Dokumentácia systému ochrany osobných údajov

pre Úrad Predsedníctva SAV

Spracoval:	kolektív autorov RATIO SERVICES, s.r.o.
Prevzal:	Ing. Ján Malík, CSc., Vedúci Úradu SAV
Dátum:	5.5.2018
Podpis:	.....

Dokumentácia je vypracovaná pre spoločnosť **Úrad Predsedníctva SAV**, so sídlom: Štefánikova 49, 814 38 BRATISLAVA, IČO: 00037869, DIČ: 2020844914 (ďalej len „**spoločnosť**“, alebo „**klient**“), v súlade so známymi bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Ak nakladanie s informáciami v tomto dokumente nepodlieha podmienkam osobitnej, písomne uzatvorenej zmluvy medzi spoločnosťou Ratio Services s. r. o. (ďalej aj "**Ratio**" alebo "**dodávateľ**") a klientom, budú tieto informácie považované za dôverné a sú určené výhradne pre internú potrebu klienta. Takéto informácie sa nesmú bez predchádzajúceho povolenia INFO CONSULT, s.r.o., postúpené tretej strane ani používané či rozmnožovať na iné účely.

V rámci dokumentu sú použité označenie a mená, ktoré sú chránené ochrannými známkami a registrovanými ochrannými známkami. Tieto mená a označenia sú použité pri plnom rešpektovaní všetkých práv ich príslušných vlastníkov.

Obsah

STRATÉGIA OCHRANY ÚDAJOV

1 ÚVODNÉ USTANOVENIA

1.1 Účel dokumentu

Tento dokument je spracovaný k kontexte na požiadavky 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 (ďalej len „**GDPR**“).

Medzi základné zásady spracúvania osobných údajov (ďalej len „**OÚ**“) v zmysle čl. 5 GDPR patrí, že osobné údaje musia byť:

- spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („**zákonnosť, spravodlivosť a transparentnosť**“),
- získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi („**obmedzenie účelu**“),
- primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“),
- správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („**správnosť**“)
- uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú („**minimalizácia uchovávania**“);
- spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („**integrita a dôvernosť**“).

V zmysle čl. 5 ods. 2. GDPR Prevádzkovateľ je zodpovedný za súlad a **musí vedieť tento súlad preukázať** („zodpovednosť“).

Zároveň v zmysle čl. 24 GDPR platí, že:

- S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil **a bol schopný preukázať**, že spracúvanie sa vykonáva v súlade s Nariadením.
- Ak je to primerané vzhľadom na spracovateľské činnosti, opatrenia zahŕňajú **zavedenie primeraných politík ochrany údajov** zo strany prevádzkovateľa.

Dokumentácia systému ochrany osobných údajov je preto vypracovaná najmä s ohľadom na požiadavku čl. 5 ods. 2 a čl. 24 GDPR.

Táto dokumentácia zároveň vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na spracovateľské operácie.

1.2 Predmet dodávky

Predmetom dodávky je:

- Vytvorenie zoznamu operácií potenciálne súvisiacich so spracovaním osobných údajov
- Hodnotenie súčasného stavu procesov v kontexte GDPR
- Zhodnotenie vyspelosti analyzovaných procesov
- Porovnanie súladu dokumentácie voči požiadavkám GDPR
- Schéma analyzovaných procesov
- Posúdenie súčasného IT prostredia analyzovaných procesov v kontexte spracovateľských činností
- Identifikácia účelov a právneho základu spracovateľských činností
- Identifikácia osobných údajov v analyzovaných procesoch
- Posúdenie bezpečnostnej architektúry v kontexte analyzovaných procesov
- Identifikácia zraniteľností a hrozieb
- Kvantifikácia rizík
- Návrh opatrení

Predmetom tejto analýzy NIE JE:

- posúdenie efektivity
- mapovanie a nákres existujúcej IT architektúry
- posúdenie ceny komponentov alebo spôsobu využitia stávajúcich investícií
- zhodnotenie využiteľnosti komponentov
- návrh bezpečnostnej architektúry
- analýza technických požiadaviek na funkcie bezpečnosti

1.3 Vysvetlenie pojmov a skratiek

Pojem	Skratka	Výklad
analýza IT rizík		Analýza IT rizík je proces identifikácie a ohodnocovania zraniteľností a hrozieb ktoré by mohli spôsobiť riziko straty dôvernosti, integrity, dostupnosti a sledovateľnosti informačných aktív. Analýza IT rizík je súčasť manažmentu rizík.
Bezpečnostný úschovný objekt		uzamykací systém určený na bezpečné uloženie hotovosti, cenín a dokumentov v súvislosti s potrebou zabezpečenia ochrany osobných údajov a utajovaných skutočností, pričom je zároveň prístup technicky možný len za dodržania predpísaných režimových opatrení. Za úschovné objekty sa pre účely tohoto dokumentu považujú všetky druhy trezorov vrátane komorových trezorov a uzamykateľných kovových skríň.
cieľový bod obnovenia	RPO	Maximálne množstvo dát, ktoré môže byť stratené, kým je služba obnovená po jej prerušení. Cieľový bod obnovenia je vyjadrený ako maximálna doba povolená medzi posledným uložením údajov a udalosťou, ktorá spôsobila haváriu samotnej IT služby. Napríklad cieľový bod obnovenia jedného dňa, môže byť podporený dennými zálohami, a teda môžu byť stratené dáta najviac za 24 hodín. Cieľové body obnovenia pre každú IT službu by mali byť dojednané, odsúhlasené, zdokumentované v SLA.
cieľový čas obnovy	RTO	Maximálny prípustný čas pre obnovenie IT služby po jej prerušení. Poskytovaná úroveň služby môže byť nižšia, ako je normálna cieľová úroveň služby. Cieľové časy obnovenia pre každú IT službu by mali byť dojednané, odsúhlasené a zdokumentované v SLA.
CIO		Chief Information Officer - zamestnanec zodpovedný za oblasť informatiky ako celku
CISO		Chief Information Security Officer - zamestnanec zodpovedný za informačnú bezpečnosť
Compliance		Compliance Officer - zamestnanec zodpovedný za oblasť riadenia súladu s legislatívou a za vybavovanie podnetov
CRO		Chief Risk Officer - zamestnanec zodpovedný za manažment rizík
CSO		Chief Security Officer - zamestnanec zodpovedný za bezpečnosť ako celok
CTO		Chief Technology Officer - zamestnanec zodpovedný za oblasť prevádzky IT
dohoda o úrovni služby	SLA	Dohoda medzi poskytovateľom IT služieb a zákazníkom. SLA popisuje IT službu, dokumentuje cieľovú úroveň služieb a špecifikuje zodpovednosti poskytovateľa IT služby a zákazníka. Jedna SLA môže pokrývať niekoľko IT služieb alebo niekoľko zákazníkov.
dopad		Dopad popisuje závažnosť ujmy, resp. rozsah škody ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou. Miera potenciálneho dopadu zároveň predurčuje relatívnu hodnotu informačného aktíva a všetkých dotknutých zdrojov (napr. kritickosť a citlivosť komponentov IT systému a príslušných dát).
dopadová analýza	BIA	Zhodnotenie dopadu na činnosť podľa krízového scenára, kedy boli napadnuté zdroje a aktíva a/alebo služby sa tak stali nedostupnými. BIA poskytuje základné informácie, ktoré slúžia na

		plánovanie riešení kontinuity činnosti. (systémové a kritické procesy, ich vlastníkov, kritičnosť, RTO a RPO procesu, lokalitu procesu, užívateľské IT aplikácie, HW, SW, špeciálne zariadenia, dokumentáciu, kritické ľudské zdroje).
hrozba		Akákoľvek okolnosť či udalosť ktorá môže potenciálne využiť zraniteľné miesto informačného aktíva a spôsobiť škodu.
informačné aktívum		Na účel tohto dokumentu sú za informačné aktíva považované všetky objekty a entity súvisiace so spracúvaním informácií, ktoré pre Spoločnosť priamo predstavujú hodnotu alebo narušenie ich bezpečnosti môže mať pre Spoločnosť negatívny dopad.
informačný systém OÚ	IS	informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom sa na účely tohto dokumentu rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania
inherentné riziko		Riziko späté s informačným aktívom, s jeho podstatou, aktívu vlastné riziko, bez implementácie dodatočných bezpečnostných protiopatrení.
ISMS		Information Security Management System (Systém manažérstva informačnej bezpečnosti) – proces založený na medzinárodných normách ISO/IEC radu 27 000.
IT prostriedok		Každý IT komponent zabezpečujúci prevádzku IT služby.
IT služba		Služba poskytovaná prevádzkou IT pre interného a externého klienta, je súčasťou servisného katalógu vytvoreného procesom SLM (Service Level Management). Podmienky a parametre poskytovania IT služby sú definované v SLA (Service Level Agreement).
ITSC plán		Plán / Súbor dokumentov a postupov, definujúci kroky potrebné na obnovu jednej, alebo viacerých IT služieb.
ITSM		IT Service Management (Riadenie služieb IT) – disciplína pre riadenie veľkého rozsahu informačných a komunikačných technológií, filozoficky zameraná na zákaznícku perspektívu IT podpory pre „business“ založená na medzinárodných normách ISO/IEC radu 20000.
kontinuita IT služieb		Súbor aktivít zabezpečujúce poskytovanie IT služieb po mimoriadnych udalostiach alebo v krízových situáciách za účelom opätovného zahájenia obchodných operácií na prijateľnej súčasnej úrovni.
kritické procesy		hlavné obchodné procesy (RTO ≤120 hod.), ktoré môžu spôsobiť podniku významné straty z hľadiska finančných ukazovateľov, postavenia na trhu, dobrého mena alebo nedodržania záväzkov voči partnerom, alebo regulátorom. Proces, ktorý kvôli významnosti poškodenia vyplývajúceho z nedostupnosti, vyžaduje implementáciu preventívnych opatrení kontinuity činnosti a pohotovostných riešení na vysokej úrovni s cieľom predchádzať havariám.

NIST		National Institute of Standards and Technology – Ústav technickej normalizácie v USA.
oprávnená osoba		každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení
osobný údaj	OÚ	sú akékoľvek informácie tykajúce 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
ošetrovanie rizika		Jeden z troch podprocesov procesu riadenia rizík (analýza rizík, ošetrovanie rizika a prehodnocovanie rizík) v rámci ktorého sú prehodnocované odporúčané technické, organizačné a procedurálne protiopatrenia. Následne sú tieto protiopatrenia priorizované a implementované
používateľ		Osoba, ktorá spracúva (vytvára, používa, mení, premiestňuje, maže) informačné aktíva Spoločnosti v preddefinovaných procedúrach počas vykonávania pridelených úloh.
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.
priestory Spoločnosti		Priestory, ktoré sú vlastnené alebo prenajaté Spoločnosťou a ktoré sú chránené technickými zabezpečovacími prostriedkami a mechanickými zábrannými prostriedkami.
prijateľné riziko		Prijateľné riziko je riziko, ktoré. je také nízke (t.j. nepresahuje referenčnú úroveň), že pre Spoločnosť nepredstavuje významný negatívny dopad a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.
riziko		Riziko je funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.
rizikový apetít		definuje sa ako ochota Spoločnosti prijať finančné riziká tak, ako sú kvantifikované príslušnými ukazovateľmi, t.j. ako meradlo chovania sa Spoločnosti pri hľadaní rizika.
sprostredkovateľ		je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa
systémové procesy		Vysoko kritické procesy (RTO ≤4 hod.), ktoré v domino efekte môžu spôsobiť ochabnutie alebo úplné zničenie podniku.
spracúvanie OÚ, spracovateľská operácia		je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo

		zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami
tretia strana		orgán verejnej moci, právnická osoba alebo fyzická osoba, ktorá sa vo vzťahu k dôvernej informácii považuje za neautorizovanú osobu, pokiaľ nie je týmto dokumentom určené inak. Na účely tohto dokumentu každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou.
účel spracovania OÚ		vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť
zraniteľnosť		Slabé miesto v informačnom systéme, bezpečnostných procedúrach systému, opatreniach alebo implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb.
zvyškové riziko		Zvyškové riziko je riziko, na ktoré boli uplatnené všetky dostupné opatrenia na komplexné ošetrenie rizík t.j. boli implementované základné, dodatočné a vylepšené opatrenia na ošetrenie rizika

1.4 Analytické zdroje

Podklady sú rozdelené podľa zdroja, z ktorého boli získané na:

- východiskové podklady získané od Klienta
- podklady získané z verejne dostupných zdrojov.

Pri spracovaní tejto analýzy vychádzame z toho, že informácie získané z podkladov predložených Klientom sú vierohodné a správne a nie sú teda vo všetkých prípadoch overované z hľadiska ich presnosti a úplnosti.

Podľa nášho názoru analýza nezávisle, nestranne a komplexne zohľadňuje všetky známe relevantné skutočnosti, ktoré by mali byť pri jeho spracovaní zohľadnené (**zásada komplexnosti**).

Aby výsledok analýzy mohol byť podrobený nezávislému posúdeniu, musí analýza spĺňať atribúty zákonnosti, integrity, opakovateľnosti a nezaujatosti.

V tejto analýze boli dôvodne a odôvodnene použité také metodické postupy, ktoré boli vhodné, primerané a plne vyhovujúce relevantným informáciám, ktoré sme mali k dispozícii (**zásada dôvodnosti a opodstatnenosti**).

1.5 Normatívny základ

Na účely tohto dokumentu sú uplatnené najmä bezpečnostné opatrenia, ktoré sú odporúčané medzinárodnou normou **STN ISO/IEC 27002 Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti**.

Organizácie môžu použitím rodiny noriem systému riadenia bezpečnosti informácií (ISMS) vyvinúť a implementovať rámec pre riadenie bezpečnosti svojich informačných aktív a pripraviť nezávislé ohodnotenie svojich systémov riadenia týkajúcich sa ochrany informácií, napr. finančných informácií, duševného vlastníctva a podrobností o zamestnancoch, alebo informácií, ktoré im boli zverené.

Rodina noriem ISMS pozostáva z nasledujúcich medzinárodných noriem so súhrnným názvom Informačné technológie – Bezpečnostné metódy:

- ISO/IEC 27000, Systémy riadenia informačnej bezpečnosti – prehľad a slovník

- ISO/IEC 27001, Systémy riadenia informačnej bezpečnosti – požiadavky
- ISO/IEC 27002, Pravidlá dobrej praxe riadenia informačnej bezpečnosti
- ISO/IEC 27003, Návod na implementáciu systému riadenia informačnej bezpečnosti
- ISO/IEC 27004, Riadenie bezpečnosti informácií – Meranie
- ISO/IEC 27005, Riadenie rizík informačnej bezpečnosti
- ISO/IEC 27006, Požiadavky na orgány vykonávajúce audit a certifikáciu systémov riadenia informačnej bezpečnosti
- ISO/IEC 27007, Návod na audit systémov riadenia informačnej bezpečnosti

Okrem vyššie uvedených noriem z rodiny ISMS sa odvolávame na normy týkajúce sa metód hodnotenia bezpečnosti systémov, riadenia kontinuity a ochrany osobných údajov:

- ISO/IEC 15408 Informačné technológie – Bezpečnostné metódy – Kritériá pre hodnotenie bezpečnosti IT
- ISO 22301 Ochrana spoločnosti – Systémy riadenia kontinuity činnosti – Požiadavky
- ISO 22313 Ochrana spoločnosti Systémy riadenia kontinuity činnosti – Pokyny
- ISO/IEC 29134 Informačné technológie – Bezpečnostné metódy – Návod na posúdenie vplyvu na ochranu osobných údajov

V texte sa tiež opierame o odporúčania niektorých štandardov NIST:

- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
- NIST Special Publication 800-39, Managing Risk from Information Systems
- NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- NIST Special Publication 800-18, Guide For Developing Security Plans for Information Technology Systems.
- NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle
- NIST Special Publication 800-27, Engineering Principles for IT Security
- NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment

Opis bezpečnostných opatrení a spôsob uplatnenia opatrení v konkrétnych podmienkach je uvedený v prílohe č. 1 tejto Dokumentácie.

Rozdelenie opatrení je v zmysle audítorskej časti normy STN ISO / IEC 27000 v kapitole 5.4.

Štruktúra ISO/IEC 27000 je rozdelená do nasledujúcich kapitol (čísla reflektujú čísla kapitol predmetnej normy):

- A.05 Politiky informačnej bezpečnosti
- A.06 Organizácia informačnej bezpečnosti
- A.07 Personálna bezpečnosť
- A.08 Riadenie aktív
- A.09 Riadenie prístupov
- A.10 Šifrovanie, kryptografia
- A.11 Fyzická bezpečnosť a bezpečnosť prostredia

- A.12 Prevádzková bezpečnosť
- A.13 Komunikačná bezpečnosť
- A.14 Akvizícia, vývoj a údržba informačných systémov
- A.15 Riadenie vzťahov s dodávateľmi
- A.16 Riešenie incidentov informačnej bezpečnosti
- A.17 Riadenie kontinuity činností
- A.18 Riadenie súladu

2 STANOVENIE STRATÉGIE OCHRANY ÚDAJOV

Stratégia ochrany údajov vymedzuje okrem iného základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti. Bezpečnostný zámer obsahuje:

a) vymedzenie spracovateľských operácií a príslušného právneho základu spracúvania,

b) formuláciu základných bezpečnostných cieľov,

c) špecifikáciu technických opatrení a organizačných opatrení na zabezpečenie ochrany osobných údajov a spôsob ich využitia,

d) vymedzenie bezpečnostnej, aplikačnej a sieťovej architektúry, perimetra informačného systému a vzťah IT architektúry k možnému narušeniu bezpečnosti,

e) vymedzenie hraníc určujúcich množinu zostatkových rizík pričom zostatkovým rizikom sa rozumie bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami

2.1 Bezpečnostné ciele

Riadenie bezpečnosti a ochrany údajov v Spoločnosti prebieha v súlade so stanovenými strategickými cieľmi.

Dokument bezpečnostnej politiky reflektuje legislatívu Slovenskej republiky, regulatívne požiadavky ako aj medzinárodné normy a štandardy pre oblasť bezpečnosti, najmä systém riadenia informačnej bezpečnosti Spoločnosti podľa ISO/IEC 27 000. Bezpečnostná politika Spoločnosti je schválená vedením Spoločnosti.

Spoločnosť si je vedomá, že ochrana majetku a ostatných aktív závisí na špecifických právomociach v oblasti bezpečnosti, ako aj na každodennom konaní všetkých strán, ktoré sa rôznou mierou podieľajú na jej podnikateľských aktivitách. Spoločnosť vníma aktivity vrcholového manažmentu, riadiacich a dozorných orgánov ako aj stredného manažmentu ako príležitosť na šírenie pozitívnej kultúry v oblasti bezpečnosti v rámci celej Spoločnosti.

Celá Spoločnosť a každá jej zložka počnúc riadiacimi pracovníkmi musia prijať záväzok brať ohľad na bezpečnostné požiadavky zainteresovaných strán pri budovaní bezpečného prostredia vrátane všetkých prevádzkových oblastí a pri šírení cieľov, hodnôt a poznatkov spoločných pre celú Spoločnosť.

Presadzovanie základných bezpečnostných princípov v každodennej činnosti Spoločnosti je trvalý, cieľavedome riadený a organizovaný proces v metodickej, výkonnej a kontrolnej oblasti.

Základným bezpečnostným cieľom je zabezpečiť osobné údaje a ostatné citlivé informačné aktíva v informačnom systéme Spoločnosti proti odcudzeniu, strate, poškodeniu, zničeniu, kompromitácii, neoprávnenému alebo nedovolenému prístupu, sprístupneniu neoprávneným osobám, neoprávnenej zmene a neoprávnenému rozširovaniu a pred akýmikoľvek neprístupnými a zlomyseľnými formami spracúvania. Na tento účel Spoločnosť prijíma primerané technické a, organizačné opatrenia, ktorých funkčnosť sa bude navzájom prekrývať a vytvárať integrovanú ochranu informačného systému.

Spoločnosť sa zaväzuje implementovať najmä nasledovné bezpečnostné funkcie:

a) Zabezpečenie dôvernosti citlivých informačných aktív,

b) Zaručenie integrity citlivých informačných aktív,

c) Zaručenie dostupnosti citlivých informačných aktív,

d) Zaručenie odolnosti systémov spracúvania a služieb,

e) Zaistenie schopnosti včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu,

f) Proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania

g) Relevantné preukázanie zodpovednosti a sledovateľnosť prístupu k citlivým informačným aktívam

h) Dokumentáciu systému ochrany osobných údajov (ďalej len „**Dokumentácia**“) ktorá je vypracovaná za účelom schopnosti preukázať, že boli prijaté vhodné technické a organizačné opatrenia a že spracúvanie sa vykonáva v súlade s Nariadením.

Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie.

Ustanovenia tohto dokumentu a všetkých príslušných súvisiacich dokumentácií sa vzťahujú na všetky útvary, ktoré sa podieľajú na obchodných a podporných aktivitách Spoločnosti.

Pri zmene bezpečnostnej politiky, technických opatrení alebo organizačných opatrení, pri zmene používaných informačných systémov a/alebo ich konfigurácie a/alebo ich umiestnenia, alebo pri zmene všeobecne záväzných právnych predpisov Slovenskej republiky alebo legislatívy Európskej Únie sa Spoločnosť zaväzuje dokumentáciu bezodkladne upraviť a doplniť o potrebné zmeny.

2.2 Politika riadenia rizika

Riadenie rizika v informačnej bezpečnosti je systematický proces, v ktorom sa identifikujú a analyzujú hrozby a zraniteľnosti a posúdi sa miera rizika, súvisiaceho s obstaraním, dodávkou resp. vývojom aplikácií a informačných systémov, so spracovaním, prenášaním a ukladaním informácií pomocou IT prostriedkov a ktorým sa definuje optimálny spôsob ošetrenia rizika pri minimálnych nákladových aspektoch a rešpektovaní strategických cieľov Spoločnosti.

Úlohou manažmentu IT rizík je predovšetkým dosiahnutie primeranej bezpečnosti a ochrany informačných aktív, vypracovaním optimálnej stratégie riadenia rizík, ako hlavných nositeľov možných budúcich škôd.

Manažment rizík v informačnej bezpečnosti musí spĺňať nasledujúce požiadavky:

- sú identifikované hrozby a zraniteľnosti
- je stanovená metrika pre hodnotenie rizík,
- úroveň rizík je posudzovaná z hľadiska ich dopadu na práva dotknutých osôb, a dopadu na obchodnú stratégiu Spoločnosti, t.j. z hľadiska pravdepodobnosti výskytu príslušných hrozieb a z hľadiska závažnosti príslušných zraniteľností,
- miera a dopady identifikovaných rizík sú oznámené vedeniu Spoločnosti,
- sú identifikované opatrenia na znižovanie pravdepodobnosti a / alebo dopadov hrozieb a zraniteľností (t.j. opatrenia na znižovanie rizika),
- sú stanovené priority ošetrovania rizík,
- sú stanovené priority implementácie opatrení na ošetrovanie rizík,
- všetky strany zúčastnené v procese riadenia rizík sa podieľajú na rozhodovaní o riadení rizík a sú priebežne informované o stave ošetrovania rizík,
- monitoruje sa účinnosť procesu ošetrovania rizík,

- proces riadenia rizík je sledovaný a pravidelne vyhodnocovaný za účelom zlepšenia prístupu k riadeniu rizík,
- manažéri a zamestnanci sú pravidelne oboznamovaní o rizikách a prijatých opatreniach na ich zmiernenie.

Politika riadenia rizika v informačnej bezpečnosti musí byť v Spoločnosti aplikovaná vždy ako celok, nikdy nie len ako oddelená časť procesov alebo systémov (napr. len v rámci odboru, len v rámci fyzického umiestnenia aktíva, len v rámci služby), ani ako jediný existujúci, či plánovaný aspekt riadenia Spoločnosti (napr. len riadenie kontinuity činností).

2.3 Dobrá prax

Každý používateľ v Spoločnosti JE POVINNÝ používať štandardné pracovné postupy, procesy a procedúry t.j. vnútorné predpisy, štandardy a inštrukcie zamestnancov zodpovedných za oblasť riadenia rizík.

Všetci zamestnanci SÚ POVINNÍ aplikovať s najlepším vedomím všetky dostupné teoretické poznatky a známe pracovné postupy na zaručenie nepretržitého ošetrovania rizika v informačnej bezpečnosti, resp. jeho udržania na akceptovateľnej úrovni, stanovenej vedením Spoločnosti.

