

Realizačná zmluva č. VO1-2024/000328-004

uzatvorená podľa čl. III Rámcovej dohody o poskytovaní poradenských služieb v oblasti auditu č. OVO2-2020/000354 6 zo dňa 14.07.2020
(ďalej len „Realizačná zmluva“)

Článok I Zmluvné strany

Audítor:	stengl a.s.
Sídlo:	Sumbalova 1/A, 841 04 Bratislava
Zastúpený:	Miroslav Novotný - predseda predstavenstva Ing. Andrej Petrovaj - podpredseda predstavenstva
IČO:	35873426
DIČ alebo IČ DPH:	2021772720
Bankové spojenie:	XXXXX
IBAN:	XXXXX
BIC/SWIFT kód:	XXXXX

(ďalej len „Audítor“)

a

Klient:	Sociálna poisťovňa
Sídlo:	Ulica 29. augusta 8 a 10, 813 63 Bratislava
Zastúpený:	Ing. Michal Tariška, generálny riaditeľ Sociálnej poisťovne
IČO:	30807484
Bankové spojenie:	Štátna pokladnica
IBAN:	SK40 8180 0000 0070 0016 4314
BIC/SWIFT kód:	SPSRSKBA

(ďalej len „Klient“)

(ďalej Audítor a Klient spolu aj ako „zmluvné strany“)

Článok II Predmet Realizačnej zmluvy

- 2.1. Predmetom tejto Realizačnej zmluvy je určenie obsahu a rozsahu Audítorských služieb, ktoré sa Audítor zaviazal poskytovať podľa **Rámcovej dohody o poskytovaní poradenských služieb v oblasti auditu** č. OVO2-2020/000354 6 zo dňa 14.07. 2020 (ďalej len „Dohoda“), lehoty ich poskytovania, odmena Audítora za ich poskytovanie a ďalšie podrobnosti ich poskytovania v súlade so Dohodou.
- 2.2. Pojmy použité v tejto Realizačnej zmluve majú rovnaký význam, ako pojmy v Dohode, ak nie je v tejto Realizačnej zmluve výslovne dohodnuté inak.

Článok III
Rozsah Audítorských služieb

- 3.1. Vecný rozsah Audítorských služieb a lehoty plnenia sú určené v Špecifikácii plnenia, ktorá tvorí prílohu č. 1 Rozsah a lehoty plnenia k tejto Realizačnej zmluve.

Článok IV
Odmena Audítora

- 4.1. Odmena Audítora je určená v prílohe č. 2 Odmena Audítora k tejto Realizačnej zmluve.

Článok V
Záverečné dojednania

- 5.1. Realizačná zmluva je vyhotovená v takom počte rovnopisov, aby 3 (tri) rovnopisy dostal Klient a 1 (jeden) rovnopis Audítora.
- 5.2. Zmluvné strany sa dohodli, že právne vzťahy, práva a povinnosti založené Realizačnou zmluvou sa riadia právnym poriadkom Slovenskej republiky, a to najmä Obchodným zákonníkom.
- 5.3. Realizačná zmluva nadobúda platnosť dňom jej podpisu všetkými Zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia podľa osobitného zákona.
- 5.4. Zmluvné strany vyhlasujú, že si Realizačnú zmluvu riadne prečítali, jej obsahu porozumeli a táto plne zodpovedá ich skutočnej vôli, ktorú prejavili slobodne, vážne, určite a zrozumiteľne, bez omylu, bez časového tlaku alebo za jednostranne nápadne nevýhodných podmienok, na znak čoho ju podpísali.
- 5.5. Neoddeliteľnou súčasťou tejto Realizačnej zmluvy, sú prílohy:
- Príloha č. 1: Rozsah a lehoty plnenia
- Príloha č. 2: Odmena Audítora
- Príloha č. 3: Menný zoznam expertov
- Príloha č. 4: Sprostredkovateľská zmluva
- Príloha č. 5: Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Klient:

Audítor:

Podpis: _____

Podpis: _____

Meno a priezvisko: Ing. Michal Tariška

Meno a priezvisko: Miroslav Novotný

Obchodné meno, funkcia: generálny riaditeľ
Sociálnej poisťovne

Obchodné meno, funkcia: predseda
predstavenstva stengl a.s.

V, dňa:

Podpis: _____

Meno a priezvisko: Ing. Andrej Petrovaj

Obchodné meno, funkcia: podpredseda
predstavenstva stengl a.s.

V, dňa:

Príloha č. 1 k Realizačnej zmluve č. VO1-2024/000328-004

Rozsah a lehoty plnenia

1. Predpokladaný maximálny rozsah predmetu plnenia

Položka	Predpokladaný maximálny rozsah osobohodín
Expert 2	50 688
Expert 4	3 840
Celkom	54 528

Skutočný rozsah expertných prác bude vzájomne odsúhlasený klientom a audítorom na základe akceptačného protokolu podpísaného zástupcami oboch zmluvných strán.

2. Lehoty dodania predmetu plnenia

a) Lehota:

Audítor je povinný dodať celý predmet zákazky **do 24 mesiacov** odo dňa účinnosti Realizačnej zmluvy. V prípade omeškania Klienta s poskytnutím dostatočnej súčinnosti pre dodanie predmetu plnenia Audítorom, Audítor nebude v omeškaní s dodaním predmetu plnenia. Doba účinnosti realizačnej zmluvy sa automaticky predĺži o dobu, počas ktorej bude Klient v omeškaní s poskytnutím súčinnosti Audítorovi.

b) Fakturačné obdobie:

Fakturačným obdobím je kalendárny mesiac. Výstupy Audítora budú odovzdávané a preberané priebežne s mesačnou frekvenciou. Fakturácia bude prebiehať po uplynutí posledného dňa kalendárneho mesiaca za predchádzajúci kalendárny mesiac na základe odovzdaných a prevzatých výstupov. Neoddeliteľnou prílohou faktúry je vzájomne odsúhlasený výkaz realizovaných prác. Splatnosť faktúry je najneskôr do tridsať (30) dní odo dňa jej doručenia do podateľne Klienta. Audítor sa zaväzuje vystavené faktúry zaslať listinne poštou a súčasne aj v textovo čitateľnom súbore vo formáte PDF elektronicky na e-mailovú adresu Klienta: faktury@socpoist.sk, a to bezodkladne po ich vystavení. Audítor vyhlasuje, že obsah faktúr poslaných poštou sa bude zhodovať s faktúrami poslanými v elektronickej podobe na e-mailovú adresu Klienta. Miestom doručenia faktúry v listinnej forme je Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava.

c) Akceptačné konanie výkazu realizovaných prác:

Audítor je povinný predložiť výkaz prác za predchádzajúci kalendárny mesiac najneskôr do 5 pracovných dní od skončenia predchádzajúceho mesiaca v členení a forme podľa pokynov Klienta. Klient je povinný výkaz skutočne vykonaných expertných prác schváliť alebo vrátiť na doplnenie do 5 pracovných dní od predloženia.

d) Miesto a termín plnenia predmetu zmluvy:

Miestom plnenia je Sociálna poisťovňa ústredie, ul. 29. augusta 8-10, 813 63 Bratislava.

Ďalšie súvisiace podmienky nevyhnutné k plneniu Realizačnej zmluvy:

e) Poskytovanie podkladov a vecného zadania pre Audítora:

Ak podklady a vecné zadanie pre Audítora pre jeho rozsiahlosť a povahu nie je možné v plnom rozsahu doručiť Audítorovi poštou, elektronickou poštou alebo telefonicky v zmysle článku V Dohody a tam kde je to technicky možné, Klient doručí podklady napríklad vo forme individuálneho prístupu do dátového úložiska alebo elektronického prístupu, osobitne zriadeného na účely poskytovania expertných služieb Audítora.

- f) Sprostredkovateľská zmluva podľa čl. 28 ods.3 Nariadenia európskeho parlamentu a rady (EÚ) 2016/679:

Na základe písomnej výzvy Klienta Audítorovi počas účinnosti Realizačnej zmluvy, Audítor súhlasí, že uzavrie s Klientom Sprostredkovateľskú zmluvu, ktorá je uvedená v Prílohe č. 4 tejto Realizačnej zmluvy.

- g) Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností:

Na základe písomnej výzvy Klienta Audítorovi počas účinnosti Realizačnej zmluvy, Audítor súhlasí, že v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a podľa § 8 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, uzavrie s Klientom Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, ktorá je uvedená Prílohe č. 5 tejto zmluvy.

Príloha č. 1 k Realizačnej zmluve č.: VO1-2024/000328-004

Podrobný opis predmetu plnenia

Návrh Jednotného systému dávkovej agendy

IDENTIFIKÁCIA PROJEKTU

Projekt návrhu Jednotného systému dávkovej agendy – JSDA

ÚVOD

Sociálna poisťovňa (ďalej ako „SP“) bola zriadená 1. novembra 1994 zákonom č. 274/1994 Z. z. o Sociálnej poisťovni ako verejnoprávna inštitúcia poverená výkonom nemocenského poistenia a dôchodkového zabezpečenia. Od 1. januára 2004 vykonáva sociálne poistenie na základe zákona č. 461/2003 Z. z. o sociálnom poistení v aktuálnom znení, t. j. nemocenské poistenie, dôchodkové poistenie - starobné a invalidné, ďalej úrazové poistenie, garančné poistenie a poistenie v nezamestnanosti. Od 1. januára 2005 Sociálna poisťovňa na základe zákona č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov vykonáva aj činnosti v rámci starobného dôchodkového sporení – predovšetkým vyberá príspevky, postupuje ich dôchodkovým správcovským spoločnostiam a registruje zmluvy o starobnom dôchodkovom sporení.

SP je verejnoprávna inštitúcia, ktorá v súlade s platnou legislatívou vykonáva agendy v úsekoch verejnej správy (ďalej aj ako "VS"): Sociálne poistenie a Starobné dôchodkové sporenie . V rámci uvedených úsekov VS bude projekt riešiť nasledujúce agendy:

- Výber poistného a príspevkov na starobné dôchodkové sporenie, správa a vymáhanie pohľadávok;
- Konanie o dávkach a výplata dlhodobých a krátkodobých dávok sociálneho poistenia: dôchodkového poistenie, nemocenského poistenia, úrazového poistenia, poistenia v nezamestnanosti a garančného poistenia;
- Vykonávanie kontrolnej činnosti, konzultačnej a poradenskej činnosti vo veciach sociálneho poistenia;
- Vykonávanie lekárskej posudkovej činnosti;
- Postupovanie príspevkov sporiteľov na starobné dôchodkové sporenie.

V rámci uvedených agend SP poskytuje služby sociálneho poistenia a dôchodkového sporení pre klientov SP tzn. občanov a podnikateľov.

VÝCHODISKOVÉ PODKLADY

Východiskové podklady, ktoré priamo súvisia s realizáciou projektu a ich obsah je relevantný k definícii projektu:

Zmluva o poskytnutí prostriedkov

Zmluva o poskytnutí prostriedkov mechanizmu na podporu obnovy a odolnosti č. CEZ MIRRI SR: 1593/2023; č. SP: 34406-1/2023-BA pre projekt **Budovanie životných situácií pre organizáciu Sociálna poisťovňa** podpísaná medzi Ministerstvom investícií, regionálneho rozvoja a informatizácie SR a Sociálnou poisťovňou.

ZÁMER A CIELE BUDÚCEHO RIEŠENIA

V rámci návrhu JSDA, ktorého hlavným cieľom je zavedenie elektronických služieb pre klientov, digitalizácia a optimalizácia procesov SP, bude SP inovovať svoje služby aby dosiahla nasledovné vlastnosti služieb:

- služby v kontexte životných situácií,
- pro-klientsky prístup ku klientom je zabezpečený pro-klientsky orientovanými procesmi, službami a dátami, proaktívne služby,
- užívateľsky prívetivé služby, prehľad o stave realizácie služby a služba „moje údaje“,
- nástroje pre spätnú väzbu od klientov, hodnotenie kvality služieb.

