

ZMLUVA O DIELO

uzatvorená podľa ustanovenia § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka
v znení neskorších predpisov

medzi zmluvnými stranami:

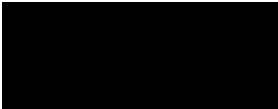
Objednávateľ:

Názov: **Sociálna poisťovňa**
Sídlo: Ul. 29. augusta 8 a 10, 813 63 Bratislava
IČO: 308 074 84
DIČ: 2020592332
V zastúpení: Ing. Michal Ilko
generálny riaditeľ Sociálnej poisťovne
Bankové spojenie: Štátna pokladnica, Bratislava
Číslo účtu: SK40 8180 0000 0070 0016 4314
SWIFT: SPSRSKBA

(ďalej ako „objednávateľ“)

a

Zhotoviteľ:

Obchodné meno: **Alanata a. s.**
Sídlo: Krasovského 14, 851 01 Bratislava – mestská časť Petržalka
IČO: 54 629 331
DIČ: 2121747573
IČ DPH: SK2121747573
V zastúpení: Ing. Andrej Bališ
člen predstavenstva
Zapísaný: v Obchodnom registri Mestského súdu Bratislava III,
Oddiel: Sa, Vložka číslo: 7425/B
Bankové spojenie: 
Číslo účtu:
SWIFT:

(ďalej ako „zhotoviteľ“)

(objednávateľ a zhotoviteľ ďalej jednotlivo aj ako „zmluvná strana“ alebo spoločne ako „zmluvné strany“)

PREAMBULA

Východiskovým podkladom na uzatvorenie tejto zmluvy o dielo (ďalej len „zmluva“) je ponuka zhotoviteľa zo dňa 03.08.2023, predložená objednávateľovi v rámci zadávania civilnej zákazky s nízkou hodnotou na vypracovanie diela „Dizajn a konfigurácia Identity Management“ podľa ustanovenia § 5 ods. 4 a § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov.

Článok I. PREDMET ZMLUVY

1. Predmetom tejto zmluvy je úprava vzájomných práv a povinností zmluvných strán v súvislosti so záväzkom zhotoviteľa zhotoviť dielo - spracovať a implementovať Dizajn a konfiguráciu RedHat Identity Management v rozsahu podľa ustanovení tejto zmluvy ako aj Prílohy č. 1 – Opis predmet zmluvy (ďalej len „dielo“) a v súvislosti so záväzkom objednávateľa riadne a včas vykonané dielo prevziať a zaplatiť zaň zhotoviteľovi cenu určenú podľa článku IV tejto zmluvy.
2. Predmetom zmluvy je záväzok zhotoviteľa vykonať dielo pre objednávateľa tak, že zhotoviteľ spracuje a implementuje Dizajn a konfiguráciu RedHat Identity Management za účelom kontroly autentifikácie a autorizácie Linux prostredia v Sociálnej poisťovni.

Článok II. PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

1. Objednávateľ je povinný poskytnúť včas zhotoviteľovi pravdivé informácie, všetky dostupné podklady a dokumenty, ktoré majú vplyv na povahu a spôsob zhotovenia diela a nesmie zamlčať žiadne informácie dôležité pre zhotovenie diela.
2. Zhotoviteľ je povinný oznámiť objednávateľovi všetky okolnosti, ktoré zistil pri plnení svojich záväzkov, a ktoré môžu mať vplyv na zmenu pokynov objednávateľa. Zhotoviteľ sa zaväzuje bezodkladne písomne informovať objednávateľa o každom prípadnom zdržaní, či iných skutočnostiach, ktoré by mohli ohroziť včasné a riadne dodanie diela.
3. Zhotoviteľ sa zaväzuje chrániť práva a právom chránené záujmy objednávateľa, dôsledne využívať všetky zákonné prostriedky a uplatňovať všetky dostupné možnosti, čo podľa svojich odborných vedomostí a pokynov objednávateľa považuje za účelné.
4. Zhotoviteľ sa zaväzuje vykonať dielo vo vlastnom mene a na vlastnú zodpovednosť riadne a včas v požadovanej kvalite a s odbornou starostlivosťou, a to v súlade s podmienkami tejto zmluvy a pokynmi objednávateľa.
5. Zmluvné strany sa zaväzujú, že si budú poskytovať potrebnú súčinnosť pri plnení záväzkov z tejto zmluvy a navzájom si budú oznamovať všetky okolnosti a informácie, ktoré môžu mať vplyv na riadne plnenie predmetu zmluvy.
6. Objednávateľ sa zaväzuje riadne a včas zhotovené dielo prevziať a zaplatiť zaň dohodnutú cenu, uvedenú v článku IV. ods. 1 tejto zmluvy.
7. Zhotoviteľ odovzdá dielo, poverenej osobe Objednávateľa v písomnej a zároveň aj v editovateľnej forme spôsobom dohodnutým v článku III tejto zmluvy.
8. Zhotoviteľ zodpovedá za kvantitatívne a kvalitatívne vady diela.
9. Objednávateľ nezodpovedá za škodu, ktorá vznikne pri vytváraní diela alebo v súvislosti s ním.
10. Zmluvné strany sa dohodli, že od pokynov objednávateľa sa môže zhotoviteľ odchýliť, len ak je to naliehavo nevyhnutné v záujme objednávateľa a zhotoviteľ nemôže včas

dostať jeho súhlas. Zhotoviteľ je však povinný písomne o takomto postupe objednávateľa informovať bez zbytočného odkladu.

11. Zmluvné strany sa dohodli, že vlastníkom zhotoveného diela je objednávateľ, ktorý je oprávnený s ním disponovať v zmysle licenčných podmienok uvedených v tejto zmluve.

Článok III.

TERMÍN A SPÔSOB VYKONANIA/ZHOTOVENIA DIELA

1. Zhotoviteľ sa zaväzuje, že dielo vykoná riadne a včas, t. j. v celom rozsahu podľa tejto zmluvy, bez väd a v lehote do 3 mesiacov odo dňa nadobudnutia účinnosti tejto zmluvy a odovzdá ho objednávateľovi. Dielo je zhotovené riadne, ak spĺňa všetky požiadavky podľa tejto zmluvy a podľa pokynov objednávateľa a zodpovedá účelu sledovanému zmluvou. Dielo musí byť zhotovené a odovzdané v kvalite určenej objednávateľom, v súlade s právnymi predpismi a bez väd, ktoré by mohli mať následok vznik škody na strane objednávateľa alebo tretej osoby.
2. Dňom doručenia diela, resp. jeho časti do sídla objednávateľa uvedeného v záhlaví tejto zmluvy začína preberacie konanie, ktorého účelom je zistenie skutočnosti, či dielo spĺňa kvantitatívne a kvalitatívne vlastnosti uvedené v tejto zmluve.
3. Ak objednávateľ počas preberacieho konania zistí, že dielo, resp. jeho časť má zjavné vady a nedostatky, oznámi bezodkladne písomne túto skutočnosť zhotoviteľovi odoslaním doporučenej zásielky adresovanej do sídla zhotoviteľa, alebo do elektronickej schránky, v lehote do 10 pracovných dní od jeho doručenia (ďalej len „oznámenie o zjavných vadách“). V oznámení o zjavných vadách určí objednávateľ súčasne zhotoviteľovi lehotu na odstránenie zjavných väd, ktorá nesmie byť kratšia ako 5 pracovných dní odo dňa doručenia oznámenia o zjavných vadách. Zhotoviteľ sa zaväzuje zjavné vady v takto stanovenej lehote odstrániť a dodať objednávateľovi dielo bez väd.
4. Na účely tejto zmluvy dielo, resp. jeho časť nespĺňa kvantitatívne a kvalitatívne vlastnosti uvedené v tejto zmluve, ak má vady, ktoré sú objednávateľom zistiteľné pri vynaložení náležitej starostlivosti počas preberacieho konania, alebo nespĺňa ďalšie požiadavky uvedené v tejto zmluve (ďalej len „zjavné vady“).
5. Pre vylúčenie pochybností platí, že ak dielo k dátumu odovzdania podľa ods. 1 tohto článku zmluvy vykazuje zjavné vady zistené v rámci preberacieho konania, má sa za to, že zhotoviteľ sa dostal do omeškania s riadnym a včasným plnením ku dňu odovzdania diela podľa ods. 1 tohto článku zmluvy. Odstránenie zjavných väd zhotoviteľom, v náhradnej lehote podľa ods. 3 tohto článku zmluvy nezbavuje zhotoviteľa zodpovednosti za škodu a objednávateľa nezbavuje nároku na zmluvnú pokutu v súlade s článkom VI. ods. 1 tejto zmluvy.
6. Preberacie konanie je skončené dňom podpísania preberacieho protokolu objednávateľom a zhotoviteľom. Preberací protokol sa vyhotovuje vo 2 rovnopisoch, po jednom rovnopise pre každú zmluvnú stranu. Preberací protokol musí byť podpísaný oboma zmluvnými stranami, a to zodpovednou osobou objednávateľa, ktorým je riaditeľ sekcie informatiky a za zhotoviteľa account manager.
7. Za vady vzniknuté po odovzdaní zodpovedá zhotoviteľ iba vtedy, ak boli spôsobené porušením jeho povinností vyplývajúcich zo zmluvy a nedodržaním všeobecne

záväzných právnych predpisov.