2.4 Kľúčové faktory úspechu

Úspešná implementácia a trvalá udržateľnosť programu riadenia IT rizika je závislá od nasledujúcich faktorov:

- Je formálne deklarovaný záväzok vedenia Spoločnosti riadiť a znižovať riziko,
- Je zaručená účasť riadiacich zamestnancov na programe riadenia rizika,
- Je formálne stanovený tím zodpovedný a odborne zdatný správne identifikovať riziká, ako aj aplikovať metodiku hodnotenia rizík na špecifické systémy,
- Je zaručená plná podpora a participácia zamestnancov zodpovedných za IT na riadení rizika,
- Výkon analýzy rizík začína na úrovni biznis procesov, identifikáciou a hodnotením informácií nimi riadených a spracovaných, identifikáciou hrozieb a slabín a opatrní procesov,
- Je zabezpečená konzistencia výsledkov analýz rizík a jednotný pohľad na identifikované riziká a to bez ohľadu na to aký prístup, metodika alebo detail bol zvolený pri výkone jednotlivých čiastkových analýz rizík,
- Je neustále zvyšované povedomie a spolupráca používateľov IT systémov pri dodržiavaní procesov a udržiavaní súladu s implementovanými opatreniami,
- Je zaručený nepretržitý proces oceňovania a hodnotenia IT rizika.

ANALÝZA SÚLADU

1 ROZDIELOVÁ ANALÝZA

1.1 Všeobecný návrh prístupu k rozdielovej analýze

Cieľom rozdielovej analýzy je pomôcť určiť aktuálnu úroveň súladu Spoločnosti s požiadavkami GDPR. Tzv. GAP analýza umožní určiť priority a oblasti ktoré je potrebné riešiť, aby sa Spoločnosť ako Prevádzkovateľ uistila, že organizácia spĺňa požiadavky GDPR.

Pre účely GAP analýzy kolektív Ratio používa vlastnú vyvinutú metodiku, ktorá vychádza z pôvodných požiadaviek a článkov GDPR, prioritizuje ich a zoskupuje do tematických oblastí.

1.2 Právny základ spracúvania osobných údajov

Právnym základom spracúvania osobných údajov v Spoločnosti sú nasledujúce právne predpisy:

Číslo predpisu	Názov predpisu
311/2001 Z. z.	Zákonník práce v znení neskorších predpisov
400/2009 Z. z.	Zákon o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
552/2003 Z. z.	Zákon o výkone práce vo verejnom záujme v znení neskorších predpisov
553/2003 Z. z.	Zákon o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
580/2004 Z. z.	Zákon o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
461/2003 Z. z.	Zákon o sociálnom poistení v znení neskorších predpisov
595/2003 Z. z.	Zákon o dani z príjmov v znení neskorších predpisov
43/2004 Z. z.	Zákon o starobnom dôchodkovom sporení v znení neskorších predpisov
650/2004 Z. z.	Zákon o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
5/2004 Z. z.	Zákon o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
462/2003 Z. z.	Zákon o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
152/1994 Z. z.	Zákon o sociálnom fonde a o zmene a doplnení zákona Č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov
355/2007 Z. z.	Zákon o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
124/2006 Z. z.	Zákon o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
570/2005 Z. z.	Zákon o brannej povinnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
314/2001 Z. z.	Zákon o ochrane pred požiarmi v znení neskorších predpisov
283/2002 Z. z.	Zákon o cestovných náhradách v znení neskorších predpisov

1.3 Účel spracovania osobných údajov

Základnou **zákonnou podmienkou spracúvania osobných údajov je stanovenie účelu spracúvania**. Účelom spracúvania osobných údajov vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť. Spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:

1. **dotknutá osoba vyjadrila súhlas** so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely
2. **spracúvanie je nevyhnutné na plnenie zmluvy**, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy
3. **spracúvanie je nevyhnutné na splnenie zákonnej povinnosti** prevádzkovateľa
4. **spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby** alebo inej fyzickej osoby
5. **spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme** alebo pri výkone verejnej moci zverenej prevádzkovateľovi
6. **spracúvanie je nevyhnutné na účely oprávnených záujmov**, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.

Účel spracúvania osobných údajov musí byť vymedzený jednoznačne a konkrétne; účel spracúvania musí byť jasný a nesmie byť v rozpore s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná. Účel spracúvania osobných údajov vymedzuje:

a) Spoločnosť pred začatím spracúvania osobných údajov, alebo

b) osobitný zákon v súlade s vyššie uvedenými podmienkami.

Spoločnosť ako prevádzkovateľ spracúva osobné údaje dotknutých osôb predovšetkým na nasledujúce účely:

- uzatváranie a vykonávanie obchodov s klientmi;
- ochrana a domáhanie sa práv voči klientom;
- zdokumentovanie činnosti Spoločnosti;
- poskytovanie údajov orgánom verejnej moci
- vedenie personálnej a mzdovej agendy a evidencia zamestnancov

Spoločnosť ako prevádzkovateľ ďalej spracúva osobné údaje dotknutých osôb – svojich zamestnancov predovšetkým na účely stanovené Zákonníkom práce a ostatnými vyššie uvedenými právnymi predpismi v oblasti pracovnoprávnej a v oblasti zdravotného a sociálneho zabezpečenia.

Predmetom činnosti Spoločnosti nie je priamy marketing, uvedené osobné údaje neposkytuje, nesprístupňuje a nezverejňuje.

Iný účel spracúvania osobných údajov môže Spoločnosť ako prevádzkovateľ stanoviť v súlade so zákonom a spôsobom popísaným v tomto bezpečnostnom projekte.

2 HODNOTENIE VYSPELOSTI PROCESOV

2.1 Všeobecný návrh prístupu k hodnoteniu vyspelosti procesov

Hodnotenie procesov informačnej bezpečnosti navrhujeme riešiť prostredníctvom posúdenia vyspelosti Systému riadenia informačnej bezpečnosti podľa ISO/IEC 27000 (ďalej len „**ISMS**“).

Medzinárodná norma ISO/IEC 27001 špecifikuje požiadavky na vytvorenie, zavedenie, údržbu a stále zlepšovanie systému riadenia informačnej bezpečnosti v kontexte organizácie. Norma obsahuje aj ciele a požiadavky na ošetrenie rizík informačnej bezpečnosti prispôsobených potrebám organizácie. ISO/IEC 27002 následne poskytuje návod na organizovanie informačnej bezpečnosti a skúsenosti na riadenie informačnej bezpečnosti vrátane výberu, zavedenia a riadenia opatrení, ktoré treba zohľadniť v organizácii v prostredí bezpečnostných rizík.

Hodnotenie hrozieb a rizík navrhujeme oprieť o metodiku danú medzinárodnou normou ISO/IEC 27001, o katalóg hrozieb, ktorý je jej prílohou a rozšíriť tento katalóg o hrozby identifikované metodikou LINDDUN. Niektoré postupy sú tiež založené na odporúčaniach National Institute of Standards and Technology, najmä NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.

Medzinárodná norma ISO/IEC 27005 poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti a podporuje všeobecné koncepty špecifikované podľa normy ISO/IEC 27001. Norma má za cieľ pomáhať pri uspokojivom implementovaní informačnej bezpečnosti, ktorej základom je riadenie rizík.

Celkovým riešením analýzy rizík je teda nasledujúca postupnosť:

1. posúdiť riziká pre jednotlivé hrozby identifikované podľa katalógu hrozieb z prílohy normy ISO/IEC 27005
2. posúdiť riziká pre jednotlivé hrozby identifikované podľa katalógu hrozieb LINDDUN
3. vypočítať celkovú rizikovú expozíciu pre proces
4. vybrať opatrenia v rámci procesov zavedenia riadenia informačnej bezpečnosti podľa normy ISO/IEC 27002

2.2 Použitá metodika hodnotenia

Hodnotenie vyspelosti procesov je založené na metodike CMMI (z angl. Capability Maturity Model Integration).

CMMI je model základných procesov v organizácii spolu s odporúčaniami ako ich efektívne implementovať. Tento model pomáha integrovať tradične oddelené funkcie v organizácii, stanovuje k tomu základné ciele a priority.

Pri určovaní hodnotiacich bodov bola preto použitá práve stupnica podľa "CMMI. Pôvodných päť úrovní definovaných metodikou je rozšírených o úroveň 0 - neexistujúci proces.

Hodnotenie jednotlivých opatrení bolo vykonané z pohľadu atribútov uvedených v nasledujúcej kapitole 2.2, pričom každý atribút samostatne bol ohodnotený známkou podľa CMMI na stupnici 0-5. V závere bola vždy zhodnotená celková vyspelosť príslušného opatrenia, ako priemerná hodnota pre všetky hodnotené atribúty. Ak pre niektorý atribút nebolo hodnotenie podľa CMMI aplikovateľné, hodnotenie je vynechané a do priemeru nie je započítané.

2.3 Hodnotené atribúty procesov

Funkcie

Akým spôsobom a či vôbec sú plnené základné funkcie procesu

Dokumentácia

Ako je proces zdokumentovaný, či existujú záväzné nariadenia a predpisy a či bola vykonaná ich publikácia

Role

Ako sú definované a obsadené jednotlivé role, rozsah ich právomocí a zodpovedností

Činnosti

Či sú v rámci procesu vykonávané všetky činnosti, ktoré sú vymedzené podľa ISMS

Nástroje

Ako nástroje používané na podporu procesu splňuje požiadavky popísané ISMS (vrátane reportovacích systémov)

Údaje

Aká je kvalita údajov, ktoré proces využíva, ich použiteľnosť, atď.

Merania

Ako sú stanovené kritériá pre meranie procesu, ako sa tieto merania spracovávajú a vyhodnocujú.

Charakteristika vyspelosti / zrelosti pro jednotlivé atribúty je popísaná v nasledujúcej tabuľke.

Tabuľka č. 1.: Stupnica vyspelosti procesov

Stupnica zrelosti		**Popis zrelosti**
0	Neexistuje	Proces neexistuje
1	Počiatočný	Vykonávaný ad-hoc; bez stanovených aktivít, procedúr; závislý na individuálnom prístupe a konkrétnych jednotlivcoch
2	Opakovateľný	Proces je ustanovený; prebieha rovnakým spôsobom; býva centrálne riadený; chýba dokumentácia, merania, optimalizácia
3	Definovaný	Proces je ustanovený; prebieha rovnakým spôsobom; je zdokumentovaný; existuje lepší prehľad o procese; je centrálne riadený; Ale bez meraní a optimalizácie
4	Riadený	Proces je kontrolovaný; meraná účinnosť a produktivita; obsahuje potrebné formálne prvky; bez optimalizácie
5	Optimalizovaný	Proces je kontrolovaný; meraná účinnosť a produktivita; obsahuje potrebné formálne prvky; priebežne optimalizovaný

Tabuľka č. 2.: Charakteristika atribútov vyspelosti procesov

	Funkcia	Dokumentácia	Role	Činnosti	Nástroje	Údaje	Metrika
0	Nie sú plnené	Neexistuje	Nie sú definované	Nie sú vykonávané	Neexistuje	Neexistujú	Bez metriky
1	Je plnená iba malá časť funkcií	Iba základné nejednotné informácie	Role sú vykonávané iba ad-hoc „dostupnými pracovníkmi“	Sú vykonávané iba základné činnosti	Využívajú sa len jednoduché pomôcky na podporu procesu	Využívajú sa len náhodné zdroje údajov	Neexistujú podklady, zriedkavé merania
2	Sú plnené niektoré zo základných funkcií	Dokumentácia je čiastočná bez jednotného prístupu	Sú priradené osoby	Väčšina základných činností je plne vykonávaná	Podporuje výhradne proces a iba v základnej funkčnosti	Proces využíva vlastné oddelené údaje	Proces nemá vlastnú metriku, merania sú vykonávané nepriamo
3	V plnom rozsahu sú plnené základné funkcie	Systém dokumentácie je definovaný, avšak je obsahovo neúplná	Väčšina rolí je definovaná a majú priradené osoby	Všetky základné činnosti sú plne vykonávané	Schopný plne podporovať proces, ale bez integrácie do ďalších procesov	Údaje sú dostupné, majú požadovanú kvalitu, nie sú zdieľané	Sú vykonávané len čiastočné merania procesu
4	Funkcie procesu sú plnené	Dokumentácia pokrýva potreby procesu	Role procesu sú definované, majú priradené osoby	Všetky činnosti procesu sú vykonávané	Plne funkčný s čiastočnou integráciou iných procesov	Existuje jednotná údajová základňa	Proces je meraný v odporúčanom rozsahu
5	Funkcie procesu sú plnené a optimalizované	Kompletná dokumentácia vrátane definovaného svojho životného cyklu	Role sú definované, majú priradené osoby a právomoci	Všetky činnosti procesu sú vykonávané; je definovaný systém zlepšovania	Plne podporuje prostredie	Jednotná údajová základňa s plánom rozvoja	Merania sú vykonávané a využívané k optimalizácii

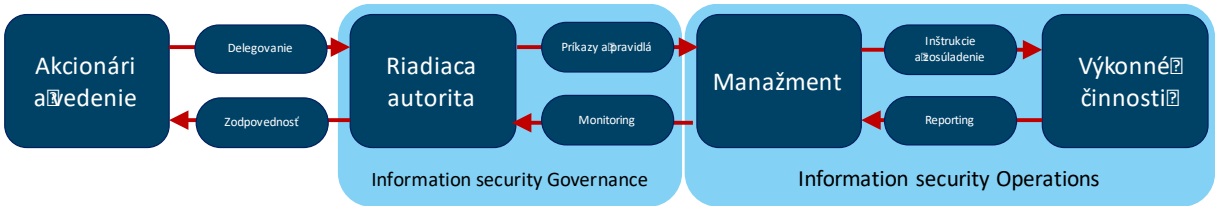
2.4 Rámec riadenia

Ako základná metodika riadenia je naprieč celým dokumentom použitý rámec COBIT 5.

COBIT 5 (Control Objectives for Information and related Technology) je medzinárodne uznávaný rámec z oblasti strategického riadenia a manažmentu informačných technológií (IT Governance and Management). Bol vytvorený a je udržiavaný medzinárodnou organizáciou ISACA a je predurčený pre manažérov, IT manažérov a IT špecialistov k efektívnemu a účelné využitie IT zdrojov v prospech dosiahnutia firemných cieľov a súvisiacich IT cieľov.

COBIT 5 predstavuje ucelený rámec, ktorý napomáha firmám a organizáciám dosiahnuť ich ciele v oblasti strategického riadenia (governance) a manažmentu IT. COBIT 5 umožňuje vytvárať optimálnu hodnotu realizovanú z IT cestou udržiavania rovnováhy medzi realizovanými prínosmi, optimalizáciou úrovne rizík a použitými zdrojmi. Tento prístup umožňuje holistický spôsob riadenia IT rizík v rámci celej Spoločnosti. COBIT 5 berie do úvahy ako samotný biznis, tak i funkčné oblasti zodpovednosti IT a súčasne posudzuje záujmy interných a externých zainteresovaných strán vo vzťahu k IT.

Obrázok č.1. Kľúčové role, aktivity a vzťahy podľa COBIT 5



Základné princípy rámca COBIT hodnotené v kontexte sú nasledovné:

- Splnenie potrieb akcionárov a obchodnej stratégie
- Pokrytie celej štruktúry Spoločnosti ako celku
- Uplatnenie jednotného, integrovaného rámca riadenia
- Holistický prístup (Vlastnosti systému nemožno určiť len pomocou vlastností jeho častí. Naopak celok ovplyvňuje podobu a fungovanie svojich častí.)
- Oddelenie operatívnej a strategickej úrovne riadenia (information security governance vs. information security operations)

3 ZOZNAM SPRACOVATEĽSKÝCH ČINNOSTÍ

„**Spracúvanie**“ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami, napríklad:

- získavanie,
- zaznamenávanie,
- usporadúvanie,
- štruktúrovanie,
- uchovávanie,
- prepracúvanie alebo zmena,
- vyhľadávanie,
- prehliadanie,
- využívanie,
- poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom,
- preskupovanie alebo kombinovanie,
- obmedzenie, vymazanie alebo likvidácia.

V zmysle čl. 30 ods. 1 GDPR musí prevádzkovateľ na účely preukázania súladu s GDPR uchovávať záznamy o spracovateľských činnostiach, za ktoré je zodpovedný. Tieto záznamy musia obsahovať všetky tieto informácie:

- meno/názov a kontaktné údaje prevádzkovateľa
- účely spracúvania
- opis kategórií dotknutých osôb a kategórií osobných údajov
- kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo medzinárodných organizácií v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 dokumentáciu primeraných záruk
- podľa možností predpokladané lehoty na vymazanie rôznych kategórií údajov
- podľa možností všeobecnýʹ opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods.1. GDPR

Zoznam spracovateľských operácií je možné oprieť o schému pracovných procesov Spoločnosti. Na základe tejto grafickej notácie je možné prehľadne identifikovať a označiť všetky relevantné spracovateľské operácie.

Podľa čl. 30 ods. 5 GDPR sa však tieto povinnosti nevzťahujú na podnik alebo organizáciu, ktorá zamestnáva menej ako 250 osôb, pokiaľ nie je pravdepodobné, že spracúvanie, ktoré vykonáva, povedie k riziku pre práva a slobody dotknutej osoby, pokiaľ je toto spracúvanie príležitostné alebo nezahŕňa osobitné kategórie údajov podľa článku 9 ods. 1 GDPR alebo osobných údajov tykajúcich sa uznaní viny za trestné činy a priestupky podľa článku 10 GDPR.

Žiadna z vyššie uvedených podmienok pre Spoločnosť nie je splnená a z toho dôvodu **nie je povinnosťou Spoločnosti ako prevádzkovateľa uchovávať záznamy o spracovateľských činnostiach**. Napriek tomu dodávateľ odporúča, aby Spoločnosť tieto záznamy evidovala za účelom udržania prehľadu o informačných aktívach Spoločnosti. Schémy a zoznam spracovateľských činností sú uvedené v prílohe č. 2 tejto dokumentácie.

3.1 Informačný systém

Za informačný systém osobných údajov (ďalej len „**informačný systém**“)sa považuje taký informačný systém, alebo rozhranie informačného systému, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Informačným systémom sa rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými, ako automatizovanými prostriedkami spracúvania.

Pre účely tejto Dokumentácie bude za „informačný systém“ považované celé IT prostredie Spoločnosti.

4 ANALÝZA ARCHITEKTÚRY

4.1 Bezpečnostná architektúra

Pod pojmom „bezpečnostná architektúra“ je myslené vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti informačného systému.

Informačná architektúra je vo všeobecnosti dizajn podniku, štruktúry a pomenovania častí procesov, systémov, sietí a softvéru s cieľom podporiť čo najlepšiu použiteľnosť. IT architektúra zvyčajne obsahuje model alebo koncept informácii, ktoré budú používané v komplexnom informačnom systéme. Jestvuje niekoľko rôznych notácií a rámcov pre IT architektúry.

Všetky definície informačných architektúr majú tieto spoločné body:

- určenie cieľov
- určenie nárokov
- štruktúrovaný dizajn zdieľaného prostredia
- metódy organizácie a pomenovaní prvkov
- predpríprava pre implementáciu.

Pre účely tohto dokumentu bude pod pojmom architektúra myslený opis charakteristiky a bezpečnostných aspektov informačných systémov, ako aj popis okolia aplikácií a systémov Spoločnosti.

V grafickej notácii pre účely dokumentácie GDPR je typicky použitá 2-vrstvá architektúra:

- funkčná (sieťová topológia, bezpečnosť)
- dátová (aplikačná, interakcia s užívateľom).

Schémy funkčnej a dátovej architektúry sú v prílohe č. 4.

4.2 Charakteristika čiastočne automatizovaných prostriedkov spracúvania

Informačným systémom sa rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými, ako automatizovanými prostriedkami spracúvania.

V čiastočne materializovanej forme, t.j. mimo automatizovaných prostriedkov sú spracúvané najmä údaje o ľudských zdrojoch Spoločnosti, životopisy uchádzačov o zamestnanie a účtovné a daňové údaje ktoré sú spracúvané podľa osobitných zákonov.

Agenda Mzdy spolu s agendou Personalistika zabezpečujú evidenciu zamestnancov, spracovanie miezd, automatický výpočet dávok nemocenského poistenia a odvodov do poistných fondov, dane z príjmu a ostatné zrážka zo mzdy. V tomto procese sú spracúvané všeobecne použiteľné identifikátory,

ktoré je možné zaradiť do osobitnej kategórie osobných údajov podľa Zákona. Spracovanie uvedenej agendy je zabezpečované Sprostredkovateľom na báze zmluvného vzťahu.

V čiastočne materializovanej forme, t.j. mimo automatizovaných prostriedkov sú spracúvané najmä údaje o ľudských zdrojoch Spoločnosti, životopisy uchádzačov o zamestnanie a účtovné a daňové údaje ktoré sú spracúvané podľa osobitných zákonov.

Tabuľka č. 3.: Zoznam informačných systémov osobných údajov

P. č.	Názov IS	Sprostredkovateľ	Osobitné kategórie OÚ	Verejná sieť
1	Osobné zložky zamestnancov	Nie	Áno	Nie
2	Účtovné a daňové doklady	Nie	Áno	Nie
3	Archívy	Nie	Nie	Nie

4.3 Charakteristika automatizovaných prostriedkov spracúvania

4.3.1 Lokácie

IT infraštruktúra je prevádzkovaná v Bratislave (Štefániková 49 – budova Úradu SAV).

4.3.2 Operačné systémy

Použité sú operačné systémy na platforme Windows.

Pracovné stanice sú vybavené OS Windows 7, Windows 8 a Windows 10.

4.3.3 Databázové systémy

Organizácia prevádzkuje viacero inštancií proprietárneho systému riadenia bázy dát MS SQL Server, ako aj inštaláciu databázového systému MySQL.

Jestvuje niekoľko lokálnych súborov formátu MS Excel, alebo množín súborov formátu MS Excel a MS Word zdieľaných prostredníctvom počítačovej siete na zdieľaných adresároch lokálneho úložiska dát.

4.3.4 Infraštruktúrne systémy

Organizácia prevádzkuje jeden doménový radič na báze MS Windows Server (AD) pre systém EIS SAV (Ekonomický Informačný Systém SAV – pre celú SAV). Dedikovaný súborový server báze NAS serveru, ktorý zabezpečuje zdieľanie diskového priestoru s jednotným zabezpečením, riadením prístupu a konfiguráciou.

Ďalšie typy serverov:

- Citrix farma,
- 6 virtuálnych serverov na báze Hyper-V,
- 1 virtuálny server na baze VMware,
- FTP, SFTP servery pre systém e-VEGA,
- Aplikačné servery (13 kusov),
- Testovacie servery.

4.3.5 Sieť

Sieť je rozdelená do 5 VLAN (servery, užívatelia a tlačiarne, VoIP, Softip, WiFi).
Všetky zariadenia sú za hardwarovým firewalom FortiNet. Na ktorom je zabezpečená správa povolení len na určité porty, potrebné pre komunikáciu, všetko ostatné (porty a služby) je prioritne zakázané. Ďalej je nastavené filtrovanie web stránok (porno, herne a pod). Vstup do siete z vonku je riadený cez VPN.

4.3.6 Zálohovanie

- V sieti (vo VLAN10) máme umiestnené 2 NAS servery určené pre uchovávanie záloh
- Pre zálohu MS SQL dát slúži inštalovaný systém MS Center 2012 R2 Data Protection Manager ukladanie záloh na diskové pole.

4.3.7 Kamerové monitorovacie systémy

Spoločnosť prevádzkuje kamerový systém, ktorým sa monitoruje prevádzkový priestor Spoločnosti. Vstup do monitorovaných priestorov je opatrený elektronickým vrátnikom a systémom vstupovej kontroly. Priestor je zreteľne označený ako monitorovaný.

Všetci zamestnanci sú oboznámení o výkone kamerového dohľadu, o účele výkonu a spôsobe využitia. Iné osoby bez dozoru niektorej oprávnenej osoby do monitorovaných priestorov nemajú povolený prístup. Povaha priestoru vylučuje prítomnosť širokej verejnosti, do ktorého možno voľne vstupovať a v ktorom sa možno voľne zdržiavať bez časového obmedzenia. Z uvedených dôvodov máme za to, že sa nejedná o priestory, kde človek očakáva súkromie a na kamerový systém sa nevzťahujú ustanovenia na monitorovanie priestorov prístupného verejnosti.

Z uvedeného monitorovania sa uchováva vizuálny záznam po dobu 15 dní, ktorý sa vyhodnocuje len v prípade identifikovaného incidentu. K záznamom má prístup len vopred vymedzený okruh oprávnených osôb.

Kamerový systém je prevádzkovaný za účelom kontrolného mechanizmu zamestnávateľa voči zamestnancom a jeho výkon sa uskutočňuje podľa článku 11 Zákonníka práce za účelom ochrany práva a právom chránených záujmov prevádzkovateľa alebo tretej strany. K monitorovacím a záznamovým zariadeniam kamerového systému majú zamestnanci Spoločnosti riadený prístup.

5 POSÚDENIE BEZPEČNOSTI SPRACÚVANIA

5.1 Bezpečnostné opatrenia

Prijatím bezpečnostných opatrení Spoločnosť znemožní neoprávneným osobám akýkoľvek nedovolený prístup k spracúvaným osobným údajom, manipuláciu s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov a oprávneným osobám zabezpečí prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení oprávnených osôb.