Riešenie splní **cieľ optimalizácie procesov** nasledovným spôsobom:

- **transformácia existujúcich procesov** viazaných na konanie o dlhodobých a krátkodobých dávkach na jeden proces s jasne definovanými rozhraniami na prierezové procesy sociálneho poistenia,
- prierezové procesy sociálneho poistenia (v súčasnosti ide o procesnú oblasť s najväčším výskytom duplicit, ktoré budú realizáciou projektu minimalizované).

Riešenie splní **cieľ digitalizácie procesov** nasledovným spôsobom:

- zavedenie elektronického dávkového spisu
- zavedenie bezpapierového spracovania podaní
- navrhnúť spôsob simultánnej práce existujúcich systémov a JSDA vrátane delby práce

Cieľ projektu zo zmluvy:

Cieľom je zminimalizovať administratívne úkony občana v procese využitia elektronických služieb Sociálnej poisťovne. Základným cieľom je zvýšenie dostupnosti a efektívny prístup k online službám, ktoré pokrývajú životné situácie Plánu obnovy a odolnosti (ďalej ako „POO“). Rozvojom informačných systémov Sociálnej poisťovne sa zníži administratívna záťaž vo forme manuálnej práce na strane užívateľov dotknutých informačných systémov, čím sa zrýchli proces vybavenia žiadostí pre klientov Sociálnej poisťovne.

Strategické ciele:

- spokojnosť občanov,
- používanosť elektronických služieb štátu,
- kvalita poskytovaných elektronických služieb štátu.

Dotknuté ukazovatele v súvislosti s cieľmi POO v danom projekte sú nasledovné:

- Net promoter score užívateľov e-služieb štátu,
- Customer effort score pre riešenie úradných záležitostí,
- Online komunikácia s úradmi a inštitúciami,
- ÚPVS ako zdroj informácií na vybavenie úradných záležitostí.

Predmetom návrhu JSDA sú nasledovné životné situácie:

1. Strata zamestnania
2. Odchod do dôchodku
3. Narodenie dieťaťa
4. Presťahovanie
5. Som chorý, mám chorého člena rodiny
6. Som odkázaný, mám odkázaného člena rodiny
7. Administratívny chod podniku
8. Úmrtie a dedičské konanie

LEGISLATÍVNY RÁMEC

Legislatívny rámec tvorený nižšie uvedenými právnymi dokumentmi musí byť zohľadnený pri výkone všetkých aktivít súvisiacich s realizáciou predmetu plnenia.

Základný zákonný rámec súvisiaci s predmetom plnenia a s výkonom kompetencií SP je nasledovný:

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/241 z 12. februára 2021, ktorým sa zriaďuje Mechanizmus na podporu obnovy a odolnosti
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/435 z 27. februára 2023, ktorým sa mení nariadenie (EÚ) 2021/241, pokiaľ ide o kapitolu REPowerEU v plánoch obnovy a odolnosti, a ktorým sa menia nariadenia (EÚ) č. 1303/2013, (EÚ) 2021/1060 a (EÚ) 2021/1755 a smernica 2003/87/ES
- Vykonávacie rozhodnutie Rady o schválení posúdenia plánu obnovy a odolnosti Slovenska č. 10156/21
- Zákon č. 368/2021 Z. z. o mechanizme na podporu obnovy a odolnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov;
- Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;

- Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Zákon č. 437/2004 Z. z. o náhrade za bolesť a o náhrade za sťaženie spoločenského uplatnenia a o zmene a doplnení zákona Národnej rady Slovenskej republiky č. 273/1994 Z. z. o zdravotnom poistení, financovaní zdravotného poistenia, o zriadení Všeobecnej zdravotnej poisťovne a o zriaďovaní rezortných, odvetvových, podnikových a občianskych zdravotných poisťovní v znení neskorších predpisov;
- Vyhláška ministerstiev zdravotníctva a spravodlivosti, Štátneho úradu sociálneho zabezpečenia a Ústrednej rady odborov č. 32/1965 Zb. o odškodňovaní bolesti a sťaženia spoločenského uplatnenia;
- Zákon č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci a o zmene niektorých zákonov v znení neskorších predpisov;
- Zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov;
- Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov;
- Zákon č. 592/2006 Z. z. o poskytovaní vianočného príspevku niektorým poberateľom dôchodku a o doplnení niektorých zákonov v znení neskorších predpisov;
- Zákon č. 296/2020 Z. z. o 13. dôchodku a o zmene a doplnení niektorých zákonov
- Zákon č. 112/2015 Z. z. o príspevku športovému reprezentantovi a o zmene a doplnení zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov v znení neskorších predpisov;
- Zákon č. 285/2009 Z. z. o poskytovaní príspevku účastníkom národného boja za oslobodenie a vdovám a vdovcom po týchto osobách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 274/2007 Z. z. o príplatku k dôchodku politickým väzňom v znení neskorších predpisov;
- Zákon č. 305/1999 Z. z. o zmiernení niektorých krívd osobám deportovaným do nacistických koncentračných táborov a zajateckých táborov v znení neskorších predpisov;
- Zákon č. 119/1990 Zb. o súdnej rehabilitácii v znení neskorších predpisov;
- Zákon č. 87/1991 Zb. o mimosúdnych rehabilitáciách v znení neskorších predpisov;
- Zákon Slovenskej národnej rady č. 319/1991 Zb. o zmiernení niektorých majetkových a iných krívd a o pôsobnosti orgánov štátnej správy Slovenskej republiky v oblasti mimosúdnych rehabilitácií v znení neskorších predpisov;
- Zákon Národnej rady Slovenskej republiky č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení ďalších zákonov v znení neskorších predpisov;
- Nariadenie vlády Slovenskej republiky č. 268/2006 Z. z. o rozsahu zrážok zo mzdy pri výkone rozhodnutia v znení neskorších predpisov;
- Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov;
- Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 274/2018 Z. z. o zrážkach z čistej pracovnej odmeny obvinených a odsúdených a určení zrážok na úhradu trov výkonu trestu odňatia slobody a výšky zvýšených trov výkonu väzby a zvýšených trov výkonu trestu odňatia slobody v znení vyhlášky č. 29/2019 Z. z.;
- Zákon č. 65/2001 Z. z. o správe a vymáhaní súdnych pohľadávok v znení neskorších predpisov;
- Zákon Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov;
- Zákon č. 564/1991 Zb. o obecnej polícii.
- Zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Pre definované oblasti platí nadnárodná legislatíva:

- Nariadenie (ES) Európskeho parlamentu a Rady 883/2004 z 29. apríla 2004 o koordinácii systémov sociálneho zabezpečenia v platnom znení;
- Nariadenie Európskeho parlamentu a Rady (ES) č. 987/2009 zo 16. septembra 2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia v platnom znení;
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1724 z 2. októbra 2018 o zriadení jednotnej digitálnej brány na poskytovanie prístupu k informáciám, postupom a asistenčným službám a službám riešenia problémov a o zmene nariadenia (EÚ) č. 1024/2012

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 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 Rady (EHS, Euratom, ESUO) č. 259/1968 z 29. februára 1968, ktorým sa ustanovuje Služobný poriadok a podmienky zamestnávania ostatných zamestnancov Európskych spoločenstiev a osobitné pravidlá, ktoré sa dočasne uplatňujú na úradníkov Komisie (Ú. v. ES L 56, 4.3.1968) v platnom znení, (pozn. na základe tohto nariadenia SP vykonáva prevod dôchodkových práv).

Predmet plnenia musí byť v súlade s platnými predpismi v oblasti elektronizácie verejnej správy, údajov a kybernetickej bezpečnosti:

- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov;
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov;
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 373/2018 Z. z.;
- Vyhláška ÚPVII č. 78/2020 o štandardoch pre informačné technológie verejnej správy;
- Zákon 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.

Iné východiskové dokumenty:

Dokumenty na regionálnej, národnej a európskej úrovni, ktoré priamo súvisia s realizáciou projektu, a ktoré prijala Rada vlády pre digitalizáciu verejnej správy a digitálny jednotný trh:

- Aktualizovaná metodika projektového riadenia projektov informatizácie verejnej správy, schválený dňa 10.11.2017,
- Detailný akčný plán informatizácie verejnej správy (2017-2020) , schválený dňa 10.11.2017,
- Koncepcia riadenia informatizácie verejnej správy, schválený dňa 10.11.2017,
- Referenčná architektúra Informačného systému verejnej správy v cloude, schválený dňa 10.11.2017,
- Strategická priorita Interakcia s verejnou správou, životné situácie a výber služby navigáciou, schválený dňa 10.11.2017,
- Strategická priorita Komunikačná infraštruktúra, schválený dňa 10.11.2017,
- Strategická priorita Otvorené údaje, schválený dňa 10.11.2017,
- Strategická priorita Rozvoj agendových informačných systémov a využívanie centrálnych spoločných blokov, schválený dňa 10.11.2017,
- Strategická priorita Manažment údajov schválený dňa 28.2.2017,
- Strategická priorita Integrácia a orchestrácia schválená 28.2.2017,
- Strategická priorita Multikanálový prístup schválený 28.2.2017,
- Operačný program integrovaná infraštruktúra schválený Európskou komisiou dňa 28.10.2014,
- Národná koncepcia informatizácie verejnej správy schválená vládou 28.9.2016, kde sa definuje vízia, strategické ciele a smery e-Governmentu v SR,
- Národný program reforiem schválený uznesením vlády č. 198 z 24.4.2013, kde jedným z opatrení je modernizácia verejnej správy,
- Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 - 2020)
- KOMPONENT 17: DIGITÁLNE SLOVENSKO Plánu obnovy a odolnosti vypracovaný a schválený na základe kritérií Nariadenia európskeho parlamentu a rady (EÚ) 2021/241 z 12. februára 2021, ktorým sa zriaďuje mechanizmus na podporu obnovy a odolnosti.

ZÁKLADNÉ CHARAKTERISTIKY

V rámci projektu návrhu JSDA bude navrhnutá transformácia existujúceho spôsobu výkonu agend sociálneho poistenia s použitím overených najnovších IT nástrojov. Výsledkom bude analýza a dizajn potrebný pre implementáciu a nasadenie:

- optimalizovaného procesu konania o dávkach,

- prierezových procesov¹ súvisiacich s konaním o dávkach sociálneho poistenia (lekárska posudková činnosť, vybavovanie odvolaní, vybavovanie sťažností, výplata dávky, ...).

Navrhovaný Informačný systém, ktorý bude vytvorený na základe výstupov projektu návrhu JSDA zabezpečí podporu výkonu transformovaných procesov tak, aby bolo možné dosiahnuť:

- vyššiu úroveň automatizácie procesov výkonu sociálneho poistenia,
- skrátenie konania o sociálnych dávkach,
- zvýšenie flexibility pri zavádzaní legislatívnych zmien,
- dlhodobu udržateľnú prevádzku informačných systémov Sociálnej poisťovne (ďalej aj „IS SP“),
- prepojenie existujúcej funkcionality s novo vyvíjanými komponentami všade tam kde tomu nebudú brániť autorské práva existujúcu funkcionality,
- zníženie nárokov na zastupiteľnosť pre výkon jednotlivých agend zamestnancami SP,
- zásadné zlepšenie používateľskej skúsenosti (user experience).

Naplnenie vyššie uvedených cieľov projektu návrhu JSDA umožní Sociálnej poisťovni prostredníctvom ďalších projektov adresovať ciele súvisiace so:

- zvýšením kvality, štandardu a dostupnosti koncových služieb sociálneho poistenia pre občanov,
- zvýšením kvality, štandardu a dostupnosti koncových služieb pre podnikateľov.

Súčasťou projektu je vytvorenie predpokladov pre zavedenie princípu „1x a dost“ a realizáciu konceptu digitálnej transformácie existujúcich procesov, tzn. zmenu súčasného, prevažne hierarchicky organizovaného poskytovania služieb na model agilných procesov, ktorý umožní:

- odstránenie duplicitných činností,
- plnú elektronizáciu procesov,
- zavedenie plnej automatizácie tých činností, kde je to efektívne,
- zrušenie činností, ktoré sú nahraditeľné dátovou alebo procesnou/servisnou integráciou a orchestráciou,
- monitoring, meranie a kontinuálne zlepšovanie procesov.