8. Zhotoviteľ sa zaväzuje, že na pripomienkovanie dodá objednávateľovi dielo v elektronickej forme (MS Office, PDF) a odsúhlasené dielo bude objednávateľovi dodané v písomnej forme v 2 (dvoch) vyhotoveniach a v elektronickej forme (MS Office, PDF, DWG). Nedostatočné dodržanie a/alebo zlyhanie v preukázaní alebo akejkol'vek pochybnosti o dodržaní formy a spôsobu doručenia, sa bude považovať za závažné porušenie zmluvy.
9. Kontrolu plnenia predmetu plnenia budú vykonávať poverení zamestnanci Sociálnej poisťovne, čím nie je dotknuté právo vykonať kontrolu plnenia predmetu plnenia aj bez uvedenia dôvodu, a to kedykoľvek.
10. Vlastnícke právo a zodpovednosť za nebezpečenstvo škody na zhotovenej veci prechádza na objednávateľa odovzdaním diela objednávateľovi, t. j. podpísaním preberacieho protokolu podľa ods. 6 tohto článku.
11. Zhotoviteľ vyhlasuje, že má k dispozícii špecialistov v súlade s požiadavkami objednávateľa na preukázanie technickej a odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Zhotoviteľ sa zaväzuje, že požadované služby bude poskytovať objednávateľovi prostredníctvom osôb, ktorými preukazoval splnenie podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Nahradenie alebo doplnenie týchto osôb inými osobami je možné len so súhlasom objednávateľa. V prípade nahradenia osôb musia osoby, ktoré ich nahradia, spĺňať rovnaké podmienky ako sa požadovali v rámci preukázania splnenia podmienok účasti technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní.
12. V prípade zmeny niektorého zo špecialistov podľa predchádzajúceho bodu, ktorí sú uvedení v prílohe č. 2 k tejto zmluve je zhotoviteľ povinný písomne oznámiť objednávateľovi najneskôr do 5 pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví zmluvy údaje o navrhovanom novom špecialistovi. Nový špecialista musí spĺňať podmienky podľa bodu 11. tohto článku zmluvy. Zmena nového špecialistu sa vykoná zápisom o zmene prílohy k zmluve, ktorý nadobudne platnosť dňom jeho podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky (ďalej len „register“); vzor zápisu o zmene prílohy k zmluve tvorí prílohu č. 4 k tejto zmluve; osobami oprávnenými konať vo veciach zmeny prílohy č. 2 k zmluve sú:
za zhotoviteľa: account manager
za objednávateľa: riaditeľ sekcie informatiky.

Článok IV.

CENA ZA DIELO A PLATOBNÉ PODMIENKY

1. Cena za zhotovenie a dodanie diela podľa článku I. tejto zmluvy je stanovená v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov (ďalej len „zákon o cenách“) a vyhlášky Ministerstva financií Slovenskej republiky č. 87/1996 Z. z., ktorou sa vykonáva zákon o cenách (ďalej len „vyhláška“) nasledovne:

Cena bez DPH: 12 500,00 EUR (slovom dvanásťtisícpäťsto eur)

DPH 20 %: 2 500,00 EUR (slovom dvetisícpäťsto eur)
Cena vrátane DPH: 15 000,00 EUR (slovom pätnásťtisíc eur).

Zhotoviteľ je platcom DPH. DPH bude účtovaná v aktuálnej sadzbe podľa všeobecne záväzných právnych predpisov, platných v čase zdaniteľného plnenia.

2. Zmluvné strany sa dohodli, že zhotoviteľ je oprávnený po splnení záväzkov vystaviť faktúru na cenu podľa ods. 1 tohto článku po podpísaní preberacieho protokolu podľa článku III ods. 6 tejto zmluvy, ktorý bude tvoriť prílohu k faktúre.
3. Cena uvedená v ods. 1 tohto článku je dohodnutá ako cena maximálna a konečná. Pre vylúčenie akýchkoľvek pochybností platí, že dohodnutá cena zahŕňa všetky náklady činnosti, práce, výkony alebo služby súvisiace s riadnym dodaním diela ako aj všetky náklady zhotoviteľa nevyhnutne vynaložené v súvislosti s realizáciou predmetu zmluvy, vrátane odplaty za licenciu a tiež tých nákladov, ktoré nie sú konkrétne uvedené v zmluve.
4. Zmluvné strany sa dohodli, že stanovená cena za dielo bude uhradená objednávatelom bezhotovostným prevodom na účet zhotoviteľa uvedený v záhlaví tejto zmluvy, na základe faktúry vystavenej zhotoviteľom a doručenej objednávatelovi.
5. Lehota splatnosti faktúry je 30 kalendárnych dní odo dňa jej doručenia objednávatelovi. Faktúra musí obsahovať všetky náležitosti účtovného a daňového dokladu podľa platných právnych predpisov a špecifikáciu fakturovanej sumy.
6. Zhotoviteľ sa zaväzuje vyhotovenú faktúru zaslať listinne poštou a súčasne v textovo čitateľnom súbore vo formáte PDF elektronicky na e-mailovú adresu objednávatela faktury@socpoist.sk, a to bezodkladne po jej vystavení. Takto predložená faktúra nesmie byť vo forme obrázku, ale musí byť strojovo čitateľná. Zhotoviteľ vyhlasuje, že obsah faktúry poslanej poštou sa bude zhodovať s faktúrou poslanou v elektronickej podobe na e-mailovú adresu objednávatela. Miestom doručenia faktúry v listinnej forme je Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava. Všetky faktúry vyplývajúce z tejto zmluvy a objednávky podliehajú povinnosti zverejnenia zo strany objednávatela.
7. Zhotoviteľom vystavená faktúra ako daňový doklad musí byť vyhotovená v súlade s ustanoveniami zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov. V prípade, ak faktúra vystavená zhotoviteľom nebude obsahovať všetky zákonom stanovené náležitosti alebo bude obsahovať nesprávne alebo neúplné údaje, objednávatel má právo takúto faktúru vrátiť zhotoviteľovi na jej doplnenie, resp. opravu a zhotoviteľ je povinný podľa charakteru nedostatku vystaviť novú, opravenú, resp. doplnenú faktúru s novou lehotou splatnosti. Zhotoviteľ je zároveň povinný bezodkladne poslať opravenú alebo novú faktúru znovu aj v elektronickej podobe na e-mailovú adresu uvedenú v predchádzajúcom bode tohto článku zmluvy.
8. Zhotoviteľ sa zaväzuje uhradiť všetky správne a iné poplatky, ktoré súvisia s plnením záväzku podľa tejto zmluvy.
9. Objednávatel neposkytuje preddavok ani zálohovú platbu.
10. V prípade, že dôjde k zrušeniu alebo odstúpeniu od tejto zmluvy na strane objednávatela, bude zhotoviteľ fakturovať objednávatelovi práce rozpracované ku dňu zrušenia alebo odstúpenia vo výške percentuálneho podielu z dohodnutej ceny jednotlivých prác v súlade s ods. 1 tohto článku.

Článok V. LICENCIE

1. Ku všetkým výstupom spojeným s realizáciou predmetu zmluvy, ktoré podliehajú ochrane podľa zákona č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov (ďalej len „Autorský zákon“) sa zhotoviteľ zaväzuje poskytnúť objednávateľovi podľa § 70 autorského zákona výhradnú licenciu - súhlas na použitie diela alebo jeho časti, a to akýmkoľvek spôsobom podľa § 19 odsek 4 autorského zákona, ktorý je v čase nadobudnutia účinnosti zmluvy technicky možný a právne prípustný, no najmä na:
 - a) použitie diela vcelku alebo len čiastočne (po častiach) všetkými spôsobmi známymi ku dňu účinnosti zmluvy o dielo, najmä na jeho priame používanie objednávateľom pri výkone jeho činnosti,
 - b) vyhotovenie rozmnoženiny diela,
 - c) spracovanie, preklad a adaptáciu diela,
 - d) zaradenie diela do súborného diela,
 - e) verejné vystavenie diela,
 - f) verejné vykonanie diela,
 - g) verejný prenos diela,
 - h) zmenu, úpravu, dokončenie diela alebo na prenechanie na spracovanie, zmenu, úpravu, preklad resp. dokončenie diela, ako aj na použitie takéhoto diela,
 - i) spracovávanie, upravovanie a vytváranie odvodeného diela z diela, ako aj právo udeľovať súhlas tretím osobám k vykonávaniu týchto činností a takto spracované, upravené alebo odvodené dielo ďalej užívať v rozsahu podľa tejto zmluvy,
 - j) udeľovať práva na využívanie diela v rozsahu práv poskytnutých zhotoviteľom objednávateľovi zmluvou o dielo akejkoľvek tretej osobe, ktorá bude oprávnená poskytovať plnenie objednávateľovi v súvislosti s dielom.
2. Zhotoviteľ udeľuje objednávateľovi:
 - a) výhradnú licenciu na použitie diela alebo jeho časti,
 - b) v územnom rozsahu neobmedzenom,
 - c) vo vecnom rozsahu neobmedzenom,
 - d) v časovom rozsahu na dobu trvania majetkových práv zhotoviteľa podľa § 32 Autorského zákona.
3. Zmluvné strany sa dohodli, že odmena zhotoviteľa za udelenie licencie k dielu je zahrnutá v cene za dielo podľa článku IV. ods. 1 tejto zmluvy.
4. Zhotoviteľ vyhlasuje, že je oprávnený udeliť objednávateľovi licenciu a ostatné oprávnenia na používanie diela podľa tejto zmluvy a že udelenie licencií podľa tejto zmluvy nie je v rozpore so žiadnym jeho zmluvným záväzkom alebo platným právnym predpisom. V prípade, ak sa toto vyhlásenie ukáže ako nepravdivé, objednávateľ je oprávnený od zmluvy odstúpiť a zhotoviteľ je povinný nahradiť objednávateľovi škodu, ktorá mu tým vznikla.
5. Objednávateľ je oprávnený udeliť sublicenciu tretím osobám nielen štátnym orgánom a orgánom verejnej správy Slovenskej republiky alebo právnickým osobám založenými týmito orgánmi a právnickým osobám založeným na základe zákona na osobitný účel plnenia potrieb vo všeobecnom záujme alebo iným osobám, na ktoré bude prenesený výkon štátnej alebo verejnej správy, s čím zhotoviteľ vyjadruje svoj súhlas.