Špecifikácia opatrení je sústredená najmä na nasledujúci obsah:

a) popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,

b) rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb; ak to automatizované prostriedky spracúvania osobných údajov umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času zabezpečí zaznamenanie každého vstupu oprávnenej osoby do informačného systému,

c) rozsah zodpovednosti oprávnených osôb a zodpovednej osoby,

d) spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení,

e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

Popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia sa rozdeľuje na:

- špecifikáciu technických opatrení,
- špecifikáciu organizačných opatrení

Popis bezpečnostných opatrení, stav súladu s požiadavkami na bezpečnostné opatrenia je uvedený v prílohe č. 1 tejto Dokumentácie.

5.2 Špecifikácia technických opatrení

5.2.1 Technické opatrenia realizované prostriedkami fyzickej povahy

Úlohou **mechanických zábranných prostriedkov** (napr. mechanických zábran, mreží, kovových dverí, závor, oplotení a ďalších možných prekážok) je sťažiť alebo úplne znemožniť neoprávneným osobám vniknutie do chráneného objektu. Charakteristickým znakom mechanických zábranných prostriedkov je prielomová odolnosť. Rozdeľujú sa podľa základných skupín na vonkajšie mechanické zábranné prostriedky, stavebné prvky budov, otvorové výplne, úschovné objekty.

Úlohou **technických zabezpečovacích prostriedkov** (napr. poplachových systémov na hlásenie narušenia, systémov priemyselnej televízie, systémov kontroly vstupov do objektov a systémy slúžiace na elektronické preukazovanie totožnosti a oprávnenosti osôb, systémov na evidenciu dochádzky a systémov elektronickej požiarnej signalizácie, tiesňové systémy, zariadenia na detekciu látok a predmetov) je najmä detegovať, vyhodnocovať a zaznamenávať informácie z prostredia chráneného objektu o vstupe, prítomnosti, zásahoch a pohybe osôb, zariadení, vecí alebo dopravných prostriedkov v chránených objektoch.

Súvisiace opatrenia:

Opatrenie č. 1110	Zabezpečenie objektu pomocou mechanických zábranných prostriedkov a pomocou technických zabezpečovacích prostriedkov
Opatrenie č. 1120	Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu
Opatrenie č. 1130	Kontrola vstupu do objektu a chránených priestorov prevádzkovateľa
Opatrenie č. 1140	Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia
Opatrenie č. 1150	Bezpečné uloženie fyzických nosičov osobných údajov, vrátane bezpečného uloženia listinných dokumentov
Opatrenie č. 1160	Opatrenia pre zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek

5.2.2 Ochrana pred neoprávneným prístupom

Ochrana pred neoprávneným prístupom je zaručenie jedného z troch základných atribútov informačnej bezpečnosti „Dôvernosť“ (Confidentiality). Dôvernosť znamená, že k informáciám alebo dátam majú prístup len oprávnené osoby. Narušenie dôvernosti sa označuje ako nežiaduce sprístupnenie (disclosure).

Prístup k informáciám oprávnených osôb je nutné riešiť minimálne na úrovni právomocí a zodpovedností vyplývajúcich z pracovných náplní. Ak je potrebné rozlíšiť stupňa dôvernosti informácií, je možné použiť tzv. klasifikačnú schému informácií ktorá rozdelí informácie od voľne dostupných až po dôverné informácie.

Súvisiace opatrenia:

Opatrenie č. 1210	Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia
Opatrenie č. 1220	Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza

5.2.3 Riadenie prístupu oprávnených osôb

Virtuálny priestor je interaktívne prostredie informačných systémov, umelá skutočnosť vytvorená programovými prostriedkami počítača. Virtuálna alebo tiež digitálna identita je individuálny prejav jedinca v tomto virtuálnom priestore. Pojmom virtuálna alebo digitálna identita sú označované akékoľvek autentizačné informácie v informačných systémoch, t.j. prístupové práva do systémov, prihlasovacie mená, certifikáty, užívateľské profily, užívateľské kontá, atď.

Manažment identít (Identity management, IdM) sú všetky úlohy v súvislosti s vytvorením, identifikáciou, administráciou, klasifikáciou, zmenami, zálohovaním, auditom, reportingom a rušením virtuálnych identít, t.j. spravovanie virtuálnych identít počas celého ich životného cyklu. Týmto procesom je riadený rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb.

Riadenie prístupu oprávnených osôb je implementácia a prevádzkovanie procesu a systému určeného na manažment identít, napr. vytvárania, údržby a rušenia používateľských účtov v aplikáciách, prideľovanie oprávnení používateľom, centralizovaná správa používateľov a riadenie ich prístupových práv do rôznych aplikácií.

Prístupové práva v aplikáciách a systémoch sú spravované pomocou systému MS Active Directory (ďalej len AD). Systém AD umožňuje automatizovať a zjednotiť procesy manažmentu identít, prideľovania a riadenia prístupových práv používateľov IS.

Podstatou riešenia je centralizovaná administrácia identít používateľov informačného systému a prístupových práv nezávislá na cieľových systémoch v ktorých sú prístupové práva riadené. Popis organizačného zaradenia a pracovnej pozície sa premieta do prístupových práv používateľov v aplikáciách (cieľových systémoch).

Manažment logov (log management, LM) Týmto procesom je riešená spätná identifikácia osoby, miesta a času zaznamenanie každého vstupu oprávnenej osoby do informačného systému.

LOG (inak tiež „denník“) je riadkový referenčný záznam o udalostiach a aktivitách systému, siete, aplikácie alebo používateľa. Log sa skladá z logovacích záznamov; každý záznam v sebe nesie informáciu súvisiacu s konkrétnou udalosťou. Logy sú kategorizované z hľadiska typu aktivity.

Log manažment pokrýva nasledujúce podprocesy:

- prenos a zber logov
- agregácia a rotácia logov
- dlhodobé uchovanie a zabezpečenie logov
- analýza logov (v reálnom čase, ad hoc analýza, forenzná analýza)
- vyhľadávanie logov a reporting
- prehliadanie logov, korelácia logov a vizualizácia hlásení

Pri návrhu auditných politík jednotlivých systémov je potrebné mať za cieľ získať najmä nasledujúce typy logov:

- Pokusy o získanie prístupu k existujúcim identitám
- Pokusy o prístup ku zdrojom
- Neautorizované zmeny používateľských účtov, skupín alebo služieb
- Podozrivé, alebo neautorizované vzorky sieťovej prevádzky

Súvisiace opatrenia:

Opatrenie č. 1310	Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov
Opatrenie č. 1320	Riadenie privilegovaných prístupov v informačných systémoch

Opatrenie č. 1330	Zaznamenávanie prístupu a aktivít jednotlivých oprávnených osôb v informačnom systéme

5.2.4 Riadenie zraniteľností

Riadenie zraniteľností, alebo vyhľadávanie a odstraňovanie technických zraniteľností („**vulnerability assessment**“), je aktivita zameraná na minimalizáciu dopadov zneužitia zistených technických zraniteľností systémov.

Škodlivý kód (**Malware**) je taký počítačový kód, ktorý spôsobuje narušenie zabezpečenia za účelom poškodenia počítačového systému. Výraz „Malware“ pochádza zo spojenia dvoch anglických slov malicious (škodlivý) a software (softvér).

Proces aktualizácie operačného systému a programového aplikačného vybavenia sa tiež nazýva „**manažment záplat**“ („patch management“). Jedná sa o proces riadenia zmien medzi starými a novými súbormi a proces aplikácie tohto súpisu zmien na staré súbory tak, že sú získané súbory nové. Aplikáciou záplat je vykonávaná aktualizácia softvéru. Aktualizácia softvéru je postup, pri ktorom je do počítača inštalovaná novšia verzia programového vybavenia zvyčajne z dôvodu nových vlastností SW.

Súvisiace opatrenia:

Opatrenie č. 1410	Opatrenia pre detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu
Opatrenie č. 1420	Ochrana pred nevyžiadanou elektronickou poštou
Opatrenie č. 1430	Používanie legálneho a prevádzkovateľom schváleného softvéru
Opatrenie č. 1440	Opatrenia pre zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia
Opatrenie č. 1450	Vynútenie pravidiel sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania, filtrovanie sieťovej komunikácie.
Opatrenie č. 1460	Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík

5.2.5 Sieťová bezpečnosť

Sieťová bezpečnosť je vo všeobecnosti implementácia a prevádzkovanie bezpečnostných prvkov týkajúcich sa zabezpečenia informačných aktív na úrovni prevádzky v sieťovej a komunikačnej infraštruktúre.

Súvisiace opatrenia:

Opatrenie č. 1510	Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
Opatrenie č. 1520	Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti, segmentácia počítačovej siete
Opatrenie č. 1530	Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia pre zamedzenie pripojenia k určitým adresám, pravidlá pre používanie sieťových protokolov
Opatrenie č. 1540	Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete

5.2.6 Zálohovanie

Zálohovanie je implementácie a prevádzkovanie systému a procesu určeného na vytváranie kópií dát pre prípad potreby obnovenia aktuálne spracúvaných alebo nedávno uložených dát, ak došlo k ich poškodeniu alebo zničeniu.

Súvisiace opatrenia:

Opatrenie č. 1610	Testovanie funkčnosti záložných dátových nosičov
Opatrenie č. 1620	Vytváranie záloh s vopred zvolenou periodicitou
Opatrenie č. 1630	Určenie doby uchovávanie záloh a kontrola jej dodržiavania
Opatrenie č. 1640	Test obnovy informačného systému zo zálohy
Opatrenie č. 1650	Bezpečné ukladanie záloh

5.2.7 Likvidácia osobných údajov a dátových nosičov

Implementácia a prevádzkovania systému a procesu nenávratného zničenia údajov po skončení ich životnosti, alebo pri pominutí účelu ich spracovania, vrátane postupov fyzickej likvidácie pamäťových médií.

Súvisiace opatrenia:

Opatrenie č. 1710	Technické opatrenia pre bezpečné vymazanie osobných údajov z dátových nosičov
Opatrenie č. 1720	Zariadenie na mechanické zničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií)

5.3 Špecifikácia organizačných opatrení

5.3.1 Personálne opatrenia

Personálne opatrenia sú procesy a aktivity súvisiace s výberom, určením a kontrolou osôb, ktoré majú mať prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení, ktoré môžu manipulovať s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a ktoré môžu manipulovať s nosičmi osobných údajov. Oblasť personálnej bezpečnosti je preto zameraná predovšetkým na nasledujúce činnosti:

- **Prijímanie zamestnancov do pracovného pomeru** (Pri prijímaní zamestnancov do zamestnaneckého pomeru sa bežne overuje dosiahnuté vzdelanie a potrebná kvalifikácia spolu s odbornými predpokladmi pre vykonávanie novej funkcie)
- **Činnosť zamestnancov počas pracovného pomeru** (Pre pracovný pomer je nevyhnutné stanovenie povinností, práv a zodpovednosti pre každého zamestnanca, vrátane definície možných sankcií, alebo postihov v prípade neplnenia povinností a zodpovedností)
- **Hodnotenie zamestnancov** (V priebehu pracovného pomeru sa pri pravidelnom hodnotení zamestnancov vytvárajú príležitosti, smerujúce k predchádzaniu nespokojnosti, ktorá by mohla viesť k spôsobeniu škody)
- **Vzdelávanie zamestnancov** (zabezpečenie pravidelného vzdelávania zamestnancov, a to nielen pre zvýšenie ich kvalifikácie, ale aj pre utváranie ich bezpečnostného povedomia)
- **Riešenie problémov pri ohrození zamestnancov** (zamestnanci sa môžu stať terčom útokov, alebo nátlaku zo strany kriminálneho prostredia. Pre eliminovanie takýchto prípadov je nevyhnutné vypracovanie a prijatie jednoznačných postupov, ktoré umožnia minimalizovať dopady súvisiace s možným vydieraním, alebo nátlakom na zamestnancov organizácie)
- **Ukončenie pracovného pomeru zamestnancov** (významné z pohľadu zrušenia existujúcich prístupových práv zamestnanca ku všetkým zdrojom a aktívam organizácie. Zamestnanci s prístupom k citlivým údajom musia byť poučení a zaviazaní k mlčanlivosti aj po ukončení pracovného pomeru na definované časové obdobie.)

Súvisiace opatrenia:

Opatrenie č. 2110	Poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi
Opatrenie č. 2111	Poučenie o právach a povinnostiach vyplývajúcich zo zákona alebo osobitného predpisu a zodpovednosti za ich porušenie
Opatrenie č. 2112	Vymedzenie osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh
Opatrenie č. 2113	Určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov
Opatrenie č. 2114	Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi
Opatrenie č. 2115	Vymedzenie zodpovednosti za porušenie zákona alebo osobitného predpisu
Opatrenie č. 2120	Poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a

	mimo týchto priestorov)
Opatrenie č. 2130	Určenie zodpovednej osoby
Opatrenie č. 2140	Vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií)
Opatrenie č. 2150	Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)
Opatrenie č. 2160	Práca na diaľku a pravidlá mobilného spracovania dát

5.3.2 Riadenie aktív

Proces sa tiež nazýva „**konfiguračný manažment**“, t.j. proces zodpovedný za udržiavanie informácií o informačných aktívach a konfiguračných položkách vyžadovaných pre dodávku IT služby vrátane vzájomných vzťahov konfiguračných položiek a to počas celého životného cyklu informačných aktív. Proces úzko súvisí s procesom manažmentu zmien, ktorý zodpovedný za sledovanie a reportovanie hodnoty a vlastníctva informačných aktív počas ich životného cyklu.

Súvisiace opatrenia:

Opatrenie č. 2210	Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia
Opatrenie č. 2220	Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou
Opatrenie č. 2230	Určenie vlastníctva aktív a zodpovednosti za riziká
Opatrenie č. 2240	Pravidlá a postupy pre klasifikáciu informácií a súbor postupov na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou
Opatrenie č. 2250	Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií
Opatrenie č. 2260	Opatrenia pre vrátenie aktív patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo prevádzkovej zmluvy

5.3.3 Riadenie prístupu oprávnených osôb k osobným údajom

Proces, ktorý je zodpovedný za znemožnenie akéhokoľvek nedovoleného prístupu neoprávnených osôb k spracúvaným osobným údajom, manipulácii s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov a zároveň zabezpečenie prístupu oprávneným osobám k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení oprávnených osôb.

Súvisiace opatrenia:

Opatrenie č. 2310	Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa
Opatrenie č. 2320	Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)
Opatrenie č. 2330	Pravidlá pre prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb
Opatrenie č. 2340	Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov
Opatrenie č. 2350	Pravidlá pre vzájomné zastupovanie oprávnených osôb
Opatrenie č. 2360	Pravidlá pre odstránenie alebo zmenu prístupových práv oprávnených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, prípadne prispôsobenie zmenám rolí

5.3.4 Organizácia spracúvania osobných údajov

Implementácia a údržba procesu, ktorým Spoločnosť zabezpečí bezpečný, udržateľný, opakovateľný a kontrolovateľný proces spracúvania osobných údajov alebo manipulácie s nosičmi osobných údajov v rozsahu zodpovedajúcom účelu spracovania.

Súvisiace opatrenia:

Opatrenie č. 2410	Pravidlá spracúvania osobných údajov v chránenom priestore
Opatrenie č. 2420	Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby
Opatrenie č. 2430	Režim údržby a upratovania chránených priestorov
Opatrenie č. 2441	Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie)

	mimo chránených priestorov a vymedzenie zodpovedností
Opatrenie č. 2442	Pravidlá používania automatizovaných prostriedkov spracúvania (napr. počítače, notebooky) mimo chránených priestorov a vymedzenie zodpovedností
Opatrenie č. 2443	Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností

5.3.5 Likvidácia osobných údajov

Implementácia a prevádzkovanie procesu nenávratného zničenia osobných údajov po skončení ich životnosti, alebo pri pominutí účelu ich spracovania, vrátane postupov fyzickej likvidácie pamäťových médií.

Súvisiace opatrenia:

Opatrenie č. 2510	Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)

5.3.6 Porušenia ochrany osobných údajov

Jednou z kľúčových zodpovedností vedenia Spoločnosti pri spracúvaní osobných údajov je zavedenie procesu riešenia bezpečnostných incidentov. Schopnosť Spoločnosti efektívne reagovať na identifikovaný incident je závislá od kvalitnej prípravy na všetky potenciálne udalosti, ktoré by mohli nepriaznivo pôsobiť na citlivé informačné aktíva Spoločnosti.

Ak sa incident týka kritických informačných aktív, jeho zvládnutie si vyžaduje komplexné podchytenie, presnú analýzu a uvážlivú reakciu. Príprava riešenia incidentov preto musí byť nevyhnutne založená na dôkladnom plánovaní zdrojov ale najmä na včasnom vybudovaní a otestovaní reakčných procedúr. Implementácia procesov reakcie na bezpečnostné incidenty je podmienená správnym pochopením celého životného cyklu incidentu od jeho vzniku až po uzatvorenie a ponaučenie.

Najmä pri vyššej komplexite informačných systémov je nanajvýš vhodné, aby bol vopred ustanovený a priebežne školený špecializovaný tím, ktorého úlohou bude správne reagovať na identifikované incidenty, ktorý bude schopný včas prijať protiopatrenia, zabezpečiť zber dôkazov pre ďalšie vyšetrovanie incidentu a prípadné vyvodenie pracovnoprávnych alebo trestnoprávnych dôsledkov.

Proces má opisovať životný cyklus incidentu, aktivity, z ktorých je zložený proces riešenia incidentu.

Hlavným cieľom procesu **Manažment kontinuity IT služieb** (ITSCM) je zabezpečiť schopnosť ďalej poskytovať vopred určený a dohodnutý stupeň IT služieb, ktoré sú potrebné na fungovanie biznis procesov v prípade závažných incidentov alebo katastrof tak, aby sa obmedzila úroveň prípadnej škody vyplývajúcej z havárií a katastrof. V záujme dosiahnutia tohto cieľu, proces ITSC management podporuje BCM proces zabezpečením toho, aby potrebná IT infraštruktúra (počítačové systémy, siete, aplikácie, telekomunikačné služby, technická podpora) mohla byť obnovená v potrebnom a dohodnutom časovom rámci a rozsahu.

Proces ITSCM nepokrýva dlhotrvajúce riziká spojené napr. so zmenou orientácie biznisu, diverzifikáciou, alebo reštrukturalizáciou. Analýza, ošetrenie alebo akceptácia tohto typu rizika musí byť riešená súčasne s implementáciou takého typu zmeny.

Proces ITSCM taktiež nepokrýva malé technické chyby, pokiaľ nemajú závažný dopad na biznis (toto rieši proces zvaný incident management).

ITSC plán

ITSC plán je formalizovaný dokument, ktorý popisuje všetky kroky potrebné pre obnovu IT služby a zabezpečenie jej dostupnosti v dopredu definovanej lokalite a to v prípade závažných incidentov alebo katastrof. Jeho základným poslaním je umožniť vykonávateľovi ITSC plánu poskytnúť návod pre konateľnú obnovu IT služby resp. oblasti IS.

ITSC plán pre každý systém by mal obsahovať Konkrétna situácia, ktorej riešenie popisuje ITSC plán. Každý ITSC plán by mal obsahovať 4 základné scenáre, pokiaľ infraštruktúra konkrétnej technologickej oblasti je pre nich prispôsobená:

- nedostupnosť budovy,
- nedostupnosť SW,
- nedostupnosť HW,
- nedostupnosť dát.

V rámci procesu nasadzovania nových riešení do prevádzky je odporúčaná príprava tzv. ITSC plánu, ktorý musí byť otestovaný ešte pred oficiálnym odovzdaním riešenia do prevádzky. ITSC plán by mal byť súčasťou dokumentácie každého informačného systému

Manažment kontinuity činností alebo tiež **Business continuity management** (BCM) je riadiaci proces, ktorý preventívne identifikuje predbežné ohrozenia spoločnosti a prípadný dopad týchto ohrození na jej činnosť a tým umožňuje Spoločnosti ubrániť sa strate časti alebo celej prevádzkovej kapacity. Referencie sa týkajú série iniciatív, ktorých cieľom je obmedziť úroveň škody vyplývajúcej z havárií a katastrof priamo alebo nepriamo ovplyvňujúcich Spoločnosť.

Tabuľka č. 4.: Kategorizácia udalostí s dopadom na kontinuitu činností

Typy udalostí	Popis udalosti s dopadom na kontinuitu	Príklady udalostí s dopadom na kontinuitu
Nepatrné (akceptovateľné) prerušenia kontinuity činnosti	Nepatrné (akceptovateľné) prerušenia kontinuity predstavujú najčastejšie prípady prerušení. Sú spôsobené udalosťami s malým dopadom na prevádzku spoločnosti a sú spôsobené nefunkčnosťou služby/zdroja, ktoré nie sú kritické pre obchod alebo kritické udalosti charakterizované krátkym trvaním	Táto kategória zahŕňa napr. nedostupnosť aplikácií, ktoré majú nízky dopad na obchodné procesy, nedostupnosť, ktorá je ohraničená v čase, dočasná nedostupnosť nie kritických objektov, krátka strata kritických aplikácií bez rizika dopadu na obchodné činnosti, atď.
Potenciálne riziká prerušenia kontinuity činnosti	I keď nespôsobujú okamžitú nedostupnosť, potenciálne riziká sú kritické udalosti, ktoré ukazujú na významné prerušenie prevádzky.	Táto kategória udalostí zahŕňa napr. zlyhanie dodávky elektrickej energie v budove, v ktorej fungujú kritické zdroje spoločnosti, aktiváciu zdrojov neprerušiteľného napájania elektrickej energie spôsobenej black out-om v strategických objektoch spoločnosti, nefunkčnosť protipožiarnych systémov v lokalitách, ktoré sú kritické pre spoločnosť, teroristický poplach, protesty aktivistov, poplach civilnej ochrany (napr. povodeň, požiar), pripravovaná systémová údržba, záťažový test výpadku elektrickej energie, a pod.
Vážne prerušenie kontinuity činnosti	kritické udalosti, ktoré spôsobujú prerušenie vitálnych a nepretržite dôležitých procesov resp. služieb kritických pre obchod. Môžu byť spôsobené logistickými, organizačnými, technologickými alebo aplikačne orientovanými udalosťami.	Táto kategória zahŕňa aj udalosti ako sú úplná alebo čiastočná dočasná nedostupnosť priestorov alebo zamestnancov s právom rozhodovania, spôsobenú vyhrážkou bombou, požiarom, atď.

Úroveň riadenia krízových situácií

Úroveň 1 – **Bežné riadenie**: situácia, ktorá môže byť riadená samotnými útvarmi prostredníctvom bežných procesov v spoločnosti. Platí to pre všetky udalosti, ktoré môžu spôsobiť nepatrné (akceptovateľné) prerušenia kontinuity činnosti.

Úroveň 2 – **Monitoring/ pohotovosť**: situácia, ktorá vytvára alebo môže vytvoriť významné dopady na ľudí a/alebo infraštruktúru, ktoré znamenajú možnú vážnu hrozbu, aj keď v špecifickej oblasti, pre reputáciu alebo fungovanie spoločnosti. Toto je úroveň krízovej udalosti spojená s vážnymi prerušeniami kontinuity činnosti a potenciálnymi rizikami prerušenia kontinuity činnosti.

Úroveň 3 – **Stav krízy**: situácia, ktorá vytvára alebo je schopná vytvoriť katastrofálne zničenie, t.j. trvalú stratu aktív (IT systém, infraštruktúra, budovy) alebo ľudských zdrojov. To je úroveň krízy spojená s haváriou/katastrofou. Na tejto úrovni krízového stavu môže byť rozhodnuté o zavedení opatrení kontinuity činnosti, ktoré sú spracované v pláne kontinuity činností a riadené sú procesmi manažmentu kontinuity IT služieb.

Súvisiace opatrenia:

Opatrenie č. 2610	Postup pri oznamovaní porušenia ochrany osobných údajov dozornému orgánu a dotknutej osobe na účel včasného prijatia preventívnych alebo nápravných opatrení
Opatrenie č. 2620	Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách
Opatrenie č. 2630	Evidencia porušení ochrany osobných údajov a použitých riešení
Opatrenie č. 2640	Postupy pre identifikáciu a riešenie jednotlivých typov porušení ochrany osobných

	údajov
Opatrenie č. 2650	Postupy pre odstraňovanie následkov porušení ochrany osobných údajov
Opatrenie č. 2660	Postupy zaručenia kontinuity činností pri haváriách, poruchách a iných mimoriadnych situáciách
Opatrenie č. 2670	Postupy pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania

5.3.7 Kontrolná činnosť

Hlavným poslaním procesu kontroly je včasné a hospodárne preverovanie, analýza a regulácia odchýlok zisteného skutočného stavu spracúvania osobných údajov so stavom predpísaným, to znamená stavom ustanoveným týmto bezpečnostným projektom. Kontrola je dynamický a permanentne prebiehajúci proces, je nástrojom na meranie a hodnotenie výkonnosti, efektívnosti a kvality.

