejto zmluvy a dohody o poskytovaní služieb a len v rozsahu nevyhnutnom na jej plnenie,
   c) údaje dotknutých osôb nezverejňovať, nešíriť či neodovzdávať ďalším osobám,
   d) zaistiť, aby jeho zamestnanci a ďalšie osoby, ktoré využije na plnenie podľa tejto zmluvy, dodržiavali podmienky stanovené GDPR, vnútroštátnymi predpismi a touto zmluvou a boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti,

e) ak všeobecne záväzné právne predpisy neustanovujú inak, osobné údaje, s ktorými sa dostal do styku v súvislosti s realizáciou dohody o poskytovaní služieb nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,

f) zachovávať mlčanlivosť a zabezpečiť diskrétnosť pri akomkoľvek spracúvaní osobných údajov,

g) ak zmluva alebo všeobecne záväzný právny predpis neustanovuje inak, nevyhotovovať kópie akýchkoľvek nosičov obsahujúcich osobné údaje a ani z nich nevyhotovovať výpisy alebo odpisy, ktoré by obsahovali osobné údaje,

h) ak všeobecne záväzné právne predpisy upravujúce problematiku archívov a registratúr neustanovujú inak, bezodkladne odovzdávať prevádzkovateľovi všetky získané materiály obsahujúce osobné údaje, ktoré už pre realizáciu zmluvy nepotrebuje, resp. všetky osobné údaje, ktoré bude spracúvať v súvislosti s plnením dohody o poskytovaní služieb, bezodkladne po tom, čo pominie dôvod na ich spracúvanie podľa zmluvy, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácii (napr. pevné disky počítačov, USB kľúče, CD, DVD, dokumenty v papierovej podobe) alebo tieto nosiče zlikvidovať tak, aby nedošlo k úniku týchto údajov,

i) poučiť svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby"), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov, ako aj o iných právach a povinnostiach sprostredkovateľa upravených zmluvou alebo ustanovených všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov, o zodpovednosti za ich porušenie, a to všetko pred uskutočnením prvej operácie s osobnými údajmi,

j) zachovávať mlčanlivosť o osobných údajoch dotknutých osôb a o bezpečnostných opatreniach prijatých na zabezpečenie ochrany osobných údajov, a to aj po skončení tohto zmluvného vzťahu,

k) je povinný nakladať s údajmi ako s informáciami dôvernými v zmysle Zákona 513/1991 Zb. (Obchodný zákonník) a jeho následných novelizácií a je povinný zaviazať týmito povinnosťami aj osoby, ktoré by dojednal na činnosti na plnenie podľa tejto zmluvy (zamestnancov či iných pracovníkov),

l) plniť predmet zmluvy len prostredníctvom riadne a preukázateľne poučených alebo vyškolených oprávnených osôb pre účel plnenia predmetu zmluvy a z nej vyplývajúceho rozsahu a podmienok spracúvania osobných údajov,

m) spracúvať osobné údaje oprávnenými osobami konajúcimi za sprostredkovateľa len v rozsahu pokynov prevádzkovateľa v zmysle čl. 32 GDPR vrátane prípadnej pseudonymizácie a šifrovania s ohľadom na okolnosti konkrétneho prípadu a v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania osobných údajov, ako je uvedené v čl. II tejto zmluvy a pokynu prevádzkovateľa udeleného osobou oprávnenou konať v danom rozsahu za prevádzkovateľa, alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

n) v prípade sťažností alebo sporu týkajúceho sa spracúvania osobných údajov pri plnení predmetu zmluvy, bezodkladne informovať prevádzkovateľa o tejto skutočnosti a spolupracovať pri riešení sťažnosti alebo sporu s prevádzkovateľom,

o) nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,

p) zabrániť neoprávneným osobám v prístupe k osobným údajom a k prostriedkom na ich spracovanie, zabrániť neoprávnenému čítaniu, vytváraniu, kopírovaniu, prenosu, úprave či vymazaniu záznamov obsahujúcich osobné údaje a zabezpečiť opatrenia, ktoré umožnia určiť

a overiť, komu/kým a akým spôsobom boli osobné údaje odovzdané, resp. kým boli prevzaté a spracúvané.

2. Sprostredkovateľ je pri spracúvaní osobných údajov podľa tejto zmluvy ďalej povinný bezodkladne informovať prevádzkovateľa o
   a) poskytnutí a sprístupnení osobných údajov tretej strane spolu s odôvodnením a určením všeobecne záväzného právneho predpisu, ktorý sprostredkovateľovi ukladá povinnosť poskytnúť, sprístupniť alebo zverejniť osobné údaje dotknutých osôb spracúvaných v mene prevádzkovateľa,
   b) skutočnostiach zabraňujúcich plneniu povinností podľa tejto zmluvy,
   c) akomkoľvek porušení povinností podľa zmluvy alebo porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov,
   d) akomkoľvek porušení ochrany osobných údajov,
   e) akomkoľvek porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov zo strany prevádzkovateľa, ak sa podľa názoru sprostredkovateľa pokynom prevádzkovateľa tieto predpisy porušujú.
3. V prípade, ak sprostredkovateľ obdržal žiadosť dotknutej osoby, ktorá si uplatňuje voči prevádzkovateľovi svoje práva podľa článkov 15 až 22 GDPR a § 21 až § 28 ZOOU (napr. právo na prístup k údajom, právo na výmaz alebo opravu osobných údajov), je povinný bezodkladne, najneskôr však do troch pracovných dní od jej prijatia, takúto žiadosť zaslať prevádzkovateľovi prostredníctvom emailovej adresy: zodpovedna.osoba@socpoist.sk, spolu so žiadosťou je sprostredkovateľ povinný prevádzkovateľovi zaslať aj ďalšie relevantné informácie týkajúce sa predmetnej žiadosti, ktoré by mohli mať vplyv na postup vybavenia žiadosti dotknutej osoby zo strany prevádzkovateľa.
4. Sprostredkovateľ je povinný pomáhať prevádzkovateľovi pri zabezpečení plnenia povinností prevádzkovateľa v oblasti bezpečnosti spracúvania, zisťovania porušení ochrany osobných údajov, posudzovania vplyvu na ochranu osobných údajov a poskytovať informácie, ktoré sú mu dostupné.
5. Sprostredkovateľ je povinný dôsledne chrániť spracúvané osobné údaje podľa svojho najlepšieho vedomia, v súlade s ustanoveniami GDPR a ZOOU.
6. Oprávnené osoby sprostredkovateľa resp. subdodávateľa, ktoré budú mať prístup k osobným údajom sú viazaní povinnosťou mlčanlivosti o týchto údajoch a to aj po zániku štátnozamestnaneckého pomeru, pracovného pomeru uzatvoreného v súlade so zákonníkom práce resp. v súlade so zákonom o výkone práce vo verejnom záujme alebo dohody o práci vykonávanej mimo pracovného pomeru v súlade so zákonníkom práce.
7. Oprávnené osoby sprostredkovateľa sú oboznámené so spôsobom oznamovania podozrení z bezpečnostných incidentov v súvislosti s informačným systémom a spracúvanými osobnými údajmi. Oprávnené osoby sprostredkovateľa sú poučené, aby bezodkladne oznamovali určenej osobe prevádzkovateľa akékoľvek podozrenie z bezpečnostného incidentu, ktoré by mohlo mať dopad na bezpečnosť informačného systému s osobnými údajmi. Sprostredkovateľ je povinný bezodkladne prijať relevantné opatrenia k náprave, o bezpečnostnom incidente informovať zodpovednú osobu prevádzkovateľa a e-mailom na adresu: zodpovedna.osoba@socpoist.sk.
8. Sprostredkovateľ je povinný spracovať a dokumentovať prijaté a vykonané technicko-organizačné opatrenia na zaistenie ochrany osobných údajov v súlade s právnymi predpismi EÚ a Slovenskej republiky, k tomu sa vzťahujúcimi. Sprostredkovateľ je povinný spolupracovať s Prevádzkovateľom a byť mu nápomocný pri zaisťovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení

povinností Prevádzkovateľa reagovať na žiadosti o výkon práv Dotknutej osoby stanovených v kapitole III. GDPR (informácie a prístup k osobným údajom, oprava a výmaz, právo na obmedzenie spracovania atď.)

9. Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na doloženie toho, že boli splnené povinnosti sprostredkovateľa a stanovené ustanoveniami GDPR a umožní audity, vrátane inšpekcií, vykonávané prevádzkovateľom alebo iným audítorom, ktorého prevádzkovateľ poveril. Pri vykonávaní auditov bude spolupracovať s prevádzkovateľom alebo ním určeným audítorom. Prevádzkovateľ je oprávnený vykonať inšpekciu plnenia povinností sprostredkovateľa a audit bez predchádzajúceho upozornenia. Nespolupráca sprostredkovateľa bude považovaná za podstatné porušenie tejto zmluvy s možnosťou odstúpenia zo strany prevádzkovateľa, resp. vyvodením zodpovednosti za prípadnú škodu.
10. Po ukončení poskytovania služieb spojených so spracovaním sprostredkovateľ v súlade s rozhodnutím prevádzkovateľa všetky osobné údaje buď vymaže, alebo ich vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo členského štátu nepožaduje uloženie daných osobných údajov. Dojednáva sa, že takýto pokyn bude sprostredkovateľovi daný písomne.
11. Ak sprostredkovateľ poruší GDPR a túto zmluvu tým, že bez pokynu prevádzkovateľa sám určí účely a prostriedky spracovania osobných údajov, stane sa vo vzťahu k týmto údajom a ich spracovaniu prevádzkovateľom so všetkými dôsledkami z toho vyplývajúcimi.

Čl. VIII
Podmienky spracúvania osobných údajov

1. Sprostredkovateľ vyhlasuje, že spracúvanie osobných údajov bude vykonávať sám.
2. Sprostredkovateľ nezapojí do spracovania žiadneho ďalšieho sprostredkovateľa bez predchádzajúceho konkrétneho písomného súhlasu prevádzkovateľa. Náležitosti žiadosti o poskytnutie súhlasu sú uvedené v bode 4 tohto článku zmluvy.
3. Sprostredkovateľ nesmie zveriť spracúvanie osobných údajov subdodávateľovi, ak by tým mohli byť ohrozené práva a právom chránené záujmy dotknutých osôb. Pri zapojení ďalšieho sprostredkovateľa do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa je mu sprostredkovateľ povinný uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov, ako má on sám.
4. Žiadosť o poskytnutie súhlasu musí obsahovať aspoň nasledovné náležitosti:
   a. označenie subdodávateľa obchodným menom, identifikačnými údajmi a zápisom v obchodnom registri,
   b. odôvodnenie jeho poverenia spracúvaním osobných údajov dotknutých osôb,
   c. vyhlásenie sprostredkovateľa, že subdodávateľ poskytuje dostatočné záruky na vykonanie primeraných technických a organizačných opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov a zmluvy,
   d. vyhlásenie sprostredkovateľa, že subdodávateľ nevykonáva prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii ani iným organizáciám v SR, ktorá nezaručuje primeranú úroveň ochrany osobných údajov,
   e. vyhlásenie sprostredkovateľa, že subdodávateľ poučí svojich zamestnancov alebo iné osoby, ktoré prídu alebo môžu prísť do styku s osobnými údajmi (ďalej len „oprávnené osoby"), o povinnosti zachovávať mlčanlivosť a dôvernosť osobných údajov ako aj o iných právach a povinnostiach sprostredkovateľa upravených touto zmluvou alebo ustanovených

všeobecnými záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov.

5. Zmluvné strany sa dohodli, že sprostredkovateľ po obdržaní súhlasu na spracúvanie osobných údajov podľa tejto zmluvy prostredníctvom subdodávateľa písomne poverí subdodávateľa spracúvaním osobných údajov podľa zmluvy za podmienok, za akých je oprávnený/povinný ich spracúvať sprostredkovateľ a len v rozsahu nevyhnutnom pre realizáciu zmluvy v záujme prevádzkovateľa, resp. jeho dotknutých osôb. Sprostredkovateľ je povinný predložiť kópiu zmluvy so subdodávateľom do 5 pracovných dni od jej vyžiadania prevádzkovateľovi.
6. Subdodávateľ spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa. Ak subdodávateľ nesplní svoje povinnosti pri spracúvaní osobných údajov dotknutých osôb, sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie týchto povinnosti subdodávateľom. Sprostredkovateľ sa nemôže zbaviť zodpovednosti za porušenie povinnosti subdodávateľom tvrdením, že tieto povinnosti porušil subdodávateľ sprostredkovateľa. Ustanovenia GDPR o sprostredkovateľovi, vrátane ustanovení zmluvy upravujúcich povinnosti a podmienky spracúvania osobných údajov zo strany sprostredkovateľa sa vzťahujú aj na subdodávateľa.
7. Sprostredkovateľ je povinný oznámiť prevádzkovateľovi ukončenie spracúvania osobných údajov dotknutých osôb prostredníctvom subdodávateľa, a to bezodkladne, najneskôr však do piatich pracovných dní od ukončenia takéhoto spracúvania. Toto oznámenie musí o. i. obsahovať aj popis spôsobu splnenia povinnosti sprostredkovateľa vo vzťahu k tomuto subdodávateľovi.