6. Objednávateľ je oprávnený používať dielo spracované alebo upravené v rozsahu a spôsobmi uvedenými v tejto zmluve a postúpiť zmluvou najmä na iné štátne orgány a orgány verejnej správy Slovenskej republiky alebo právnickým osobám založenými týmito orgánmi a právnickým osobám založeným na základe zákona na osobitný účel plnenia potrieb vo všeobecnom záujme alebo iným osobám, na ktoré bude prenesený výkon štátnej alebo verejnej správy v oblasti, na ktorý bol vytvorený, k čomu zhotoviteľ touto zmluvou udeľuje svoj súhlas.
7. Ak zhotoviteľ vykonaním autorského diela, alebo časti poveril tretiu osobu, alebo zamestnanca je zhotoviteľ povinný zabezpečiť, aby mu táto tretia osoba, resp. zamestnanec udelila výhradnú licenciu na jeho použitie v rozsahu rovnakom ako je uvedené v ods. 1 a 2 tohto článku zmluvy a tak, aby ju (resp. sublicenciu) bol oprávnený udeliť objednávateľovi, resp. previesť ju na objednávateľa v súlade s touto zmluvou. Zároveň je zhotoviteľ povinný zabezpečiť, aby mu tretia osoba, resp. zamestnanec udelil prehlásenie, že si nebude uplatňovať autorské práva po celú dobu trvania autorských práv.
8. Zhotoviteľ týmto udeľuje objednávateľovi súhlas na použitie diel tretích osôb a zamestnancov podľa ods. 7 tohto článku zmluvy. Zhotoviteľ zodpovedá za porušenie práv inej osoby, t. j. subdodávateľa z priemyselného alebo iného duševného vlastníctva v dôsledku použitia autorského diela objednávateľom.
9. V prípade, že si akákoľvek tretia strana, vrátane zamestnancov zhotoviteľa alebo subdodávateľov, uplatní akýkoľvek nárok proti objednávateľovi z titulu porušenia autorských práv tejto tretej osoby alebo akékoľvek iné nároky v akejkoľvek súvislosti so zmluvou, zhotoviteľ sa zaväzuje poskytnúť objednávateľovi akúkoľvek a všetku účinnú pomoc a uhradiť akékoľvek všetky náklady, ktoré vznikli/vzniknú objednávateľovi v súvislosti s uplatnením vyššie uvedeného nároku tretej osoby a nahradiť objednávateľovi akúkoľvek a všetku škodu, ktorá mu vznikne v dôsledku uplatnenia vyššie uvedeného nároku tretej osoby, a to v plnej výške a bez akéhokoľvek obmedzenia.
10. Zhotoviteľ prehlasuje v mene svojom a v mene tretích osôb (ak budú poverené zhotovením diela/alebo jeho časti v zmysle ods. 7 tohto článku zmluvy), že po celú dobu trvania majetkových práv k autorskému dielu si nebude uplatňovať autorské práva.
11. Zmluvné strany sa dohodli, že Objednávateľ je oprávnený udeliť tretej osobe súhlas na použitie diela v rozsahu licencie (sublicencia) a/alebo je oprávnený licenciu zmluvou postúpiť. O postúpení Licencie a o osobe postupníka je Nadobúdateľ povinný informovať autora bez zbytočného odkladu.
12. Zmluvné strany sa dohodli, že v prípade zániku objednávateľa, prechádzajú všetky práva v zmysle tohto článku zmluvy na právneho nástupcu objednávateľa.
13. Zaplatením ceny za predmet zmluvy podľa článku IV. tejto zmluvy výhradná licencia v zmysle tohto článku zmluvy prechádza na objednávateľa bez ďalších finančných nárokov zhotoviteľa.

Článok VI. ZMLUVNÉ POKUTY A ÚROKY Z OMEŠKANIA

1. V prípade omeškania zhotoviteľa so zhotovením diela riadne a včas má objednávatel' nárok na zmluvnú pokutu vo výške 0,5 % z ceny diela uvedenej v článku IV. ods. 1 tejto zmluvy, a v prípade, ak je zhotoviteľ osobou registrovanou pre daň z pridanej hodnoty, aj s DPH, za každý aj začatý deň omeškania.
2. V prípade omeškania objednávatel'a so splnením povinností uhradiť faktúru v termíne splatnosti, má zhotoviteľ nárok na úrok z omeškania maximálne vo výške určenej nariadením vlády č. 21/2013 Z. z., ktorým sa vykonávajú niektoré ustanovenia Obchodného zákonníka v znení nariadenia vlády č. 303/2014 Z. z.
3. V prípade porušenia ktorejkoľvek z povinností zhotoviteľa podľa tejto zmluvy zakladajúcej právo objednávatel'a na odstúpenie od tejto zmluvy má objednávatel' právo na zaplatenie zmluvnej pokuty vo výške 10 % z celkovej ceny podľa článku IV. ods. 1 zmluvy, a v prípade, ak je zhotoviteľ osobou registrovanou pre daň z pridanej hodnoty, aj s DPH. Toto právo má objednávatel' bez ohľadu na to, či od zmluvy odstúpi alebo nie.

Článok VII. UKONČENIE ZMLUVY

1. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť písomnou dohodou zmluvných strán ku dňu v nej uvedenému, odstúpením od zmluvy alebo výpoveďou.
2. Od tejto zmluvy je možné odstúpiť v prípadoch uvedených v Obchodnom zákonníku, v tejto zmluve, alebo ak ktorákoľvek zo zmluvných strán podstatným spôsobom poruší povinnosť vyplývajúcu z tejto zmluvy. Odstúpenie je potrebné urobiť písomne a doručiť druhej zmluvnej strane, inak je neplatné. Objednávatel' má právo na náhradu škody a nákladov spôsobených odstúpením od zmluvy. Odstúpenie od zmluvy je účinné dňom nasledujúcim po dni doručenia druhej zmluvnej strane.
3. Objednávatel' má právo odstúpiť od zmluvy, ak
 - a) zhotoviteľ nebude vytvárať dielo v súlade s touto zmluvou alebo bude zanedbávať plnenie svojich zmluvných povinností spôsobom, ktorý vyvolá u objednávatel'a opodstatnenú obavu, že zhotoviteľ neplní účel tejto zmluvy a konanie zhotoviteľa bude preukázateľne v rozpore s pokynmi objednávatel'a,
 - b) nedodá dielo v lehote stanovenej v článku III ods. 1, alebo bez zjavných väd ani po uplynutí náhradnej lehoty podľa článku III ods. 3 tejto zmluvy,
 - c) v prípade porušenia ktorejkoľvek povinnosti zhotoviteľa podľa článku II a článku VIII tejto zmluvy.
 - d) nastanú dôvody uvedené v § 19 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov.
4. Túto zmluvu je možné ďalej ukončiť písomnou výpoveďou ktoroukoľvek zo zmluvných strán aj bez uvedenia dôvodu s 30 - dňovou výpovednou lehotou, ktorá začína plynúť prvým dňom nasledujúcim po dni, kedy bola doručená písomná výpoveď druhej zmluvnej strane.

5. Právo na odstúpenie od zmluvy podľa tohto článku nevznikne, pokiaľ povinná strana preukáže, že porušenie povinnosti bolo spôsobené prípadom vyššej moci.
6. Pod vyššou mocou sa rozumejú okolnosti, ktoré nastanú po uzatvorení zmluvy ako výsledok nepredvídateľných a zmluvnými stranami neovplyviteľných prekážok. V prípade, že takáto okolnosť bude brániť v plnení povinností podľa zmluvy zhotoviteľovi, alebo objednávateľovi, bude zmluvná strana dotknutá vyššou mocou zbavená zodpovednosti za čiastočné, alebo úplné nesplnenie záväzkov vyplývajúcich z tejto zmluvy primerane počas doby, po ktorú pôsobili tieto okolnosti. Ak sa plnenie zmluvy stane nemožným do 6 mesiacov od vyskytnutia sa vyššej moci, zmluvná strana, ktorá sa bude chcieť odvolať na vyššiu moc, požiada druhú zmluvnú stranu o úpravu zmluvy dodatkom. Ak nedôjde k dohode, bude mať zmluvná strana, ktorá sa odvolala na vyššiu moc, právo odstúpiť od zmluvy.