V projekte musia byť nasledovné aspekty:

- C.1 Systémová automatizácia procesov výkonu sociálneho poistenia;
- C.2 Skrátenie konania o sociálnych dávkach;
- C.3 Zníženie preťaženia zamestnancov a v rámci toho zníženie manuálnej a duplicitnej práce;
- C.4 Dlhodobu udržateľnú prevádzku IS SP;
- C.5 Plnenie požiadaviek Národnej koncepcie informatizácie verejnej správy SR (ďalej tiež ako „NKIVS“)
 - Zvýšenie kvality, štandardu a dostupnosti eGovernment služieb pre občanov,
 - Zvýšenie kvality, štandardu a dostupnosti eGovernment služieb pre podnikateľov,
 - Optimalizácia štruktúr so zameraním na interoperabilitu procesov,
 - Reforma a optimalizácia vybraných úsekov verejnej správy,
 - Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu.

V súvislosti so zavedením elektronických proaktívnych služieb pre klientov a optimalizáciou procesov SP je zámerom poskytovať služby klientom SP pohodlne, pružne, efektívne a používateľsky prívetivo v oblastiach:

- Zavedenie procesov starostlivosti o klienta znamená, že špecializovaní klientski pracovníci budú mať k dispozícii v reálnom čase kompletný profil klienta tak, aby mohli viesť s ním kvalifikovane komunikáciu bez toho, aby im klient musel vysvetľovať kto je a aký je jeho vzťah s SP.
- Zamestnanci budú môcť proaktívne kontaktovať klientov na základe očakávaných udalostí, ktoré im ponúka klientsky IS.
- Zavedenie multi-kanálového prostredia pre prístup klientov k službám SP umožní klientom vybrať si spôsob, ktorý im najviac vyhovuje pre riešenie ich životných situácií komunikáciu (pobočka, call centrum, portál SP, mobilné aplikácie, sociálne siete, API rozhrania).
- Implementácia eGovernment riešenia životných situácií s cieľom zabezpečenia jednoduchého prístupu klientov k poskytovaným službám, prehľadného vyhľadávania služieb, dostatočnej navigácie a plynulý prechod klienta celým cyklom životnej situácie, ako aj poskytovania informácií o stave spracovania podaní a služby.

¹ Pod prierezovými procesmi sa rozumejú také procesy, ktoré sa vyskytujú vo viacerých dávkových agendách SP (rozsah ŠÚ) a je ich možné riešiť jednotne.

Implementáciou navrhovaného projektu budú dosiahnuté prínosy predovšetkým z pohľadu šetrenia času občanov a zamestnávateľov, ale aj zamestnancov SP. Ďalším prínosom bude šetrenie nákladov na papier a tlač dokumentov, v niektorých prípadoch aj na doručovanie dokumentov.

ROZSAH, OBSAH, SPÔSOB DODANIA PREDMETU PLNENIA

POPIS BUDÚCEHO STAVU

V zmysle zákona o sociálnom poistení je SP poverená výkonom sociálneho poistenia, ktoré zahŕňa nemocenské poistenie, dôchodkové poistenie – starobné a invalidné, úrazové poistenie, garančné poistenie a poistenie v nezamestnanosti. V zmysle zákona č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov SP vykonáva aj činnosti v rámci starobného dôchodkového sporenia.

Zdôvodnením projektu je návrh, implementácia a nasadenie cieľového riešenia pre zavedenie procesov a elektronických služieb poskytovaných SP svojim klientom, redizajn služieb a optimalizácia procesov SP tak, aby sa v navrhovanom systéme JSDA dosiahlo:

1. vytvorenie klientskeho front-end prostredia systému:
 - a. vytvorenie koncových elektronických služieb SP, včítane integrácie so spoločnými komponentmi eGovernmentu,
 - b. eGovernment riešenie životných situácií s dôrazom na jednoduché a prehľadné vyhľadávanie služieb, navigáciu klientov pre plynulý prechod príslušnou životnou situáciou a dostupnými informáciami o stave spracovania podaní a služby,
 - c. nástroje pre spätnú väzbu od klientov, hodnotenie kvality služieb.
2. vytvorenia administratívnych a podporných služieb:
 - a. úložisko e-dokumentov a ich archivácia,
 - b. služby pre podporu orchestrácie procesov, ich monitoring a pro-klientske informovanie o stave riešenia klientskych požiadaviek,
 - c. elektronizácia interných papierových dokumentov a ich obeh,
 - d. optický archivačný systém.

BIZNIS ARCHITEKTÚRA BUDÚCEHO STAVU

Úspešnou realizáciou projektu a elektronizáciou koncových služieb v rozsahu vybraných životných situácií klientov v pôsobnosti SP sa prispeje k zvýšeniu kvality, štandardu a dostupnosti elektronických služieb SP pre jej klientov - občanov aj zamestnávateľov. Fungujúce KS na úrovni elektronizácie v zmysle platných ustanovení Vyhlášky č. 78/2020 o štandardoch pre ITVS, umožnia primárne FO podávať žiadosti a iné podania, ako aj získavať údaje, elektronickým spôsobom. Zavedením navrhovaných koncových služieb sa prispeje k zvýšenému komfortu a riešenia životných situácií v oblasti sociálneho poistenia a dôchodkového poistenia. V rámci navrhovaných koncových služieb sa počíta so službou podávania spätnej väzby užívateľa, čím bude možné následne koncové služby vyhodnocovať a následné zistenia adaptovať pri ich ďalšom rozvoji.

Navrhované služby prispejú k vyššej miere informovanosti a poskytovania údajov pre klientov, vrátane zobrazovania stavu konaní klienta voči SP, klientovi bude umožnené zobrazovanie stavu a priebehu konania v rámci dôchodkového poistenia, žiadosti o vydanie potvrdení, v rámci žiadosti o vrátenie poistného. Navrhované KS v projekte obsahujú aj služby, ktoré umožnia poskytovanie a zobrazovanie údajov klienta SP (občan) ako aj zobrazovanie stavu konaní klienta voči SP.

Poskytovanie služieb SP - základnou funkciou verejnej správy (vrátane SP) je poskytovať služby fyzickým a právnickým osobám (občanom, podnikateľom, cudzincom, organizáciám verejnej správy a európskej administratívy), v nadväznosti na príslušné životné situácie, v ktorých sa klienti SP nachádzajú resp. sa o nich informujú a to v rozsahu práv a povinností, ktoré im vyplývajú. Služby verejnej správy poskytujú viditeľnú hodnotu, napr. v podobe vydávania rozhodnutí alebo iných výstupov a umožňujú efektívne riešiť životné situácie, v ktorých sa občania alebo podnikatelia môžu nachádzať. V rámci navrhovaného riešenia sa do prostredia SP zavedú nástroje, ktoré prinesú efektívnejší a rozšírený prístup k informáciám a službám a nové riešenia, ktoré zoptimalizujú riešenie agendy SP.

PREDMET PLNENIA

Predmet zákazky tvoria odborné poradenské služby spočívajúce v spracovaní analýzy, na základe poskytnutia poradenských a konzultačných služieb, overení, kontrole, posúdení metodických materiálov a štúdií, odborných stanovísk,

ako aj prípadne zastupovanie Sociálnej poisťovne v pozícii experta na stretnutiach s tretími osobami v procese tvorby výstupných dokumentov pre hlavnú aktivitu „Analýza a dizajn“.

Príslušnými expertami budú vykonané najmä nasledovné aktivity v plnom alebo čiastkovom rozsahu za účelom vypracovania analýzy výsledkom, ktorej bude návrh **detailného zadania pre Implementáciu a Nasadenie cieľového riešenia pre JSDA**.

Rozsah činností v oblasti auditu systémov:

- poradenstvo v oblasti tvorby organizačných štruktúr a efektívnosti ich fungovania
- posúdenie vnútroorganizačných smerníc
- audit a testovanie riadiacich a kontrolných systémov
- poradenstvo v oblasti riadiacich a kontrolných systémov
- preverenie fungovania kontrolných mechanizmov
- posúdenie systému internej a externej komunikácie - komunikačný audit
- hodnotenie rizík, návrh opatrení na zmiernenie rizík
- audit riadenia krízových scenárov
- audit bezpečnosti IT

Uvedené činnosti budú zabezpečené expertmi typu č. 2 a č. 4 podľa Rámcovej Dohody.

Rozsah činností v oblasti auditu procesov a životných situácií:

- audit existujúceho procesného modelu z hľadiska organizačného, kompetenčného, legislatívneho a pokrytia prostriedkami IT/IKT a posúdenie efektívnosti nastavenia procesov v organizácii
- syntéza analytických výstupov
- revízia príslušnej procesnej dokumentácie
- poradenstvo pri zosúladovaní procesného modelu s jednotlivými internými systémami a kontrolnými mechanizmami
- posúdenie definovaných ukazovateľov výkonnosti pre implementované procesy a podprocesy nastavenie systému merania a vyhodnocovania vrátane nastavenia nových KPI
- poradenstvo v oblasti metodiky tvorby procesných modelov
- zhodnotenie systému metodík, analytických postupov a nástrojov v oblasti „LEAN“ managementu procesov s cieľom maximalizácie hodnoty pre občana, vrátane odporúčaní sady techník a návrhu nástrojov („best-practices“).

Uvedené činnosti budú zabezpečené expertmi typu č. 2 a č. 4 podľa RD.

Kvalitné výstupy analýzy je možné pripraviť len v spolupráci s vecne príslušnými zamestnancami Sociálnej poisťovni. Preto dodávateľovi bude poskytnutá súčinnosť zamestnancov a iných osôb ználych problematik, ktoré sa dotýkajú vecného rozsahu projektu.

Výsledkom hore uvedených aktivít bude vyhotovenie analýzy, ktorá poskytne detailné zadanie a kroky čiastkových nasadzovaní pre Implementáciu a Nasadenie cieľového riešenia pre JSDA.

SLUŽBY (koncové a aplikačné)

V cieľovom stave JSDA sa požaduje implementácia nasledovných služieb, ktoré budú v návrhu analyticky pokryté (nižšie zahŕňa príklad pre ŽS Odchod do dôchodku, ostatné služby budú definované analogicky s minimálnou odchýlkou na základe potreby pre ŽS):

- **Evidencia klientov** - Požaduje sa implementácia funkcií pre prijatie žiadostí o informácie, vrátane funkcií pre preverenie žiadostí a jej pridelenia na spracovania, prípadne odmietnutia. Požaduje sa implementácia funkcií pre evidenciu a správu klientov výhradne pomocou integrácie na údaje IS SP, vrátane ich správy a správy ich doplňujúcich údajov (kontakty, adresy, atď.).
- **Poskytovanie informácií o DP** - Požaduje sa implementácia funkcií pre vybavenie žiadostí o informácie, vrátane žiadostí o informáciách z nárokových podkladov. Súčasťou procesu vybavenia žiadosti o informácie sú činnosti ako vyhľadanie a sprístupnenie požadovaných informácií, vyhotovenie konceptu odpovede, vyhotovenie dokumentu, schválenie dokumentu, tlač a odoslanie dokumentu.
- **Žiadosť o dôchodok** - Požaduje sa implementácia funkcií pre spísanie žiadosti o dôchodok, jej následného prijatia, zaevidovania, vrátane vytvorenia spisu a pridelenia spisu na spracovanie. Prijatú žiadosť bude možné skontrolovať, prípadne vrátiť pobočke na prepracovanie.
- **Automatizácia vstupu údajov** - Požaduje sa podpora pre automatizovaný vstup dát zo žiadostí o dávku DP a automatizovaný vstup dát z nárokových podkladov obsahujúcich informácie nevyhnutné pre konanie.