Proces kontroly pokrýva požiadavku prevádzkovateľa na včasné a hospodárne preverovanie, analýzu a reguláciu odchýlok zisteného skutočného stavu spracúvania osobných údajov so stavom predpísaným. Kontrola je proces na meranie a hodnotenie výkonnosti, efektívnosti a kvality.

V zozname kontrolných činností je uvedený spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení.

Systém vnútornej kontroly zahŕňa všetky regulačné opatrenia, kontrolné aktivity a pôsobenie kontrolných mechanizmov, uskutočňované na všetkých úrovniach riadenia a vykonávania činností v každej oblasti práce Spoločnosti. Systém vnútornej kontroly pozostáva z troch integrálnych úrovní:

- štatutárnej
- výkonnej
- kontrolnej

Štatutárna úroveň je zabezpečovaná prostredníctvom najvyššieho kontrolného orgánu spoločnosti zodpovedného za návrh, sledovanie a zavedenie:

- vhodného a účinného systému vnútorných kontrol,
- vnútorných predpisov, zásad a postupov ako aj dodržiavanie vonkajších požiadaviek.

Výkonná úroveň je zabezpečovaná prostredníctvom vedúcich zamestnancov – výkonných manažérov, pričom každý manažér je zodpovedný za dodržiavanie vnútorných a všeobecne záväzných právnych predpisov, smerníc, zásad a postupov uplatňovaných v Spoločnosti. Každý vedúci zamestnanec je zodpovedný za plánovanie a realizáciu vlastnej kontrolnej činnosti v ním riadených organizačných útvaroch v rámci procesov ICS (Internal Control System). Kontrolné činnosti a ich periodicita sú rozpracované pre špecifické druhy procesov a aktualizujú sa podľa potreby

Kontrolnou funkciou je poverený nezávislý audítor.

Zoznam typických kontrolných činností:

Systém vnútornej kontroly Spoločnosti je rozdelený na:

- procesnú kontrolu - ktorá je vykonávaná všetkými útvarmi v rámci bežných procesov
- mimoprocesovú kontrolu – t.j. nezávislá kontrolu (ktorú vykonáva nezávislý audítor.

Procesná kontrola (t.j. kontrola vykonávaná všetkými útvarmi) môže byť:

- priama – kde kontrolné mechanizmy sú priamou súčasťou pracovných postupov a bez ich vykonania nie je pracovný postup ukončený;
- nepriama (následná) – je súčasťou riadenia a jej predmetom je kontrola plnenia stanovených úloh, vykonávajú ju vedúci zamestnanci alebo nimi poverení zamestnanci, obvykle je súčasťou popisu práce a konkrétnych vnútorných predpisov,

Zoznam kontrol špecificky musí zahŕňať:

- skúmanie postupov riadenia rizík,
- skúmanie vnútorných kontrolných systémov,
- skúmanie informačných systémov a riadiacich postupov v Spoločnosti a jej pridružených spoločnostiach

Činnosť kontroly zahŕňa aj pravidelné testovanie transakcií, špeciálne vyšetrovania, vyhodnotenie regulačných požiadaviek a opatrení na prevenciu a odhaľovanie podvodov a trestných činností, overovanie dodržiavania externej legislatívy, predpisov, regulačných rozhodnutí a vnútorných predpisov a príslušných noriem a predpisov.

Za rozhodnutie o prijatí nápravných opatrení je zodpovedný CISO, CSO, CTO alebo CIO.

Súvisiace opatrenia:

Opatrenie č. 2710	Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie
Opatrenie č. 2720	Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa alebo sprostredkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)

5.3.8 Dodávateľské vzťahy

S cieľom zistiť, či je účel ďalšieho spracúvania v súlade s účelom, na ktorý́ boli osobné údaje pôvodne získané, by mal prevádzkovateľ po splnení všetkých požiadaviek zákonnosti pôvodného spracúvania zohľadniť okrem iného aj **existenciu primeraných záruk** v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania.

S cieľom zabezpečiť súlad s požiadavkami GDPR v súvislosti so spracúvaním, ktoré má v mene prevádzkovateľa vykonať sprostredkovateľ, by mal prevádzkovateľ pri poverovaní sprostredkovateľa spracovateľskými činnosťami využívať len takých sprostredkovateľov, ktorí poskytujú **dostatočné záruky**, najmä pokiaľ ide o odborné znalosti, spoľahlivosť a zdroje, na to, že prijmú technické a organizačné opatrenia, ktoré budú spĺňať požiadavky tohto nariadenia, vrátane požiadavky na bezpečnosť spracúvania. Vykonávanie spracúvania sprostredkovateľom by sa malo riadiť zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktorými by bol sprostredkovateľ viazaný́ voči prevádzkovateľovi a v ktorých by sa stanovil predmet a dobu spracúvania, povahu a účely spracúvania, typ osobných údajov a kategórie dotknutých osôb, a ktoré by mali zohľadniť osobitné úlohy a povinnosti sprostredkovateľa v kontexte spracúvania, ktoré sa má vykonať, a riziko pre práva a slobody dotknutých osôb. Prevádzkovateľ a sprostredkovateľ si môžu vybrať použitie individuálnej zmluvy alebo štandardných zmluvných doložiek. Po ukončení spracúvania v mene prevádzkovateľa by mal sprostredkovateľ podľa rozhodnutia prevádzkovateľa vrátiť alebo vymazať osobné údaje, pokiaľ podľa práva Únie alebo práva členského štátu, ktorému sprostredkovateľ podlieha, neexistuje požiadavka na uchovanie osobných údajov.

Norma **STN ISO/IEC 27002 Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti** v oblasti **existencie primeraných záruk** odporúča nasledovné ciele:

- Požiadavky informačnej bezpečnosti na zníženie rizík spojených s prístupom dodávateľov ku aktívam Spoločnosti by mali byť vopred odsúhlasené a formálne zdokumentované.
- S každým dodávateľom, ktorý môže mať prístup k informáciám Spoločnosti, ktorý ich môže spracúvať, ukladať, komunikovať alebo poskytovať infraštruktúrne komponenty by mali byť definované a zmluvne dohodnuté všetky relevantné požiadavky informačnej bezpečnosti.
- Zmluvy s dodávateľmi by mali obsahovať požiadavky týkajúce sa rizík informačnej bezpečnosti spojených so službami IKT
- Služby dodávateľov by sa mali pravidelne monitorovať a preskúmavať

- Zmluvy s dodávateľmi by mali obsahovať právo na pravidelné vykonávanie auditu informačnej bezpečnosti.
- Mali by byť riadené zmeny v ustanoveniach úrovne služieb vrátane požiadaviek na udržiavanie a zlepšovanie aktuálnych politík informačnej bezpečnosti, postupov a opatrení, berúc do úvahy kritickosť príslušných podnikových systémov a procesov opakovaného ohodnotenia rizík.

Súvisiace opatrenia:

Opatrenie č. 2810	Postup pre overenie dostatočných záruk
Opatrenie č. 2820	Začlenenie požiadaviek na ochranu údajov do požiadaviek pre nové systémy a do pravidiel pre vývoj a nákup systémov
Opatrenie č. 2830	Začlenenie požiadaviek na ochranu údajov do zmluvných vzťahov s dodávateľmi a tretími stranami
Opatrenie č. 2840	Testovanie bezpečnostných funkcií počas vývoja systémov
Opatrenie č. 2850	Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi

5.4 Systém riadenia informačnej bezpečnosti

Posúdenie vyspelosti procesu riadenia informačnej bezpečnosti je založené na hodnotení vyspelosti procesov riadenia informačnej bezpečnosti v Spoločnosti voči požiadavkám normy ISO 27001.

Jednotlivé ciele popísané v norme sú posudzované metodikou uvedenou v kapitole 2.1.

Vyspelosť systému riadenia informačnej bezpečnosti je uvedený v kapitole 0.

5.4.1 A.05 Politiky informačnej bezpečnosti

Politiky informačnej bezpečnosti

Súbor politík informačnej bezpečnosti by mal schváliť manažment, mal by sa vydať a oznámiť všetkým zamestnancom, ako aj relevantným tretím stranám.

Preskúmanie politiky informačnej bezpečnosti

Politika informačnej bezpečnosti by sa mala preskúmať v plánovaných intervaloch, ako aj okamžite pri výskyte významných zmien, čím sa zabezpečí jej kontinuálna vhodnosť, primeranosť a efektivita.

5.4.2 A.06 Organizácia informačnej bezpečnosti

Informačná bezpečnosť v projektovom riadení

Informačná bezpečnosť by mala byť prepojená aj riadením projektov v závislosti od typu projektu.

Kontakt so špeciálnymi záujmovými skupinami

Mali by sa udržiavať príslušné kontakty so špecifickými záujmovými skupinami alebo s inými fórami bezpečnostných špecialistov a s profesijnými komorami.

Kontakty s orgánmi moci

Mali by sa udržiavať príslušné kontakty s relevantnými orgánmi štátnej moci.

Oddelenie právomocí

Konfliktné povinnosti a oblasti zodpovednosti by mali byť oddelené, aby sa znížila možnosť na neoprávnenú úpravu alebo zneužitie aktív organizácie.

Politika pre mobilné zariadenia

Na riadenie rizík, ktoré vyplývajú z používania mobilných zariadení, mala by sa prijať politika a podporné bezpečnostné opatrenia.

Práca na diaľku

Mali by sa vyvinúť a implementovať postupy, prevádzkové plány a politiky týkajúce sa práce na diaľku.

Role a zodpovednosť v informačnej bezpečnosti

Každá bezpečnostná zodpovednosť by mala byť jednoznačne zadefinovaná a zabezpečená.

5.4.3 A.07 Personálna bezpečnosť

Disciplinárny proces

Mal by existovať disciplinárny proces pre zamestnancov, ktorí spôsobili narušenie bezpečnosti.

Manažérska zodpovednosť

Manažment by mal od zamestnancov a zmluvných partnerov vyžadovať uplatňovanie bezpečnosti v súlade so zavedenými politikami a postupmi organizácie.

Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť

Všetci zamestnanci organizácie a v prípade, že je to potrebné, aj zmluvní partneri by mali absolvovať vhodné školenie v oblasti bezpečnostného povedomia a mali by sa im pravidelne poskytovať aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie.

Pracovná náplň a podmienky zamestnania

Zmluvná dohoda so zamestnancom a zmluvným partnerom by mala definovať ich zodpovednosť a zodpovednosť organizácie za informačnú bezpečnosť.

Preverovanie

Mala by sa vykonať verifikačná previerka personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s príslušnými zákonmi, právnymi nariadeniami a etikou, ako aj vzhľadom na obchodné požiadavky, klasifikačný stupeň informácií, ku ktorým sa bude pristupovať, ako aj na vnímané riziká.

Zodpovednosti pri ukončení alebo zmene zamestnania

Mali by sa definovať zodpovednosť a povinnosti v oblasti informačnej bezpečnosti, ktoré budú platiť po ukončení alebo zmene zamestnania. Tie by sa mali oznámiť a vyžadovať ich prijatie od zamestnanca alebo zmluvného partnera.

5.4.4 A.08 Riadenie aktív

Fyzický prenos médií

Médiá obsahujúce informácie by mali byť chránené pred neautorizovanými prístupmi, pred zneužitím alebo pred poskytnutím za odplatu pri prenose.

Inventárny zoznam aktív

Aktíva prepojené s informáciami a zariadeniami, ktoré informácie spracúvajú, mali by byť označené a mal by sa vytvoriť zoznam, ktorý by sa mal udržiavať.

Klasifikácia informácií

Informácie by mali byť klasifikované na základe právnych požiadaviek, hodnoty, kritickosti a citlivosti na neautorizované prezradenie alebo úpravu.

Likvidácia médií

Médiá, ak nie sú viac potrebné, mali by sa likvidovať bezpečným spôsobom použitím formálnych postupov.

Označovanie informácií

Mal by byť zostavený a implementovaný príslušný súbor postupov na označovanie informácií a zaobchádzanie s nimi, a to v súlade s klasifikačnou schémou, ktorú organizácia prijala.

Práca s aktívami

Postupy na prácu s aktívami by mali byť vytvorené v súlade so schémou klasifikácie informácií, ktorá sa prijala v organizácii.

Prijateľné používanie aktív

Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií by mali byť identifikované, zdokumentované a implementované.

Riadenie zmazateľných médií

Zavedené postupy na riadenie prepisovateľných médií by mali byť v súlade s klasifikačnou schémou, ktorú prijala organizácia.

Vlastníctvo aktív

Aktíva udržiavané v inventári by mali mať vlastníka.

Vrátenie aktív

Všetci zamestnanci a zmluvní partneri by mali vrátiť akékoľvek aktíva patriace organizácii po ukončení ich pracovného pomeru, po vypršaní uzatvorenej dohody alebo prevádzkovej zmluvy.

5.4.5 A.09 Riadenie prístupov

Bezpečné postupy prihlasovania

Kde to vyžaduje politika prístupu, prístup do operačných systémov by mal byť riadený prostredníctvom bezpečného prihlasovacieho (log-on) postupu.

Obmedzenie prístupu k informáciám

Prístup k informáciám a funkciám aplikačných systémov by sa mal riadiť definovanou politikou riadenia prístupov.

Odstránenie alebo prispôsobenie prístupových práv

Prístupové práva všetkých zamestnancov a tretích strán, ktorí používajú informácie a zariadenia, ktoré spracúvajú informácie, mali by sa odstrániť pri ukončení ich zamestnania, zmluvy alebo dohody, príp. prispôsobiť zmenám.

Politika riadenia prístupov

Mala by byť zavedená politika riadenia prístupov, dokumentovaná a preskúmaná na základe pracovných a bezpečnostných požiadaviek.

Používanie privilegovaných programov

Používanie programov, ktoré môžu mať schopnosť obísť systémové a aplikačné opatrenia, malo by byť obmedzené a prísne riadené.

Používanie utajených autentizačných údajov

Od používateľov by sa malo vyžadovať, aby pri používaní autentizačných informácií dodržiavali praktiky prijaté v organizácii.

Preskúmanie prístupových práv

Vlastníci aktív by mali preskúmavať prístupové práva používateľov v pravidelných intervaloch.

Prístup do sietí a sieťových služieb

Používateľom by mal byť udelený prístup len k službám, na ktorých používanie boli konkrétne autorizovaní.

Realizácia používateľských prístupov

Mal by byť zavedený formálny proces na ustanovenie prístupov na priradenie alebo zrušenie prístupových práv pre všetky typy používateľov, systémov a služieb.

Registrácia a deregistrácia používateľov

Na umožnenie priradenia používateľských práv by mal byť zriadený formálny proces registrovania a deregistrovania používateľov.

Riadenie prístupu k zdrojovým kódom programu

Prístup k zdrojovému kódu programu by mal byť zakázaný.

Riadenie privilégií

Prideľovanie a využívanie privilégií by malo byť obmedzené a riadené.

Riadenie utajených autentizačných údajov

Prideľovanie utajených autentizačných údajov by malo byť riadené prostredníctvom formálneho riadiaceho procesu.

Systém riadenia hesiel

Systémy na riadenie hesiel by mali byť interaktívne a mali by poskytovať kvalitné heslá.

5.4.6 A.10 Šifrovanie, kryptografia

Manažment šifrovacích kľúčov

Na používanie, ochranu a riadenie životného cyklu šifrovacích kľúčov by sa mala vytvoriť a zaviesť politika na ich celý životný cyklus.

Politika pri používaní opatrení na šifrovanie

Na používanie šifrovacích opatrení na ochranu informácií by mali byť vytvorené a zavedené politiky.

5.4.7 A.11 Fyzická bezpečnosť a bezpečnosť prostredia

Bezpečné vyradenie alebo opätovné používanie zariadení

Všetky prvky zariadení obsahujúce úložné médiá by sa mali skontrolovať, čím sa zabezpečí, že všetky citlivé dáta a licencovaný softvér sú bezpečne zmazané alebo prepísané ešte pred vyradením alebo opätovným použitím zariadenia.

Bezpečnosť kabeláže

Elektrická alebo komunikačná kabeláž prenášajúca údaje alebo podporujúce informačné služby by mala byť chránená pred odpočúvaním, manipuláciou alebo poškodením.

Bezpečnosť zariadení mimo organizácie

Bezpečnosť by sa mala aplikovať aj na zariadenia mimo priestorov organizácie, pričom je potrebné brať do úvahy rozličné riziká vyplývajúce z práce mimo priestorov organizácie.

Nepoužívané (nepripojené) zariadenia

Používatelia by mali zabezpečiť, aby aj nepripojené zariadenia mali vhodnú ochranu.

Ochrana pred externými hrozbami a hrozbami prostredia

Malo by sa počítať s vytvorením a aplikovaním fyzickej ochrany pred prírodnými katastrofami, útokmi alebo nehodami.

Odstránenie aktív

Prístroje, informácie alebo softvér by sa nemali bez autorizácie brať mimo pracoviska.

Perimeter fyzickej bezpečnosti

Bezpečnostné perimetre by mali byť použité na ochranu citlivých alebo kritických informácií a zariadení spracúvajúcich tieto informácie.

Podporné služby

Zariadenia by mali byť chránené pred výpadkami elektrickej energie a inými anomáliami spôsobenými zlyhaním dodávky podporných služieb.

Politika čistého stola a prázdnej obrazovky

Mala by byť zavedená politika čistého stola, pokiaľ ide o dokumenty a prenosné médiá, a politika čistej obrazovky, pokiaľ ide o prostriedky spracúvania informácií.

Práca v bezpečnom prostredí

Mali by sa navrhnúť a aplikovať príslušné postupy na prácu v zabezpečených oblastiach.

Riadenie fyzických prístupov

Zabezpečené oblasti by mali byť chránené primeranými opatreniami na vstupe, aby sa zabezpečilo, že vstúpiť môžu len autorizované osoby.

Údržba zariadení

Zariadenia by sa mali správne udržiavať, aby sa zaistila ich nepretržitá dostupnosť a integrita.

Umiestnenie zariadení a ich ochrana

Zariadenia by mali byť umiestnené a chránené s cieľom obmedziť riziká vyplývajúce z hrozieb prostredia a riziká a príležitosti neautorizovaného prístupu.

Zabezpečenie kancelárií, miestností a prostriedkov

Mala by sa navrhnúť a zaviesť fyzická bezpečnosť pre miestnosti, kancelárie a zariadenia.

Zásobovacie a expedičné sklady

Prístupové body, akými sú zásobovacie a expedičné priestory, ako aj iné body, kde môže neautorizovaná osoba získať prístup do priestorov organizácie, mali by byť kontrolované, a ak je to možné, aj izolované od prostriedkov na spracúvanie informácií, čím sa zabráni neautorizovanému prístupu.

5.4.8 A.12 Prevádzková bezpečnosť

Dokumentované prevádzkové postupy

Prevádzkové postupy by mali byť dokumentované a udržiavané, dostupné pre všetkých používateľov, ktorí ich potrebujú.

Inštalácia softvéru na produkčné systémy

Mali by sa zaviesť postupy na riadenie inštalovania softvéru na prevádzkových systémoch.

Obmedzenia pri inštalácii softvéru

Na strategické riadenie inštalácie softvéru používateľmi by mali byť vytvorené a zavedené pravidlá.

Ochrana záznamov informácií

Informácie obsiahnuté v záznamoch, ako aj prostriedky na ich tvorbu by mali byť chránené pred neoprávnenými zásahmi a neautorizovaným prístupom.

Oddelenie vývoja, testovania a prevádzkového prostredia

Vývojové, testovacie a prevádzkové systémy by mali byť vzájomne oddelené, čím sa zníži riziko neautorizovaného prístupu alebo zmien v prevádzkovom prostredí.

Opatrenia auditu informačných systémov

Požiadavky na audit a aktivity zahŕňajúce kontroly prevádzkových systémov by sa mali starostlivo plánovať a odsúhlasiť, aby sa minimalizovalo riziko prerušení podnikových procesov.

Opatrenia proti škodlivému kódu

Mali by byť implementované opatrenia detekcie, predchádzania a obnovy na ochranu pred škodlivým kódom, kombinované s budovaním povedomia používateľov.

Riadenie kapacít

Používanie prostriedkov by sa malo monitorovať, dolaďovať a mali by sa robiť odhady budúcich požiadaviek na kapacity, čím sa zabezpečí dosiahnutie požadovanej výkonnosti systému.

Riadenie technickej zraniteľnosti

Mali by sa zhromažďovať včasné informácie o technickej zraniteľnosti využívaných informačných systémov, mala by sa zhodnocovať miera vystavenia sa zraniteľnosti a mali by sa zaviesť príslušné opatrenia na potlačenie týchto rizík.

Riadenie zmien

Zmeny v organizácii, obchodných procesoch, na prostriedkoch spracúvajúcich informácie a na systémoch by mali byť riadené.

Synchronizácia času

Hodiny na všetkých relevantných systémoch na spracúvanie informácií v rámci organizácie alebo v zabezpečených priestoroch by mali byť synchronizované prostredníctvom schváleného presného časového zdroja.

Zálohovanie informácií

Pravidelne by sa mali robiť a testovať záložné kópie dôležitých informácií a softvéru v súlade so schválenou politikou zálohovania.

Zaznamenávanie udalostí

Záznamy udalostí zaznamenávajúce aktivity používateľov, výnimky a udalosti informačnej bezpečnosti by sa mali vytvárať, uchovávať a pravidelne preskúmavať.

Záznamy činnosti správcov a operátorov

Aktivity systémového správcu a operátora by sa mali zaznamenávať a záznamy by sa mali chrániť a pravidelne preskúmavať.

5.4.9 A.13 Komunikačná bezpečnosť

Bezpečnosť sieťových služieb

Bezpečnostné funkcie, úrovne služieb a manažérske požiadavky týkajúce sa všetkých sieťových služieb by mali byť identifikované a zahrnuté do ustanovení o sieťových službách v prípade, ak sa tieto služby poskytujú vnútropodnikovo alebo prostredníctvom outsourcingu.

Dohody o výmene informácií

Mali by sa uzavrieť dohody o výmene informácií a softvéru medzi organizáciou a tretími stranami.

Oddeľovanie sietí

Skupiny informačných služieb, používateľov a informačných systémov by mali byť na sieťach oddeľované.

Politiky a postupy pri prenose informácií

Formálne politiky, postupy a opatrenia týkajúce sa výmeny by mali byť zavedené s cieľom chrániť výmenu informácií vykonávanú prostredníctvom všetkých druhov komunikačných zariadení.

Sieťové opatrenia

Siete by mali byť primerane riadené a spravované, čím sa zabezpečí ochrana informácií v systémoch a aplikáciách.

Výmena elektronických správ

Informácie, ktoré spadajú do kategórie vymieňaných elektronických správ, mali by byť vhodne chránené.

Zmluvy o dôvernosti alebo utajení

Požiadavky na zmluvy o dôvernosti alebo utajení, ktoré zohľadňujú potreby organizácie na ochranu informácií, mali by byť jasne definované, pravidelne preskúmavané a dokumentované.

5.4.10 A.14 Akvizícia, vývoj a údržba informačných systémov

Akceptačné testy systémov

Pre nový informačný systém, aktualizáciu a novú verziu by sa mali vytvoriť programy akceptačného testovania s príslušnými kritériami.

Analýza a špecifikácia bezpečnostných požiadaviek

Požiadavky spojené s informačnou bezpečnosťou by mali byť začlenené do požiadaviek pre nové systémy alebo by sa mali rozšíriť požiadavky na existujúce informačné systémy.

Bezpečné testovanie systémov

Testovanie bezpečnostných funkcií by sa malo vykonávať počas vývoja.

Obmedzenia zmien v softvérových balíkoch

Malo by sa predchádzať neopodstatneným modifikáciám softvérových balíkov a vykonávanie nevyhnutných a všetkých zmien by malo byť riadené.

Ochrana pri transakciách aplikačných služieb

Informácie obsiahnuté v transakciách aplikačných služieb by mali byť chránené, aby sa zabránilo nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam.

Ochrana testovacích údajov

Testovacie údaje by sa mali starostlivo vyberať, chrániť a riadiť.

Politika bezpečného vývoja

Pravidlá na vývoj softvéru a systémov by mali byť vytvorené a zavedené do procesu vývoja v rámci organizácie.

Postupy riadenia systémových zmien

Implementácia zmien do systémov v rámci životného cyklu by mala byť riadená prostredníctvom formálnych postupov riadenia zmien.

Princípy bezpečného vývoja systému

Mali by sa vytvoriť, dokumentovať, udržiavať a zaviesť princípy bezpečného vývoja systémov pre všetky činnosti spojené so zavedením informačných systémov.

Prostredie na bezpečný vývoj

Organizácie by mali vytvoriť a primerane chrániť vývojové prostredie na vývoj systémov a ich integráciu s úsilím, ktoré pokryje celý životný cyklus vývoja.