Článok VIII.

OSOBITNÉ USTANOVENIA

1. Na plnenie predmetu zmluvy môže zhotoviteľ využiť subdodávateľov. Zhotoviteľ je povinný pri uzatvorení zmluvy uviesť zoznam subdodávateľov, ktorý obsahuje údaje o všetkých známych subdodávateľoch zhotoviteľa v čase uzatvorenia tejto zmluvy a údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia. Zoznam subdodávateľov tvorí prílohu č. 3 k tejto zmluve a obsahuje okrem uvedených údajov podiel plnenia zo zmluvy v % a stručný opis časti zmluvy, ktorá bude predmetom subdodávky.
2. Zhotoviteľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi, ktorý je uvedený v prílohe č. 3 k tejto zmluve najneskôr do 5 pracovných dní odo dňa uskutočnenia tejto zmeny písomnou formou na adresu uvedenú v záhlaví zmluvy.
3. V prípade zmeny subdodávateľa je zhotoviteľ najneskôr tri (3) pracovné dni pred zmenou subdodávateľa povinný písomne oznámiť objednávateľovi údaje o navrhovanom novom subdodávateľovi a o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu a dátum narodenia, resp. identifikačné údaje podnikateľského subjektu. Navrhovaný subdodávateľ musí spĺňať podmienky účasti týkajúce sa osobného postavenia podľa § 32 zákona o verejnom obstarávaní a nesmú u neho existovať dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 a 8 zákona o verejnom obstarávaní. Zmena nového subdodávateľa sa vykoná zápisom o zmene prílohy dňom jej podpísania oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky; vzor zápisu o zmene prílohy k zmluve tvorí prílohu č. 4 k tejto zmluve; osobami oprávnenými konať vo veciach zmeny prílohy č. 3 k zmluve sú:
za zhotoviteľa: account manager
za objednávateľa: riaditeľ sekcie informatiky
4. Využitím subdodávateľov nie je dotknutá zodpovednosť zhotoviteľa za plnenie predmetu zmluvy.
5. Objednávateľ podpísaním tejto zmluvy akceptuje všetkých subdodávateľov zhotoviteľa, čo však zhotoviteľa nezbaňuje zodpovednosti za kvalitu plnenia zmluvy podľa všeobecne záväzných právnych predpisov a tejto zmluvy.

6. Pri plnení zmluvy treťou osobou (subdodávateľom) má zhotoviteľ zodpovednosť akoby plnil predmet zmluvy sám.
7. Zhotoviteľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu svojich identifikačných a kontaktných údajov.
8. Ak sa zhotoviteľ v súvislosti s plnením povinností podľa zmluvy dostane do súdneho konania s treťou osobou, alebo by takéto súdne konanie hrozilo, bezodkladne o tom vyrozumie objednávateľa. Objednávateľ bude povinný na požiadanie zhotoviteľa dať ihneď k dispozícii zhotoviteľovi všetky potrebné informácie a podklady. Táto povinnosť vznikne príslušným vyrozumiením. Uvedená povinnosť bude platiť recipročne aj pre zhotoviteľa, pokiaľ by sa do takéhoto konania dostal objednávateľ. Vzájomná podpora sa poskytne iba v prípadoch, ak nedošlo k porušeniu všeobecne záväzných právnych predpisov v súvislosti s plnením tejto zmluvy.
9. Zhotoviteľ je povinný bezodkladne písomne oznámiť objednávateľovi začatie akéhokoľvek súdneho, rozhodcovského, exekučného, konkurzného, reštrukturalizačného alebo obdobného konania, ktoré sa začalo proti nemu alebo ktoré sám inicioval v súvislosti s predmetom tejto zmluvy. Ďalej je povinný bezodkladne oznámiť objednávateľovi, ak niektorý z veriteľov zhotoviteľa podal proti nemu návrh na vyhlásenie konkurzu a návrh na povolenie reštrukturalizácie alebo vstup do likvidácie a jej ukončenie.
10. Zhotoviteľ vyhlasuje, že ku dňu uzavretia tejto zmluvy nie je závislou osobou voči objednávateľovi v zmysle § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov. Každú zmenu súvisiacu s personálnym, ekonomickým alebo iným prepojením voči objednávateľovi v súvislosti s ustanovením § 2 písm. n) zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov je zhotoviteľ povinný objednávateľovi písomne oznámiť a to do 5 dní odo dňa vzniku zmeny.

Článok IX

OCHRANA DÔVERNÝCH INFORMÁCIÍ A KYBERNETICKÁ BEZPEČNOSŤ

1. Zmluvné strany, ich zamestnanci ako aj ich subdodávatelia a ich zamestnanci sú povinní zachovávať v tajnosti všetky dôverné informácie, ktoré sú uvedené v tejto zmluve a v jej prílohách a/alebo ktoré budú uvedené v jej dodatkoch a prílohách, a/alebo ktoré im boli poskytnuté, alebo ktoré inak získali v súvislosti so zmluvou, alebo s ktorými sa oboznámili počas plnenia zmluvy, resp. ktoré súvisia s predmetom plnenia, s údajmi, ktoré podliehajú ochrane podľa zákona č. 18/2018 podľa 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 nariadenia o ochrane údajov) (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s údajmi získanými v rámci predzmluvných rokovaní, ktoré súvisia s touto zmluvou, s výnimkou nasledujúcich prípadov:
 - a) ak je poskytnutie informácie od dotknutej zmluvnej strany uložené na základe všeobecne záväzných právnych predpisov alebo na základe povinnosti uloženej postupom podľa všeobecne záväzných právnych predpisov (napr. 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,

- b) ak je informácia verejne dostupná z iného dôvodu, ako je porušenie povinnosti mlčanlivosti dotknutou zmluvnou stranou, informácie, ktoré už sú v deň podpísania zmluvy verejne známe, alebo ktoré je možné už v deň podpísania tejto zmluvy získať z bežne dostupných informačných prostriedkov,
 - c) ak sa jedná o informácie, ktoré sa stanú po podpísaní zmluvy verejne známymi, alebo ktoré možno po tomto dni získať z bežne dostupných informačných prostriedkov,
 - d) ak je informácia poskytnutá odborným poradcom dotknutej zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti, alebo ak sa voči dotknutej zmluvnej strane zaviazali povinnosťou mlčanlivosti,
 - e) ak je to potrebné pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutá zmluvná strana účastníkom,
 - f) ak je informácia poskytnutá so súhlasom druhej zmluvnej strany.
2. Zhotoviteľ ako sprostredkovateľ súčasne s touto zmluvou uzavrie s objednávatelom ako prevádzkovateľom sprostredkovateľskú zmluvu v zmysle článku 28 Nariadenia Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR) a/alebo podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení, ktorá tvorí prílohu č. 5 k tejto zmluve.
 3. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany nevyužijú pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám. Za tretie osoby sa nepokladajú členovia orgánov zmluvných strán, subdodávateľa, audítori alebo právni poradcovia zmluvných strán, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.
 4. Zmluvné strany, subdodávateľa a ich zamestnanci sa zaväzujú, že všetky zúčastnené osoby a subjekty budú s poskytnutými informáciami a zistenými skutočnosťami nakladať ako s dôvernými informáciami.
 5. Zhotoviteľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov realizujúcich predmet plnenia zmluvy dodržiavanie:
 - a) povinnosti ochrany dôverných informácií a záväzku mlčanlivosti o údajoch, s ktorými počas plnenia predmetu zmluvy pre objednávatel'a prišli do styku, a to aj po ukončení pracovného, resp. služobného pomeru,
 - b) zákazu využitia dôverných informácií, s ktorými prišli do styku pre osobnú potrebu, zákazu ich zverejnenia, poskytnutia a sprístupnenia s výnimkou orgánov činných v trestnom konaní.
 6. Požiadavka v bode 5. tohto článku zmluvy bude zabezpečená podpísaním vyhlásenia o mlčanlivosti zo strany príslušného zamestnanca.
 7. Všetky podklady s dôvernými informáciami poskytnuté zhotoviteľovi a evidované údaje musia byť po ukončení obchodných vzťahov bez vyzvania odovzdané objednávatel'ovi alebo podľa jeho rozhodnutia vymazané alebo skartované. Táto povinnosť sa vzťahuje

- aj na vyhotovené kópie. Toto ustanovenie neplatí v prípade vzájomných zmlúv a projektovej dokumentácie medzi zmluvnými stranami, ktoré ale nesmú byť bez súhlasu objednávateľa sprístupnené tretej osobe inak, ako to dovoľuje táto zmluva.
8. Zhotoviteľ sa zaväzuje, že sa v žiadnom prípade bez vedomia objednávateľa nepokúsi získať prístup k informáciám, ktoré:
 - a) sú prenášané na poskytovanej infraštruktúre a sú súčasťou prenášaných údajov,
 - b) nie sú pre neho potrebné na výkon poskytovanej služby a ani ich žiadnym spôsobom nezneužíje v prípade, ak sa k nim neoprávnene dostane.
 9. Zmluvné strany sa zaväzujú, že budú ochraňovať dôverné informácie druhej zmluvnej strany s rovnakou starostlivosťou, ako ochraňujú vlastné dôverné informácie rovnakého druhu, vždy však najmenej v rozsahu primeranej odbornej starostlivosti.
 10. Ustanovenia predchádzajúcich bodov budú platiť aj po dobe platnosti a účinnosti zmluvy, a to až do doby, kedy sa informácie stanú verejne známymi.
 11. Zhotoviteľ súčasne s touto zmluvou uzavrie ako tretia osoba s Objednávatelom ako prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorá zmluva tvorí prílohu č. 6 k tejto zmluve.