- **Generovanie ELDP** - Požaduje sa implementácia funkcií pre generovanie ELDP z podkladov zo systému výberu poistného IS SP.
- **Spracovanie a evidencia ELDP** - Požaduje sa implementácia funkcií pre spracovanie a evidovanie ELDP-SZČO / DDPO, ELDP zamestnanca.
- **Spracovanie a evidencia špecifických podkladov** - Požaduje sa implementácia funkcií pre spracovanie a evidovanie špecifických podkladov, vrátane automatizovaných úkonov, pričom sa jedná o nasledovné podklady: vydanie výzvy/upovedomenia/žiadosti o súčinnosť, vydanie výzvy na dodatočné splnenie povinností s upozornením na možnosť uloženia pokuty, spracovanie podkladov k neprevzatým dávkam, spracovanie podkladov na výplatu bez doručeného VR, spracovanie podkladov na výplatu s doručeným VR (Výkonávanie zrážok), spracovanie podkladov pre bezhotovostnú výplatu dávok, evidencia avíza o platbe náhrady.
- **Spracovanie a evidencia dokumentov** - Požaduje sa implementácia funkcií pre spracovanie a evidovanie podkladových dokumentov, vrátane skenovania a uloženia dokumentu do úložiska, vytlačenie dokumentu, vyznačenie dátumov z doručky, spracovanie nedoručených/vrátených dokumentov, zaevidovanie prevzatia/neprevzatia oznámenia/výzvy, vytvorenie spisu/uloženie do spisu.
- **Rozhodovanie o dávke DP** - Požaduje sa implementácia funkcií nasledovných procesov rozhodovanie o dávke DP:
 - konanie o nároku na dávku DP a jej výplatu, vrátane prerušenia, zastavenia konania, predĺženia lehoty na konanie,
 - rozhodovanie o nároku a výpočet dávky DP, preddavkov a jej doplatkov,
 - individuálne dávky DP (dávky, ktoré je potrebné nahráť, posúdiť a vypočítať manuálne z dôvodu akýchkoľvek prekážok v automatizovanom spracovaní),
 - vydávanie rozhodnutí a iných výstupných dokumentov a ich archivácia pri zabezpečení maximálnej miery parametrizácie dokumentov.
- **Výpočet dávky DP** – Požaduje sa vytvorenie **nového základného výpočtového modulu pre dôchodkové poistenie**, prostredníctvom ktorého budú realizované výpočty pri konaniach o nároku na dôchodok a jeho sumu a konaniach o zmene v nároku na dôchodok, zmene jeho sumy a jeho výplaty, kde bude uplatňovaná legislatíva platná po 01.01.2004. Pre zabezpečenie funkcií JSDA v časti podporujúcej výkon dôchodkového poistenia v rozsahu výpočtu dávky podľa legislatívy platnej pred 01.01.2004, bude funkcionálna zabezpečená prostredníctvom rozhrania na súčasný (legacy) IS DP.
- **Výpočet dávky DP** – Požaduje sa implementácia generovania výstupných dokumentov (napr. rozhodnutí, korešpondencie s klientom, oznámenia o výplate, kontrolná zostava, ...); vrátane šablón pre tlačové zostavy s možnosťou parametrického výberu dát a zmeny textov.
- **Zmena a úprava dávky DP** – Požaduje sa implementácia funkcií nasledovných procesov pri úprave dávky DP:
 - konanie o zmene v nároku na dávku, zmene jej sumy a zmene jej výplaty
 - konanie o neprávom vyplatenej dávke
 - uplatnenie práva na vrátenie neoprávnene prevzatej sumy na dôchodku žalobou (bez dôvodného obohatenia)
 - Vybavenie opravného prostriedku
 - Vybavenie regresu
 - Identifikovanie a vygenerovanie preplatku na dávke a administratívneho preplatku
 - Realizácia zániku nároku na dávku a nároku na výplatu dávky
 - Úprava dávky – valorizácia
 - Vymáhanie a odpísanie pohľadávky
 - Uloženie pokuty (vytvorenie predpisu pokuty), overenie úhrady pokuty.
- **Zmena a úprava dávky DP** – Požaduje sa implementácia funkcií pre kontrolu nároku na dávku, vrátane pravidelných kontrol a inicializáciu následných konaní.
- **Vytvorenie podkladov pre výplatu dávok** – Požaduje sa implementácia funkcií pre vytvorenie podkladov pre výplatu dávok, vrátane spracovania, expedície (poštou, eschranky, modul CÚD) a evidencie podkladov (rozhodnutí) a opätovného vyplatenia dávky neprevzatej dávky.
- **Špecifické konania** – Požaduje sa implementácia špecifických konaní o príspevkoch alebo príplatkoch, ktorými sú:
 - Konanie o príspevku politickému väzňovi,
 - Konanie o príspevku účastníkovi odboja,
 - Vyplácanie príplatku za štátnu službu,
 - Poskytnutie vianočného príspevku.

- **Výplata dávky DP** - Požaduje sa implementácia funkcií pre zabezpečenie evidencie a výplaty dávok, vrátane evidencie preplatkov a ich vymáhanie a distribúcia dát do účtovníctva vedeného v SAP-FI. JSDA musí zabezpečiť:
 - realizácia výplaty dávky (poštovými poukazmi, prevodom na účet, zahraničie),
 - spracovanie vratiek a kreditných platieb,
 - automatizované prepojenie na účtovníctvo SP (denné účtovanie záväzkov a pohľadávok),
 - realizácia úhrady zrazenej / zúčtovanej sumy vrátane zahraničia,
 - vyhotovenie zoznamov a platobných príkazov.
- **Dávkové funkcie** - Požaduje sa implementácia špecifických dávkových funkcií ako napr. hromadné zvyšovanie dôchodkov, zvyšovanie starobných dôchodkov a predčasných starobných dôchodkov od 1. januára kalendárneho roka za obdobie dôchodkového poistenia získané po vzniku nároku na dôchodok, vianočný príspevok, rodičovský dôchodok, prepočet vyplácaných dávok pri zmene životného minima.
- **Kontrola údajov výplaty** - Požaduje sa implementácia funkcií pre kontrolovanie správnosti údajov na kontrolnej zostave verifikovaných prevodov, vrátane opravy chybných údajov.
- **Vykonávanie zrážok z dávok DP** - Požaduje sa implementácia funkcií pre vykonávanie zrážok, v nasledovnom rozsahu:
 - Spracovanie podania na vykonanie zrážok
 - Zabezpečenie podkladov na výpočet zrážky
 - Výpočet zrážky a zmeny sumy dôchodku/dávky
 - Realizácia zrážok
 - Kontrola vykonateľnosti rozhodnutia
 - Zabezpečenie mesačných úhrad zrážok
 - Spracovanie ukončenia vykonávania zrážok
 - Vystavenie oznámenia o vykonaní / nevykonaní zrážok.
- **Zúčtovanie dávok DP** - Požaduje sa implementácia funkcií zúčtovanie dávok, v nasledovnom rozsahu:
 - spracovanie podkladov na zúčtovanie
 - prijatie oznámenia o sume na zúčtovanie
 - vykonanie zúčtovania
 - zúčtovanie dávok sociálneho poistenia s dávkou v hmotnej núdzi, navzájom pri súbehu, s dávkou vyplatenou zahraničným nositeľom poistenia atď.

Minimálne požiadavky na návrh integrácie budúceho systému JSDA na IS SP a IS VS

Integrácia na MÚSP -	Požaduje sa implementácia prepojenia na IS MÚSP za účelom poskytovania údajov JSDA pre ostatné IS SP a IS VS a získavania údajov z IS SP a IS VS, ktoré súvisia s výkonom agend dôchodkového poistenia.
Integrácia na IS JVP -	Požaduje sa implementácia prepojenia s IS JVP za účelom preberania údajov o výbere poistného v jednotlivých fondoch SP predmetných pre agendy JSDA.
Integrácia na EKP -	Požaduje sa implementácia prepojenia s EKP za účelom preberania údajov viazaných na výkon agend dôchodkového poistenia.
Integrácia na IS FR -	Požaduje sa implementácia prepojenia na IS FR za účelom poskytovania údajov o finančných pohyboch, ktoré sú predmetom agend JSDA.
Integrácia na systém registratúry -	Požaduje sa implementácia prepojenia na systém registratúry za účelom poskytovania a získavania údajov o spisoch k jednotlivým konaniam a prístupu na ÚPVS (eformuláre a pod.).

Integrácia na súčasný IS DP -	Požaduje sa v rámci hlavnej aktivity Testovanie zabezpečiť porovnanie výpočtu sumy dôchodku v pôvodnom IS s výpočtom v novom IS JSDA a vyhodnocovať prípadné nezrovnalosti minimálne nasledujúcim spôsobom: - odborný zamestnanec vykoná spracovanie v JSDA, - vstupné údaje pre účely spracovania v IS DP prenesú z JSDA automatizovane(napr. webovou službou) v rozsahu potrebnom pre spracovanie v IS DP, - následne odborný pracovník vykoná spracovanie v IS DP (IBM), - výsledok spracovania v IS DP sa automatizovaným spôsobom vráti do IS JSDA na porovnanie. Požaduje sa sprístupniť funkcionality „porovnanie výpočtu sumy dôchodku“ popísanú vyššie aj pre produkčné prostredie tak, aby odborný útvar mal možnosť realizovať porovnávanie po dobu, ktorú si Sociálna poisťovňa stanoví.
Integrácia na súčasné ostatné dávkové systémy -	Pre zabezpečenie funkcií JSDA bude potrebné integrovať na existujúce dávkové systémy.
Integrácia na Optický archivačný systém DP -	Požaduje sa implementácia na prepojenie s IS OAS pre zabezpečenie prevodu písomných podkladov do elektronickej formy (skenovaný image).
Integrácia na IS VS -	Integrácia na všetky IS VS a NZIS (eZdravie), ktorým SP poskytuje informácie alebo od ktorých SP čerpá informácie v súčasnosti na základe zmluvy alebo zákona.
Integrácia na NASP	Integrácia na Národnú aplikáciu SP, prostredníctvom ktorej je zabezpečovaná elektronická komunikácia s inými inštitúciami sociálneho zabezpečenia krajín EÚ, EHP, Švajčiarskej konfederácie a Spojeného kráľovstva Veľkej Británie a Severného Írska.

POŽIADAVKY NA VÝSTUPY

Uchádzač dodá grafický návrh Biznis a IT architektúry riešenia a jej textový popis, ktorá bude rozšírením popisu podľa časti Popis budúceho stavu týchto súťažných podkladov a ktorá musí obsahovať biznis, aplikačný, technický a implementačný návrh v súlade s požiadavkami v týchto podkladoch a v súlade s už existujúcou architektúrou. Tento model bude východiskom pre dodávaný produkt pri neskoršej realizácii projektu.

Uchádzač dodá procesné diagramy obsahujúce návrh optimalizovaných procesov spracovania dôchodkovej agendy. Ďalej dodá alternatívne návrhy technologického riešenia JSDA (štandardné programy, v prípade osobitného vývoja na mieru, návrhy na vývojové prostredie, použitý softvér...)

Uchádzač pri návrhu riešenia zohľadní rôzne možnosti spôsobu budúceho dodania softvérového riešenia, ako napr. BPMS (Business Process Management System), BRMS (Business Rules Management System), BAMS (Business Automation Management System), RPA (Robotic Process Automation)

Výstup projektu návrhu JSDA bude obsahovať:

- Návrh zmien personálneho a organizačného zabezpečenia výkonu prostredníctvom JSDA.
- Návrh zavedenia elektronického dávkového spisu v rámci bezpapierového spracovania podaní.
- Návrh spôsobu simultánnej práce existujúcich systémov a JSDA vrátane delby práce.

Uchádzač vo výstupných projektoch navrhne Plán projektu v členení projektových etáp, míľnikov a súvisiacich produktov tak aby bola zachovaná úplnosť predmetu projektu (tj. Biznis architektúra budúceho stavu).

Detailná špecifikácia ponúknutá vo výstupoch uchádzača má zabezpečiť aby výstupné produkty projektu boli realizované v súlade s popisom požadovaného budúceho stavu.

Dodávateľ vytvorí požadované výstupy v zmysle požiadaviek objednávateľa a v súlade s východiskovými podkladmi ako aj legislatívnym rámcom. Dodávateľ vytvorí požadované výstupy a odovzdá ich v editovateľnom formáte v elektronickej forme.