Čl. IX
Ostatné dohodnuté podmienky

1. Sprostredkovateľ postupuje pri spracúvaní osobných údajov podľa GDPR a podľa ZOOU.
2. Sprostredkovateľ sa zaväzuje nahradiť prevádzkovateľovi v plnom rozsahu všetky škody, ktoré mu vzniknú v súvislosti s nedodržaním tejto zmluvy zo strany sprostredkovateľa a ktorá prevádzkovateľovi vznikne porušením alebo nesplnením povinností subdodávateľa sprostredkovateľa pri spracúvaní a ochrane osobných údajov vyplývajúcich z ustanovení zmluvy a všeobecne záväzných právnych predpisov.
3. Ochrana osobných údajov podľa zmluvy trvá aj po ukončení zmluvného vzťahu založeného touto zmluvou a zaväzuje aj právnych nástupcov zmluvných strán. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá prevádzkovateľovi vznikla porušením povinností sprostredkovateľa.
4. Sprostredkovateľ je poverený spracúvať osobné údaje po dobu platnosti tejto zmluvy. Okamihom skončenia jej platnosti už sprostredkovateľ nesmie disponovať žiadnymi osobnými údajmi. Sprostredkovateľ je povinný vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje, v prípade že ich spracovával, po ukončení poskytovania služieb týkajúcich sa plnenia dohody o poskytovaní služieb a vymazať existujúce kópie, ktoré obsahujú osobné údaje, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto osobných údajov, o čom vyhotoví písomné vyhlásenie, ktoré je povinný doručiť prevádzkovateľovi najneskôr do dvoch pracovných dní od skončenia platnosti zmluvy.
5. Kontakt na zástupcu prevádzkovateľa zodpovedného za ochranu osobných údajov: zodpovedna.osoba@socpoist.sk
6. Kontakt na zástupcu sprostredkovateľa: sj @datalan.sk

Čl. X
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Sprostredkovateľ berie na vedomie povinnosť prevádzkovateľa zverejniť túto zmluvu a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy v plnom rozsahu.
2. Táto zmluva nadobúda platnosť podpisom oprávnených zástupcov zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Táto zmluva sa uzatvára na dobu určitú, do dňa skončenia platnosti a účinnosti na zabezpečenie pozáručného servisu, údržby a opráv výpočtovej techniky č. 28033-5/2024 –BA.
4. Počas platnosti dohody o poskytovaní služieb je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane.
5. Práva a povinnosti neupravené touto zmluvou sa budú riadiť príslušnými ustanoveniami právnych predpisov platných na území SR.
6. Zmluvné strany štandardne komunikujú prostredníctvom elektronickej pošty. V prípadoch, keď to vyžaduje zmluva, všeobecne záväzný právny predpis alebo jedna zo zmluvných strán, doručí sa aj listinná podoba požiadavky, súhlasu a pod.
7. 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 SR.
8. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k zmluve.
9. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.
10. 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 11-07-2024

Za prevádzkovateľa:

Ing. Michal Tariška
generálny riaditeľ Sociálnej poisťovne

V Bratislave, dňa 28.06.2024

Za sprostredkovateľa:

Ing. Juraj Zelko
člen predstavenstva

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

SP číslo zmluvy: 28033-7/2024 - BA

Príloha č. 4 k zmluve

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

Čl. I
Zmluvné strany

Prevádzkovateľ

Názov:	**Sociálna poisťovňa**
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Tariška generálny riaditeľ Sociálnej poisťovne
IČO:	308 07 484
DIČ:	2020592332
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC:	SPSRSKBA

(ďalej len „**prevádzkovateľ**")

a

Obchodné meno:	DATALAN, a.s.
Sídlo:	Krasovského 14, Bratislava - mestská časť Petržalka 851 01
Štatutárny orgán:	Ing. Juraj Zelko - Člen predstavenstva
Zápis v registri:	Obchodný register Mestského súdu Bratislava III, Oddiel: Sa, Vložka číslo: 2704/B
IČO:	**35 810 734**
DIČ:	2020259175
IČ pre DPH:	SK2020259175
Bankové spojenie:	
IBAN:	

(ďalej len „**dodávateľ**")

(spolu ďalej ako „**zmluvné strany**")

Čl. II
Preambula

1. Prevádzkovateľ je podľa § 3 písm. l) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti") prevádzkovateľom základnej služby podľa § 3 písm. k) body 2 a 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti dodávateľom, ktorý na základe zmluvy na výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.

2. Zmluvné strany spolu uzatvárajú zmluvný vzťah na základe Zmluvy č. 28033-5/2024-BA

8. Dodávateľ je povinný doručiť prevádzkovateľovi zoznam zamestnancov dodávateľa subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa zmluvy na výkon činností a tejto zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa (ďalej len „zoznam osôb"). Dodávateľ je povinný oznámiť prevádzkovateľovi každú zmenu v zozname zamestnancov podľa tohto bodu a to elektronicky prostredníctvom Ústredného portálu verejnej správy (ďalej „UPVS"). Dodávateľ je povinný zabezpečiť, aby každá osoba uvedená v zozname osôb, schválená odborom bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie stratégie a informatiky prevádzkovateľa podpísala vyhlásenie o mlčanlivosti a zúčastnila sa na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností. Po podpísaní vyhlásenia o mlčanlivosti budú týmto osobám sprístupnené bezpečnostné politiky prevádzkovateľa.
9. Dodávateľ je povinný písomne informovať prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto zmluvy.
10. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Čl. V
Okolnosti plnenia zmluvy

1. Pojmy používané v tejto zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.
2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností 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 zmluvy na výkon činností. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania zmluvy na výkon činností.
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 zmluvy na výkon činností a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto zmluvy nemá nárok.

Čl. VI
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

Dodávateľ je povinný v rámci prevencie kybernetických incidentov, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa, a tým na činnosť prevádzkovateľa:

a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby pri poskytovaní elektronických komunikačných služieb a sietí cez siete a informačné systémy dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,
b. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú

8. Po schválení ochranného opatrenia prevádzkovateľom je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť prevádzkovateľovi.
9. Dodávateľ je povinný informovať prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to elektronicky prostredníctvom ÚPVS.

Čl. VIII
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 a prevádzky elektronických komunikačných služieb alebo sietí.
2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. 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.

Čl. IX
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 na základe zákona o kybernetickej bezpečnosti a tejto zmluvy.
2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
3. 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.
4. Dodávateľ je pri audite povinný spolupracovať s prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto zmluvy.
6. 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, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u dodávateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.

prevádzkovateľa.

9. 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 prevádzkovateľom, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom UPVS, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: riaditeľ odboru bezpečnosti informačných systémov.
3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je:
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: bis@socpoist.sk
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je: spetergac@datalan.sk
6. Kontaktné osoby podľa bodov 2. a 3. tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme na adresu zmluvnej strany uvedenú v záhlaví tejto zmluvy alebo elektronicky prostredníctvom UPVS.