Technické preskúmanie aplikácií po zmene operačného systému

Pri zmene operačného systému by sa mala vykonať revízia kritických aplikácií, ako aj testovanie s cieľom zabezpečiť, že to nebude mať za následok negatívny vplyv na prevádzku organizácie alebo na bezpečnosť.

Vývoj externými zdrojmi

Vývoj softvéru prostredníctvom externých zdrojov by mal byť pod dohľadom organizácie a mali by sa monitorovať aktivity vývoja systému externými zdrojmi.

Zabezpečenie aplikačných služieb vo verejných sieťach

Informácie, ktoré sa používajú v aplikačných službách, používajúc verejné dátové siete, mali by byť chránené pred podvodnými aktivitami, pred aktivitami spochybňujúcimi zmluvné podmienky a pred neautorizovaným vyzradením alebo úpravou.

5.4.11 A.15 Riadenie vzťahov s dodávateľmi

Dodávateľské reťazce informačných a komunikačných technológií

Zmluvy s dodávateľmi by mali obsahovať požiadavky týkajúce sa rizík informačnej bezpečnosti spojených s informačnými a komunikačnými službami a produktmi siete dodávateľov.

Monitorovanie a preskúmanie dodávateľských služieb

Služby dodávateľov by sa mali pravidelne monitorovať a preskúmavať a pravidelne by sa mali vykonávať audity.

Politika informačnej bezpečnosti na vzťahy s dodávateľmi

Požiadavky informačnej bezpečnosti na zníženie rizík spojených s dodávateľskými prístupmi do aktív organizácie by mali byť odsúhlasené s dodávateľmi a formálne zdokumentované.

Riadenie zmien v službách dodávateľa

Zmeny v ustanoveniach služieb vrátane udržiavania a zlepšovania aktuálnych politík informačnej bezpečnosti, postupov a opatrení by mali byť riadené, berúc do úvahy kritickosť príslušných podnikových systémov a procesov opakovaného ohodnotenia rizík.

Určenie bezpečnosti v zmluvách s dodávateľmi

Mali by byť definované všetky relevantné požiadavky informačnej bezpečnosti a odsúhlasené s každým dodávateľom, ktorý môže mať prístup k informáciám organizácie, spracúvať ich, ukladať, komunikovať alebo poskytovať infraštruktúrne komponenty.

5.4.12 A.16 Riešenie incidentov informačnej bezpečnosti

Informovanie o zraniteľnostiach

Od zamestnancov a zmluvných partnerov, ktorí používajú informačný systém a služby organizácie, malo by sa požadovať, aby zaznačovali každý pozorovaný alebo podozrivý nedostatok v systémoch alebo službách a informovali o ňom.

Informovanie o udalostiach informačnej bezpečnosti

O udalostiach informačnej bezpečnosti by sa malo informovať vhodnými riadiacimi kanálmi tak rýchlo, ako je to možné.

Reakcia na incidenty informačnej bezpečnosti

Na incidenty informačnej bezpečnosti by sa malo odpovedať v súlade s dokumentovanými postupmi.

Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o riešení

Udalosti informačnej bezpečnosti by mali byť posúdené a malo by sa rozhodnúť, či budú klasifikované ako incidenty informačnej bezpečnosti.

Poučenie z incidentov

Poznatky získané z analýzy a riešenia incidentov informačnej bezpečnosti by sa mali použiť na zníženie pravdepodobnosti alebo následkov budúcich incidentov.

Zber dôkazov

Organizácia by mala definovať a prijať postupy na identifikáciu, zber, získanie a ochranu informácií, ktoré môže poskytnúť ako dôkaz.

Zodpovednosť a postupy

Mali by sa zaviesť zodpovednosť a postupy riadenia incidentov s cieľom zaistiť rýchly, efektívny a systematický ohlas na bezpečnostné incidenty.

5.4.13 A.17 Riadenie kontinuity činností

Dostupnosť zariadení na spracúvanie informácií

Zariadenia na spracúvanie informácií by mali byť zriadené s dostatočnou redundanciou, aby sa dosiahli požiadavky na dostupnosť.

Implementácia kontinuity informačnej bezpečnosti

Organizácia by mala vytvoriť, dokumentovať, zaviesť a udržiavať procesy, postupy a opatrenia na zabezpečenie požadovanej úrovne kontinuity pre informačnú bezpečnosť počas nepriaznivých situácií.

Overenie, preskúmanie a vyhodnotenie kontinuity informačnej bezpečnosti

Organizácia by mala overiť vytvorené a zavedené opatrenia na kontinuitu informačnej bezpečnosti v pravidelných intervaloch, aby sa zabezpečila ich platnosť a efektívna funkčnosť počas nepriaznivých situácií.

Plánovanie kontinuity informačnej bezpečnosti

Organizácia by mala určiť svoje požiadavky na informačnú bezpečnosť a kontinuitu riadenia informačnej bezpečnosti v nepriaznivých situáciách, napr. počas krízy alebo katastrofy.

5.4.14 A.18 Riadenie súladu

Identifikácia platnej legislatívy a zmluvných požiadaviek

Všetky relevantné štatutárne, regulačné a zmluvné požiadavky by mali byť explicitne definované, dokumentované a udržiavané v aktuálnej podobe pre každý informačný systém a organizáciu ako celok.

Nariadenie o šifrovacích opatreniach

Opatrenia na šifrovanie by sa mali zaviesť s cieľom dosiahnuť súlad so všetkými platnými dohodami, zákonmi a právnymi nariadeniami.

Nezávislé preskúmanie informačnej bezpečnosti

Prístup organizácie k riadeniu informačnej bezpečnosti (napr. ciele riadenia, opatrenia, politiky, procesy a postupy informačnej bezpečnosti) mala by preskúmať nezávislá entita v plánovaných intervaloch, alebo keď sa uskutočnia závažné zmeny.

Ochrana záznamov

Záznamy by mali byť chránené pred stratou, zničením a falzifikáciou v súlade so štatutárnymi, regulačnými, zmluvnými alebo podnikovými požiadavkami.

Práva duševného vlastníctva

Mali by sa implementovať vhodné postupy, ktoré by zabezpečili súlad so zákonnými, regulačnými a zmluvnými požiadavkami, pokiaľ ide o používanie materiálu v zmysle práv duševného vlastníctva a používania patentovaných softvérových produktov.

Preskúmanie technického súladu

Informačné systémy by sa mali pravidelne preskúmavať z hľadiska súladu s politikami a normami informačnej bezpečnosti organizácie.

Súkromie a ochrana osobných údajov

Súkromie a ochrana osobných údajov by mali byť zabezpečené na základe požiadaviek príslušnej legislatívy a príslušných nariadení.

Súlad s bezpečnostnými politikami a normami

Manažéri by mali pravidelne preverovať súlad spracúvania informácií v rozsahu zodpovednosti so znením príslušných bezpečnostných politík, noriem a iných bezpečnostných požiadaviek.

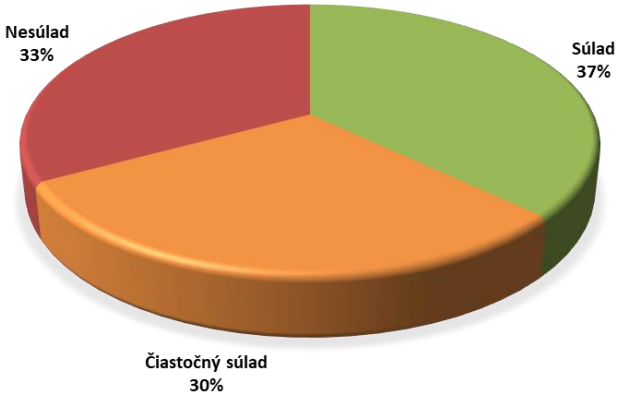
6 VÝSLEDKY ANALÝZY SÚLADU

6.1 Výsledok rozdielovej analýzy

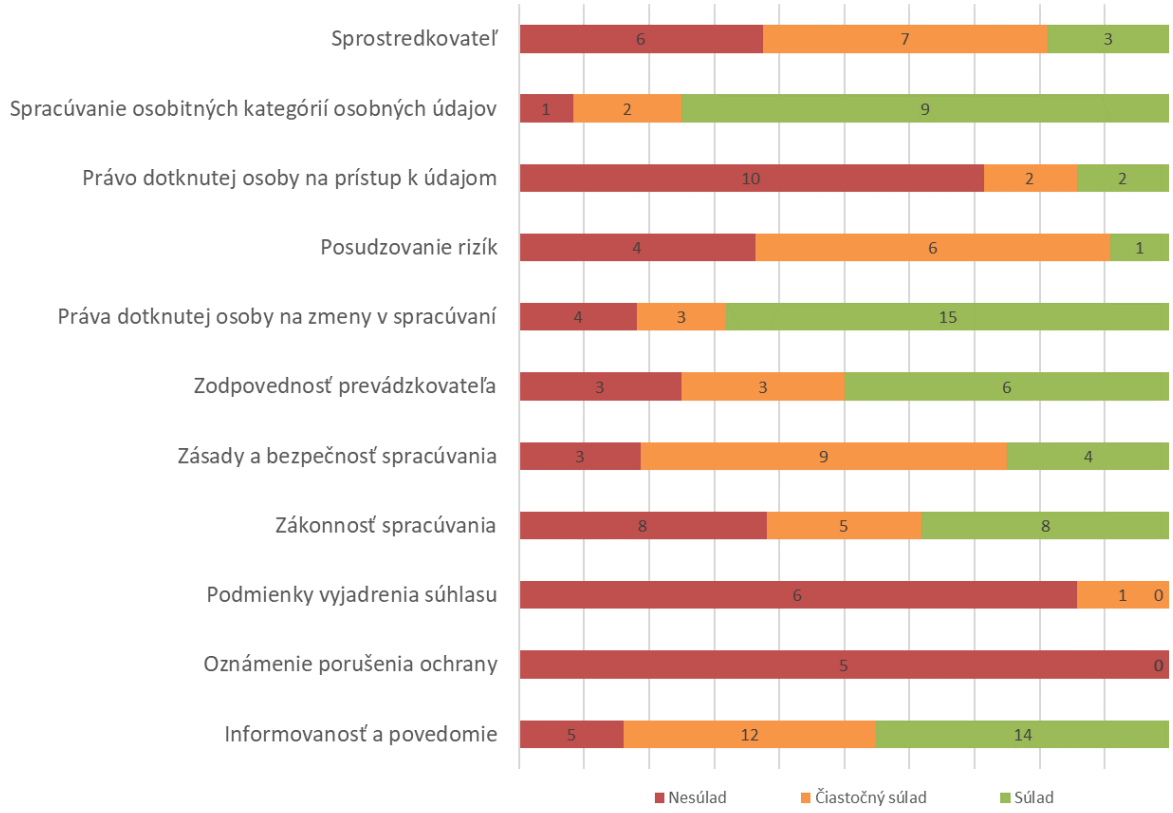
Rozdielová analýza je vykonaná najmä s ohľadom na základné zásady spracúvania osobných údajov v Spoločnosti, zmysle čl. 5 GDPR.

Graf č. 1 zobrazuje celkový stav súladu spracovania, graf č. 2 stav súladu vo vyššom detaile, podľa jednotlivých oblastí.

Graf č. 1. Celkový stav súladu voči požiadavkám GDPR



Graf č. 2. Stav súladu voči požiadavkám GDPR podľa oblastí



6.2 Výsledok hodnotenia vyspelosti procesov

Tabuľka č. 5.: Celkový stav vyspelosti procesov v roli Prevádzkovateľa

Hodnotený atribút procesu	Funkcia	Dokumentácia	Role	Činnosti	Nástroje	Údaje	Metrika
Celkový stav vyspelosti procesu podľa atribútu	3,09	2,46	3,91	3,73	3,36	2,95	2,27

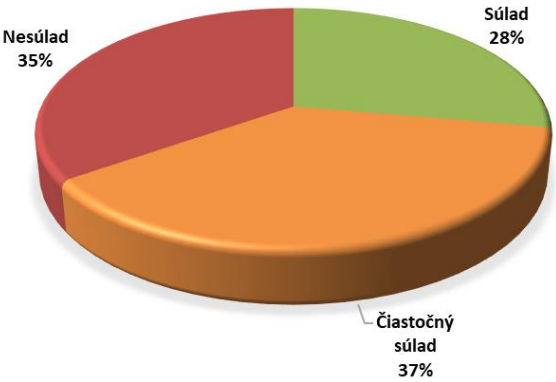
Výsledná hodnota vyspelosti procesov podľa bodového hodnotenia CMMI je **3,11**. Základné funkcie procesov sú plnené, dokumentácia je čiastočná bez jednotného prístupu , role procesov sú definované, role majú priradené osoby a právomoci, základné činnosti procesov sú vykonávané, používané nástroje sú schopné podporovať proces, ale sú bez integrácie do ďalších procesov, údaje sú dostupné, majú požadovanú kvalitu, nie sú však zdieľané v jednotnej údajovej základni, procesy nemajú vlastnú metriku, merania sú vykonávané nepriamo.

6.3 Výsledok posúdenia bezpečnosti spracúvania

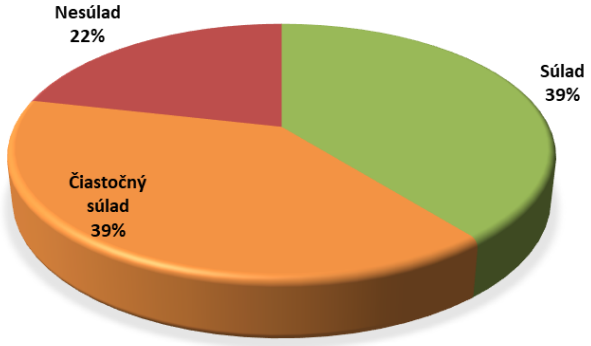
Analýza súladu je vykonaná s ohľadom na požiadavky na implementáciu technických a organizačných opatrení.

Graf č. 3 zobrazuje celkový stav súladu implementácie bezpečnostných opatrení, graf č. 4 stav súladu implementácie technických opatrení a graf č. 5 stav súladu implementácie organizačných opatrení,.

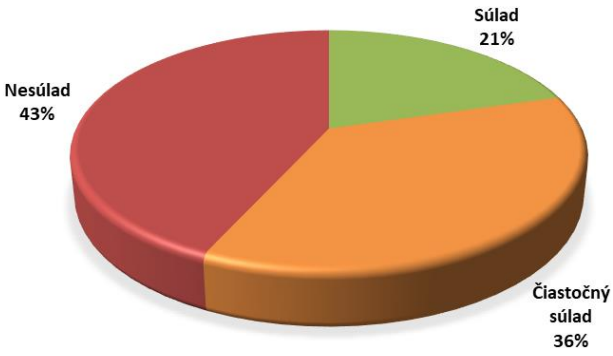
Graf č. 3. Celkový stav súladu implementácie bezpečnostných opatrení



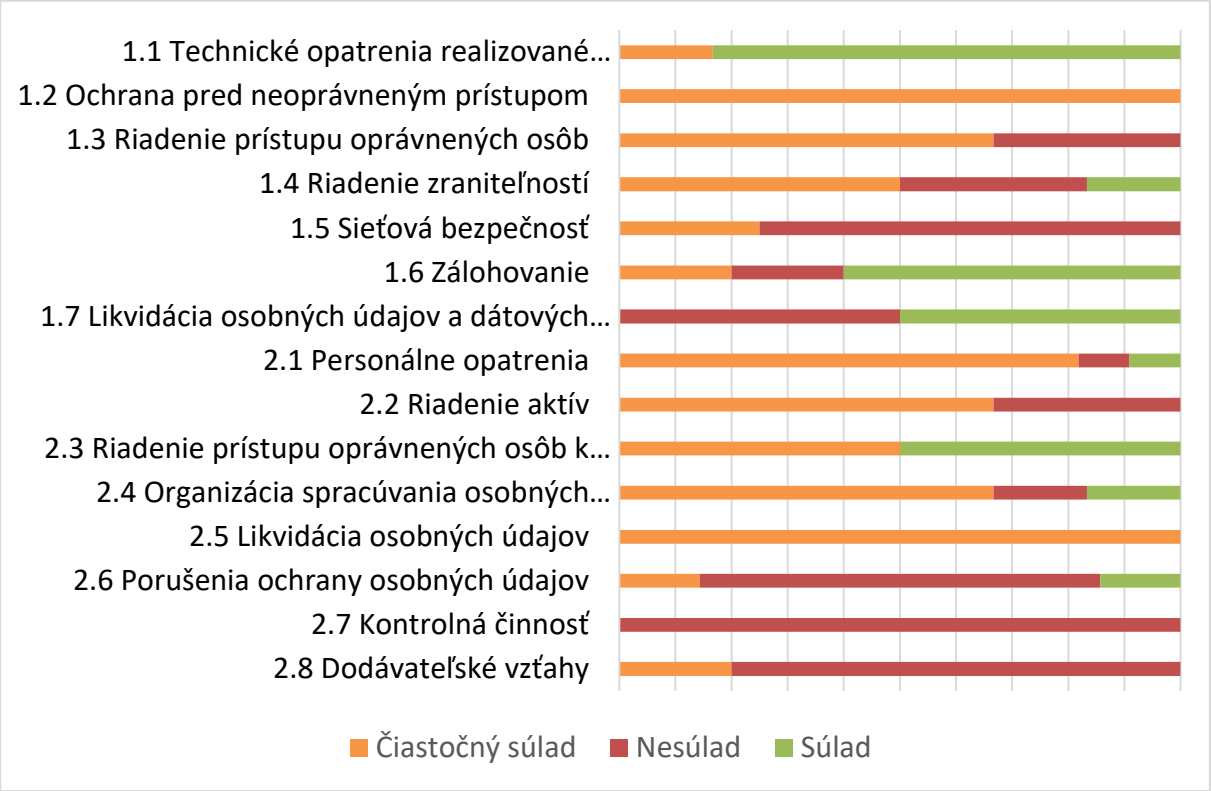
Graf č. 4. Celkový stav súladu implementácie technických opatrení



Graf č. 5. Celkový stav súladu implementácie organizačných opatrení

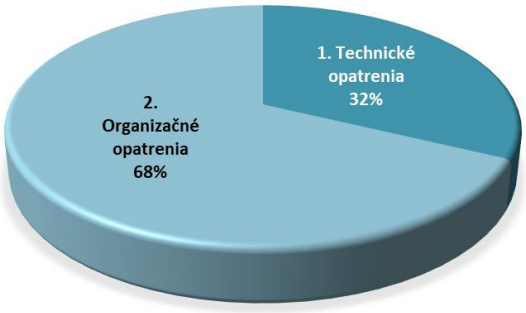


Graf č. 6. Stav súladu implementácie bezpečnostných opatrení podľa oblastí



Graf č. 7. Porovnanie súladu technických a organizačných opatrení

Graf č. 8. Porovnanie nesúladu / čiastočného súladu technických a organizačných opatrení



ANALÝZA RIZÍK

1 METODIKA ANALÝZY RIZÍK A POSÚDENIA VPLYVU NA OCHRANU ÚDAJOV

V zmysle čl. 35 ods. 1 GDPR ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.

Posúdenie má v zmysle čl. 35 ods. 1 obsahovať aspoň:

- systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ
- posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu
- posúdenie rizika pre práva a slobody dotknutých osôb a
- opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

Analýza rizík je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti a obsahuje najmä kvalitatívnu analýzu rizík. V zmysle niekoľkých medzinárodných noriem a publikácií o dobrej praxi manažmentu IT rizík je možné časť „analýza bezpečnosti informačného systému“ nazývať ďalej len „Analýza rizík“ (risk analysis).

Z dôvodu korektného uplatnenia metodiky riadenia IT rizika v Spoločnosti je riziko definované ako: **„riziko finančných a reputačných strát spôsobených narušením dôvernosti, integrity, dostupnosti, alebo sledovateľnosti informačných aktív Spoločnosti, vytvorených, uložených, spracúvaných, alebo prenášaných informačnými technológiami“.**

Používanie a rozvoj používaných informačných systémov ako aj zmeny prevádzkových procesov v závislosti na úrovni ich automatizácie môžu organizácii spôsobovať riziko.

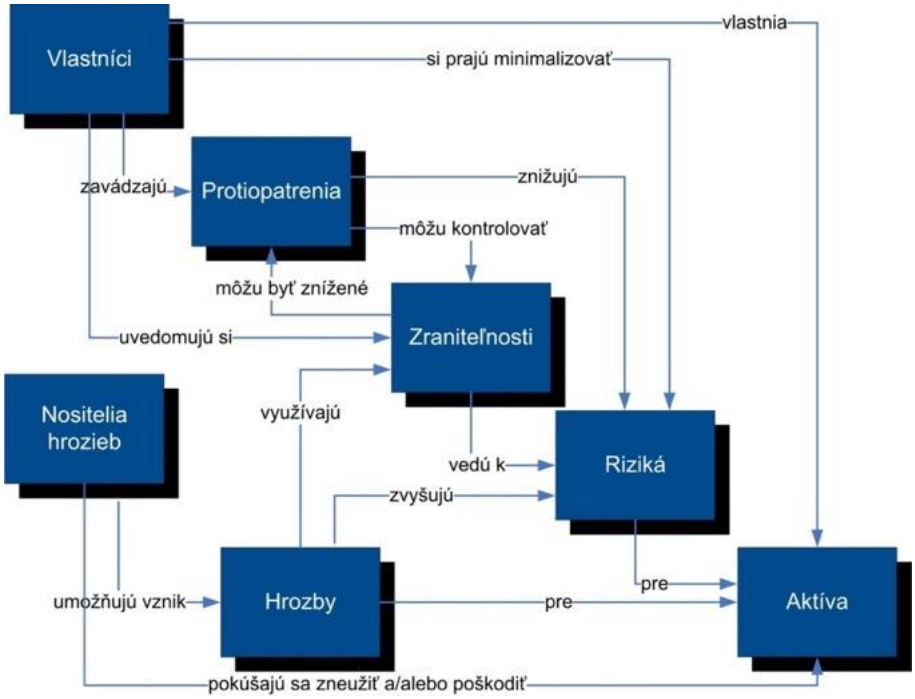
1.1 Posudzovanie rizika

Posudzovanie rizika je vo všeobecnosti prvým procesom v metodike riadenia rizika. Proces posudzovania rizika Spoločnosť používa na určenie závažnosti potenciálnej hrozby rizika asociovaného s IT systémom. Výstup procesu posudzovania rizika umožňuje navrhnúť primerané opatrenia na redukciu a elimináciu rizika v rámci procesu ošetrovania rizika.

Na určenie pravdepodobnosti budúcej škodlivej udalosti musia byť hrozby pôsobiace na informačné aktíva analyzované v spojitosti s potenciálnou zraniteľnosťou a opatreniami uplatnenými na príslušný informačný systém.

Vzťahy medzi jednotlivými entitami v procese manažmentu rizík je možné schematicky znázorniť v zmysle ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation: Security concepts and relationships:

Obrázok č.2. Vzťahy medzi jednotlivými entitami v procese manažmentu rizík



1.1.1 Posudzovanie rizík na globálnej úrovni

Klasifikácia informačných aktív priraďuje aktívam určitý stupeň dôležitosti, ktorý je založený na požiadavkách ich dostupnosti, dôvernosti, integrity a sledovateľnosti. Klasifikácia informačných aktív poskytuje základy pre stanovenie bezpečnostných požiadaviek pre informačné aktíva Spoločnosti a je základným elementom pre hodnotenie rizík informačných aktív, ktoré súvisia s nesprávnym používaním alebo narábaním s informačnými aktívami.

Informačné aktíva priamo podporujúce biznis procesy sú definované ako biznis aktíva. Biznis aktíva sa delia na nasledovné triedy:

- procesne dátové aktíva,
- aplikácie a služby,
- dokumenty.

V procese manažmentu IT rizík Spoločnosť pravidelne vykonáva analýzu rizík biznis aktív vo forme globálnej analýzy rizík (ďalej len GRA), resp. analýzu funkčného dopadu (ďalej len BIA).

V rámci GRA Spoločnosť prehodnocuje riziká obchodných a podporných procesov. Identifikuje hrozby pôsobiace na zraniteľnosti postihujúce procesy a ich podporné zdroje. V rámci GRA Spoločnosť klasifikuje procesy podľa ich kritickosti, integrity, dôvernosti a sledovateľnosti, podľa informácií ktoré sú v rámci procesu spracovávané.

GRA identifikuje na najvyššej úrovni závislosti medzi procesmi a aktívami ktoré ich podporujú. V rámci nej sú identifikované inherentné a zvyškové riziká pre všetky procesy, pričom výsledkom je rizikový profil Spoločnosti a zoznam najkritickejších rizík, ktoré Spoločnosti hrozia.

1.2 Identifikácia zraniteľností

Identifikácia rizík je založená na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužiteľných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti.

Proaktívne a realistické rozpoznanie hrozieb súvisiacich s vývojom v oblasti technológií spolu s následným prijímaním primeraných opatrení na elimináciu uvedených rizík zvyšuje účinnú ochranu majetku spoločnosti.