ROZSAH PREDMETU PLNENIA

Realizáciou daného projektu budú naplnené nasledovné hlavné aktivity projektu:

411Z27200005 - Analýza a dizajn

416Z27200001 - Analýza a dizajn

Predpokladaný počet dní vychádza z vyššie uvedených procesov a aktivít. Celková prácnosť je predpokladaná na 6 816 osobodní (jeden osobodeň sa rovná 8 osobohodinám). Požadovaní sú experti č. 2 a č. 4.

Predpokladaný maximálny rozsah osobohodín, osobodní

Položka	Predpokladaný maximálny rozsah osobohodín	Predpokladaný maximálny rozsah osobodní
Expert 2	50 688	6 336
Expert 4	3 840	480
Celkom	54 528	6 816

FINANCOVANIE

Predmet plnenia bude refundovaný zo zmluvy o poskytnutí prostriedkov mechanizmu na podporu obnovy a odolnosti č. CEZ MIRRI SR: 1593/2023; č. SP: 34406-1/2023-BA pre projekt Budovanie životných situácií pre organizáciu Sociálna poisťovňa.

PRÍLOHY

Príloha č1 – Popis súčasného stavu DP:



JSDA_1.3 - Príloha
č.1.docx

Odmena Audítora

Štruktúrovaný rozpočet ceny:

P. č.	Položka	Predpokladaný rozsah (osobo/hodín) poskytovaných služieb	Odmena za osobo/hodinu poskytovaných služieb v EUR bez DPH	Sadzba DPH v %,	Výška DPH za v EUR	Odmena za osobo/hodinu poskytovaných služieb v EUR bez DPH	Celková odmena za predpokladaný počet osobo/hodín poskytovaných služieb v EUR bez DPH	Celková odmena za predpokladaný počet osobo/hodín poskytovaných služieb v EUR s DPH
1.	Odmena za poskytovanie služieb – Expertom č. 2	50 688	59,00	20%	11,80	70,80	2 990 592,00	3 588 710,40
2.	Odmena za poskytovanie služieb - Expertom č. 4	3 840	59,00	20%	11,80	70,80	226 560,00	271 872,00
Celkom		54 528					3 217 152,00	3 860 582,40

Celková navrhovaná cena za celý predmet plnenia vyjadrená v EUR bez DPH ako aj všetky ceny uvedené v štruktúrovanom rozpočte ceny musia zahŕňať všetky náklady spojené s poskytovaním služieb uvedených v Prílohe č. 1 Opis predmetu plnenia Všetky ceny musia byť zaokrúhlené na dve (2) desatinné miesta.

Menný zoznam expertov

p.č.	Meno a Priezvisko Experta	Typ experta (Expert č.2, Expert č. 4)	Vzťah k poskytovateľovi služby
1.	Ing. Jozef Kordoš	Expert č. 2	zamestnanec
2.	Ing. Ján Drahoš	Expert č. 4	zamestnanec

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:	stengl a.s.
Sídlo:	Sumbalova 1/A, 841 04 Bratislava
Štatutárny orgán:	Miroslav Novotný - predseda predstavenstva Ing. Andrej Petrovaj - podpredseda predstavenstva
Zápis v registri:	Obchodný register Okresného súdu Bratislava III., oddiel Sa, vložka č. 4171/B
IČO:	35873426
DIČ:	2021772720
Bankové spojenie:	XXXXX
IBAN:	XXXXX

(ďalej len „Sprostredkovateľ“)

(spolu ďalej ako „Zmluvné strany“)

Preambula

Zmluvné strany spolu uzatvárajú „Realizačnú zmluvu č VO1-2024/000328-004 podľa čl. III Rámcovej dohody o poskytovaní poradenských služieb v oblasti auditu č. OVO2-2020/000354 6 zo dňa 14.07.2020, predmetom ktorej je predovšetkým poskytovanie expertných audítorských služieb v súvislosti s projektom “EZK” Sprostredkovateľom (ďalej len „zmluva „Realizačná zmluva“). Sprostredkovateľ vystupuje v tejto zmluve ako poskytovateľ týchto služieb, pričom nie je vylúčené, že v rámci plnenia predmetu zmluvy sa dostane priamo k spracovaniu osobných údajov zamestnancov prevádzkovateľa, 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 – identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú

- a) fyzické osoby, ktorých údaje sa spracúvajú na základe zákona č. 461/2003 Z. z. o sociálnom poistení a 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,

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 poskytovaním 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. Prevádzkovateľ touto Zmluvou poveruje Sprostredkovateľa spracovaním osobných údajov Dotknutých osôb v mene Prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre účely plnenia Realizačnej zmluvy.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou Realizačnej zmluvy po splnení povinností uvedených v tejto zmluve a výlučne na účel vykonávania technickej podpory, údržby a servisnej podpory počas trvania záručnej doby.
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 svojich klientov 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 Realizačnej zmluve, prípadne iné písomne zdokumentované pokyny.
5. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu Realizačnej zmluvy je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétnu zákonnú povinnosť ustanovuje Realizačná zmluva, osobitne a § 78 ods. 3 ZOOU.

Čl. III

Zoznam osobných údajov a okruh dotknutých osôb

1. Zoznam osobných údajov dotknutých osôb, ktoré môžu byť v prípade potreby realizácie predmetu Realizačnej zmluvy predmetom spracúvania:
 - a) osobné údaje fyzických osôb, spracovávané na základe zákona 431/2003 Z. z. o sociálnom poistení v znení neskorších predpisov a na základe Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia a Nariadenia (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia - a to vo vzťahu ku dátam, ktoré sa nachádzajú v IS DP a ktorý bude predmetom migrácie podľa bodu 7.17 a 7.19 článku 3 Realizačnej zmluvy č.: VO1-2024/000328-004,
2. Spracúvané osobné údaje v rozsahu bodu 1 tohto článku sú typu:

Bežné osobné údaje

Osobitné kategórie osobných údajov

Čl. IV

Spôsob výkonu Zmluvy a oprávnenia Prevádzkovateľa

1. Sprostredkovateľ môže vykonať spracúvanie osobných údajov prostredníctvom informačného systému IS DP, ktorý funguje na hardvérovom vybavení, ktorého náhrada je predmetom plnenia v zmysle Realizačnej zmluvy, č.:-/2023-BA.
2. Osobné údaje o dotknutých osobách sa získavajú 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.
3. Na spracúvanie osobných údajov sprostredkovateľom sa v zmysle § 34 ods. 1 ZOOU nevyžaduje súhlas dotknutej osoby.
4. 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) uchovávanie,
 - g) preskupovanie alebo kombinovanie,
 - h) vymazanie alebo likvidácia.
5. Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb po dobu trvania účelu spracúvania, resp. po dobu platnosti a účinnosti Realizačnej zmluvy a po dobu platnosti a účinnosti tejto zmluvy.

Čl. V

Vyhlasenie 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.

ČI. 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 spracovávaní 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.

ČI. 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 Realizačnej zmluvy a len v rozsahu nevyhnutnom na ich 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 Realizačnej zmluvy nezverejňovať, neposkytovať a neprístupňovať tretím stranám,
 - f) zachovávať mlčanlivosť a zabezpečiť diskretnosť pri akomkoľvek spracúvaní osobných údajov,
 - g) ak Realizačná 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 zmluvy, bezodkladne po tom, čo pominie dôvod na ich spracúvanie podľa zmluvy, zmazať zo všetkých elektronických, hmotných alebo iných nosičov informácií (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 zaviazat' 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) nepoužívať 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, vytváraní, kopírovaní, 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 prístupnení 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. vyodením 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 dní 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 povinností subdodávateľom. Sprostredkovateľ sa nemôže zbaviť zodpovednosti za porušenie povinností 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 nedodrzaním 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 zmluvy 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:
Meno, priezvisko: Róbert Janáček
Email: robert.janacek@stengl.sk

Čl. X

Trvanie a ukončenie Zmluvy

1. Táto Zmluva sa uzatvára po dobu trvania spolupráce Prevádzkovateľa a Sprostredkovateľa v zmysle Realizačnej zmluvy č. VO1-2024/000328-004.

Čl. XI

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 oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Zmluvné strany sa dohodli, že táto Zmluva je uzatváraná v písomnej forme a písomné budú aj zmeny Zmluvy alebo pokyny Prevádzkovateľa Sprostredkovateľovi. Na potreby pokynov na plnenie sa za písomnú formu považuje aj e-mail, ak bude pri tom zachovaná dôvernosť odovzdávaných informácií.
4. Počas platnosti Realizačnej zmluvy č. VO1-2024/000328-004 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 uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave, dňa

V Bratislave, dňa

Za Prevádzkovateľa:

Za Sprostredkovateľa:

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

Miroslav Novotný
predseda predstavenstva
stengl a.s.

Ing. Andrej Petrovaj
podpredseda predstavenstva
stengl a.s.

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:

stengl a.s.

Sídlo:

Sumbalova 1/A, 841 04 Bratislava

Štatutárny orgán:

Miroslav Novotný - predseda predstavenstva

Ing. Andrej Petrovaj - podpredseda predstavenstva

Zápis v registri:

Obchodný register Okresného súdu Bratislava III., oddiel Sa, vložka č. 4171/B

IČO:

35873426

DIČ:

2021772720

Bankové spojenie:

XXXXX

IBAN:

XXXXX

(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 Realizačnú zmluvu č VO1-2024/000328-004.ev.č v SP č. 51/2023, k Rámцovej dohode o poskytovaní poradenských služieb v oblasti auditu č. OVO2-2020/000354 6 zo dňa 14.07.2020, (ďalej len „zmluva na výkon činností“), predmetom ktorej je poskytovanie expertných auditorských služieb v súvislosti s projektom EZK.

3. Zmluvné strany uzatvárajú za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a podľa § 8 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška“) túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „zmluva“).

Čl. III Predmet zmluvy

1. Predmetom tejto zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť pri prevádzke sietí a informačných systémov prevádzkovateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom (ďalej len „kybernetický incident“), ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania sietí a informačných systémov prevádzkovateľa, s prevádzkou ktorých priamo súvisí výkon činností dodávateľa na základe zmluvy na výkon činností.
2. Výkon činností, ktoré priamo súvisia s realizáciou zmluvy na výkon činností.

Čl. IV Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné politiky prevádzkovateľa, ktoré tvoria prílohu č. 1 k tejto zmluve. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami prevádzkovateľa.
2. Dodávateľ súhlasí s tým, že bezpečnostné politiky prevádzkovateľa sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov prevádzkovateľa, aktuálnej legislatíve a aktuálnym hrozbám týkajúcim sa prevádzky sietí a informačných systémov prevádzkovateľa.
3. Dodávateľ je povinný prijímať a dodržiavať bezpečnostné opatrenia, ktoré sú súčasťou bezpečnostnej politiky prevádzkovateľa na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a bezpečnostných politikách prevádzkovateľa. Dodávateľ vyhlasuje, že s bezpečnostnými opatreniami súhlasí.
4. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve a v zákone o kybernetickej bezpečnosti.
5. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe zmluvy na výkon činností alebo tejto zmluvy, alebo ktoré mu boli poskytnuté zo strany prevádzkovateľa s tým, že všetci dotknutí zamestnanci dodávateľa jeho subdodávateľa a/alebo iné tretie osoby, prostredníctvom ktorých dodávateľ poskytuje služby podľa zmluvy na výkon činností (ďalej len „tretia osoba“) sú povinní podpísať vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.
6. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá je aktuálna a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi.
7. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto zmluvy minimálne v oblastiach podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, § 10, § 12, § 14 a § 15 vyhlášky a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa.
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 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 podieľať na plnení zmluvy na výkon činností a tejto zmluvy alebo budú mať prístup k informáciám prevádzkovateľa,
- c. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
- d. sledovať hrozby týkajúce sa dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
- e. predchádzať hrozbe vzniku kybernetických incidentov,
- f. v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
- g. prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
- h. zasielať prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak, a
- i. spolupracovať s prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa.