Čl. XII
Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) a v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
2. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády SR.
3. Táto zmluva sa uzatvára na dobu určitú po dobu platnosti a účinnosti zmluvného vzťahu na výkon činnosti definovanej v článku II – Zmluvy č. 28033-5/2024-BA na pozáručný autorizovaný servis zariadení výpočtovej techniky.
4. Počas platnosti a účinnosti zmluvy na výkon činností je možné ukončiť túto zmluvu len dohodou, alebo výpoveďou bez udania dôvodu, no len zo strany prevádzkovateľa. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane. Skončenie tejto zmluvy sa netýka tých ustanovení, 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.
5. 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.
6. 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

Príloha č. 1 k Prílohe č. 12 - zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Bezpečnostné politiky

1. Všeobecné ustanovenia

(1) Dodávateľ sa zaväzuje pri plnení zmluvy dodržiavať platné a účinné všeobecne záväzné právne predpisy Slovenskej republiky ako aj právne akty Európskej únie (ďalej „EÚ").

(2) Vstup a pohyb zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne iných tretích osôb, prostredníctvom ktorých dodávateľ poskytuje služby (ďalej len „tretia osoba") do priestorov prevádzkovateľa v súvislosti splnením predmetu zmluvy s prevádzkovateľom je možný iba v sprievode na to určeného zamestnanca prevádzkovateľa.

2. Mobilné zariadenia a práca na diaľku

2.1 Politika pre mobilné zariadenia

(1) Spracúvať osobné údaje a iné citlivé údaje prostredníctvom mobilného telefónu je možné len za predpokladu, že citlivé údaje sú uchovávané v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.

(2) Spracúvať osobné údaje prostredníctvom notebooku je možné len za predpokladu, že osobné údaje sú uchovávané v pseudonymizovanej alebo v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.

2.2 Práca na diaľku

(1) Vzdialený prístup zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne inej tretej osoby do informačných systémov a ostatného softvéru prevádzkovateľa nie je možný. Prístup je možné povoliť iba v odôvodniteľných prípadoch, a to iba s dohľadom na to určeného zodpovedného zamestnanca dodávateľa, ak sa dodávateľ s prevádzkovateľom písomne nedohodne inak.

(2) Práca na diaľku sa povoľuje len pre určitý okruh zamestnancov dodávateľa, iba pre určité druhy práce, a musí byť adekvátne zabezpečený aj priestor pracoviska, z ktorého je vykonávaná.

(3) Práca nesmie prebiehať na prostriedkoch v súkromnom vlastníctve, ktoré nie sú pod kontrolou dodávateľa.

(4) Zamestnanec dodávateľa, jeho subdodávateľa, prípadne tretia osoba musia byť adekvátne poučený a zmluvne zaviazaný neporušiť pravidlá na zabezpečenie ochrany, odcudzenia alebo vyzradenia chránených údajov.

(5) Fyzická bezpečnosť musí byť odkontrolovaná na mieste výkonu práce. Kontrolu zabezpečí dodávateľom určený zamestnanec, o čom sa vyhotoví záznam, pričom prevádzkovateľ si vyhradzuje právo kontroly priestorov dodávateľa, resp. jeho subdodávateľa, alebo tretej osoby, z ktorých sa práca na diaľku uskutočňuje.

(6) Žiadosť o zriadenie vzdialeného prístupu pre zamestnanca dodávateľa, resp. jeho subdodávateľa, alebo tretiu osobu postúpi príslušný zmluvný kontakt prevádzkovateľa oddeleniu centrálneho dispečingu a monitorovania služieb IS SP. V žiadosti špecifikuje rozsah prístupových oprávnení. Po schválení žiadosti riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie stratégie a informatiky prevádzkovateľa a po doručení záznamu

vykonáva zodpovedná osoba prevádzkovateľa.

3. Riadenie vzťahov s dodávateľom

3.1 Informačná bezpečnosť vo vzťahoch s dodávateľom

Cieľom je zabezpečiť ochranu aktív prevádzkovateľa, ku ktorým má prístup dodávateľ samostatne, prostredníctvom subdodávateľa alebo prostredníctvom tretej osoby.

3.1.1 Politika informačnej bezpečnosti na vzťahy s dodávateľom

(1) Predtým, než sa dodávateľovi, prípadne jeho subdodávateľovi, alebo tretej osobe povolí prístup k chráneným informáciám prevádzkovateľa, musí byť vykonaná identifikácia rizík informačnej bezpečnosti a implementované vhodné opatrenia na pokrytie identifikovaných rizík na strane dodávateľa, prípadne jeho subdodávateľa, alebo tretej osoby. Uvedené posúdenie rizík informačnej bezpečnosti musí byť v písomnej alebo elektronickej forme dodané prevádzkovateľovi v dostatočnom časovom predstihu pred podpisom zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností na jeho preštudovanie.

(2) Prístup zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby k chráneným informáciám prevádzkovateľa nesmie byť dovolený skôr, ako je podpísaná zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľom a ako sú realizované primerané bezpečnostné opatrenia na ochranu aktív prevádzkovateľa.

(3) Zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby sa zriaďuje prístup na dobu najdlhšie jeden rok. Po uplynutí jedného roka sa potreba prístupu prehodnocuje.

(4) Zriadenie prístupu zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osobe za účelom testovania môže byť zriadené len do testovacieho prostredia prevádzkovateľa. Nasadenie vývojovej verzie APV sa musí uskutočniť výhradne v prostredí prevádzkovateľa za prítomnosti určeného zamestnanca sekcie stratégie a informatiky. Tieto činnosti musia byť zdokumentované.

3.1.2 Ošetrenie bezpečnosti v zmluvách s dodávateľom

(1) Zmluvy na výkon činností s dodávateľom musia pokrývať všetky významné bezpečnostné požiadavky. Zmluvy na výkon činností obsahujú samostatné ustanovenia alebo klauzuly, ktoré vyplývajú z bezpečnostne relevantnej legislatívy SR, zo slovenských technických noriem a z najlepších skúseností.

(2) Pred spracúvaním osobných údajov k časti bezpečnostných formulácií v návrhu zmluvy na výkon činností zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá posúdi dostatočnosť a primeranosť špecifikovaných technických a organizačných opatrení na ochranu osobných údajov.

(3) K bezpečnostným formuláciám v návrhu zmluvy na výkon činností s dodávateľom zaujme stanovisko riaditeľ odboru bezpečnosti informačných systémov, ktorý posúdi dostatočnosť bezpečnostných opatrení a notifikačných povinností, ktoré musia platiť počas celej doby platnosti zmluvy na výkon činností pre zaistenie kybernetickej bezpečnosti.

(4) Nie je prípustné v zmluve na výkon činností špecifikovať bližšie neurčených subdodávateľov alebo tretiu osobu a tým následne zriaďovať prístup pre zamestnancov subdodávateľa alebo tretiu osobu.