Článok X.

ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Zhotoviteľ berie na vedomie povinnosť objednávateľa zverejniť túto zmluvu ako aj faktúru vyplývajúcu z tejto zmluvy a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy vrátane jej príloh v plnom rozsahu.
2. Táto zmluva sa uzatvára na dobu určitú, a to odo dňa jej účinnosti do riadneho a úplného splnenia záväzkov z nej vyplývajúcich.
3. Táto zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jej zverejnenia v registri.
4. Zmluvu je možné meniť a dopĺňať iba písomnými a číslovanými dodatkami podpísanými obidvomi zmluvnými stranami, ktoré budú jej neoddeliteľnou súčasťou. Písomná zmena špecialistu a subdodávateľa zhotoviteľa podľa článku III. ods. 12 a článku VIII. ods. 3 zmluvy sa vykoná zápisom o zmene prílohy k zmluve, ak nebude v rozpore s ustanovením § 18 zákona o verejnom obstarávaní a európskou legislatívou.
5. Skončením zmluvy zanikajú všetky práva a povinnosti zmluvných strán vyplývajúce zo zmluvy s výnimkou ustanovení, ktoré sa týkajú nároku na náhradu škody vzniknutej porušením tejto zmluvy, nároku na zaplatenie zmluvnej pokuty podľa ustanovení tejto zmluvy a ďalej ustanovení tejto zmluvy, ktoré vzhľadom na svoju povahu majú trvať aj po ukončení zmluvy, napr. záruka, dôvernosť informácií a mlčanlivosť.
6. Právne vzťahy zmluvných strán súvisiace s touto zmluvou a v tejto zmluve bližšie neupravené, sa riadia príslušnými ustanoveniami Obchodného zákonníka, Autorského zákona a ďalšími všeobecne záväznými právnymi predpismi platnými a účinnými v Slovenskej republike a súťažnými podmienkami.
7. V prípade, ak je alebo sa stane niektoré ustanovenie tejto zmluvy neplatné, neúčinné

- alebo nevykonateľné nebude tým dotknutá platnosť, účinnosť, alebo vykonateľnosť ostatného obsahu tejto zmluvy. Predmetné ustanovenie sa nahradí platným ustanovením, ktoré sa čo najviac blíži zamýšľanému účelu, sledovanému zmluvnými stranami. To isté platí aj pre prípad zmluvnej medzery.
8. Spory týkajúce sa tejto zmluvy sa zmluvné strany zaväzujú riešiť prednostne dohodou a vzájomným rokovaním. Ak dohoda nie je možná, pre riešenie sporov z tejto zmluvy sú príslušné všeobecné sudy Slovenskej republiky.
 9. V prípade rozhodnutia zhotoviteľa o zlúčení, splynutí, rozdelení spoločnosti, predaja podniku alebo jeho časti, začatia konkurzného konania alebo reštrukturalizačného konania, vyhlásenia konkurzu alebo reštrukturalizácie na majetok zhotoviteľa, jeho vstupe do likvidácie, je zhotoviteľ povinný preukázateľne oznámiť objednávateľovi uskutočnenie takejto zmeny, a to do 10 kalendárnych dní odo dňa jej účinnosti, inak zodpovedá za všetky škody z toho vyplývajúce.
 10. Táto zmluva je vyhotovená v štyroch identických rovnopisoch, z ktorých každý má platnosť originálu. Každá zmluvná strana obdrží po dva rovnopisy.
 11. Zmluvné strany vyhlasujú, že ich vôľa vyjadrená v tejto zmluve je slobodná a vážna, túto zmluvu neuzatvárajú v tiesni, za nápadne nevýhodných podmienok a ich zmluvná vôľnosť nie je inak obmedzená. Svoju vôľu byť viazané touto zmluvou zmluvné strany bez výhrad vyjadrujú svojimi podpismi.
 12. Neoddeliteľnou súčasťou tejto zmluvy je:
 - Príloha č. 1 - Opis predmetu zmluvy
 - Príloha č. 2 - Zoznam špecialistov
 - príloha č. 3 - Zoznam subdodávateľov
 - Príloha č. 4 - Vzor zápisu o zmene prílohy
 - Príloha č. 5 - Sprostredkovateľská zmluva
 - Príloha č. 6 - Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Za objednávateľa:

Za zhotoviteľa:

V Bratislave, dňa

V Bratislave, dňa

.....
Ing. Michal Ilko
generálny riaditeľ
Sociálnej poisťovne

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

OPIS PREDMETU ZMLUVY

Predmetom zmluvy je implementovanie dizajnu a konfigurácia RedHat Identity Management RH IdM za účelom kontroly autentifikácie a autorizácie Linux prostredia v Sociálnej poisťovni.

Rozsah plnenia:**Dizajn a konfigurácia RedHat idM**

Obsah prác	Predpokladaný počet človekodní
Analýza existujúceho prostredia objednávateľa a identifikácia optimálneho nasadenia RedHat Identity Management.	7
Vypracovanie low level dizajn dokumentu pre RedHat Identity Management, musí definovať minimálne všetky sieťové toky, integrácia s AD, rozdelenie a práva užívateľov, zabezpečenie riešenia, princípy nasadenia a správy, prvotné nastavenia - konfigurácie, architektúru redundantného riešenia, prvky riešenia s detailmi o zapojení, sudoers práva.	6
Konfigurácia a implementácia RedHat Identity Management do DEV-Test prostredia, integrácia s RedHat Linux servermi a CentOS.	6
Zaškolenie interných administrátorov do RedHat Identity Management užívateľskej dokumentácie poskytovanej výrobcom.	6

Súčasťou plnenia je aj dodanie dokumentácie na adresu Sociálna poisťovňa, ústredie, Ul. 29. augusta 8 a 10, 813 63 Bratislava.

ZOZNAM ŠPECIALISTOV

Pozícia špecialistu	Meno a priezvisko špecialistu
Špecialista č. 1 RedHat Identity Managment	

V Bratislave, dňa

Za zhotoviteľa:

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

ZOZNAM SUBDODÁVATEĽOV

Alanata a.s.
Krasovského 14
851 01 Bratislava – mestská časť
Petržalka
IČO: 54 629 331

Na uskutočnení plnenia zmluvy o dielo na *Dizajn a konfiguráciu Identity Management* č. 31985-7/2023-BA:

a) sa nebudú podieľať subdodávatelia a celý predmet zmluvy o dielo uskutočníme vlastnými kapacitami.*

~~b) sa budú podieľať nasledovní subdodávatelia:*~~

P. č.	Meno a priezvisko alebo obchodné meno alebo názov subdodávateľa. Adresa sídla alebo miesta podnikania subdodávateľa.	IČO	Meno a priezvisko, adresa pobytu a dátum narodenia osoby oprávnenej konať za subdodávateľa	Podiel plnenia zo zmluvy o dielo v %	Predmet subdodávok
1.					
2.					
3.					

V Bratislave, dňa

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

*Nehodiace sa prečiarknite

(VZOR)

Z Á P I S

o zmene prílohy č. X

k Zmluve o dielo

č. 31985-7/2023BA:

uzatvorenej podľa § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka
v znení neskorších predpisov
(ďalej len „zmluva“) medzi:

Zhotoviteľom **Alanata a.s.**, Krasovského 14, 851 01 Bratislava – mestská časť
Petržalka, IČO: 54 629 331 (ďalej len „zhotoviteľ“)

a

objednávateľom **Sociálna poisťovňa, Ul. 29. augusta 8 a 10, 813 63 Bratislava,**
IČO: 30807484 (ďalej len „objednávateľ“)

V súlade s čl. odsek ... zmluvy, v ktorom sa zmluvné strany dohodli o spôsobe zmeny prílohy č. X k zmluve, zmluvné strany v zastúpení ich oprávnenými zástupcami podpisujú tento zápis, ktorým sa mení príloha č. X k zmluve „Zoznam“, ktorá tvorí prílohu k tomuto zápisu.

Dôvod potreby uskutočnenia zmeny prílohy č. X k zmluve „Zoznam“:

.....
.....
.....

Tento zápis je neoddeliteľnou súčasťou zmluvy.

Tento zápis nadobúda platnosť dňom jeho podpísania oprávnenými zástupcami oboch zmluvných strán a účinnosť dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.

Nadobudnutím účinnosti tohto zápisu sa v celom rozsahu mení znenie prílohy č. X k zmluve „Zoznam“.

....., dňa

Bratislava, dňa

Za zhotoviteľa:

Za objednávateľa:

.....