Čl. VII

Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident prevádzkovateľovi, ktorý by mohol mať vplyv na bezpečnosť dát prevádzkovateľa spôsobom určeným prevádzkovateľom, ktorý je uvedený v bezpečnostnej politike, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky,

dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

2. Dodávateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident.
3. Pri riešení kybernetických incidentov je dodávateľ povinný na žiadosť prevádzkovateľa spolupracovať s prevádzkovateľom, Národným bezpečnostným úradom a Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického incidentu.
4. Dodávateľ je povinný oznámiť prevádzkovateľovi skutočnosť, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ je povinný v čase kybernetického incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho prevádzkovateľovi.
6. Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.
7. Po vyriešení kybernetického incidentu je dodávateľ na výzvu prevádzkovateľa v určenej lehote povinný predložiť prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „ochranné opatrenie“) na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom na návrhu nového ochranného opatrenia.
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 týkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa týka 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, subdodávateľa a ich zamestnanci, ako aj prípadná tretia osoba a to aj po zániku ich pracovnoprávného 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, záväzkov 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.
9. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

Čl. X Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenie kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí tak, aby nebola narušená ich dostupnosť, dôverynosť, autentickosť a integrita.
3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania kybernetických incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa mu predložiť uvedenú dokumentáciu.
4. Dodávateľ je povinný plniť povinnosti podľa tejto zmluvy odo dňa jej účinnosti.
5. V prípade, ak dodávateľ plní prevádzkovú zmluvu prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s poskytovaním elektronických komunikačných služieb alebo sietí v súvislosti s prevádzkou sietí a informačných systémov prevádzkovateľa, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ mohol vykonať audit v súlade s touto zmluvou aj u týchto subdodávateľov.
6. Všetky informácie, ktoré majú vplyv na plnenie práv a povinností uvedených v tejto zmluve sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na adresy uvedené v záhlaví tejto zmluvy, a zároveň elektronicky prostredníctvom UPVS.
7. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie jeho povinností vyplývajúcich z tejto zmluvy ohrozuje plnenie účelu tejto zmluvy, čím ohrozuje kybernetickú bezpečnosť prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, dodávateľ zodpovedá za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto zmluvy, zákona o kybernetickej bezpečnosti alebo vyhlášky a za dôsledky a škodu vzniknutú v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinností podľa tejto zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu, v celom rozsahu. Prevádzkovateľ má nárok na preukázanú náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa.
8. Po ukončení tejto zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak

osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.

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: Róbert Janáček
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: bis@socpoist.sk
5. Kontakt na zástupcu sprostredkovateľa na úseku kybernetickej bezpečnosti je: XXXXXX@stengl.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 Realizačnej zmluvy definovanej v článku II - Zmluva č. VO1-2024/0003328/004.
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 príslušný súd SR.
7. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto zmluve.
8. Ak ktorékoľvek ustanovenie tejto zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.
9. Neoddeliteľnou súčasťou tejto zmluvy je Príloha č. 1 – Bezpečnostné politiky.
10. Táto zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.

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

V Bratislave, dňa

V Bratislave, dňa

Za prevádzkovateľa:

Za dodávateľa:

Ing. Michal Tariška
generálny riaditeľ
Sociálnej poisťovne

Miroslav Novotný
predseda predstavenstva
stengl a.s.

Ing. Andrej Petrovaj
podpredseda predstavenstva
stengl a.s.

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 poučení a zmluvne zaviazaní 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 centrálnemu dispečingu a monitorovania služieb IS SP. V žiadosti špecifikuje rozsah prístupových oprávnení. Po schválení žiadosti riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa a po doručení záznamu o vykonaní kontroly fyzickej bezpečnosti na mieste výkonu práce, zrealizuje požiadavku príslušný administrátor.

2.3 Klasifikácia informácií

- (1) Pre potrebu ochrany informácií platí ich nasledovná klasifikačná schéma
 - a) citlivé,
 - b) interné,
 - c) verejné.
- (2) Citlivé - sú chránené informácie, a to
 - a) osobné údaje poistencov,
 - b) osobné údaje zamestnancov,
 - c) osobné údaje tretích strán,
 - d) mzdové náležitosti zamestnancov,
 - e) vymeriavacie základy poistencov,

- f) informácie dôležité pre ochranu osobných údajov v rozsahu: analýza rizík, posúdenie vplyvu na ochranu údajov, bezpečnostný incident, bezpečnostný monitoring, bezpečnostný audit,
- g) údaje zhromaždené v IS prevádzkovateľa (ďalej len „IS SP“).
- (3) Interné - sú chránené informácie, kam patria všetky informácie, ktoré nie sú klasifikované ako citlivé alebo verejné, a ktoré
 - a) vznikajú v súvislosti s plnením pracovných činností zamestnancov a nie sú určené pre zverejnenie,
 - b) boli poskytnuté externým subjektom a nie sú určené pre zverejnenie.
- (4) Verejné - nie sú chránené informácie. Patria sem informácie už zverejnené alebo určené na zverejnenie v zmysle platných právnych predpisov a vnútorných predpisov.

2.4 Zaobchádzanie s aktívami

K citlivým informáciám je obmedzený prístup. Prístup k nim majú len oprávnené osoby, ktoré citlivé údaje spracúvajú, alebo len úzky okruh určených osôb prostredníctvom, ktorých dodávateľ plní predmet zmluvy, schválených riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa.

2.5 Zmluvy o dôvernosti alebo utajení

Dohody o zachovaní dôvernosti sú súčasťou zmlúv prevádzkovateľa s dodávateľom. Každá zmluva je pred podpisom odkontrolovaná odborom bezpečnosti informačných systémov na bezpečnostný súlad. Ak sú súčasťou zmluvy osobné údaje, k špecifikácii opatrení na ochranu osobných údajov v oblasti technickej a organizačnej zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá vykonáva dohľad nad ochranou osobných údajov u prevádzkovateľa v zmysle GDPR a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zodpovedná osoba“).

2.6 Ochrana testovacích údajov

Ak je na účely testovania dodávateľom nevyhnutné použiť prevádzkové údaje, môže byť použitá iba ich pseudonymizovaná kópia na základe súhlasu riaditeľa odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa. Kópia prevádzkových údajov musí byť bezpečne vymazaná ihneď po skončení testovania. Dozor 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 informatiky. Tieto činnosti musia byť zdokumentované.

3.1.2 Ošetrovanie 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 preskúvanie 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 dohodnuté. Cieľom je overenie, že opatrenia na zaistenie informačnej bezpečnosti sú dodržiavané, že sú dostatočné a že vzniknuté bezpečnostné incidenty sú riešené adekvátnym spôsobom.
- (2) V prípade osobných údajov spracúvaných dodávateľom, jeho subdodávateľom alebo treťou osobou túto kontrolu vykonáva aj zodpovedná osoba prevádzkovateľa.

3.1.4 Riadenie zmien v službách dodávateľa

Zmeny v službách poskytovaných dodávateľom sú závislé od systémov a procesov a sú súčasťou hodnotenia rizík.

3.1.5 Zodpovednosť, postupy a informovanie o udalostiach informačnej bezpečnosti

- (1) Udalosť, ktorá je považovaná za podozrenie z bezpečnostného incidentu, môže byť spôsobená objektívnymi príčinami (napr. technickou poruchou, priemyselnou haváriou), konaním fyzických osôb (napr. nedbalosť, krádež, prepad, teroristický čin) alebo živelnou pohromou (napr. zemetrasenie, povodeň).
- (2) Každé podozrenie z bezpečnostného incidentu musí byť nahlásené a posúdené.
- (3) Každý zamestnanec dodávateľa, jeho subdodávateľa alebo tretia osoba, ktorý má podozrenie, že odhalil slabé miesto, alebo zistil podozrenie z bezpečnostného incidentu, je povinný to bezodkladne oznámiť. Oznámenie vykoná nasledovne:
 - a) e-mailom odboru bezpečnosti informačných systémov prevádzkovateľa na adresu BIS@socpoist.sk a,
 - b) e-mailom oddeleniu centrálného dispečingu a monitorovania služieb IS SP na adresu dispecing@socpoist.sk a v kópii tomu zamestnancovi prevádzkovateľa, ktorému oznámil podozrenie ústne alebo telefonicky.

3.1.6 Informovanie o slabínach informačnej bezpečnosti

Každý zamestnanec prevádzkovateľa môže informovať o odhalení slabého miesta osobne, telefonicky, emailom alebo interným listom. Informáciu môže odovzdať ľubovoľnému zamestnancovi odboru bezpečnosti, alebo emailom zaslať oddeleniu centrálného dispečingu a monitorovania služieb IS SP na adresu dispecing@socpoist.sk.

3.1.6.1 Hlavné kategórie bezpečnostných incidentov

- (1) V oblasti ochrany zdravia zamestnancov a klientov
 - a) registrovaný pracovný úraz, ktorým bola spôsobená pracovná neschopnosť zamestnanca trvajúca viac ako tri dni alebo smrť zamestnanca, ku ktorej došlo následkom pracovného úrazu,

- b) technický stav majetku a zariadení (napr. výťah, varič, nevykonávané dezinfekcie klimatizácií, nevykonávané tepovanie kobercov aspoň raz za dva roky a pod.) ohrozujúci zdravie zamestnancov a klientov,
- c) technický stav elektrických, plynových a iných rozvodov ohrozujúci zdravie zamestnancov a klientov,
- d) konanie tretích osôb v priestoroch prevádzkovateľa ohrozujúce zdravie zamestnancov a klientov.

(2) V oblasti majetku prevádzkovateľa

- a) poškodenie majetku (napr. havária vodovodného potrubia spojená so zatopením prostriedkov informačnej komunikačnej infraštruktúry prevádzkovateľa, prašnosť a pod.),
- b) odcudzenie majetku, napr. notebook, osobný počítač a pod.,
- 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 dôvernosti, 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 (cudzía 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 dodávateľa, resp. subdodávateľa a/alebo tretia osoba pri nástupe na výkon zmluvných činností na základe zmluvy na výkon činností, pretože z charakteru činností prevádzkovateľa je zrejmé, že každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba by mohli aj náhodne prísť do styku s osobnými údajmi. Za zabezpečenie poučenia zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby je zodpovedný odbor bezpečnosti informačných systémov prevádzkovateľa a to vo vzťahu ku všetkým zamestnancom dodávateľa, prípadne zamestnancom subdodávateľa a/alebo tretej osobe uvedených v Zozname osôb podľa čl. IV ods. 8 zmluvy, ktoré boli riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky schválené ako osoby, prostredníctvom ktorých dodávateľ plní predmet zmluvy na výkon činností. Absolvovaním tohto vstupného poučenia sa zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba nestáva oprávnenou osobou na spracúvanie osobných údajov. Dodávateľ zabezpečí, aby každý zamestnanec dodávateľa, jeho subdodávateľa a/alebo tretia osoba, ktorý majú plniť povinnosti dodávateľa, podpísal pred začatím prác u prevádzkovateľa vyhlásenie o mlčanlivosti.

(2) Za nahlásenie a zabezpečenie účasti zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností je zodpovedný dodávateľ. Nahlásenie vykoná kontaktná osoba dodávateľa u príslušného zmluvného kontaktu prevádzkovateľa.

Kyberbezpečnostný štandard

pre projekty a IT v Sociálnej poisťovni

Obsah

Úvod	38
Cieľ dokumentu	39
Obmedzenia	39
I. Štandardy implementácie	40
II. Konfigurácia webového servera.....	43
III. Interná infraštruktúra a vývojové prostredie.....	52
IV. Štandardy prepojenia	52
V. Prenos elektronickej pošty	54
VI. Štandardy prístupu k elektronickým službám	55
VII. Štandardy webovej služby.....	56
VIII. Štandardy integrácie dát.....	56
IX. Formáty kompresie súborov.....	57
X. Dátové štandardy.....	57
XI. Šifrovanie	58
XII. Šifrovacie kľúče a protokoly.....	59
XIII. Firewall	59
XIV. Zabezpečenie iných služieb.....	60
XV. Požiadavky z pohľadu BIS vo vzťahoch s tretími stranami	60
Dodatky	61
Vysvetlenie skratiek	61
Zdroje a Legislatívne východiská	62
Klasifikačné stupne informačných aktív	64

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 zložitý 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 materiáloch, 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 verzii 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).

1 Štandardy implementácie

1.1 Bezpečnosť životného cyklu

Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôbiť tomu návrh aj implementáciu samotného riešenia počas jednotlivých fáz.