3.1.3 Monitorovanie a preskúmanie dodávateľských služieb

(1) Služby a záznamy poskytované dodávateľom sú priebežne kontrolované osobou zodpovednou za výkon zmluvy na výkon činností, a sú monitorované vnútornou kontrolou, bezpečnostným monitoringom, interným auditom alebo externým auditom, tak ako je to zmluvne

c) pokus a narušenie jednotlivých prvkov zabezpečovacieho systému,
d) neoprávnený pobyt v objektoch prevádzkovateľa,
e) násilné vniknutie do budovy, do zariadení (serverovňa, pokladňa, technologická miestnosť), prípadne do automobilov (s následkom odcudzenia spisov, dát a zariadení, ktoré obsahujú informácie, ktorých stratou, zneužitím prípadne zničením by došlo k obmedzeniu služieb poistencom, porušením dôverností, finančným stratám),
f) poškodenie a zničenie majetku (časti majetku, napr. klimatizačná jednotka, UPS),
g) následky havárií (prasknutie potrubia, výpadok náhradného zdroja, požiar, zatopenie, zatečenie),
h) odcudzenie (strata) dokladov o poistencovi prevádzkovateľa,
i) podvod, sprenevera,
j) preukázané použitie násilia alebo hrozby bezprostredného násilia v úmysle zmocniť sa aktív prevádzkovateľa.

(3) V oblasti informačnej bezpečnosti prevádzkovateľa

a) zverejnenie hesla používateľa,
b) zmena alebo resetovanie hesla na účte alebo zariadení neoprávnenou osobou,
c) diskreditácia bezpečnostného predmetu (GRID karty, tokenu, prvkov PKI),
d) prístup neoprávnenej (cudzia osoba, nevyškolená obsluha a pod.) osoby do IS SP,
e) vírusová infiltrácia do IS SP, zasielanie nežiadúceho obsahu, škodlivý kód,
f) prienik do IS alebo pokus o prienik,
g) kybernetický bezpečnostný incident,
h) inštalácie neschváleného hardvéru a softvéru na komponentoch IS SP,
i) neoprávnené premiestnenie technických komponentov IS SP,
j) používateľom vykonané zmeny hardvérovej konfigurácie počítača, servera, siete, komunikačných prvkov a pod.,
k) nevykonávanie záloh na serveroch zaradených do systému centralizovaných záloh alebo serverov s inak definovanou zálohovacou stratégiou,
l) zničenie alebo odcudzenie médií, na ktorých sú bezpečnostné zálohy serverov,
m) prepisovanie auditných záznamov,
n) krádež hardvéru alebo softwaru, ktorá ovplyvňuje prevádzky schopnosť IS SP,
o) krádež a deštrukcia dát IS SP,
p) zámerné zneužitie prístupu k zariadeniam IS SP,
q) neplánovaný výpadok elektrického prúdu,
r) poskytnutie, sprístupnenie, alebo zverejnenie osobných údajov konaním osoby alebo technickou poruchou IS v rozpore s pravidlami platných vnútorných predpisov prevádzkovateľa,
s) neoprávnené použitie vstupno-výstupných zariadení nepatriacich do vlastníctva prevádzkovateľa, spôsobujúce hrozbu nebezpečnej infiltrácie,
t) spracúvanie osobných údajov inou ako oprávnenou osobou,
u) porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,
v) porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

3.1.7 Poučenie a záväzok mlčanlivosti

(1) Vstupné poučenie o ochrane osobných údajov musí absolvovať každý zamestnanec

Príloha č. 2 k Prílohe č. 12 - zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Kyberbezpečnostný štandard

pre projekty a IT v Sociálnej poisťovni

Úvod

Informačné systémy, technológie a prostriedky používané v Sociálnej Poisťovni – SP musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované. To znamená, že ak útočník kompromituje časť infraštruktúry, je pre neho zložité dostať sa ďalej a kompromitovať ďalšiu časť infraštruktúry – to znamená je obmedzená možnosť pivotingu. Je nutné implementovať viacúrovňovú hĺbkovú ochranu – to znamená že bude bezpečnostná kontrola na viacerých miestach a prelomením jednej úrovne nedôjde priamo ku kompromitácii dát.
Vzhľadom na neustále sa vyvíjajúce a meniace techniky útokov a obrany je táto metodika žijúcim dokumentom.

Cieľ dokumentu

Tento dokument vyberá a sumarizuje minimálne bezpečnostné zásady a opatrenia potrebné na zabezpečenie informačných systémov, technológií a infraštruktúry SP ako aj pre novovznikajúce či existujúce projekty, procesy, zmeny a ostatné aktivity majúce vplyv na bezpečnosť informačných systémov (BIS) v SP tak aby platili princípy uvedené v úvode.
V dokumente sa používajú kľúčové slová „musí", „malo by byť", „odporúča sa". Tieto sú ohodnotením dôležitosti daného opatrenia s ohľadom na jeho implementačnú náročnosť.
Dokument vznikol na základe podkladov z originálu Metodiky zabezpečenia IKT verejnej správy v oblasti informačnej bezpečnosti, ktorého autorom je CSIRT.SK (*MetodikaZabezpeceniaIKT_v2.1.pdf (gov.sk)*) ako aj zo Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, a zo Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, z Vyhlášky č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy a aj z Vyhlášky č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú musieť byť vypracované v projektovej dokumentácii, zmenovej dokumentácii a ostatných podkladových materiálov, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru BIS na validáciu.

Obmedzenia

Dokument sa v tejto verzií nezaoberá špecifickými požiadavkami na: fyzickú bezpečnosť infraštruktúry, bezpečnosť mobilných zariadení, bezpečnosť Internetu vecí (IoT – Internet of Things), bezpečnosť ICS systémov (Industrial Control Systems), zabezpečenie služieb využívajúcich IPv4 multicast, zabezpečenie webových služieb (web services).

8) Počas vývoja musí byť vedená vývojárska dokumentácia:
   a) dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii,
   b) v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.
9) Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením.
10) Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:
   a) autentifikačné údaje musia byť uložené iba v podobe osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256,
   b) ostatné osobné údaje (adresy, čísla platobných kariet, čísla občianskych preukazov,...) je odporúčané neukladať v čistej podobe, ale chránené šifrovaním.
11) Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:
   a) (úspešné aj neúspešné) prihlásenie a odhlásenie,
   b) (úspešné aj neúspešné) vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny,
   c) (úspešné aj neúspešné) pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie),
   d) (úspešné aj neúspešné) pokusy o kritické operácie,
   e) zaznamenávajú sa úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
   f) zaznamenávajú sa úspešné a neúspešné prístupy k log súborom,
   g) zaznamenávajú sa úspešné a neúspešné prístupy k systémovým zdrojom,
   h) zaznamenáva sa vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
   i) zaznamenávajú sa zmeny v prístupových oprávneniach,
   j) zaznamenáva sa aktivácia a deaktivácia bezpečnostných mechanizmov,
   k) zaznamenáva sa spustenie a zastavenie procesov,
   l) zaznamenávajú sa konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
   m) zaznamenáva sa spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
   n) zaznamenávajú sa významné aktivity v sieťovej komunikácii,
   o) zaznamenáva sa požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
   p) zaznamenávajú sa IP adresy pridelené prostredníctvom služby DHCP,
   q) záznamy v log súboroch obsahujú ku každej udalosti (ak je k dispozícii) čas a dátum udalosti,
   r) záznamy v log súboroch obsahujú ku každej udalosti identifikáciu používateľa,
   s) záznamy v log súboroch obsahujú ku každej udalosti identifikáciu zariadenia,
   t) záznamy v log súboroch obsahujú ku každej udalosti informáciu týkajúcu sa udalosti,
   u) záznamy v log súboroch obsahujú ku každej udalosti indikáciu úspešnosti, alebo zlyhania operácie,
   v) záznamy v log súboroch obsahujú ku každej udalosti pri sieťových službách zdrojovú IP adresa, cieľovú IP adresa, protokol, zdrojový port, cieľový port,
   w) na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja,
   x) záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií

funkcionality.
5) Na serveri musia byť zatvorené všetky nepotrebné porty.
6) Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:
   a) nepotrebné implicitné účty musia byť odstránené alebo zneplatnené,
   b) neaktívne kontá musia byť zneplatnené.
7) Na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín.
8) Heslo ku kontu musí zodpovedať požiadavkám organizácie na komplexnosť hesiel a má byť znemožnený útok hádaním či hrubou silou, viď príloha dokumentu.
9) Právo na vykonávanie systémových úkonov musí byť obmedzené na poverených administrátorov. Tí by sa navyše vzdialene mali prihlasovať iba v restricted režime, ak sa používa RDP (RDP restricted admin).
10) Lokálny administrátor webservera musí byť unikátny pre každý webový server.
11) Servery s OS Windows buď nesmú byť v doméne alebo musia byť spravované RO doménovým radičom (RODC – read-only domain controller).

Webový server

1) Pri inštalácií webového servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:
   a) sw webového servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS,
   b) musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností,
   c) pre webový obsah by mal byť vytvorený dedikovaný fyzický disk alebo logická partícia (separátne od OS a SW webového servera),
   d) všetky služby inštalované popri webovom serveri, ktoré nie sú potrebné (napr. FTP server alebo služba vzdialenej administrácie) musia byť vypnuté alebo odstránené,
   e) nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté,
   f) z webového servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu,
   g) odporúčame na server aplikovať hardenovací skript alebo bezpečnostnú šablónu, vhodný pre daný OS a webový server. Info možno čerpať z príručiek dostupných na webstránke CSIRT.SK,
   h) banner HTTP služby by mal byť rekonfigurovaný, podľa potreby aj s ďalšími bannermi tak, aby nereportovali typ a verziu webového servera a podkladového OS.
2) Webový server by mal podporovať iba HTTP metódy POST a GET.
3) Webový server nesmú podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
4) Webový server musí byť odolný voči SlowHTTP DoS útokom (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty, implementácia loadbalancerov).
5) Z webového servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.
6) Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.
7) Na serveri musí byť nakonfigurovaný defaultný virtuálny host na obsluhu prístupu na webserver prostredníctvom IP adresy (cez prehliadač). Nesmie byť zobrazovaná defaultná stránka použitého frameworku a pod.
8) Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.

minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by mali byť logy kontrolované denne.

6) Webový server musí byť pravidelne zálohovaný nasledovným spôsobom:
   a) zálohovanie servera má byť upravené organizačnými opatreniami organizácie,
   b) archívna záloha musí byť vytvorená minimálne raz ročne,
   c) diferenciálna alebo zmenová záloha webového servera má byť vytvorená na dennej až týždennej báze,
   d) plný backup webového servera by mal byť vytváraný v týždňových až mesačných intervaloch,
   e) zálohy servera by mali byť periodicky archivované na externé médiá,
   f) mala by byť uchovávaná autoritatívna kópia webovej stránky/stránok.

Kontrola prístupu OS a webového servera

1) Proces webového servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.
2) Webový server by mal byť konfigurovaný tak, aby súbory s webovým obsahom boli procesom prislúchajúcim službe webového servera prístupné na čítanie, no nie na zápis. Procesy webového servera by nemali mať právo zápisu do priečinkov, kde je uchovávaný verejný webový obsah (web content).
3) OS by mal byť nakonfigurovaný tak, aby proces webového servera mohol vytvárať log záznamy, no nemohol ich čítať.
4) OS by mal byť podľa možnosti nakonfigurovaný, aby dočasné súbory vytvorené procesmi webového servera boli obmedzené na určený a vhodne zabezpečený priečinok. Ak je to možné, prístup k dočasným súborom by mal byť obmedzený na procesy, ktoré ich vytvorili.
5) Webový obsah a všetky logy ním vytvárané by mali byť umiestnené na separátnom pevnom disku alebo na inej logickej partícii, ako OS a webový server.
6) Odporúča sa webový server izolovať od iných procesov použitím prostriedkov ako napríklad chroot, kontajnery, virtualizácia a pod.
7) Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).
8) Mal by byť stanovený maximálny počet procesov webového servera a/alebo sieťových spojení, ktoré by server mal povoliť.
9) Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).
10) Použitie symbolických linkov by malo byť pre procesy webového servera zakázané.
11) Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.
12) V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr. CAPTCHA, nofollow, filtrovanie kľúčových slov).

HTTP hlavičky a cookies

1) Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security. Nastavené by mali byť direktívy:
   a) max-age=<číslo> – počet sekúnd, počas ktorých má prehliadač automaticky konvertovať všetky HTTP požiadavky do HTTPS,
   b) includeSubDomains – indikuje, že všetky subdomény aplikácie musia používať HTTPS.

aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.

10) Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.
11) Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.
12) Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.
13) Aplikácia musí pri zmene hesla vyžadovať opakované zadanie nového hesla (2 krát), pričom nové zadané heslá sa musia zhodovať.
14) Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, KeyCloak, ...).
15) Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.
16) Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.
17) Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať soľ (angl. salt).
18) Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.
19) Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.
20) Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu.
21) Odporúča sa naviazanie relácie na parameter User-Agent.
22) Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lockout) po istom počte neúspešných pokusov (maximálne 5) o prihlásenie.
23) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie musí trvať aspoň 10 minút.
24) Zamknutie účtu po stanovenom počte neúspešných pokusov o prihlásenie do kritického systému by malo trvať aspoň hodinu.
25) Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla).
26) V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.
27) Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako admin, administrator, user a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).
28) Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.
29) Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.
30) Používateľské kontá, ktoré neboli použité do 3 mesiacov od ich vytvorenia (používateľ sa počas danej doby nikdy neprihlásil), by mali byť deaktivované.
31) Každý používateľ a administrátor musia mať jedinečné ID.
32) Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. (admin, administrator, helpdesk, support a pod.).
33) Aplikácia musí korektne inštruovať prehliadač, aby neukladal citlivé informácie, prenášané prostredníctvom HTTPS, do cache (a aby neboli bez kontroly opäť prístupné z histórie prehliadania) minimálne v rozsahu:
    a) Server musí nastavovať vo svojich odpovediach hlavičky:
        - Cache-Control: no-cache, no-store, private, must-re-validate, max-age=0, no-transform,

7) Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia zneplatniť ostatné relácie príslušného používateľa.
8) Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.
9) Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.
10) Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.
11) Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).
12) Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.
13) Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.
14) Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.
15) Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

Nahrávanie súborov

1) Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root) na separátnu partíciu disku (inú, ako je vyhradené na zápis logov), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP, ...).
2) Aplikácia nesmie spúšťať a vyhodnocovať (evaluate) nahraté súbory.
3) Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.
4) Aplikácia by mala obmedzovať počet súborov nahraných za hodinu.
5) Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ.
6) Aplikácia by mala nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.
7) Nahrávané súbory by sa nemali ukladať pod pôvodným názvom.