V rámci podprocesov riadenia rizík (analýza rizík, ošetrovanie rizika a prehodnocovanie rizík) sú prehodnocované odporúčané, technické, organizačné a procedurálne protiopatrenia. Následne sú tieto protiopatrenia prioritizované a implementované.

1.2.1 Zdroje informácií o zraniteľnostiach

Technické a netechnické zraniteľnosti asociované s prostredím prevádzky IT by mali byť identifikované predovšetkým prostredníctvom zberu informácií z oficiálnych zdrojov (napr. od výrobcov a dodávateľov SW a HW, od systémových integrátorov atď.).

Dokumentované zdroje informácií o zraniteľnostiach ktoré môžu byť po zvážení zahrnuté do analýzy zraniteľností (bez garancie správnosti informácie) sú nasledujúce:

- Dokumentácia o výsledkoch predchádzajúcich analýz zraniteľností,
- Správy z auditu,
- Reporty o anomáliách a poruchách systémov,
- Bezpečnostné reporty,
- Záverečné správy o incidentoch,
- Testovacie správy SW a HW,
- Databázy známych zraniteľností,
- CVE and CCE Vulnerability Database NIST I-CAT (http://icat.nist.gov) SP 800-30),
- The Open Source Vulnerability Database (http://osvdb.org/),
- Bezpečnostné poradenstvo a konzultácie,
- Odborné publikácie,
- Poradenstvo dodávateľov,
- Komerčné tímy reakcie na počítačové incidenty (CERT, CSIRT),
- Internetové diskusné fóra o bezpečnosti a mailinglist-y (bez garancie správnosti – ako doplnkový zdroj informácií),
- Protokol o odovzdaní systému do prevádzky IT,
- Technicko-prevádzková dokumentácia.

1.3 Identifikácia hrozieb

V analýze hrozieb sa všeobecne vychádza z dostupných zoznamov (katalógov) hrozieb uvedených v nasledujúcich referenčných dokumentoch:

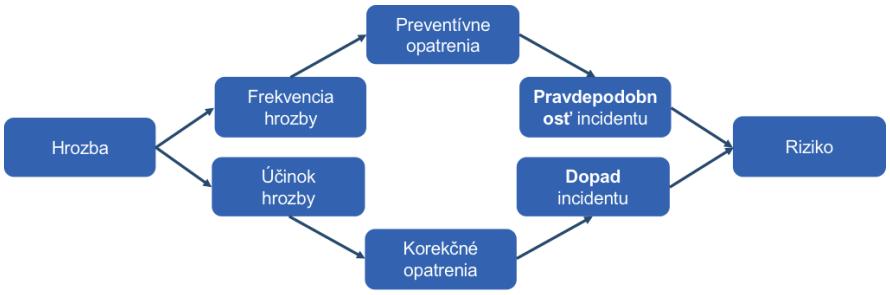
- STN ISO/IEC 27005 Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
- ISO/IEC 29134 Information technology – Seciruty techniques – Guideline for privacy impact assessment
- LINDDUN Privacy by Design framework
- NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems
- OWASP Risk Rating Methodology
- SANS Institute: Realistic Risk Management Using the CIS 20 Security Controls

- WP29: Usmernenie týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely Nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“
- materiál MV SR, odb. Civilnej ochrany „Prehľad zdrojov rizík a ohrození nevojenského charakteru“, (KMCO-144-14/KM-2008).

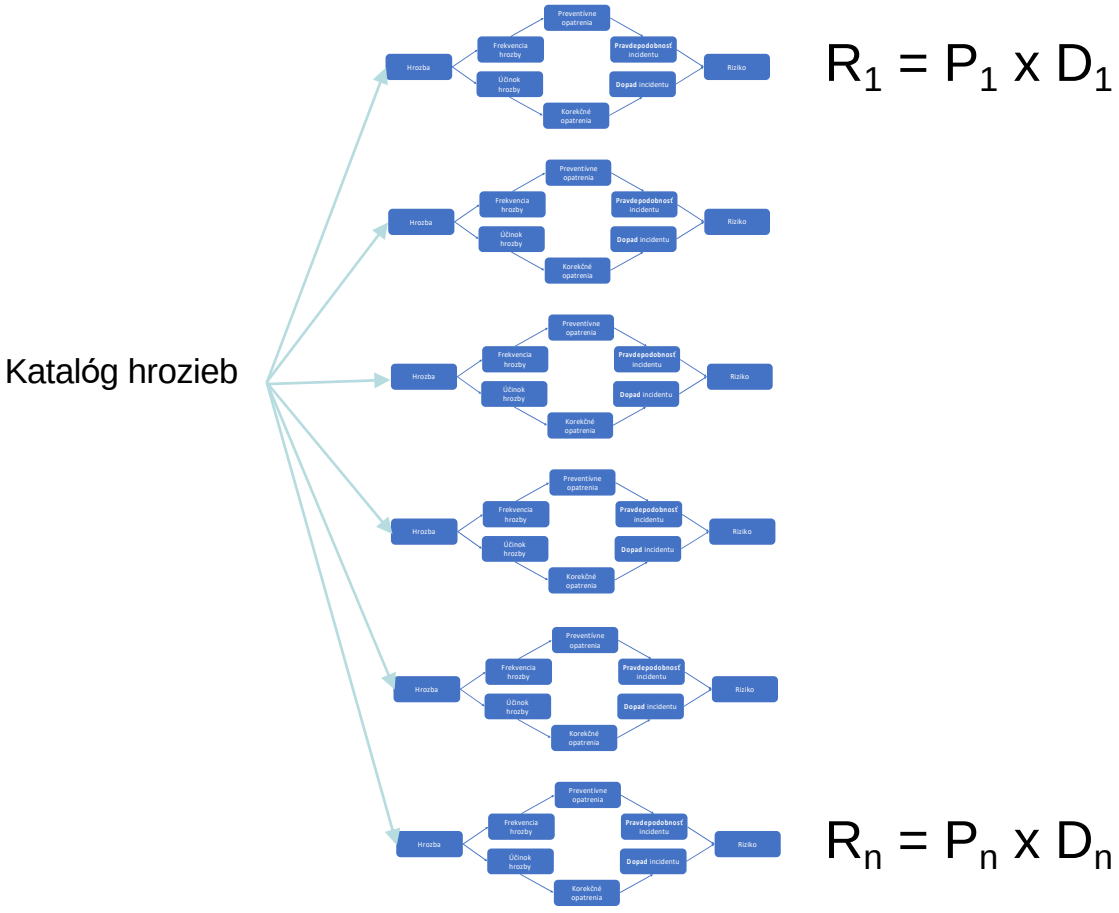
1.3.1 Použitý katalóg hrozieb

Proces analýzy rizík sa opiera o základný vzorec, podľa ktorého riziko je násobkom pravdepodobnosti hrozby a jej potenciálneho dopadu.

Obrázok č.3. Všeobecný postup pri analýze rizík



Obrázok č.4. Všeobecný postup pri analýze rizík - aplikácia katalógu hrozieb



Z vyššie uvedeného vyplýva, že celková riziková expozícia Spoločnosti sa vypočíta ako súčet všetkých čiastkových rizík vyplývajúcich z jednotlivých analyzovaných hrozieb, podľa použitého katalógu, t.j.:

R = ∑ R1 ... Rn

Riziko spracovateľskej činnosti je súčtom rizika každej z hrozieb uvedených v referenčnom katalógu.

S cieľom vyhnúť sa subjektivite v analýze rizík je potrebné čo najpresnejšie vymedziť množinu potenciálnych hrozieb. Z toho dôvodu je typickým prístupom k analýze rizík stanovenie referenčného katalógu hrozieb.

Definitívnym referenčným katalógom hrozieb použitým v tejto dokumentácii sú spojené katalógy:

- STN ISO/IEC 27005 Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
- LINDDUN Privacy by Design framework

Pre potreby analýzy rizík je zoznam hrozieb združený do skupín, tak, aby hrozby bolo možné použiť univerzálne pre väčšinu aktív. Pre jednotlivé aktíva nemusia byť posudzované všetky hrozby, hodnotené budú len hrozby relevantné pre dané aktívum.

1.3.2 Katalóg hrozieb podľa „LINDDUN privacy threat methodology“

- **Linkability** - (Spojiteľnosť linkovateľnosť): (napr. predmetu, správy, aktivity) umožňuje útočníkovi rozpoznať podstatu entity, alebo vzájomné vzťahy entít
- **Identifiability** – (Identifikovateľnosť): útočník môže dostatočne identifikovať dotknuté osoby asociované na predmety záujmu (napr. odosielateľa správy). Identifikovateľnosť je špeciálny typ spojiteľnosti, kde sú zahrnuté aj atribúty dotknutých osôb.
- **Non-repudiation** – (Nepopierateľnosť): Umožňuje útočníkovi zhromaždiť dôkazy proti nárokom odporujúcej strany a dokázať, že používateľ vie, že niečo urobil, alebo že niečo povedal. Opakom je Plausible deniability (prijateľné popretie)
- **Detectability** – (Detekovateľnosť) predmetu záujmu znamená, že útočník dokáže dostatočne rozlíšiť, či takáto položka jestvuje alebo nie. (napr. ak považujeme správy za predmet záujmu, znamená to, že správy sú dostatočne rozoznateľné od náhodného šumu.).
- **Information Disclosure** - (Odtajnenie informácie): znamená sprístupniť informáciu osobám, ktoré k nej nemajú mať prístup.
- **Content Unawareness** – (Neznalosť obsahu): indikuje, že používateľ si neuvedomuje citlivosť informácie spracovanej v systéme. Používateľ následne napr. zverejňuje príliš veľa informácií, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie.
- **Policy and consent Noncompliance** (Nesúlad spracovania): s politikami a poskytnutým súhlasom znamená, že i keď informačný systém na spracovanie osobných údajov deklaruje svojim používateľom, že spracovanie prebieha v súlade s politikami, neexistuje záruka, že systém skutočne vyhovuje prijatým pravidlám. Tým následne môže nastať porušenie práv na ochranu osobných údajov.

1.3.3 Pôvod hrozieb

V rámci hodnotenia rizík je potrebné identifikovať zoznam všetkých relevantných hrozieb ktoré môžu spôsobiť negatívny dopad na IS.

V prílohe č. 3 sú uvedené príklady typických hrozieb ktoré môžu viesť napríklad k poškodeniu alebo strate základnej služby. Zoznam je používaný v procese posudzovania hrozieb.

Hrozby sú rozdeľované podľa ich pôvodu do troch kategórií. Podľa ISO/IEC 27005:2008 je označenie pôvodu hrozieb nasledovné:

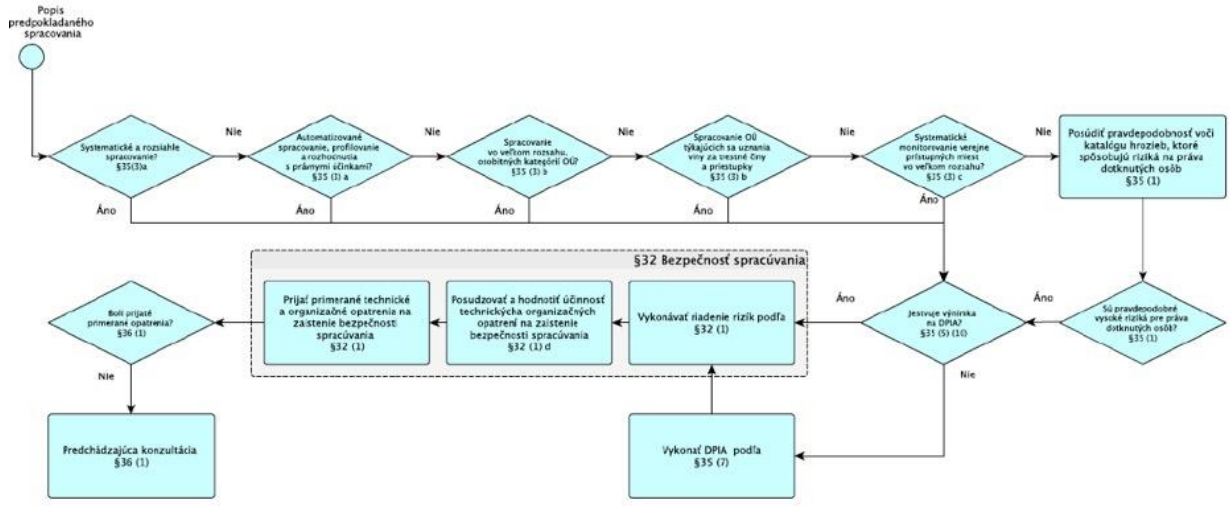
- **D („deliberate“ - úmyselné)** - označenie kategóriou D je používané pre všetky úmyselné aktivity zamerané na informačné aktíva,
- **A („accidental“ - náhodné)** - kategória A sa používa pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť informačné aktíva,
- **E („environmental“ - spôsobené vplyvom prostredia)** - kategória E sa používa na všetky udalosti, ktoré vznikli nezávisle na ľudskej činnosti.

1.4 Rozhodnutie o vykonaní posúdenia vplyvu na ochranu údajov

Spoločnosť musí rozhodnúť, **či typ spracúvania, s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb**, t.j. posúdiť pravdepodobnosť takých hrozieb, ktoré potenciálne pôsobia na práva a slobody fyzických osôb. Inými slovami, že je potrebné vykonať posúdenie voči takému katalógu hrozieb, ktorý postihuje subjektívne riziká.

Až v prípade, že je identifikované, že typ spracúvania, s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, potom je nutné **posúdiť pravdepodobnosť hrozieb a ich dopad na ochranu údajov** (Data protection impact assessment – „**DPIA**“), Inými slovami, že je potrebné vykonať posúdenie vplyvu plánovaných spracovateľských operácií voči takému katalógu hrozieb, ktorý postihuje úroveň informačnej bezpečnosti (objektívne riziká). Tento rozhodovací proces je možné znázorniť aj graficky nasledujúcim spôsobom:

Obrázok č.5. Rozhodovanie o vykonaní DPIA



1.5 Stanovenie dopadu rizika

Dopad popisuje závažnosť ujmy, resp. rozsah škody ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou. Miera potenciálneho dopadu zároveň predurčuje relatívnu hodnotu informačného aktíva a všetkých dotknutých zdrojov (napr. kritickosť a citlivosť komponentov IT systému a príslušných dát).

V rámci procesu zabezpečovania kontinuity činnosti Spoločnosť vykonáva analýzu funkčného dopadu (tzv. „**Business impact analýza**“ - BIA), ktorá pozostáva z hodnotenia dopadu na činnosť (ekonomicko-finančnú, právnu, reputácia), spôsobeného krízovým scenárom, ktorý zasiahol zdroje a aktíva podporujúce procesy Spoločnosti a tak spôsobil nedostupnosť činností a/alebo služieb.

Úlohou BIA je identifikovať pre každý proces základné vlastnosti (typológia, závažnosť, dopad, atď.), konkrétne - identifikovať činnosti a čas obnovy dát po výpadku prevádzky (**cieľový čas obnovy – RTO** a **cieľový bod obnovy - RPO**), identifikovať všetky požiadavky nevyhnutné na zabezpečenie prevádzky, aby mohli byť určené implementačné riešenia na základe rôznych úrovní závažnosti.

Hodnotenie závažnosti procesu musí byť vykonané na základe logiky “najhoršieho scenára” („**worst case**“), ktorý by mohol potenciálne nastať i keď by bola takáto závažnosť málo pravdepodobná.

Na určenie úrovne rizika je nutné vopred nastaviť súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov stanoviť merateľné a objektívne hodnoty rizika.

Na hodnotenie rizika budú pre potreby Spoločnosti používané oblasti, uvedené v nasledujúcej tabuľke.

Tabuľka č. 6.: Definícia dopadu rizika

Hodnota	Opis dopadu	Finančný dopad	Prevádzkový dopad	Legislatívny dopad	Strata dôvery	Poznámka
0	Riziko nemá dopad -	0	Žiaden prevádzkový dopad	Regulácie a nariadenia neporušené	Žiaden reputačný dopad	
20	zanedbateľný vplyv, strata	1 – 1 000 €	interne, jedno oddelenie	zlyhanie interného procesu	určité prekážky v komunikácii v rámci spoločnosti	Dopad sa týka z veľkou pravdepodobnosťou nekritických alebo podporných aktív, IT systémov, aplikácií, procesov, alebo zdrojov Spoločnosti
40	malý vplyv, strata	1 001 – 10 000 €	interne, viacero oddelení	začatie správneho konania smerujúce k opatreniu na nápravu	závažné prekážky v komunikácii v rámci spoločnosti	
60	stredný vplyv, strata	10 001 – 100 000 €	Spoločnosť, malá časť klientov	začatie správneho konania smerujúce k uloženiu pokuty	určitá nepriaznivá publicita na národnej úrovni	Dopad sa týka väčšinou hlavných, kritických aktív, IT systémov, aplikácií, procesov, alebo zdrojov Spoločnosti Môže sa týkať ale aj iných nekritických systémov.
80	značný vplyv, strata	100 001 – 1 000 000 €	Spoločnosť, značná časť klientov	Pozastavenie / ukončenie činnosti časti služieb	intenzívna nepriaznivá publicita na národnej úrovni	Dopad sa týka z veľkou pravdepodobnosťou hlavných, kritických aktív, IT systémov, aplikácií, procesov, alebo zdrojov Spoločnosti Narušenie integrity, dôvernosti alebo dostupnosti týchto aktív je pre Spoločnosť kritické, intenzívna nepriaznivá publicita na národnej úrovni.
100	katastrofický vplyv, strata	Viac ako 1 000 000 €	Spoločnosť, všetci klienti	Pozastavenie / ukončenie činnosti – kľúčové služby	nepriaznivá medzinárodná publicita	

Na základe stanovenej hodnoty dopadu je možné prijať potrebné, vhodné a primerané opatrenia na ošetrenie rizika.

Úrovne rizík používané v metodike riadenia IT sú slovne popísané podľa dopadov. Tento spôsob hodnotenia rizika je použitý a konsolidovaný vo všetkých dokumentoch a výstupoch hodnotenia IT rizika.

Cieľom tejto metriky je zaviesť možnosti porovnávania ohodnoteného rizika medzi jednotlivými systémami, procesmi, alebo jednotlivými analýzami rizík. Hodnotu dopadu je možné stanoviť v šiestich (resp. v piatich aktívnych) úrovniach, pričom popis dopadov v jednotlivých oblastiach by mal po riadkoch medzi sebou korelovať.

Hodnotiteľ by sa mal pokúsiť opísať dopad prostredníctvom všetkých oblastí. Hodnota dopadu potom bude určená ako najvyššia dosiahnutá úroveň zo všetkých hodnotených oblastí.

1.6 Stanovenie pravdepodobnosti výskytu hrozby

Na určenie celkovej pravdepodobnosti ktorá naznačuje šancu že potenciálna zraniteľnosť môže byť zneužitá v rámci existujúcej infraštruktúry a prostredia, musia byť zvážené nasledujúce faktory:

- motivácia a zdatnosť zdroja hrozby,
- podstata zraniteľnosti,
- existencia a efektivita aktuálne uplatnených opatrení

Pri stanovovaní pravdepodobnosti je potrebné prihliadať aj na frekvenciu výskytu incidentov v minulosti, ktorých podstatou bolo zneužitie príslušnej slabiny. Ak takýto údaj existuje, mal by byť v súlade so stanovenou úrovňou pravdepodobnosti.

Pravdepodobnosť že potenciálna zraniteľnosť môže byť zneužitá zo strany zdroja hrozby môže byť popísaná ako vysoká, stredná, alebo nízka. Podrobnejšie rozdelenie a popis je v nasledujúcej tabuľke:

Tabuľka č. 7.: Definícia pravdepodobnosti rizika

Hodnota	Pravdepodobnosť	Frekvencia slovne	Pravdepodobnosť popisne
10	Vysoká	Riziko je očakávateľné vo väčšine okolností	Zdroj hrozby je vysoko motivovaný a je dostatočne technicky zdatný; uplatnené protiopatrenia na prevenciu identifikovanej zraniteľnosti sú neefektívne. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola už mnoho krát zneužitá.
7	Stredná	Riziko je pravdepodobné vo väčšine okolností	Zdroj hrozby je motivovaný a technicky zdatný; uplatnené opatrenia čiastočne bránia úspešnému zneužitiu zraniteľností. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola už niekoľko krát zneužitá..
4	Malá	Riziko sa môže niekedy vyskytnúť	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Z minulosti existuje ojedinelá skúsenosť zneužitia danej zraniteľnosti.
2	Veľmi malá	Riziko sa môže vyskytnúť za mimoriadnych okolností	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľnosti. Neexistuje historická skúsenosť so zneužitím danej slabiny..

1.7 Stanovenie úrovne rizika

Úroveň rizika je vyhodnocovaná ako násobok stanovenej pravdepodobnosti rizika a stanoveného dopadu rizika. Výsledné hodnoty množiny je následne možné zaradiť v dvojrozmernej matici.

Tabuľka č. 8.: Matica pre stanovenie úrovne rizika

Pravdepodobnos	**Dopad**				
	Zanedbateľný (20)	Malý (40)	Stredný (60)	Značný (80)	Katastrofický (100)
Vysoká (1)	20*1=20	40*1=40	60*1=60	80*1=80	100*1=100
Stredná (0,7)	20*0,7=14	40*0,7=28	60*0,7=42	80*0,7=56	100*0,7=70
Malá (0,4)	20*0,4=8	40*0,4=16	60*0,4=24	80*0,4=32	100*0,4=40
Veľmi malá (0,2)	20*0,2=4	40*0,2=8	60*0,2=12	80*0,2=16	100*0,2=20

V metodike riadenia IT rizika Spoločnosti budú používané hodnoty v rozsahu predchádzajúcej matice. Identifikované riziko bude rozdeľované do šiestich úrovní podľa nasledovnej tabuľky.

Tabuľka č. 9.: Úrovne rizika

Riziko	**Zodpovedajúca číselná hodnota**
Extrémne vysoké	od 86 do 10
Veľmi vysoké	od 69 do 85
Vysoké	od 51 do 68
Stredné	od 36 do 50
Malé	od 18 do 35
Zanedbateľné	od 1 do 17

Tento spôsob hodnotenia rizika je použitý a konsolidovaný vo všetkých dokumentoch a výstupoch hodnotenia IT rizika.

1.8 Návrh prístupu k ošetreniu rizika

Po tom, ako budú identifikované bezpečnostné požiadavky a je stanovená úroveň rizika, mali by byť vybrané a implementované opatrenia, ktoré zaistia zníženie rizika na prijateľnú úroveň.

Výber vhodných bezpečnostných opatrení je závislý od rozhodnutia vedenia Spoločnosti, malo by vychádzať z kritérií akceptácie rizika, reálnych možností ošetrenia rizika a všeobecných princípov manažmentu rizík, aplikovaných v rámci Spoločnosti.

V nasledujúcej tabuľke sú slovne popísané úrovne rizík z matice úrovní rizika (2.5). Na základe stanovenej úrovne rizika je možné prijať potrebné, vhodné a primerané opatrenia na jeho ošetrenie.

Tabuľka č. 10.: Opatrenia pre jednotlivé úrovne rizika

Úroveň rizika	Opatrenia
Extrémne vysoké	Bezpečnostné opatrenia sú bezpodmienečne nutné a je potrebné prijať ich bezodkladne. Odporúča sa bezodkladne odstaviť systém / prerušiť výkon procesu.
Veľmi vysoké	Bezpečnostné opatrenia sú bezpodmienečne nutné a je potrebné prijať ich bezodkladne. Je pravdepodobne nutné odstaviť systém / prerušiť výkon procesu.
Vysoké	Bezpečnostné opatrenia sú nutné a je potrebné prijať ich čo najskôr. Odporúča sa zvážiť aj možnosť odstavenia systému / prerušenia procesu.
Stredné	Bezpečnostné opatrenia sú potrebné a mali by byť implementované v dohľadnej dobe. Systém / proces nemusí byť pozastavený a môže byť i naďalej prevádzkovaný / vykonávaný.
Malé	Vlastník aktíva musí stanoviť, či je nutné prijať bezpečnostné opatrenia, alebo či v minulosti prijaté opatrenia sú naďalej potrebné. Po vyhodnotení bude pravdepodobne možné akceptovať riziko ako zvyškové.
Zanedbateľné	Opatrenia nie sú potrebné.

* Kritickosť aktív môže byť porovnaná s ich ohodnotením v rámci globálnej analýzy rizík, BIA, alebo DPIA.

1.9 Výber opatrení na ošetrenie rizík

Na minimalizáciu a elimináciu identifikovaných rizík by pri návrhu vhodných protiopatrení a alternatívnych riešení mali byť do úvahy vzaté nasledujúce faktory:

- efektivita a náklady odporúčaných opatrení,
- kompatibilita opatrení s existujúcou IT architektúrou a procesmi,
- požiadavky legislatívy a opatrení regulátora,
- obchodná politika Spoločnosti v príslušnej oblasti,
- možné dopady na prevádzku,
- bezpečnosť a spoľahlivosť navrhnutého opatrenia.