1.2 Návrh riešenia

- 1) Navrhnuté riešenie musí mať modulárnu štruktúru, pričom
 - a) pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege a všetky entity (t.j. používatelia aj systémy) musia mať prístup iba k údajom / aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú,
 - b) architektúra riešenia by mala byť trojvrstvová – mala by pozostávať z prezentačných serverov, aplikačných serverov a databázových serverov,
 - c) odporúčané je použitie overených návrhových vzorov, napr. MVC, resp. MVP.
- 2) Musia byť identifikované všetky súčasti (interné aj externé), od ktorých závisí riešenie. Pre jednotlivé súčasti musia byť identifikované zraniteľnosti, ktoré sa v nich môžu vyskytnúť a vyhodnotiť riziká zneužitia týchto zraniteľností na základe:
 - a) prístupového vektoru útočníka (lokálny prístup/sieť),
 - b) náročnosti získania prístupu,
 - c) potreby autentifikácie,
 - d) dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.
- 3) Na základe analýzy rizík musia byť navrhnuté opatrenia, ako predchádzať možným incidentom a ako postupovať v prípade vzniku incidentu. Tieto opatrenia musia byť zapracované v návrhu riešenia.

1.3 Implementácia riešenia

- 1) Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí.
- 2) Pri implementácii by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky / knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.
- 3) V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.
- 4) Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie, pričom:
 - a) jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
 - b) commity by mali mať zmysluplné popisy,
 - c) mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commitu.
- 5) Nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.
- 6) Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:

- a) zapnuté všetky varovania a ochrany vývojových nástrojov,
 - b) varovania vývojového prostredia.
- 7) Všetky varovania z predchádzajúceho bodu by mali byť opravené.
- 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 špecifikácii a jej dôvody a každá takáto zmena musí byť schválená objednávatelom.
- 9) Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávatelovi 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 prístupit' 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 adresu, cieľovú IP adresu, 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 verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
- 12) Logy musia byť centrálné ukladané a archivované minimálne 6 mesiacov.
- 13) Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server.

1.4 Testovanie a verifikácia riešenia

- 1) Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:
- a) vývojári by mali overiť aspoň pomocou automatizovaných nástrojov štandardné zraniteľnosti. Malo by prebehnúť minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leaky, memory corruption),
 - b) vývojári musia zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia,
 - c) musí byť vykonané penetračné testovanie externou organizáciou,
 - d) zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

1.5 Nasadenie a prevádzka riešenia

- 1) Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry.
- 2) Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami. Aplikovanie týchto záplat musí podliehať opatreniam uvedeným v smernici pre riadenie záplat.

1.6 Bezpečný návrh – Webové aplikácie

- 1) Webová stránka by mala pozostávať z verejných a neverejných zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.
- 2) Citlivé informácie by mali byť uchovávané v zašifrovanej podobe.

- 3) Validácia vstupov musí byť vykonávaná na strane servera a odporúča sa, aby bola vykonávaná aj na strane klienta.
- 4) Prezentačný server musí byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby. Aplikačný a databázový server by mali byť umiestnené v internej sieti neprístupnej z Internetu.
- 5) Kód musí byť udržiavaný, prehľadný a dokumentovaný.
- 6) Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

2 Konfigurácia webového servera

2.1 Systém

- 1) Systém, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.
- 2) Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.
- 3) Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete organizácie alebo byť umiestnené v izolovaných sieťach.
- 4) Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a 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).

2.2 Webový server

- 1) Pri inštalácii 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 inštalácii 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.
 - 9) Webový server by nemal podporovať funkcionality listovania adresára (Directory listing, Microsoft IIS tilde directory enumeration).
 - 10) Súbor robots.txt nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).
 - 11) Webový server by mal byť chránený WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:
 - a) detekcia a prevencia známych útokov (Code injection – SQL, XSS, Command, XPATH, ...),
 - b) kontrola používateľských vstupov prostredníctvom whitelingu a ich prekódovanie do HTML entít alebo podobných bezpečných náhrad.
 - 12) Webový server s aplikáciou spracúvajúcou citlivé údaje a/alebo klasifikované informácie, musí byť chránený WAF, ktorého konfigurácia musí byť reštriktívna (kontrola business logiky a pod).
 - 13) Na zvýšenie dostupnosti webového servera odporúčame použiť load balancery. Podľa možnosti môžu byť rozšírené o web cache. V prípade podpory web cache nesmú byť cacheované administrátorské stránky, prístupové údaje a podobné citlivé informácie.
 - 14) Na zvýšenie dostupnosti webového servera môžu byť ako bezpečnostné brány použité reverzné proxy. Podľa možnosti môžu byť rozšírené o funkcie akcelerácie šifrovania, používateľskej autentifikácie alebo filtrovania obsahu.

- 15) Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov (kvôli DoS útoku).
- 16) Webový server musí dodržiavať negotačný postup negotaácie TLS spojenia, popísaný v RFC 5746, kvôli zraniteľnosti Insecure renegotiation a riziku útoku typu MitM.
- 17) Webový server by mal podporovať bezpečnú renegociáciu (Secure renegotiation).
- 18) V prípade viacerých virtuálnych hostov musí byť oddelené úložisko cookies minimálne na úrovni adresárov.

2.3 Administrácia, logovanie a zálohovanie

- 1) Správčovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).
- 2) Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.
- 3) Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.
- 4) Webové správčovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.
- 5) Na serveri musí byť aktívne logovanie:
 - a) malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent,
 - b) pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log,
 - c) v logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná,
 - d) logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii,
 - e) na uchovávanie logov musí byť vyhradená dostatočná kapacita,
 - f) logy by mali byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov,
 - g) logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, 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.

2.4 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).

2.5 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.
- 2) V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.).
- 3) V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.
- 4) Server by mal používať hlavičky:

- a) X-Frame-Options: SAMEORIGIN (alebo DENY),
 - b) X-XSS-Protection: 1,
 - c) X-Content-Type-Options: nosniff,
 - d) Strict-Transport-Security.
- 5) V odpovediach webového servera by sa nemali nachádzať hlavičky X-Forwarded-For a HTTP_PROXY.

2.6 Aplikácia (webový portál)

- 1) Aplikácia musí ošetrovať všetky chyby a výnimky.
- 2) Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.
- 3) V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.
- 4) Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).
- 5) Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.
- 6) Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.
- 7) Aplikácia nesmie ukladať citlivé údaje (napríklad identifikátor relácie) v URL adrese. V prípade zakázania cookies v prehliadači musí stránka zobraziť hlásenie o nutnosti použitia cookies (ak sa používajú).
- 8) Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy prevádzkovateľa alebo inštitúcie verejnej správy na SR).
- 9) Aplikácie nesmie používať odkazy na nedôveryhodné externé zdroje.
- 10) Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).
- 11) Aplikácia nesmie používať funkciu eval() alebo jej alternatívy.
- 12) Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

2.7 Autentifikácia a autorizácia

- 1) Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).
- 2) Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).
- 3) Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.
- 4) Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.
- 5) Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.
- 6) Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupná až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.
- 7) Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.

- 8) Aplikácia musí vyžadovať používanie silných hesiel.
- 9) V prípade použitia iníciaľných náhodne generovaných hesiel pre nového používateľa musí 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 zadanie hesla 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 funkcionality 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 funkcionality 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,
 - Expires: 0,
 - Pragma: no-cache.

2.8 Používateľské vstupy

- 1) Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.
- 2) Aplikácia musí brať ako vstupy a primerane ošetrovať všetky používateľom ovplyvniteľné časti dopytu, vrátane HTTP hlavičiek, URL, Cookies a pod. Bez ošetrenia nesmú byť reflektované v odpovedi servera. Napríklad:
 - a) aplikácia musí byť odolná voči HTTP Spitting/Smuggling útokom,
 - b) aplikácia by mala byť odolná voči HTTP Parameter Pollution (HPP) útokom,
 - c) aplikácia/webový server musí byť odolný voči Host Header útoku.
- 3) Aplikácia by mala používať parametrizované SQL požiadavky (queries), tzv. prepared statements.
- 4) Aplikácia nesmie na tvorenie SQL dotazov využívať používateľské vstupy bez ich dôkladnej kontroly a ošetrenia.
- 5) Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím. Minimálne:
 - a) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek,
 - b) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dopyte alebo parametri príkazu operačného systému,
 - c) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML,
 - d) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript,
 - e) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API,
 - f) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch,
 - g) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query),
 - h) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets,
 - i) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI (Server-Side Inclusion statements) príkazoch, ak je použitie SSI nutné a povolené,
 - j) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách,
 - k) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch,
 - l) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách,

- m) aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch,
- n) aplikácia musí ošetrovať vstupy/dátové prúdy prechádzajúce medzi modulmi aplikácie.

2.9 Relácie

- 1) Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.
- 2) Aplikácia by nemala povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.
- 3) Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.
- 4) Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.
- 5) Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie. Identifikátor predchádzajúcej neautentickej relácie musí byť zneplatnený.
- 6) Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia znovu vygenerovať identifikátor relácie.
- 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 zamietat' neznáme relačné identifikátory zo strany klienta.
- 15) Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia. Aplikácia musí vynucovať periodickú expiráciu a zneplatnenie relácií.

2.10 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.

2.11 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.

2.12 Rôzne

- 1) Aplikácia by nemala podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.
- 2) Aplikácia by mala obmedziť (krížový) prístup k (cudzím) doménam prostredníctvom whitelistingu.
 - a) ak je na riadenie prístupu medzi doménami používané CORS (Cross Origin Resource Sharing), konfigurácia by mala byť obmedzená na dôveryhodné domény. Napr. nemala by byť použitá direktíva Access-Control-Allow-Origin:*,
 - b) ak aplikácia používa na kontrolu prístupu k zdrojom na externých doménach súbory crossdomain.xml a/alebo clientaccesspolicy.xml, obsah by mal mať obmedzený na nutné domény, porty a protokoly. Nemali by byť používané nadmerne voľné pravidlá s „*“. Crossdomain.xml a clientaccesspolicy.xml nesmú byť prístupné koncovému používateľovi.
- 3) Aplikácia by mala pre všetky emailové funkcionality implementovať rate limiting.
- 4) Aplikácia by mala pre všetky funkcionality vyžadujúce veľa zdrojov (napríklad CPU čas) implementovať rate limiting.
- 5) Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

3 Interná infraštruktúra a vývojové prostredie

3.1 Interná infraštruktúra riešenia

- 1) Jednotlivé vrstvy (databázová, aplikačná, prezentačná) by mali byť umiestnené v separátnych segmentoch a komunikácia medzi nimi musí byť filtrovaná.
- 2) Jednotlivé servery musia byť hardenované minimálne v rozsahu:
 - a) vypnuté všetky nepotrebné procesy a služby,
 - b) implementovaný host-based firewall, ktorý kontroluje všetku komunikáciu IN aj OUT a je nakonfigurovaný na princípe „least privilege“,
 - c) všetky administrátorské účty spĺňajú politiku hesiel pre administrátorské účty,
 - d) servery a všetok softvér je aktualizovaný minimálne raz za 6 (šesť) mesiacov, odporúča sa aktualizovať aspoň raz za mesiac,
 - e) na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálné spravované a centrálné logované,
 - f) všetky servery majú nastavené lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery,
 - g) všetky zariadenia musia byť hardenované podľa odporúčaní výrobcu.

3.2 Vývojové prostredie

- 1) Vo vývojovom prostredí musia byť použité iba nástroje spĺňajúce nasledovné:
 - a) musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
 - b) musia byť stále podporované výrobcom (t.j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,
 - c) musia byť aktualizované minimálne raz za 6 (šesť) mesiacov a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.
- 2) Vo vývojovom prostredí (vývojárske nástroje a podporné informačné systémy vrátane použitých knižníc tretích strán), v ktorom bude vyvíjané riešenie, musia byť implementované tieto opatrenia:
 - a) musia byť implementované príslušné opatrenia na zabezpečenie integrity vyvíjaného 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

4.1 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 Protocol Security (IPSEC) na zabezpečenie sieťových protokolov.