Obsah

1) Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.
2) Aplikácia by mala pre všetky poskytované stránky definovať „character set".
3) Zabezpečenie aktívneho obsahu (skripty, spustiteľné súbory):
    a) právo na čítanie a zápis do súborového systému by malo byť limitované alebo zakázané,
    b) mala by byť povolená žiadna alebo len limitovaná interakcia s inými programami,
    c) nemala by byť potrebná žiadna akcia so SUID privilégiami (OS UNIX/Linux),
    d) skripty by pri spúšťaní externých programov mali používať absolútne cesty alebo nepoužívať žiadne cesty a spoliehať sa na premennú PATH, pričom tá musí obsahovať len bezpečné adresáre,
    e) žiadne priečinky nesmú mať súčasne práva na zápis a vykonávanie,
    f) spustiteľné súbory by mali byť umiestnené vo vyhradených priečinkoch,
    g) SSI (Server-Side Inclusion) by mali byť zakázané, resp. nie je možné ich spúšťať.

4) Spracovanie XML
    a) aplikácia nesmie podporovať XML External entity expansion,
    b) aplikácia nesmie podporovať parsovanie XML External DTD,
    c) aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia,
    d) aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

Rôzne

riešenia na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení,

b) ak samotné vyvíjané riešenie obsahuje informácie, ktoré je potrebné chrániť z hľadiska dôvernosti, musia byť vo vývojovom prostredí implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

4 Štandardy prepojenia

Sieťové protokoly

1) Štandardom sieťových protokolov je
   a) pre informačné systémy a ich komponenty, ktoré sú zavedené po 1. septembri 2009, používanie sieťového protokolu Internet Protocol vo verzii 6 (IPv6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
   b) pre informačné systémy a ich komponenty, ktoré sú zavedené do 31. augusta 2009 podpora sieťového protokolu Internet Protocol vo verzii 4 (IPv4) s podporou sieťovej technológie Dual stack spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP) pre informačné systémy alebo sieťového protokolu Internet Protocol vo verzii 6 (IPv6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
   c) používanie skupiny protokolov Internet Procotol Security (IPSEC) na zabezpečenie sieťových protokolov.

Prenos dát

1) Štandardom prenosu dát je

   a) používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext Transfer Protocol (HTTP) a

   b) podpora chráneného prenosu dát cez kryptografický protokol Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group.

2) Špecifikácie prepojenia pomocou sieťových služieb

   Štandardom špecifikácie prepojenia pomocou sieťových služieb je používanie Domain Name Services (DNS) ako hierarchickej služby name servera v centrálnych bodoch internetu.

3) Sieťová a komunikačná bezpečnosť

   a) aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov,
   b) na prenos informácií k tretím stranám uzatvorenie zmluvy o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami,
   c) všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany

Nesmie byť možné zistiť verziu použitého softvéru prostredníctvom help príkazov.

3) Mailové správy odchádzajúce z organizácie by nemali obsahovať informácie o infraštruktúre organizácie (napríklad privátne IP adresy v hlavičke Received-From).
4) Odpoveď na príkaz VRFY by nemala obsahovať informáciu o existencií adresy alebo používateľského mena. Odporúča sa odpovedať kódom 252 s generickou hláškou.
5) Nemala by byť povolená metóda EXPN.
6) SMTP server by nemal preposlať e-mail, ktorý neobsahuje zdrojovú hlavičkovú e-mailovú adresu.
7) SMTP server musí prijímať správy na doručenie z externých sietí len pre spravované domény.
8) SMTP server musí prijímať správy na preposlanie len od autentifikovaných používateľov alebo z určených SMTP serverov.
9) Server by mal detegovať a blokovať pokusy o rozoslanie veľkého množstva e-mailov.
10) SMTP server musí kontrolovať správy pomocou anti-spam filtra.
11) SMTP server musí kontrolovať správy na prítomnosť škodlivého kódu.
12) SMTP server musí logovať všetky detegované anomálie.
13) SMTP server musí logovať informácie o spracovávaných e-mailoch a tieto informácie by mali byť uchovávané aspoň 6 (šesť) mesiacov. Musia byť uchovávané aspoň 3 (tri) mesiace.
14) Prístup k e-mailovým účtom musí byť možný len prostredníctvom šifrovaného kanála.
15) Odporúča sa na prístup k e-mailovej schránke nepoužívať proprietárne protokoly.
16) Z externých sietí by sa malo pristupovať na e-mail len prostredníctvom HTTPS alebo použitím štandardných protokolov POP3S alebo IMAPS. Odporúča sa autentifikovať klienta aj na základe certifikátu alebo vyžadovať použitie VPN. V prípade použitia iných protokolov by sa malo pristupovať prostredníctvom VPN pripojenia.

5.2 Prístup k elektronickej poštovej schránke

1) Štandardom prístupu k elektronickej poštovej schránke je
   a) používanie protokolu Post Office Protocol vo verzii 3 (POP3) alebo protokolu Internet Message Access Protocol v revidovanej verzii 4.1 (IMAP4rev1) pre prístup k verejným elektronickým poštovým službám,

   b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group pri chránenom prístupe k verejným elektronickým poštovým službám. Formát elektronických poštových správ.

2) Štandardom formátu elektronických poštových správ je používanie formátu
   a) Multipurpose Internet Mail Extensions (MIME) pri prenose elektronických poštových správ,
   b) Secure/Multipurpose Internet Mail Extensions (S/MIME) pri chránenom prenose elektronických poštových správ.