.....

oprávnená osoba

riaditeľ sekcie informatiky

Príloha:

Príloha č. X k zmluve – „Zoznam“

Sprostredkovateľská zmluva č. 31985-8/2023-BA

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

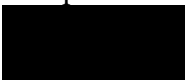
Prevádzkovateľ

Názov:	Sociálna poisťovňa
Sídlo:	Ulica 29. augusta 8 a 10 813 63 Bratislava
Štatutárny orgán:	Ing. Michal Ilko 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:	Alanata a.s.
Sídlo:	Krasovského 14 851 01 Bratislava – mestská časť Petržalka
Štatutárny orgán:	Ing. Andrej Bališ člen predstavenstva
Bankové spojenie:	
IBAN:	
IČO:	54 629 331
DIČ:	2121747573
IČ DPH:	SK2121747573

Zapísaný v Obchodnom registri Mestského súdu III, oddiel Sa, vložka č. 7425/B

(ďalej len „sprostredkovateľ“)

(spolu ďalej ako „zmluvné strany“)

Preambula

Zmluvné strany spolu uzatvárajú Zmluvu o dielo č. 31985-7/2023-BA uzatvorenú podľa § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov, predmetom ktorej je predovšetkým Dizajn a konfigurácia Identity Management (ďalej len „zmluva o dielo“).

Sprostredkovateľ vystupuje v tejto zmluve ako zhotoviteľ, 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 je identifikovaná, alebo identifikovateľná fyzická osoba, ktorej sa spracúvané osobné údaje týkajú:

- a) 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. Predmetom tejto zmluvy je poverenie sprostredkovateľa na spracovanie osobných údajov dotknutých osôb v mene prevádzkovateľa a podľa pokynov prevádzkovateľa v rozsahu osobných údajov, spracúvanie ktorých je potrebné pre plnenie účelu zmluvy o dielo.
2. Sprostredkovateľ je oprávnený spracúvať osobné údaje po splnení povinností uvedených v tejto zmluve.
3. Účel spracúvania osobných údajov je vymedzený v zákone č. 461/2003 Z. z. o sociálnom poistení, v Nariadení (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, v Nariadení (ES) Európskeho parlamentu a Rady č. 987/2009, ktorým sa stanovuje postup vykonávania nariadenia (ES) č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, podľa ktorých je prevádzkovateľ oprávnený spracúvať osobné údaje dotknutých osôb za účelom výkonu sociálneho poistenia.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje výhradne pre poskytovanie služieb prevádzkovateľovi, a to na základe pokynov prevádzkovateľa podľa podmienok stanovených v tejto zmluve v súlade so všeobecne záväznými právnymi predpismi upravujúcimi ochranu a spracúvanie osobných údajov. Za pokyny prevádzkovateľa sa považujú pokyny uvedené v tejto zmluve, v servisnej zmluve, prípadne iné písomne zdokumentované pokyny alebo požiadavky prevádzkovateľa na poskytnutie služby v zmysle servisnej zmluvy.
5. Sprostredkovateľ je oprávnený spracúvať osobné údaje, s ktorými príde do styku v súvislosti s realizáciou zmluvy o dielo a to na účel:
 - Účelom spracúvania osobných údajov zhotoviteľom je Dizajn a konfigurácia Identity Management.
6. Zmluvné strany prehlasujú, že právnym základom spracúvania osobných údajov v rozsahu zmluvy o dielo je splnenie zákonnej povinnosti podľa čl. 6 ods. 1 písm. c) GDPR, pričom konkrétnu zákonnú povinnosť ustanovuje zmluva o dielo osobitne a § 78 ods. 3 ZOOU.

Čl. III

Zoznam osobných údajov a okruh dotknutých osôb

1. Zmluva, v rámci plnenia predmetu ktorej je sprostredkovateľ poverený spracúvať osobné údaje klientov prevádzkovateľa:

Zmluva o dielo uzatvorená podľa § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov (ev. č. zmluvy 31985-7/2023-BA).
2. Zoznam osobných údajov, ktoré môžu byť realizácii predmetu zmluvy o dielo predmetom spracúvania:

Sprostredkovateľ je oprávnený spracúvať osobné údaje v rozsahu najmä meno, priezvisko, titul, telefón a emailová adresa dotknutých osôb a iné údaje spracované v informačných systémoch prevádzkovateľa v rozsahu, aký je nevyhnutný na plnenie predmetu zmluvy č. 31985-7/2023-BA o dielo.

3. Spracúvané osobné údaje sú povahy:

Iné osobné údaje v rozsahu bodu 2 tohto článku.

4. Spracúvané osobné údaje sú typu:

adresné, zamestnanecké, ekonomické, sociálne, elektronické.

Čl. IV

Spôsob výkonu a oprávnenia sprostredkovateľa

1. Osobné údaje o dotknutých osobách prevádzkovateľ spracúva v súlade so zákonom o sociálnom poistení, s Nariadením (ES) Európskeho parlamentu a Rady č. 883/2004 o koordinácii systémov sociálneho zabezpečenia, s Nariadením (ES) Európskeho parlamentu a Rady č. 987/2009 za účelom výkonu sociálneho poistenia a vedenia ekonomickej, prevádzkovej, personálnej a mzdovej agendy Sociálnej poisťovne.
2. Na spracúvanie osobných údajov sprostredkovateľom sa v zmysle § 34 ods. 1 ZOOU nevyžaduje súhlas dotknutej osoby.
3. Sprostredkovateľ má v rámci spracúvania osobných údajov podľa tejto zmluvy povolené operácie s osobnými údajmi v rozsahu najmä:
 - a) zaznamenávanie
 - b) usporadúvanie,
 - c) štruktúrovanie,
 - d) uchovávanie,
 - e) zmena,
 - f) vyhľadávanie,
 - g) prehľadávanie,
 - h) vymazanie alebo likvidácia,
 - i) zálohovanie,
 - j) poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom.
4. Sprostredkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb po dobu trvania účelu spracúvania, resp. po dobu platnosti a účinnosti zmluvy o dielo a po dobu platnosti a účinnosti tejto zmluvy.

Čl. V

Vyhlásenie prevádzkovateľa

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

Čl. VI

Vyhlásenie sprostredkovateľa

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

Čl. VII

Povinnosti sprostredkovateľa

1. Sprostredkovateľ sa pri spracúvaní osobných údajov podľa tejto zmluvy zaväzuje najmä:
 - a) postupovať s náležitou starostlivosťou a v súlade s GDPR, ZOOU a súvisiacimi všeobecne záväznými právnymi predpismi Slovenskej republiky, dodržiavať povinnosti vyplývajúce z tejto zmluvy a pokynov prevádzkovateľa, a dodržiavať zásady ochrany osobných údajov zverejnené Prevádzkovateľom,
 - b) akékoľvek spracúvanie osobných údajov vykonávať len za účelom plnenia predmetu tejto zmluvy a servisnej zmluvy a len v rozsahu nevyhnutnom na jej plnenie,
 - c) údaje dotknutých osôb nezverejňovať, nešíriť či neodovzdávať ďalším osobám,

- d) zaistiť, aby jeho zamestnanci a ďalšie osoby, ktoré využije na plnenie podľa tejto zmluvy, dodržiavali podmienky stanovené GDPR, vnútroštátnymi predpismi a touto zmluvou a boli pred spracúvaním osobných údajov poučené o zásadách spracúvania osobných údajov a o zachovaní mlčanlivosti,
- e) ak všeobecne záväzné právne predpisy neustanovujú inak, osobné údaje, s ktorými sa dostal do styku v súvislosti s realizáciou zmluvy o dielo nezverejňovať, neposkytovať a nesprístupňovať tretím stranám,
- f) zachovávať mlčanlivosť a zabezpečiť diskretnosť pri akomkoľvek spracúvaní osobných údajov,
- g) ak zmluva alebo všeobecne záväzný právny predpis neustanovuje inak, nevyhotovovať kópie akýchkoľvek nosičov obsahujúcich osobné údaje a ani z nich nevyhotovovať výpisy alebo odpisy, ktoré by obsahovali osobné údaje,
- h) ak všeobecne záväzné právne predpisy upravujúce problematiku archívov a registratúr neustanovujú inak, bezodkladne odovzdávať prevádzkovateľovi všetky získané materiály obsahujúce osobné údaje, ktoré už pre realizáciu zmluvy nepotrebuje, resp. všetky osobné údaje, ktoré bude spracúvať v súvislosti s plnením zmluvy o dielo, 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) nepoužiť spracúvané osobné údaje v mene prevádzkovateľa pre vlastnú potrebu, pokiaľ všeobecne záväzné platné právne predpisy neustanovujú inak,
 - p) zabrániť neoprávneným osobám v prístupe k osobným údajom a k prostriedkom na ich spracovanie, zabrániť neoprávnenému čítaniu, vytváraniu, kopírovaniu, prenosu, úprave či vymazaniu záznamov obsahujúcich osobné údaje a zabezpečiť opatrenia, ktoré umožnia určiť a overiť, komu/kým a akým spôsobom boli osobné údaje odovzdané, resp. kým boli prevzaté a spracúvané.
2. Sprostredkovateľ je pri spracúvaní osobných údajov podľa tejto zmluvy ďalej povinný bezodkladne informovať prevádzkovateľa o
- a) poskytnutí a sprístupnení osobných údajov tretej strane spolu s odôvodnením a určením všeobecne záväzného právneho predpisu, ktorý sprostredkovateľovi ukladá povinnosť poskytnúť, sprístupniť alebo zverejniť osobné údaje dotknutých osôb spracúvaných v mene prevádzkovateľa,
 - b) skutočnostiach zabraňujúcich plneniu povinností podľa tejto zmluvy,
 - c) akomkoľvek porušení povinností podľa zmluvy alebo porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov,
 - d) akomkoľvek porušení ochrany osobných údajov,
 - e) akomkoľvek porušení všeobecne záväzných právnych predpisov upravujúcich ochranu a spracúvanie osobných údajov zo strany prevádzkovateľa, ak sa podľa názoru sprostredkovateľa pokynom prevádzkovateľa tieto predpisy porušujú.
3. V prípade, ak sprostredkovateľ obdržal žiadosť dotknutej osoby, ktorá si uplatňuje voči prevádzkovateľovi svoje práva podľa článkov 15 až 22 GDPR a § 21 až § 28 ZOOU (napr. právo na prístup k údajom, právo na výmaz alebo opravu osobných údajov), je povinný bezodkladne, najneskôr však do troch pracovných dní od jej prijatia, takúto žiadosť zaslať prevádzkovateľovi prostredníctvom emailovej adresy: zodpovedna.osoba@socpoist.sk, spolu so žiadosťou je sprostredkovateľ povinný prevádzkovateľovi zaslať aj ďalšie relevantné informácie týkajúce sa predmetnej žiadosti, ktoré by mohli mať vplyv na postup vybavenia žiadosti dotknutej osoby zo strany prevádzkovateľa.
4. Sprostredkovateľ je povinný pomáhať prevádzkovateľovi pri zabezpečení plnenia povinností prevádzkovateľa v oblasti bezpečnosti spracúvania, zisťovania porušení ochrany osobných údajov, posudzovania vplyvu na ochranu osobných údajov a poskytovať informácie, ktoré sú mu dostupné.
5. Sprostredkovateľ je povinný dôsledne chrániť spracúvané osobné údaje podľa svojho najlepšieho vedomia, v súlade s ustanoveniami GDPR a ZOOU.
6. Oprávnené osoby sprostredkovateľa resp. subdodávateľa, ktoré budú mať prístup k osobným údajom sú viazaní povinnosťou mlčanlivosti o týchto údajoch a to aj po zániku štátnozamestnaneckého pomeru, pracovného pomeru uzatvoreného v súlade so zákonníkom práce resp. v súlade so zákonom o výkone práce vo verejnom záujme alebo dohody o práci vykonávanej mimo pracovného pomeru v súlade so zákonníkom práce.