4.2 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 prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu,
- d) pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii,
- e) vzdialený prístup do vnútornej siete SP musí podliehať autentifikácii a autorizácii, vyžaduje sa použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- f) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 (štyri) mesiace,
- g) na všetkých serveroch podporujúcich základné služby informačných technológií SP sa implementujú sondy detekcie a prevencie prieniku technológia HIPS,
- h) všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom,
- i) implementácia druhého sieťového firewallu od iného výrobcu tak, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi,
- j) implementácia Web Application Firewallu (WAF) na všetkých verejne dostupných a kritických webových aplikáciách,
- k) implementácia manažmentu logov,

- l) implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby,
- m) konfigurácia a izolovanie klientskych portov na prístupových switchoch tak, aby pracovné stanice spolu nemohli priamo komunikovať (technológia PVLAN). Táto požiadavka nahrádza požiadavku zo Z2-FI) o maximálnom počte MAC adries,
- n) zabezpečenie prístupu používateľov k Internetu a k službám mimo siete SP cez proxy server a uchovávanie prístupových logov aspoň 6 (šesť) mesiacov,
- o) používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 (štyri) mesiace,
- p) uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 (šesť) mesiacov,
- q) rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia,
- r) zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni šiestice časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 (šesť) mesiacov.

5 Prenos elektronickej pošty

5.1 Prenos elektronickej pošty

- 1) Štandardom prenosu elektronickej pošty je
 - a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronickej pošty,
 - b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na zabezpečenie prenosu elektronickej pošty.
- 2) SMTP banner by nemal obsahovať informácie o použítom softvéri ani iné citlivé informácie. 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 existencii 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 blokovat' 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,
 - b) podpora protokolu Hypertext Transfer Protocol (HTTP) vo verzii 1.1 a Hypertext Transfer Protocol (HTTP) vo verzii 1.0 pri webových serveroch,
 - c) používanie mechanizmu Hypertext Transfer Protocol State Management Mechanism (HTTP Management Mechanism) na Hypertext Transfer Protocol Session Management (HTTP Session Management) a cookies,
 - d) používanie protokolu Hypertext Transfer Protocol (HTTP) s Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na zabezpečenie prenosu dát medzi klientom a webovým serverom a medzi webovými servermi,
 - e) používanie protokolu HTTP Strict Transport Security (HSTS) pri poskytovaní elektronických služieb a rozhraní prostredníctvom modulu procesnej integrácie a integrácie údajov.

6.2 Adresárové služby

- 1) Štandardom adresárovej služby je
 - a) používanie aplikačného protokolu Lightweight Directory Access Protocol vo verzii 3 (LDAP v3) na verejný prístup k adresárovým službám,
 - b) používanie jazyka Directory Services Markup Language v2 (DSML v2),

- c) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group pri chránenom verejnom prístupe k adresárovým službám.

7 Štandardy webovej služby

7.1 Middleware protokoly sieťovej komunikácie

- 1) Štandardom middleware protokolov sieťovej komunikácie je používanie
 - a) protokolu Simple Object Access Protocol (SOAP) najmenej vo verzii 1.2 alebo protokolu Representational State Transfer (REST) pri komunikácii medzi servermi v rámci jednej správy a komunikácii medzi klientom a serverom; pri poskytovaní elektronických služieb potrebných na spracovanie elektronických podaní alebo úspešné vyplnenie a prípravu elektronického podania prostredníctvom modulu procesnej integrácie a integrácie údajov sa používa protokol Representational State Transfer (REST) a kódovanie UTF-8,
 - b) webových služieb na prístup klientskych aplikácií prostredníctvom internetu na serverové aplikácie správy,
 - c) protokolu Hypertext Transfer Protocol (HTTP) na poskytnutie vrstvy webovej služby pre existujúcu serverovú aplikáciu a komunikáciu na aplikačnej úrovni,
 - d) jazyka Web Services Description Language (WSDL) na definíciu webovej služby,
 - e) registra Universal Description, Discovery and Integration (UDDI) najmenej vo verzii 1.0 na komunikáciu medzi klientom a serverom,
 - f) špecifikácií podľa Open Geospatial Consortium (OGC) mapových služieb pod OpenGIS,
 1. WebMap Service (WMS),
 2. Web Feature Service (WFS),
 3. Web Coverage Service (WCS),
 4. Web Processing Service (WPS),
 5. Catalog Service for Web (CSW),
 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) znakovkej 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.

9 Formáty kompresie súborov

- 1) Štandardom formátov kompresie súborov je
 - a) prijímanie a čítanie všetkých doručených formátov kompresie súborov, ktorými sú:
 1. ZIP (.zip) vo verzii 2.0,
 2. TAR (.tar),
 3. GZIP (.gz),
 4. TAR kombinovaný s GZIP (.tgz, .tar.gz).

10 Dátové štandardy

10.1 Výmena údajov

- 1) Štandardom výmeny údajov je
 - a) pri výmene obsahovo príslušných informácií použitie dátových prvkov uvedených v Centrálnom modeli údajov, pričom ak neexistujú obsahovo vhodné dátové prvky v Centrálnom modeli údajov použijú sa

dátové prvky uvedené v Prílohe č. 3 Vyhlášky č. 78/2020 Z. z.; v ostatných prípadoch sa použijú vlastné dátové prvky,

- b) používanie technických parametrov dátových prvkov podľa dátových štruktúr vo formáte Extensible Markup Language Schema Definition (XSD) zverejnených na webovom sídle orgánu vedenia pri tvorbe definície vlastných dátových štruktúr vo formáte Extensible Markup Language Schema Definition (XSD),
- c) rozširovanie typov dátových prvkov na osobitné dátové typy Centrálného modelu údajov, ak je to potrebné,
- d) použitie vlastných dátových prvkov podľa písmena a) spravidla tak, že referenčné údaje určené na automatizované spracovanie a tvoriace súčasť dátového obsahu sú v dátovej štruktúre uvedené ako samostatné dátové prvky na automatizované spracovanie,
- e) Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou,
- f) Informácie v transakciách informačných technológií alebo medzi informačnými technológiami sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpoveďami, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti) certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.

11 Šifrovanie

- 1) Webový portál musí byť prístupný prostredníctvom protokolu HTTPS.
- 2) K webovému portálu by sa nemalo pristupovať prostredníctvom HTTP.
- 3) Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu na ktorej je dostupný webový portál.
- 4) Identita webového portálu by mala byť zabezpečená certifikátom s Extended Validation.
- 5) Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.
- 6) Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.
- 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.

13 Firewall

- 1) Všetky prepoje medzi segmentami a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povolené iba na princípe least privilege.
- 2) Smerom do vnútra musia byť povolené len špecifikované služby umiestnené v DMZ (politika "default deny").
- 3) Smerom do externých sietí by mala byť povolená len špecifikovaná komunikácia (pre interné siete by to malo byť len HTTP a HTTPS).
- 4) Všetky spojenia do externých sietí musia byť smerované cez dedikovaný sieťový firewall. Všetky spojenia do externých sietí okrem VoIP by mali byť smerované aj cez IPS (ak je IPS použité) - výnimkou je VoIP, pre ktoré sa toto odporúča ak to výkon a funkcionality IPS dovoľuje.
- 5) Musí byť obmedzená táto komunikácia:

- a) DNS požiadavky smerom do externých sietí (dport UDP/TCP 53) môžu iniciovať len autorizované rekurzívne DNS servery,
- b) SMTP správy smerom do externých sietí (dport TCP 25) môžu posilať len autorizované (t.j. na to určené) SMTP servery,
- c) SMTP smerom do externých sietí môžu iniciovať len autorizované SMTP servery,
- d) Odporúča sa nepovoľovať smerom do externých sietí komunikáciu na TCP/445 (SMB), TCP/6697 (IRC).

14 Zabezpečenie iných služieb

- 1) Pre prístup k neštandardným službám, ktoré nie je možné hardenovať a zabezpečiť štandardným spôsobom (napr. TLS) sa odporúča využiť prístup cez VPN.

15 Požiadavky z pohľadu BIS vo vzťahoch s tretími stranami

- 1) V zmluve s dodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa BIS. Môže byť uvedený odkaz na zákon, vyhlášku alebo na osobitný predpis.
- 2) Požiadavky v oblasti BIS sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií SP.
- 3) Zmluvné požiadavky na BIS obsahujú najmenej záväzok:
 - a) plnenia určených požiadaviek a kritérií pre oblasť BIS pri dodávke predmetu zmluvy,
 - b) ochrany informácií, ku ktorým je poskytnutý prístup,
 - c) oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa BIS a ďalších opatrení a postupov BIS špecifických na plnenie predmetu zmluvy,
 - d) riadenia a monitorovania prístupov do informačných technológií SP vrátane spôsobu a mechanizmu,
 - e) možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
 - f) oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií SP zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrovania,
 - g) spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
 - h) zachovania úrovne BIS pri významných zmenách vrátane spôsobu a formy prechodu k 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 filtrovaná 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, nahrádzajúci ARP z IPv4

NTP - Network Time Protocol

OS - Operačný systém PVLAN – Private VLAN princíp least privilege

RDP - Remote Desktop Protocol

QoS - Quality of Service

Sieťový firewall - firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)

SNMP – Simple Network Management Protocol

SSO – Single Sign-On

Telepresence

UAC – User Access Control

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VOIP – Voice over IP

WAF – Webaplikačný firewall - špeciálny typ firewallu, prispôbený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.

Whitelisting - metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje

XSS - Cross-Site Scripting

Zdroje a Legislatívne východiská

- [Slov-lex](#)
- [Eur-lex](#)
- [Sémantický znalostný strom vedomostí Knowww EU portál](#)
- [Vláda SR](#)
- [Ústredný portál verejnej správy](#)
- [Rokovania legislatívnej rady vlády SR](#)
- [Zoznam uznesení vlády SR](#)
- [Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky](#)
- [CSIRT](#)
- [NASES](#)
- [NBÚ](#)
- [Interné normy SP](#)
- [NIST](#)
- [NSA](#)
- [OWASP](#)
- [IETF](#)
- [IAB](#)
- [RFC](#)
- Zákon č. **395/2002** Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
- Zákon č. **461/2003** Z. z. o sociálnom poistení
- Zákon č. **215/2004** Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
- Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí)
- Zákon č. **45/2011** Z. z. o Kritickej infraštruktúre
- Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti OVM a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)
- Zákon č. **272/2016** Z. z. o dôverných službách (elektronický podpis) pre elektronické transakcie na vnútornom trhu (eIDAS) a o zmene a doplnení niektorých zákonov
- Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov 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. **438/2019** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente

- 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. **547/2021** Z. z. o elektronizácii agendy VS
- Vyhláška Ministerstva vnútra Slovenskej republiky č. **29/2017** Z. z. o alternatívnom autentifikátore
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **85/2020** Z. z. o riadení projektov v znení neskorších predpisov
- Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej 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,
- Vyhláška Národného bezpečnostného úradu č. **48/2019** Z. z. ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností
- 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 kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
- Smernica Európskeho parlamentu a Rady (EÚ) **2016/2102** z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora
- Smernica Európskeho parlamentu a Rady (EÚ) **2019/1024** z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora
- Smernica č. **7/2019** o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
- Metodika Jednotný dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVS č. 002089/2018/oLSISVS-7 zo dňa 11.05.2018 <https://www.mirri.gov.sk/wp-content/uploads/2018/10/Metodicke-usmernenie-ID-SK-publikovat.pdf>
- Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI) <https://www.mirri.gov.sk/wp-content/uploads/2019/04/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-verejnej-spravy.pdf>
- Metodika riadenia QAMPR <https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html>
- Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich https://www.mirri.gov.sk/wp-content/uploads/2020/02/Metodicky_pokyn_ORACLE_CRD_2019.pdf
- Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.html>
- Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT) – aktuálne znenie [MetodikaZabezpeceniaIKT v2.1.pdf \(gov.sk\)](#)

Klasifikačné stupne informačných aktív

Klasifikačné stupne informačných aktív opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktíva“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

Dôvernosť

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

- **verejné** informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,
- **interné** informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v 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 privilegií“ 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.