6 Štandardy prístupu k elektronickým službám

6.1 Aplikačné protokoly elektronických služieb

1) Štandardom aplikačných protokolov elektronických služieb je
   a) používanie protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 s prenosom dát vo formáte Extensible HyperText Markup Language (XHTML) vo verzii 1.0 na komunikáciu medzi klientom a webovým serverom,

6. Web Map Tile Service (WMTS).

g) schémy správ Sk-Talk najmenej vo verzii 3.0 pre asynchrónnu komunikáciu s ústredným portálom verejnej správy podľa aktuálne platnej osobitnej špecifikácie zverejnenej po dohode s orgánom vedenia podľa § 24 ods. 5 Zákona č. 95/2019 na ústrednom portáli verejnej správy,

h) špecifikácie OpenAPI Specification najmenej vo verzii 3.0 na definíciu webovej služby pri použití protokolu Representational State Transfer (REST),

i) špecifikácie OpenID Connect podľa OpenID Foundation s OAuth2 podľa osobitnej špecifikácie RFC 6749, ak sa pri použití protokolu Representational State Transfer (REST) vyžaduje autentifikácia a určenie rozsahu oprávnení.

8 Štandardy integrácie dát

8.1 Opisný jazyk dátových prvkov

1) Štandardom opisného jazyku dátových prvkov je používanie jazyka Extensible Markup Language (XML) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pre dátové prvky pri vstupe na rozhranie informačného systému verejnej správy.

8.2 Prenos dátových prvkov

1) Štandardom prenosu dátových prvkov je používanie

a) jazyka schém XML Schema Definition (.xsd) najmenej vo verzii 1.0 podľa World Wide Web Consortium (W3C) na výmenu dátových prvkov medzi všetkými informačnými systémami verejnej správy,

b) jazyka Extensible Markup Language (.xml) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pri výmene dátových prvkov, a to s hodnotou atribútu pre deklaráciu menného priestoru spravidla v tvare referencovateľného identifikátora, pričom ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov, je možné namiesto Extensible Markup Language použiť dátový model Resource Description Framework (RDF) opísaný formátmi RDF/XML podľa World Wide Web Consortium (W3C) alebo JSON-LD; pri otvorených údajoch je možné použiť aj formát CSV podľa Vyhlášky č. 78/2020, § 24 písm. e) alebo formát JavaScript Object Notation (JSON),

c) znakovej sady Unicode Character Set (UCS) podľa technickej normy v 8 bitovom kódovaní UTF-8,

d) transformačného jazyka XSL Transformations (XSLT) podľa World Wide Web Consortium (W3C) pri transformácii dátových prvkov,

e) formátu Geography Markup Language (GML) pri výmene priestorových dátových prvkov alebo ak sa na tom zasielateľ a prijímateľ dohodnú jeden z formátov uvedených v štandardoch poskytovania otvorených údajov Vyhlášky č. 78/2020 Z. z. § 40 písm. i),

f) jazyka Web Ontology Language (OWL) pre ontológie, ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov,

g) jazyka Shapes Constraint Language (SHACL) podľa World Wide Web Consortium (W3C) pre validáciu dátového modelu Resource Description Framework (RDF) v Centrálnom modeli údajov.

7) Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.
8) Webový portál by nemal ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.
9) Webový portál by nemal vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/ TLS.
10) Pri informačných technológiách s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.
11) Pri informačných technológiách s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä elektronických dokumentov a technológií v nasledujúcich riadkoch:
    a) šifrovanie dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
    b) šifrovanie emailovej komunikácie prostredníctvom PGP alebo S/MIME,
    c) šifrovanie komunikačných kanálov na výmenu nešifrovaných dát,
    d) šifrovanie centrálnych úložísk,
    e) šifrovanie záloh.

12 Šifrovacie kľúče a protokoly

1) Webový server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0 a TLS 1.1.
2) Webový server musí podporovať TLS 1.2.
3) Webový server by mal podporovať TLS 1.3.
4) Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.
5) Webový server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.
6) Webový server nesmie podporovať tzv. Export (EXP) šifry.
7) Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia by mala byť vypnutá).
8) Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov.
9) X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5).
10) Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).
11) Webový server by nemal podporovať RC4, DES a 3DES.
12) Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).
13) Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.
14) Konfiguráciu odporúčame otestovať v SSL/TLS teste.
15) Pri správe SSL/TLS je nutné sledovať a v konfigurácii reflektovať aktuálne odporúčania. V prípade použitia WAF/FW pre SSL/TLS preň platia všetky vyššie uvedené požiadavky.

inému dodávateľovi.

4) Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká BIS a posúdia sa najmä:
   a) kritické komponenty a prvky služby,
   b) možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
   c) možné riziká BIS vo vzťahoch medzi dodávateľmi a subdodávateľmi,
   d) ďalšie možné riziká BIS vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému dodávateľovi.
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 BIS v SP.
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 SP, 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) Zamedzenie prístupu tretích strán ku všetkým údajom v IT SP, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom len na základe zmluvy tak, aby nebola narušená bezpečnosť IT SP a bezpečnostná politika SP.

Dodatky

Vysvetlenie skratiek
ACL - Access Control List
AP - Access Point
BIS – Bezpečnosť informačných systémov
CSRF - Cross-Site Request Forgery
DHCP - Dynamic Host Configuration Protocol
DMZ - Demilitarized Zone - VLAN, v ktorej sú umiestnené servery poskytujúce služby do externej siete, ktorá je logicky oddelená od internej siete (komunikácia je fultrovaná sieťovým firewallom)
DNS - Domain Name System
DoS – Denial of Service
FW – Firewall
IB – Informačná bezpečnosť
ICS - Industrial Control System
MitM útok – Man in the Middle útok
MVC – návrhový vzor Model–View–Controller
MVP - návrhový vzor Model–View–Presenter
NAC – Network Access Control
NAP - Network Access Protection
NDP - Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4
NTP - Network Time Protocol
OS - Operačný systém PVLAN – Private VLAN princíp least privilege
RDP - Remote Desktop Protocol
QoS - Quality of Service

a odporúčacích opatrení (zákon o ochrane osobných údajov),

- Zákon č. **69/2018** Z. z., o Kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov,
- Zákon č. **95/2019** Z. z., o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov,
- Zákon č. **452/2021** Z. z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení),
- Vyhláška 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,
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **78/2020** Z. z. o štandardoch pre informačné technológie verejnej správy,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **85/2018** Z. z., ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **70/2021** Z. z. o zaručenej konverzii,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **438/2019** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy VS,
- Vyhláška Ministerstva vnútra Slovenskej republiky č. **29/2017** Z. z. o alternatívnom autentifikátore,
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **401/2023** Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy,
- Vyhláška Národného bezpečnostného úradu č. **48/2019** Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností,
- Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov v aktuálne platnom znení,
- Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
- Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- Nariadenie GDPR - 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),
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2018/1725** z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES,
- Nariadenie Európskeho parlamentu a Rady (EÚ) **2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii

rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,

- **chránené** informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené" je riadený pomocou zásady „potreby vedieť" a zásady „najnižších privilégií" a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,
- **prísne** chránené informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené" je riadený pomocou zásady „potreby vedieť" a zásady „najnižších privilégií" a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

Ak nie je informačné aktívum explicitne klasifikované je považované za interné.

Integrita

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

- **nízka** zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,
- **stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,
- **vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby.

Dostupnosť

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

- **nízka** zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,
- **stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,
- **vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.