7. Oprávnené osoby sprostredkovateľa sú oboznámené so spôsobom oznamovania podozrení z bezpečnostných incidentov v súvislosti s informačným systémom a spracúvanými osobnými údajmi. Oprávnené osoby sprostredkovateľa sú poučené, aby bezodkladne oznamovali určenej osobe prevádzkovateľa akékoľvek podozrenie z bezpečnostného incidentu, ktoré by mohlo mať dopad na bezpečnosť informačného systému s osobnými údajmi. Sprostredkovateľ je povinný bezodkladne prijať relevantné opatrenia k náprave, o bezpečnostnom incidente informovať zodpovednú osobu prevádzkovateľa a e-mailom na adresu: zodpovedna.osoba@socpoist.sk.
8. Sprostredkovateľ je povinný spracovať a dokumentovať prijaté a vykonané technicko-organizačné opatrenia na zaistenie ochrany osobných údajov v súlade s právnymi predpismi EÚ a Slovenskej republiky, k tomu sa vzťahujúcimi. Sprostredkovateľ je povinný spolupracovať s Prevádzkovateľom a byť mu nápomocný pri zaistovaní plnenia jeho povinností pri prevencii rizík a ďalších povinností Prevádzkovateľa podľa ustanovení čl. 32 – 36 GDPR. K vyžiadaniu Prevádzkovateľa je mu nápomocný technickými a organizačnými prostriedkami pri plnení povinností Prevádzkovateľa reagovať na žiadosti o výkon práv Dotknutej osoby stanovených v kapitole III. GDPR (informácie a prístup k osobným údajom, oprava a výmaz, právo na obmedzenie spracovania atď.).
9. Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na doloženie toho, že boli splnené povinnosti sprostredkovateľa a stanovené ustanoveniami GDPR a umožní audity, vrátane inšpekcií, vykonávané prevádzkovateľom alebo iným audítorom, ktorého prevádzkovateľ poveril. Pri vykonávaní auditov bude spolupracovať s prevádzkovateľom alebo ním určeným audítorom. Prevádzkovateľ je oprávnený vykonať inšpekciu plnenia povinností sprostredkovateľa a audit bez predchádzajúceho upozornenia. Nespolupráca sprostredkovateľa bude považovaná za podstatné porušenie tejto Zmluvy s možnosťou odstúpenia zo strany prevádzkovateľa, resp. vyvodením zodpovednosti za prípadnú škodu.
10. Po ukončení poskytovania služieb spojených so spracovaním sprostredkovateľ v súlade s rozhodnutím prevádzkovateľa všetky osobné údaje buď vymaže, alebo ich vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo členského štátu nepožaduje uloženie daných osobných údajov. Dojednáva sa, že takýto pokyn bude sprostredkovateľovi daný písomne.
11. Ak sprostredkovateľ poruší GDPR a túto zmluvu tým, že bez pokynu prevádzkovateľa sám určí účely a prostriedky spracovania osobných údajov, stane sa vo vzťahu k týmto údajom a ich spracovaniu prevádzkovateľom so všetkými dôsledkami z toho vyplývajúcimi.

Čl. VIII

Podmienky spracúvania osobných údajov

1. Sprostredkovateľ vyhlasuje, že spracúvanie osobných údajov bude vykonávať sám. Prevádzkovateľ so spracúvaním osobných údajov uvedenými subdodávateľmi súhlasí. Subdodávatelia budú spracúvať osobné údaje na zodpovednosť sprostredkovateľa v rozsahu a za podmienok stanovených v tejto zmluve. Sprostredkovateľ nezapojí do spracovania žiadneho ďalšieho sprostredkovateľa bez predchádzajúceho konkrétneho

písomného súhlasu prevádzkovateľa. Náležitosti žiadosti o poskytnutie súhlasu sú uvedené v bode 3 tohto článku zmluvy.

2. 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.
3. 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.
4. 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.
5. 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.
6. Sprostredkovateľ je povinný oznámiť prevádzkovateľovi ukončenie spracúvania osobných údajov dotknutých osôb prostredníctvom subdodávateľa, a to bezodkladne, najneskôr však do piatich pracovných dní od ukončenia takehoto spracúvania. Toto oznámenie musí o. i.

obsahovať aj popis spôsobu splnenia povinnosti sprostredkovateľa vo vzťahu k tomuto subdodávateľovi.

Čl. IX

Ostatné dohodnuté podmienky

1. Sprostredkovateľ postupuje pri spracúvaní osobných údajov podľa GDPR a podľa ZOOU.
2. Sprostredkovateľ sa zaväzuje nahradiť prevádzkovateľovi v plnom rozsahu všetky škody, ktoré mu vzniknú v súvislosti s nedodržaním tejto zmluvy zo strany sprostredkovateľa a ktorá prevádzkovateľovi vznikne porušením alebo nesplnením povinností subdodávateľa sprostredkovateľa pri spracúvaní a ochrane osobných údajov vyplývajúcich z ustanovení zmluvy a všeobecne záväzných právnych predpisov.
3. Ochrana osobných údajov podľa zmluvy trvá aj po ukončení zmluvného vzťahu založeného touto zmluvou a zaväzuje aj právnych nástupcov zmluvných strán. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá prevádzkovateľovi vznikla porušením povinností sprostredkovateľa.
4. Sprostredkovateľ je poverený spracúvať osobné údaje po dobu platnosti tejto zmluvy. Okamihom skončenia jej platnosti už sprostredkovateľ nesmie disponovať žiadnymi osobnými údajmi. Sprostredkovateľ je povinný vymazať osobné údaje alebo vrátiť prevádzkovateľovi osobné údaje, v prípade že ich spracovával, po ukončení poskytovania služieb týkajúcich sa plnenia zmluvy o dielo 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: [REDACTED].
6. Kontakt na zástupcu sprostredkovateľa: [REDACTED].

Čl. X

Záverečné ustanovenia

1. Táto zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a zákona č. 546/2010 Z. z., ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Sprostredkovateľ berie na vedomie povinnosť prevádzkovateľa zverejniť túto zmluvu a svojim podpisom dáva súhlas na zverejnenie tejto zmluvy v plnom rozsahu.
2. Táto zmluva nadobúda platnosť podpisom oprávnených zástupcov zmluvných strán a účinnosť dňom nasledujúcim deň po dni zverejnenia v Centrálnom registri zmlúv vedenom na Úrade vlády Slovenskej republiky.
3. Táto zmluva sa uzatvára na dobu určitú, po dobu platnosti a účinnosti zmluvy o dielo.
4. Počas platnosti zmluvy o dielo 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 Ilko
generálny riaditeľ
Sociálnej poisťovne

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

Zmluva č. 31985-9/2023-BA

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 Ilko, 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:

Sídlo:	Alanata a. s. Krasovského 14 851 01 Bratislava – mestská časť Petržalka
Štatutárny orgán:	Ing. Andrej Bališ člen predstavenstva
Zápis v registri:	Obchodný register Mestského súdu III, oddiel Sa, vložka č. 7425/B
IČO:	54 629 331
DIČ:	2121747573
IČ pre DPH:	SK2121747573
Bankové spojenie:	
IBAN:	

(ďalej len „dodávateľ“)

(spolu ďalej ako „zmluvné strany“)

Čl. II

Preambula

1. Prevádzkovateľ je podľa § 3 písm. l) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“) prevádzkovateľom základnej služby podľa § 3 písm. k) body 2 a 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej

bezpečnosti dodávateľom, ktorý na základe zmluvy o dielo poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.