Zoznam opatrení na zníženie rizika je výsledkom procesu hodnotenia rizika a poskytuje vstup pre proces ošetrovania rizika, v rámci ktorého sú navrhnuté opatrenia a odporúčané technické a procesné zmeny prehodnotené, prioritizované a implementované.

1.9.1 Proces ošetrovania rizika

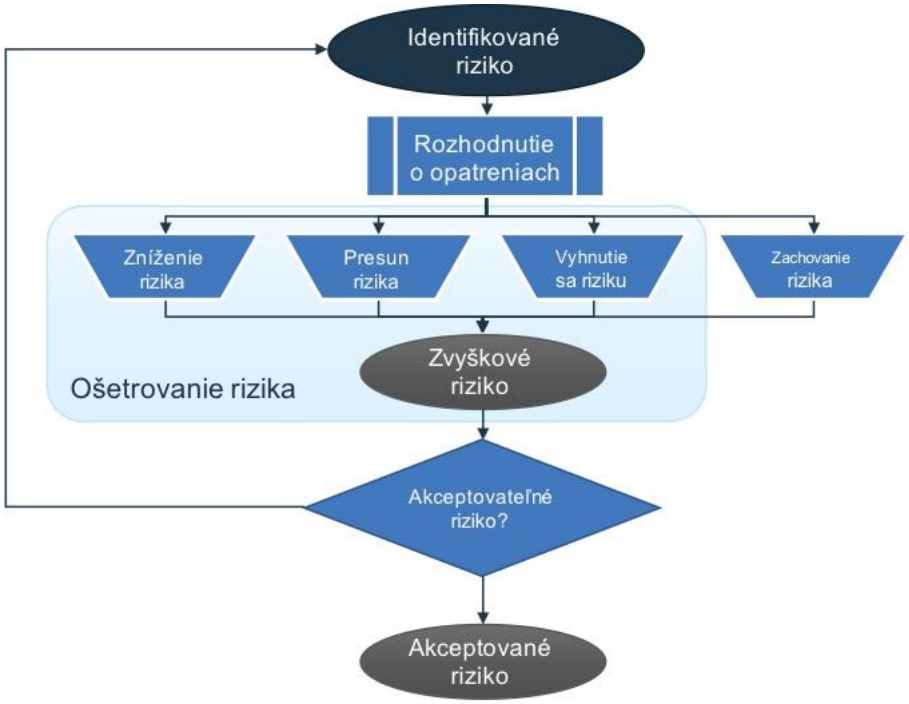
Na ošetrenie rizika je vždy nutné použiť minimálne jeden z možných prístupov:

- zníženie rizika,
- presun rizika,
- vyhnutie sa riziku,

- zachovanie rizika.

V zmysle ISO 27005 je všeobecný proces ošetrovania rizika možné znázorniť nasledujúcou schémou:

Obrázok č.6. Schéma generického procesu ošetrovania rizík



1.9.2 Zníženie rizika

Zníženie rizika je metóda ošetrenia rizika, pri ktorej je uplatnený výber vhodných opatrení tak, aby riziko bolo znížené až na úroveň zostatkového rizika, ktoré môže byť následne prehodnotené ako akceptovateľné.

Vhodné a opodstatnené opatrenia by mali byť vybrané tak, aby spĺňali požiadavky stanovené ohodnotením rizika. Výber opatrení by mal brať do úvahy kritéria akceptácie rizika ako napr. právne, regulačné a zmluvné požiadavky. Výber opatrení by mal taktiež vziať do úvahy primeranosť nákladov a časový rámec na implementáciu opatrení ale tiež napr. technické a kultúrne aspekty. Okrem toho by mala byť vzatá do úvahy návratnosť investície, súvisiacej so znížením rizika a potenciál na využívanie nových obchodných príležitostí, získaný implementáciou opatrení.

1.9.3 Presun rizika

Presun rizika je metóda ošetrenia rizika, pri ktorej bude určitá časť rizika zdieľaná s externými subjektmi.

Presun rizika sa môže uskutočniť napr. poistením, ktoré znižuje následky, alebo výberom zmluvného partnera, ktorého úlohou bude monitorovať proces, alebo informačný systém a prijať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda.

1.9.4 Vyhnutie sa riziku

Vyhnutie sa riziku je metóda ošetrenia rizika, pri ktorej bude riziko obídené nevykonaním príslušných rizikových aktivít, alebo uplatnením špecifických podmienok na vykonanie aktivity.

Keď je identifikované riziko považované za príliš vysoké, alebo náklady na implementáciu ošetrenia rizika presahujú prínosy, rozhodnutím môže byť aj úplné vyhnutie sa riziku, a to odobratím plánovanej

alebo existujúcej aktivity alebo súboru aktivít, alebo zmenou podmienok, podľa ktorých je činnosť prevádzkovaná.

1.9.5 Zachovanie rizika

Zachovanie rizika je metóda ošetrenia rizika, pri ktorej nie sú uplatnené žiadne opatrenia a riziko zostane zachované v pôvodne ohodnotenej úrovni.

Ak úroveň rizika spĺňa kritériá na prijatie rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované.

Z hľadiska realizácie opatrení na zníženie rizika je potrebné rozdeliť ich na:

- **Operatívne** – t.j. opatrenia ktorých implementácia je z časového a finančného hľadiska nenáročná, ale ktorých účinok prináša veľký efekt na zníženie rizika,
- **Systémové** - t.j. organizačné a rozsiahlejšie technické opatrenia s dlhodobým účinkom na znižovanie rizika.

Postupnosť, akou budú navrhované opatrenia realizované, tzv. implementačný plán, je rozpracovaná v rámci programu zvýšenia bezpečnosti IS Spoločnosti. Tento program závisí od viacerých faktorov, ktoré je potrebné pri jeho návrhu zohľadniť. K takýmto faktorom prináležia:

- priority vyplývajúce z ohodnotenia rizík,
- výška nákladov potrebných na realizáciu opatrení,
- pripravenosť organizácie na realizáciu opatrení (technická, organizačná, finančná),
- podpora manažmentu organizácie na realizáciu opatrení.

V programe zvýšenia bezpečnosti IS Spoločnosti je spôsob realizácie opatrení rozpracovaný do podoby konkrétnych projektov.

Operatívne opatrenia

Cieľom operatívnych opatrení je uplatnenie takých zmien procesov a technológií, ktoré budú viesť k urýchlenému zníženiu identifikovaného rizika s čo najnižšími nákladmi a najvyšším účinkom.

Za rozhodnutie o prijatí operatívnych opatrení je zodpovedný CISO, CSO, alebo CTO.

Prijaté operatívne opatrenia musia byť prediskutované na najbližšom rokovaní predstavenstva Spoločnosti.

Systémové opatrenia

Cieľom systémových opatrení je zvoliť optimálnu hranicu medzi účinnosťou bezpečnostných mechanizmov a požiadavkami, ktoré sú kladené na prevádzku aktív. Výsledkom systémových opatrení musí byť proaktívny prístup k riadeniu rizika, ktoré umožní:

- identifikovať IT riziko v počiatočnom štádiu pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
- monitorovať IT riziko počas pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
- eliminovať dopad hrozby na funkčnosť IS,
- zdokumentovať priebeh IT rizika.

Za rozhodnutie o prijatí systémových opatrení je zodpovedný CISO, CSO, alebo CIO, s následnou povinnosťou potvrdenia prijatých opatrení zo strany vedenia Spoločnosti.

1.10 Zvyškové riziko

1.10.1 Prijateľné riziko

Za prijateľné IT riziko je možné označiť riziko, ktoré je také nízke (t.j. nepresahuje referenčnú úroveň), že pre Spoločnosť nepredstavuje významný negatívny dopad a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.

Referenčná úroveň je hranica miery rizika (stanovená hodnota rizika), ktorá rozhoduje o tom, či je riziko zvyškové (veľkosť rizika je menšia než referenčná úroveň), alebo nie je zvyškové (veľkosť rizika je väčšia alebo rovná referenčnej úrovni). Tým sa rozhodne, či proti riziku je alebo nie je potrebné uplatniť ďalšie opatrenia pre jeho zníženie. Referenčná úroveň by mala byť na takej úrovni, aby dopad hrozby bol taký nízky, že ho bude možné zanedbať.

Na výpočet a odhad prijateľného rizika je nutné použiť rovnakú metódu analýzy rizika, aká bola použitá na výpočet vstupného, resp. celkového rizika.

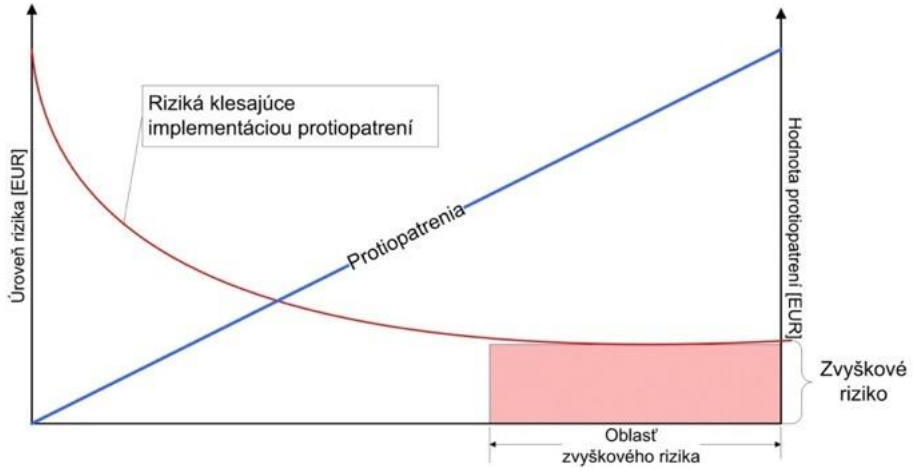
1.10.2 Akceptácia zvyškového rizika

Zvyškové riziko je riziko, na ktoré boli uplatnené všetky dostupné opatrenia na komplexné ošetrenie rizík t.j. boli implementované základné, dodatočné a vylepšené opatrenia na ošetrenie rizika

Za predpokladu, že náklady implementovaných protiopatrení lineárne stúpajú, riziká budú sústavne klesať a zastavia sa na zvyškovej hodnote, ktorá nebude mať ďalšiu tendenciu poklesu ani po implementácii ďalších protiopatrení.

Referenčná hodnota zvyškového rizika by mala byť stanovená na takej úrovni, aby dopad hrozby bol tak nízky, že ho bude možné zanedbať. Túto hodnotu rizika je možné označiť za zvyškovú. Pre pochopenie tohto fenoménu je možné vzájomného pôsobenie protiopatrení a rizík zobraziť schematicky, na nasledujúcom grafe:

Obrázok č.7. Vplyv protiopatrení na zvyškové riziko



V praxi pravdepodobne žiaden informačný systém nie je bez rizík a je možné, že ani všetky implementované opatrenia neznížia riziko tak, aby dosahovalo nulovú hodnotu, ani za predpokladu neobmedzených nákladov.

Zvyškové riziko musí byť vždy zásadne akceptované vedením Spoločnosti.

1.10.3 Náležitosti návrhu na akceptáciu zvyškového rizika

Akceptácia zvyškového IT rizika je proces, v ktorom vedenie Spoločnosti formálne vezme na vedomie eskalované riziko. Vedenie v zápise skonštatuje, že konkrétne identifikované riziko je pre Spoločnosť

prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie. Zároveň stanoví termín prehodnotenia rizika. Návrh na akceptáciu zvyškového rizika predkladá vedeniu CIO, CISO, alebo CSO.

Súčasťou návrhu na akceptáciu zvyškového rizika majú byť nasledovné atribúty:

- Číslo rizika (t.j. jeho jedinečná identifikácia)
- Kategória
- Oblasť
- Opis rizika
- Pravdepodobnosť
- Dopad
- Kvantitatívne hodnotenie rizika
- Dotknuté aktíva
- Riziko identifikoval
- Spôsob identifikácie
- Dátum identifikácie
- Priorita / dátum prehodnotenia
- Protiopatrenia implementované doteraz
- Obmedzenia ktoré bránia ďalšiemu ošetrovaniu identifikovaného rizika

1.10.4 Obmedzenia brániace ďalšiemu ošetrovaniu identifikovaného rizika

Časové obmedzenia

Ak potenciálne protiopatrenia môžu byť z rôznych dôvodov implementované iba v časovom horizonte dlhšom než je životný cyklus príslušného informačného systému, riziko identifikované v takomto časovom úseku môže byť označené za akceptovateľné.

Finančné obmedzenia

Náklady na protiopatrenia by nemali byť vyššie než je kvantifikovaná hodnota identifikovaných rizík (viď obr. č. 5). Výnimkou môže byť iba taký prípad, keď je protiopatrenie explicitne vyžadované zákonom, alebo zo strany regulátora príslušného odvetvia.

Taktiež aj prácnosť potrebná na implementáciu protiopatrení by nemala prekročiť hodnotu plánovaného rozpočtu, alebo hodnotu potenciálneho finančného prínosu plynúceho z implementácie protiopatrenia. Vyššia obozretnosť v hodnotení rizík je vyžadovaná v prípade, ak dodatočné škrty rozpočtu môžu mať negatívny vplyv na kvalitu protiopatrení. To môže viesť ku implicitnému zachovaniu (retencii) vyššieho rizika, než bolo pôvodne predpokladané.

Technické obmedzenia

Technickým problémom, ako napríklad kompatibilite programov, alebo hardvéru možno predísť tak, že budú brané do úvahy už v procese plánovania a výberu protiopatrení. Technické obmedzenia tohto typu však môžu vzniknúť pri dodatočnej implementácii nových protiopatrení na jestvujúce systémy.

Niekedy môže vzniknúť potreba revidovať bezpečnostnú architektúru z dôvodu nutnosti dosiahnutia zmenených cieľov. Toto sa môže stať v prípade, že protiopatreniami nie sú dosiahnuté požadované výsledky bez toho, aby zároveň došlo ku zníženiu produktivity.

Operatívne obmedzenia

Operatívne obmedzenia (ako napríklad požiadavka na prevádzku 24x7) môžu spôsobiť nárast nákladov na protiopatrenia nezávisle od toho, či boli zahrnuté do riešenia od samého začiatku.

Právne obmedzenia

Zákonné dôvody ako napríklad hrozba, že sa implementáciou protiopatrení naplní skutková podstata trestného činu, alebo že implementácia protiopatrení voči jednému riziku vznikne iné riziko, ktoré spôsobí priestupok proti zákonu, jednoznačne ovplyvňujú uskutočniteľnosť protiopatrení. Zákon, alebo rôzne požiadavky na súlad môžu vyžadovať povinný auditing, alebo reporting, takéto požiadavky však majú nepriamy dopad uskutočniteľnosť iných typov protiopatrení, ako napr. použitia prostriedkov šifrovej ochrany informácií. Obmedzenia voči možnosti implementácie protiopatrení môžu byť tiež spôsobené požiadavkami zákonných noriem na ochranu pred požiarmi, na zaručenie bezpečnosti a ochrany zdravia pri práci, alebo v neposlednom rade aj zákonmi na reguláciu trhu, a daňovými a účtovnými zákonmi.

Obmedzenia v zložitosti

Chatrné možnosti rozhrania medzi človekom a technológiou vedú k ľudským chybám, ktoré následne činia niektoré implementované protiopatrenia nepoužiteľnými. Protiopatrenia by mali byť zvolené tak, aby poskytovali optimálnu jednoduchosť, s cieľom dosiahnuť akceptovateľnú úroveň zvyškových rizík.

Protiopatrenia ktoré sú príliš zložité, majú dopad na ich efektivitu, pretože používatelia majú tendenciu ich obchádzať ako je to len možné, alebo ich priamo ignorovať. Napríklad príliš zložitý systém riadenia prístupových práv môže povzbudiť používateľov ku hľadaniu alternatívnych neautorizovaných metód prístupu.

Personálne obmedzenia

Pri návrhu protiopatrení je nutné vziať do úvahy dostupnosť ľudských zdrojov, ich operabilitu a mzdové náklady na získanie ľudských zdrojov ktoré disponujú špeciálnymi zručnosťami. Expertná úroveň znalostí nie je bežne k dispozícii a kapacita špeciálnych ľudských zdrojov je i v prípade ich dostupnosti v podniku obmedzená.

Iným, nepriamym aspektom ktorý ovplyvňuje úroveň bezpečnostnej politiky a implementácie protiopatrení, je tendencia personálu diskriminovať inú časť personálu, ktorá nepodlieha rovnakým bezpečnostným obmedzeniam, alebo monitoringu.

V neposlednom rade, najímanie správnych, zodpovedných a kvalifikovaných ľudí, ktorí by boli ešte pred prijatím podrobení bezpečnostnej previerke je veľmi zložitá úloha. Potreba získania nového zamestnanca z dôvodu požiadavky na vykrytie zvýšenej prácnosti má mnohokrát prednosť pred overením dôveryhodnosti a schopnosti uchádzača.

Obmedzenie v súvislosti s integráciou nových a existujúcich opatrení

Integrácia nových protiopatrení do jestvujúcej infraštruktúry a vzájomné závislosti medzi protiopatreniami sú často prehliadané. Nové protiopatrenia môžu byť implementované jednoducho, ak existuje nezhoda, alebo nekompatibilita s už implementovanými, predchádzajúcimi protiopatreniami.

Aby boli pôvodné protiopatrenia v súlade s plánom nových protiopatrení, mali by byť v pláne brané do úvahy aj pôvodné protiopatrenia. Prvky, ktoré budú pridané ku celkovému riešeniu na ošetrenie rizika vygenerujú náklady aj na zmenu už implementovaných protiopatrení. Tento úmysel však môže byť v niektorých prípadoch nepriechodný.

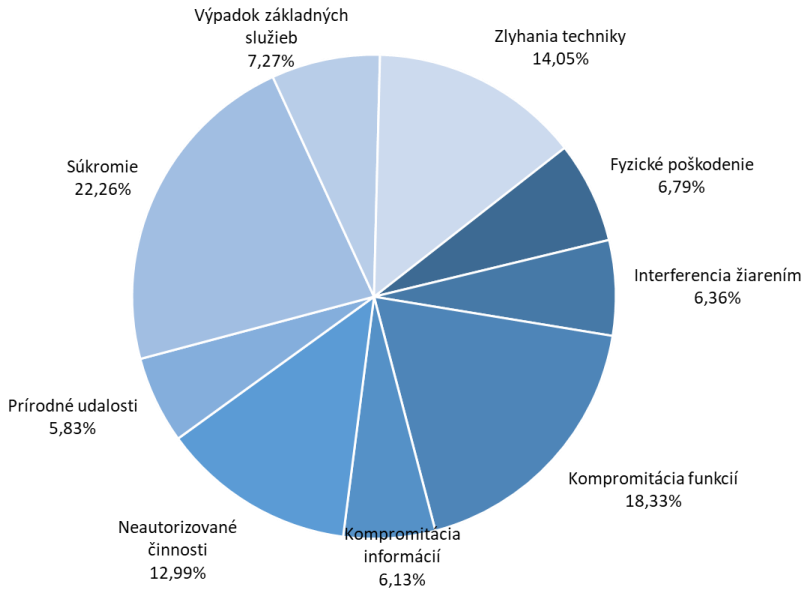
2 VÝSLEDKY ANALÝZY RIZÍK A POSÚDENIA VPLYVU NA OCHRANU ÚDAJOV

Na základe vyššie opísanej metodiky sú výsledky analýzy rizík a posúdenia vplyvu na ochranu údajov nasledujúce.

Tabuľka č. 11.: Riziková expozícia Spoločnosti podľa jednotlivých kategórií hrozieb

Kategória hrozieb	Kumulovaná hodnota rizika	Počet rizík v kategórii	Riziková expozícia	% pomer expozície
Súkromie	294	7	42,00	22,26%
Kompromitácia funkcií	242	7	34,57	18,33%
Zlyhania techniky	106	4	26,50	14,05%
Neautorizované činnosti	196	8	24,50	12,99%
Výpadok základných služieb	96	7	13,71	7,27%
Fyzické poškodenie	64	5	12,80	6,79%
Interferencia žiarením	36	3	12,00	6,36%
Kompromitácia informácií	104	9	11,56	6,13%
Prírodné udalosti	44	4	11,00	5,83%

Graf č. 9. Riziková expozícia podľa jednotlivých kategórií hrozieb



Kumulovaná hodnota rizík Spoločnosti v čase vykonania posúdenia je **1182** bodov. Ak v rámci použitej metodiky analýzy rizík je celkový možný (teoreticky dosiahnuteľný) počet bodov rizika **5400** bodov (tzv. kritická expozícia), potom reálna riziková expozícia Spoločnosti je **21,89%**. To s porovnateľným trhom predstavuje pre podnik nízku rizikovú expozíciu, s indexom rizika „**malé**“.

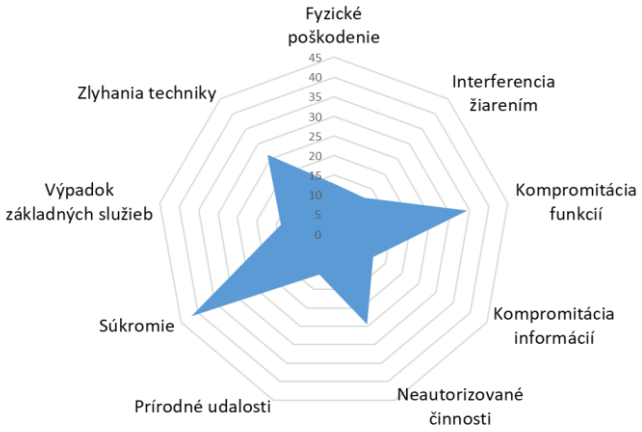
Z grafickej reprezentácie úrovní rizika pre jednotlivé kategórie hrozieb vyplýva, že najvyššiu úroveň rizikovej expozície predstavuje kategória „Súkromie“, t.j. hrozby pôsobiace na práva dotknutých osôb (s podielom **22,26%** na kumulovanej hodnote rizík Spoločnosti).

Ďalšie hodnoty v kategóriách rizika s významným pomerom expozície pre kategóriu sú:

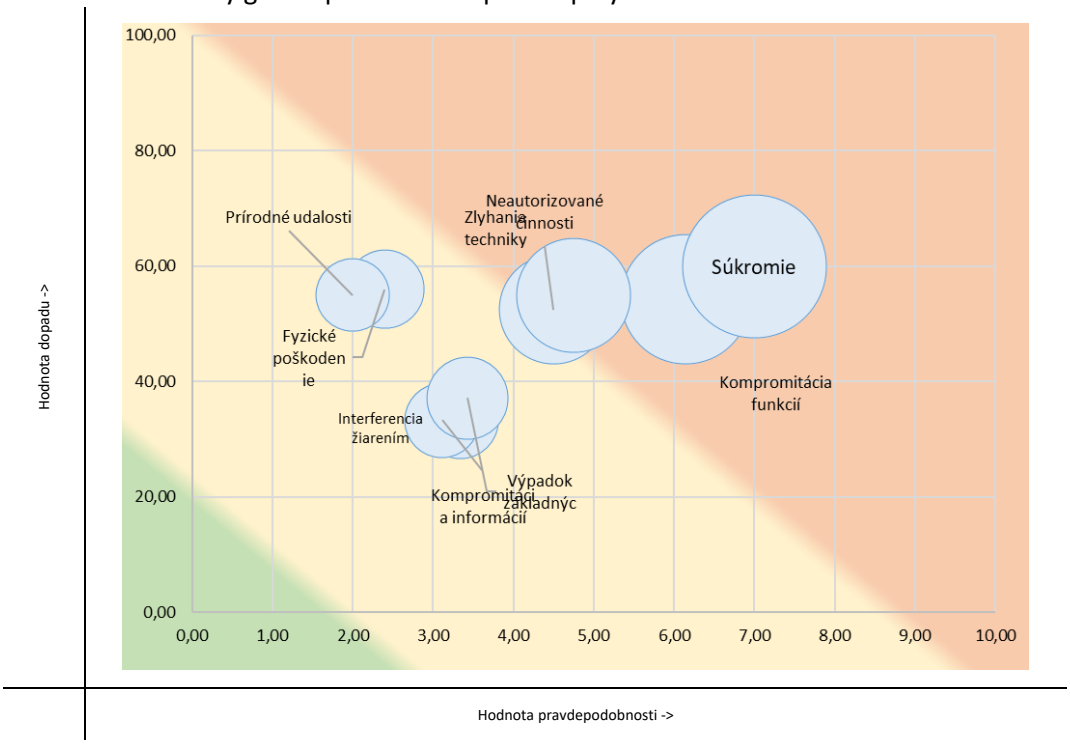
- „Kompromitácia funkcií“ (s podielom **18,33 %** na kumulovanej hodnote rizík Spoločnosti).
- „Zlyhania techniky“ (s podielom **14,05%** na kumulovanej hodnote rizík Spoločnosti)
- „Neautorizované činnosti“ (s podielom **12,99%** na kumulovanej hodnote rizík Spoločnosti).