2. Zmluvné strany spolu uzatvárajú Zmluvu o dielo č. 31985/2023-BA podľa § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov, predmetom ktorej je predovšetkým Dizajn a konfigurácia RedHat Identity Management (ďalej len „zmluva o dielo“).
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 o dielo.
2. Výkon činností, ktoré priamo súvisia s realizáciou zmluvy na výkon činnosti.

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 o dielo 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 činnosti (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 o dielo 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 o dielo. 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 o dielo. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy počas celej doby trvania zmluvy o dielo.
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 o dielo 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 o dielo 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 bode 3.1.5 bezpečnostnej politiky

prevádzkovateľa, ktorá tvorí prílohu č. 1 k tejto zmluve, 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, ohrozením 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 Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“), 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 skutočnosti, 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 o dielo a tejto zmluvy a ktoré nie sú verejne známe,

pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí.

2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávateľia a ich zamestnanci, ako aj prípadná tretia osoba a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.

Čl. IX

Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov na základe zákona o kybernetickej bezpečnosti a tejto zmluvy.
2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
3. Prevádzkovateľ môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti prevádzkovateľa pri výkone auditu realizuje prevádzkovateľom poverená tretia osoba.
4. Dodávateľ je pri audite povinný spolupracovať s prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto zmluvy.
6. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u dodávateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti dodávateľa za plnenie jeho povinností vyplývajúcich z tejto zmluvy.
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 MIRRI, ak boli vydané, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenia kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí tak, aby nebola narušená ich dostupnosť, dôvernosť, 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: Manažér bezpečnosti
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: [REDACTED]
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je: [REDACTED].
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 zmluvy o dielo definovanej v článku II - Zmluva o dielo č. 31985-7/2023-BA, podľa § 536 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov, predmetom ktorej je predovšetkým Dizajn a konfigurácia RedHat Identity Management.
4. Počas platnosti a účinnosti zmluvy o dielo 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,
Príloha č. 2 – Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni.
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 Ilko
generálny riaditeľ
Sociálnej poisťovne

.....
Ing. Andrej Bališ
člen predstavenstva
Alanata 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 poučený a zmluvne zaviazaný neporušiť pravidlá na zabezpečenie ochrany, odcudzenia alebo vyzradenia chránených údajov.
- (5) Fyzická bezpečnosť musí byť odkontrolovaná na mieste výkonu práce. Kontrolu zabezpečí dodávateľom určený zamestnanec, o čom sa vyhotoví záznam, pričom prevádzkovateľ si vyhradzuje právo kontroly priestorov dodávateľa, resp. jeho subdodávateľa, alebo tretej osoby, z ktorých sa práca na diaľku uskutočňuje.
- (6) Žiadosť o zriadenie vzdialeného prístupu pre zamestnanca dodávateľa, resp. jeho subdodávateľa, alebo tretiu osobu postúpi príslušný zmluvný kontakt prevádzkovateľa oddeleniu centrálného 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 o dielo s dodávateľom musia pokrývať všetky významné bezpečnostné požiadavky. Zmluvy o dielo 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 o dielo 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 o dielo 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 o dielo pre zaistenie kybernetickej bezpečnosti.

(4) Nie je prípustné v zmluve o dielo špecifikovať bližšie neurčených subdodávateľov alebo tretiu osobu a tým následne zriaďovať prístup pre zamestnancov subdodávateľa alebo

tretiu osobu.

3.1.3 Monitorovanie a preskúmanie dodávateľských služieb

(1) Služby a záznamy poskytované dodávateľom sú priebežne kontrolované osobou zodpovednou za výkon zmluvy o dielo, 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 [REDACTED] a,
- b) e-mailom oddeleniu centrálnemu dispečingu a monitorovania služieb IS SP na adresu [REDACTED] 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 centrálnemu dispečingu a monitorovania služieb IS SP na adresu [REDACTED].

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 poisťovcom, 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 poisťencovi prevádzkovateľa,
- i) podvod, sprenevera,
- j) preukázané použitie násilia alebo hrozby bezprostredného násilia v úmysle zmocniť sa aktív prevádzkovateľa.

(3) V oblasti informačnej bezpečnosti prevádzkovateľa

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

- t) spracúvanie osobných údajov inou ako oprávnenou osobou,
- u) porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,
- v) porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

3.1.7 Poučenie a záväzok mlčanlivosti

(1) Vstupné poučenie o ochrane osobných údajov musí absolvovať každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba pri nástupe na výkon zmluvných činností na základe zmluvy o dielo, 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 o dielo. 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 o dielo je zodpovedný dodávateľ. Nahlásenie vykoná kontaktná osoba dodávateľa u príslušného zmluvného kontaktu prevádzkovateľa.

Kyberbezpečnostný štandard pre projekty a IT v Sociálnej poisťovni

Úvod

Informačné systémy, technológie a prostriedky používané v Sociálnej Poisťovni – SP musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované. To znamená, že ak útočník kompromituje časť infraštruktúry, je pre neho zložitá 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 nezaobrá 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).

Štandardy implementácie

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.

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.

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 commiti.
- 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.

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.

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.

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.

1 Konfigurácia webového servera

System

- 1) System, 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).

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 webservice 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 whitelistingu 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 negociácie 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.

Administrácia, logovanie a zálohovanie

- 1) Správcovské 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 správcovské 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 prispôbenie 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.

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, obsahujúcim autorizované skripty).
- 10) Použitie symbolických linkov by malo byť pre procesy webového servera zakázané.
- 11) Odporúčame vytvoriť kompletnú maticu prístupov k webovému obsahu (access matrix). V nej by malo byť definované, ktoré súbory a priečinky majú byť prístupné a pre koho.
- 12) V odôvodnených prípadoch odporúčame zaviesť kontrolu proti botom (napr.

CAPTCHA, nofollow, filtrovanie kľúčových slov).

HTTP hlavičky a cookies

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

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 zobrazovať 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.

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 prvé 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 iníciačných 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 zadané heslá sa musia zhodovať.
- 14) Odporúčame pri zmene hesla používať viacfaktorové potvrdenie, napríklad Out-Of-Band kanálom (mail, SMS, KeyCloak, ...).
- 15) Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.
- 16) Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.

- 17) Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať sol' (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.

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 akejkoľvek 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.

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 neautentifikovanej 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.

Nahrávanie súborov

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

Obsah

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

Rôzne

- 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.

2 Interná infraštruktúra a vývojové prostredie

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.

Vývojové prostredie

- 1) Vo vývojovom prostredí musia byť použité iba nástroje splňajúce 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.

3 Štandardy prepojenia

Sieťové protokoly

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

Prenos dát

- 1) Štandardom prenosu dát je
 - a) používanie protokolu File Transfer Protocol (FTP) alebo protokolu Hypertext

Transfer Protocol (HTTP) a

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

2) Špecifikácie prepojenia pomocou sieťových služieb

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

3) Sieťová a komunikačná bezpečnosť

- a) aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov,
- b) na prenos informácií k tretím stranám uzatvorenie zmluvy o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami,
- c) všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany 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 použitie 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-F1) 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 šesticte časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 (šesť) mesiacov.

4 Prenos elektronickej pošty

4.1 Prenos elektronickej pošty

- 1) Štandardom prenosu elektronickej pošty je
 - a) používanie e-mailových protokolov, ktoré zodpovedajú špecifikáciám Simple Mail Transfer Protocol (SMTP) na prenos elektronických poštových správ,
 - b) podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group na zabezpečenie prenosu elektronických poštových správ.
- 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.

4.2 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.

5 Štandardy prístupu k elektronickým službám

5.1 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.

5.2 Adresárové služby

- 1) Štandardom adresárovej služby je
 - a) používanie aplikačného protokolu Lightweighted 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.

6 Štandardy webovej služby

6.1 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.

7 Štandardy integrácie dát

7.1 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.

7.2 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.

8 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).

9 Dátové štandardy

9.1 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, nesprávne 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.

10 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.

11 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.

12 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 funkcionálnosť 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).

13 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.

14 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, nahradzujúci ARP z IPv4

NTP - Network Time Protocol

OS - Operačný systém PVLAN – Private VLAN princíp least privilege

RDP - Remote Desktop Protocol

QoS - Quality of Service

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, prispôsobený 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)
- Nariadenie GDPR – Nariadenie Európskeho parlamentu a Rady (EÚ) **2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- 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. **331/2018** Z. z. o zaručenej konverzii
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **438/2019** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy VS
- Vyhláška Ministerstva vnútra Slovenskej republiky č. **29/2017** Z. z. o alternatívnom autentifikátore
- Vyhláška 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. **338/2004** Z. z. o administratívnej bezpečnosti
- 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
- Výnos MF SR č. **55/2014** Z. z., o štandardoch pre IS VS v aktuálne platnom znení
- 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 Používateľské princípy pre návrh a rozvoj elektronických služieb verejnej správy <https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/index.html>
 - Metodika Jednotný dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-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 dôverylosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

Dôvernosť

Z hľadiska dôverylosti 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 privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

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

Integrita

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

- **nízka** zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohroží 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.