Hodnota rizikovej expozície v kategórie „Prírodné udalosti“ (s podielom **5,83%** na kumulovanej hodnote rizík Spoločnosti) má typicky vplyv na atribút „dostupnosť“. V prípade, že sa hrozba uplatní, hrozby v tejto kategórii majú vysoké hodnoty dopadu. Avšak vzhľadom na problematický odhad pravdepodobnosti týchto hrozieb, je výsledný rating rizika zvyčajne nízky. Spôsob ošetrenia rizika je potom navrhovaný v závislosti na type podnikania. V prípade, že náklady na opatrenia by boli neefektívne, možnosťou je aj akceptácia rizika.

Graf č. 10. Kumulatívne riziko pre jednotlivé kategórie hrozieb

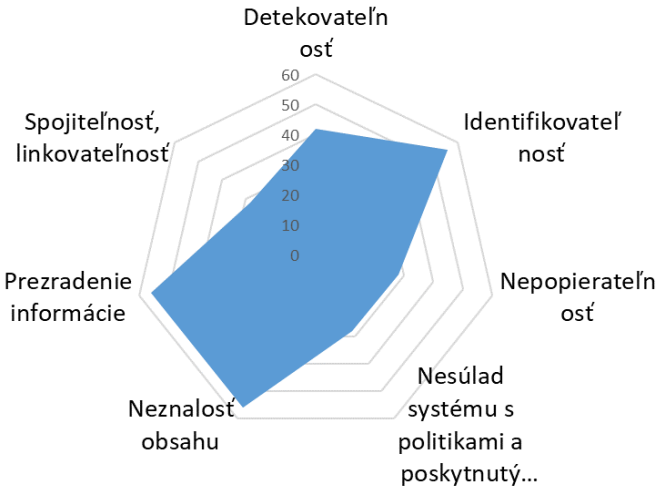


Graf č. 11. Bublinový graf expozícia rizika pre skupiny hrozieb

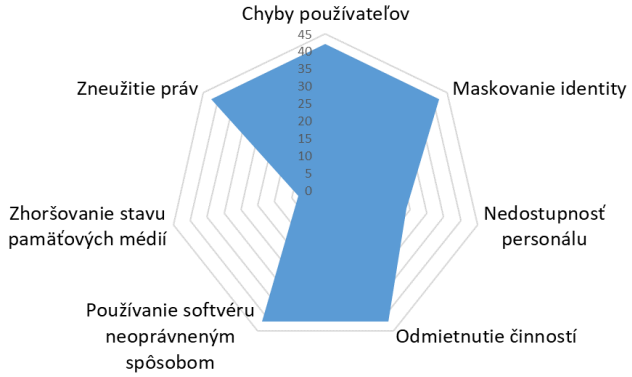


Bližšia analýza kategórií s vyšším rizikom naznačuje aj následný návrh opatrení.

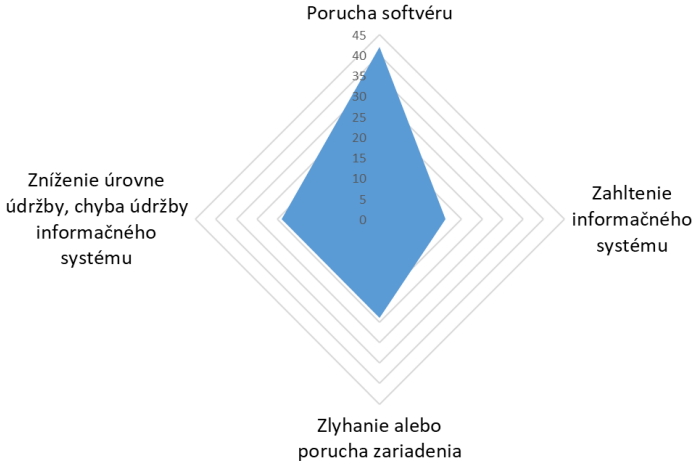
Graf č. 12. Úroveň rizika pre kategórie hrozby „Súkromie“



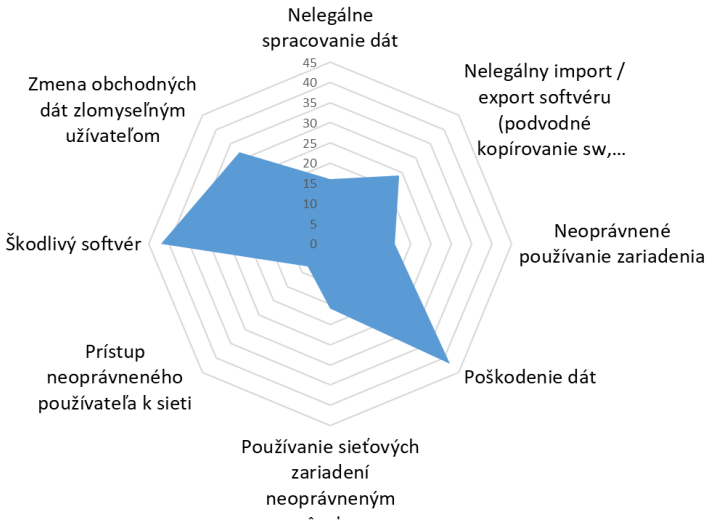
Graf č. 13. Úroveň rizika pre kategórie hrozby „Kompromitácia funkcií“



Graf č. 14. Úroveň rizika pre kategórie hrozby „Zlyhania techniky“



Graf č. 15. Úroveň rizika pre kategórie hrozby „Neautorizované činnosti“



PLÁN SÚLADU

1 NÁVRH VŠEOBECNÉHO PRÍSTUPU

Napriek tomu, že identifikovaná riziková expozícia Spoločnosti je s porovnateľným trhom „malá“, je celkový stav súladu implementácie bezpečnostných opatrení nedostatočný.

Z analýzy rizík pre jednotlivé kategórie hrozieb vyplýva, že najvyššiu úroveň rizikovej expozície predstavuje kategória „Súkromie“ (s podielom **22,26%** na kumulovanej hodnote rizík Spoločnosti). Z toho dôvodu je potrebné uprednostniť také opatrenia, ktorých cieľom je zníženie hrozieb najmä v uvedenej kategórii.

Zistenia o stave súladu v implementácii bezpečnostných opatrení je možné posudzovať najmä podľa kapitoly 0.

Na základe výsledkov zobrazených v grafe č. 8. „Porovnanie nesúladu / čiastočného súladu technických a organizačných opatrení“ je vo všeobecnosti možné tvrdiť, že pozornosť pri snahe o dosiahnutie súladu by mala byť venovaná najmä organizačným opatreniam, keďže z celkového počtu opatrení v nesúlade, alebo čiastočnom súlade predstavujú organizačné opatrenia až **68%**.

Z analýzy rizík Spoločnosti ku dňu odovzdania tejto dokumentácie vyplývajú nasledujúce návrhy protiopatrení (podrobný zoznam je uvedený v prílohe č. 1).

2 NÁVRHY NA REDESIGN BEZPEČNOSTNEJ ARCHITEKTÚRY

Spoločnosť má vzhľadom na podstatu hlavnej obchodnej činnosti relatívne vysokú komplexitu IT prostredia. Napriek niekoľkým zisteniam v oblasti IT architektúry pre Spoločnosť by bol návrh na rozsiahly redesign aplikačnej architektúry nadbytočným a teda neefektívnym, neprimeraným opatrením.

V rozsahu úpravy IT prostriedkov vyplývajú z analýzy rizík nasledovné opatrenia:

Opatrenie	Kategória hrozby	Riziková expozícia
Formálne stanoviť retenčnú dobu pre jednotlivé kategórie OÚ a jednotlivé spracovateľské činnosti	Súkromie	22,26
Zvážiť implementáciu riešenia pre zaručené vymazávanie osobných údajov	Súkromie	22,26
Zvážiť implementáciu komplexného zálohovacieho riešenia pre súbory používateľov	Zlyhania techniky	14,05
Preveriť potrebu používania privilegovaných účtov, zabezpečiť odobratie práv pri neodôvodnenom používaní privilegovaných účtov	Neautorizované činnosti	12,99
Vykonávať pravidelnú kontrolu neautorizovanej interkonektivity a vykonávať pravidelné penetračné testy	Neautorizované činnosti	12,99
Zaručiť technické obmedzenie svojvoľnej inštalácie SW a odobrať privilegované práva bežným používateľom	Neautorizované činnosti	12,99
Zvážiť dovybavenie mechanickými zábrannými prostriedkami (turnikety, mreže) a Elektronickou požiarnou signalizáciou	Neautorizované činnosti	12,99
Zvážiť implementáciu log managementu pre všetky kritické systémy	Kompromitácia informácií	6,13

Zvážiť implementáciu ďalších prostriedkov šifrovej ochrany informácií, najmä na notebookoch používaných mimo fyzického perimetra	Kompromitácia informácií	6,13
Zvážiť implementáciu riešenia pre hodnotenie zraniteľností a vykonávať hodnotenie technických zraniteľností v pravidelných intervaloch	Kompromitácia informácií	6,13

3 NÁVRHY NA IMPLEMENTÁCIU PROCESOV

Spoločnosť danej veľkosti má minimálny počet pracovných procesov. Procesy sú podrobne popísané notáciou BMP/DfD v prílohe č. 2.

Procesy sú prehľadné a zdokumentované. Pre Spoločnosť danej veľkosti by bol návrh na nadbytočnú formalizáciu procesov neefektívnym, neprimeraným opatrením.

Odporúčané je upraviť niektoré procesy nasledujúcim spôsobom:

Opatrenie	**Kategória hrozby**	**Riziková expozícia**
Formálne stanoviť retenčnú dobu pre jednotlivé kategórie OÚ a jednotlivé spracovateľské činnosti	Súkromie	22,26
Zvážiť implementáciu riešenia pre zaručené vymazávanie osobných údajov	Súkromie	22,26
Zvážiť implementáciu komplexného zálohovacieho riešenia pre súbory používateľov	Zlyhania techniky	14,05
Preveriť potrebu používania privilegovaných účtov, zabezpečiť odobratie práv pri neodôvodnenom používaní privilegovaných účtov	Neautorizované činnosti	12,99
Vykonávať pravidelnú kontrolu neautorizovanej interkonektivity a vykonávať pravidelné penetračné testy	Neautorizované činnosti	12,99
Zaručiť technické obmedzenie svojvoľnej inštalácie SW a odobrať privilegované práva bežným používateľom	Neautorizované činnosti	12,99
Zvážiť dovybavenie mechanickými zábrannými prostriedkami (turnikety, mreže) a Elektronickou požiarnou signalizáciou	Neautorizované činnosti	12,99
Zvážiť implementáciu log managementu pre všetky kritické systémy	Kompromitácia informácií	6,13
Zvážiť implementáciu ďalších prostriedkov šifrovej ochrany informácií, najmä na notebookoch používaných mimo fyzického perimetra	Kompromitácia informácií	6,13
Zvážiť implementáciu riešenia pre hodnotenie zraniteľností a vykonávať hodnotenie technických zraniteľností v pravidelných intervaloch	Kompromitácia informácií	6,13

4 NÁVRH ZMIEN INTERNÝCH SMERNÍC A PROCESOV

Pre Spoločnosť danej veľkosti je nutná komplexnejšia štruktúra interných štandardov. Z toho dôvodu je navrhovaná aj zmena štruktúry štandardov. Odporúčané je vydať stručné smernice pre príslušné procesy:

Opatrenie	Kategória hrozby	Riziková expozícia
Rozšíriť jestvujúcu smernicu o používaní IKT o postupy pre overenie dostatočných záruk	Kompromitácia funkcií	18,33
Navrhnúť a implementovať proces manažmentu identít a implementovať riadenie prístupov prostredníctvom domény	Neautorizované činnosti	12,99
Rozšíriť jestvujúcu smernicu o používaní IKT o postupy ochrany údajov v požiadavkách pre nové systémy a v pravidlách pre vývoj a nákup systémov	Kompromitácia informácií	6,13
Rozšíriť jestvujúcu smernicu o používaní IKT o pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.	Kompromitácia informácií	6,13
Rozšíriť jestvujúcu smernicu o používaní IKT o pravidlá spracúvania OÚ mimo chránených priestorov	Kompromitácia informácií	6,13

5 NÁVRH NA ZMENY V BEZPEČNOSTI SPRACÚVANIA

Spoločnosť má väčšinu pracovných procesov sformalizovaných, zdokumentovaných smernicami. Pre potreby tohto dokumentu sú procesy sú podrobne zakreslené notáciou BMP/DfD v prílohe č. 2..

Spoločnosť má zavedený a certifikovaný komplexný systém riadenia informačnej bezpečnosti (podľa ISO 27000.

V rozsahu zmien v bezpečnosti spracúvania vyplývajú z analýzy rizík nasledovné opatrenia:

Opatrenie	Kategória hrozby	Riziková expozícia
Navrhnúť mechanizmus kontroly súladu spracovateľov a sub-spracovateľov s GDPR	Súkromie	22,26
Navrhnúť štandardnú doložku pre zmluvy s tretími stranami o dodávkach tovaru a služieb.	Súkromie	22,26
Prehodnotiť doby retencie pre všetky kategórie spracúvaných OÚ	Súkromie	22,26
Prehodnotiť text súhlasu v kontexte prezenčnej listiny	Súkromie	22,26
Upraviť text súhlasu tak, aby v ňom bolo zachytené vzdanie sa právnej zodpovednosti	Súkromie	22,26
Uviesť právne základy v zozname spracovateľských činností	Súkromie	22,26
Vymenovať Zodpovednú osobu	Súkromie	22,26
Vypublikovať na webe možnosť odvolania súhlasu vztiahnutého na konkrétny účel	Súkromie	22,26

Vykonať a cyklicky opakovať v odpovedajúcom rozsahu poučenia oprávnených osôb. Zvážiť formálne zavedenie vzdelávacieho procesu zvyšovania bezpečnostného povedomia.	Kompromitácia funkcií	18,33
Zvážiť uchovávanie záloh mimo budovy	Zlyhania techniky	14,05
Navrhnúť internú smernicu o Exit managemente, resp. zapracovať povinnosti vyplývajúce z exit management procesu do smernice o IKT	Neautorizované činnosti	12,99
Upraviť zmluvy ošetrujúce potenciálny prístup tretích strán ku osobným údajom	Kompromitácia informácií	6,13
Vyriešiť bezpečnú likvidáciu HDD prípadne iných médií interne alebo dodávateľským spôsobom.	Kompromitácia informácií	6,13

Odporúčania v súvislosti s bezpečnosťou spracúvania sú zachytené najmä v odporúčaniach predchádzajúcich kapitol 2, 0 a 0 v tejto časti dokumentu.

ZOZNAM PRÍLOH

1 ZOZNAM PRÍLOH

2 ZOZNAM OBRÁZKOV

3 ZOZNAM TABULIEK

4 ZOZNAM GRAFOV

Popis uplatnenia bezpečnostných opatrení a stav súladu

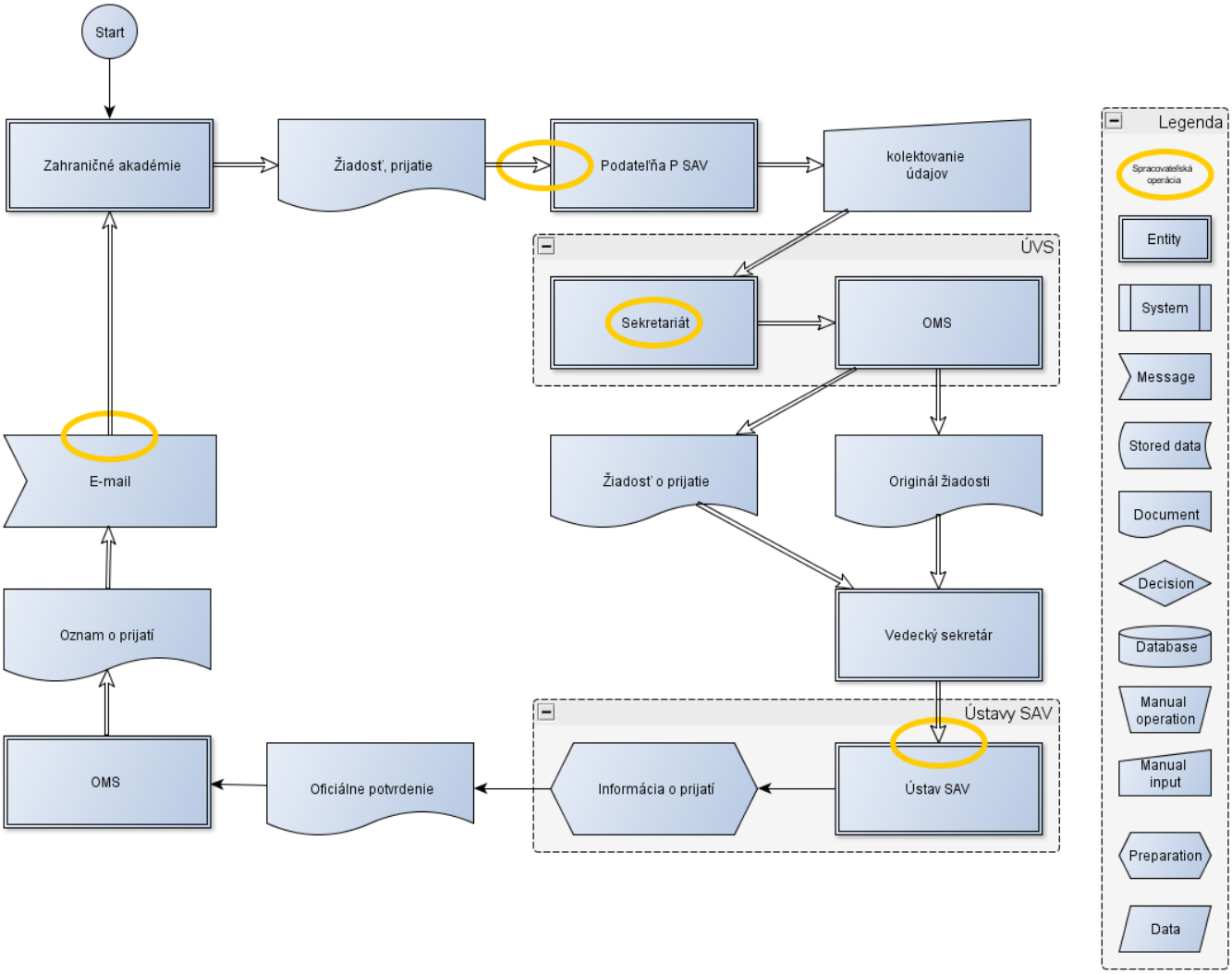
Cislo	Kategoria	Oblast	Poziadavka	Stav suladu	Jestvujuci stav	Osetrenie rizika	Navrh opatreni
1110	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Zabezpečenie objektu pomocou mechanických zábranných prostriedkov a pomocou technických zabezpečovacích prostriedkov	ČIASTOČNÝ SÚLAD	Služba 11/5, zamknuté, KS, EZS=áno	zníženie / ďalšie ošetrovanie rizika	Zvážiť dovybavenie prostriedkami fyzickej ochrany (turnikety, mreže) a EPS
1120	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu	SÚLAD	Miestnosti v ktorých sú spracúvané osobné údaje sú oddelené od ostatných častí objektu a opatrené zámkami.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1130	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Kontrola vstupu do objektu a chránených priestorov prevádzkovateľa	SÚLAD	Miestnosti v ktorých sú spracúvané osobné údaje sú oddelené od ostatných častí objektu a čipovými zámkami. Vstupy do objektu sú riadené na recepcii.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1140	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia	ČIASTOČNÝ SÚLAD	Samostatná miestnosť, IS umiestnený v osobitej serverovni. Záložná serverovňa nedostatočne chránená.	zníženie / ďalšie ošetrovanie rizika	Zvýšenie fyzickej bezpečnosti 2. serverovne
1150	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Bezpečné uloženie fyzických nosičov osobných údajov, vrátane bezpečného uloženia listinných dokumentov	SÚLAD	Fyzické nosiče osobných údajov sú umiestnené lokálne v kancelárii, v uzamykateľných skriniach, zamykateľný archív	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1160	1. Technické opatrenia	1.1 Technické opatrenia realizované prostriedkami fyzickej povahy	Opatrenia pre zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek	SÚLAD	Všetky monitory sú otočené od klienta (za pultom), náhodné odpozorovanie nie je možné	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1210	1. Technické opatrenia	1.2 Ochrana pred neoprávneným prístupom	Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia	NESÚLAD	Šifrová ochrana dát nie je aplikovaná, nie sú definované pravidlá.	zníženie / ďalšie ošetrovanie rizika	Zvážiť celoplošnú implementáciu šifrovej ochrany najmä na notebookoch vynášaných z perimetra spoločnosti.
1220	1. Technické opatrenia	1.2 Ochrana pred neoprávneným prístupom	Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza	ČIASTOČNÝ SÚLAD	Prístup tretích strán ku automatizovaným prostriedkom spracovania OÚ jestvuje, nie sú definované pravidlá.	zníženie / ďalšie ošetrovanie rizika	Upraviť zmluvy ošetrujúce potenciálny prístup tretích strán ku osobným údajom.
1310	1. Technické opatrenia	1.3 Riadenie prístupu oprávnených osôb	Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov	NESÚLAD	Identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme len cez lokálne účty. Proces je manažovaný neformálne. Nie je definovaná heslová politika. Neidentifikovateľný rozsah používateľov s administrátorskými právami.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť predpis o manažmente identít. Implementovať v praxi. Zaviesť systém AD.
1320	1. Technické opatrenia	1.3 Riadenie prístupu oprávnených osôb	Riadenie privilegovaných prístupov v informačných systémoch	ČIASTOČNÝ SÚLAD	Nie všetky počítače majú zablokované privilegované účty	zníženie / ďalšie ošetrovanie rizika	Preveriť potrebu privilegovaných účtov, zabezpečiť zmeny pri neodôvodnenom privilegovanom statuse.
1330	1. Technické opatrenia	1.3 Riadenie prístupu oprávnených osôb	Zaznamenávanie prístupu a aktivít jednotlivých oprávnených osôb v informačnom systéme	ČIASTOČNÝ SÚLAD	Logovanie na úrovni OS - Windows logy na štandardnej úrovni servera, Ekon.SW logovanie na úrovni užívateľa	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu procesu log managementu pre všetky kritické systémy
1410	1. Technické opatrenia	1.4 Riadenie zraniteľností	Opatrenia pre detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu	SÚLAD	Decentralizovaný manažovaný antimalware systém ESET. Administrátorská konzola je nasadená.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1420	1. Technické opatrenia	1.4 Riadenie zraniteľností	Ochrana pred nevyžiadanou elektronickou poštou	SÚLAD	Decentralizovaný manažovaný antimalware systém ESET. Administrátorská konzola je nasadená.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1430	1. Technické opatrenia	1.4 Riadenie zraniteľností	Používanie legálneho a prevádzkovateľom schváleného softvéru	ČIASTOČNÝ SÚLAD	Ošetrené smernicou, problém s používateľmi s administrátorskými právam a nadužívaním licencií ošetrené, nadužívanie licencií.	zníženie / ďalšie ošetrovanie rizika	Technické obmedzenie svojvoľnej inštalácie SW - odstránenie používateľov s nedôvodnými administrátorskými právami.
1440	1. Technické opatrenia	1.4 Riadenie zraniteľností	Opatrenia pre zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia	SÚLAD	Automatické systémy, Windows update	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1450	1. Technické opatrenia	1.4 Riadenie zraniteľností	Vynútenie pravidiel sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania, filtrovanie sieťovej komunikácie.	SÚLAD	Riešenie pre vynútenie pravidiel sťahovania súborov z verejne prístupnej počítačovej siete a spôsobu ich overovania, resp. filtrovanie sieťovej komunikácie je vynucované technologicky.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
1460	1. Technické opatrenia	1.4 Riadenie zraniteľností	Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík	NESÚLAD	Technické zraniteľnosti informačných systémov nie sú pravidelne hodnotené, vyhodnocovanie úrovne rizík a opatrenia na potlačenie týchto rizík nie sú uplatnené.	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu riešenia pre hodnotenie zraniteľností, resp. vyknávať hodnotenie technických zraniteľností v pravidelných intervaloch
1510	1. Technické opatrenia	1.5 Sieťová bezpečnosť	Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou	SÚLAD	Firewall Fortinet s aktívnou ochranou	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu pravidelnej kontroly a penetračné testy
1520	1. Technické opatrenia	1.5 Sieťová bezpečnosť	Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti, segmentácia počítačovej siete	SÚLAD	Firewall Fortinet s aktívnou ochranou	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu pravidelnej kontroly a penetračné testy
1530	1. Technické opatrenia	1.5 Sieťová bezpečnosť	Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia pre zamedzenie pripojenia k určitým adresám, pravidlá pre používanie sieťových protokolov	ČIASTOČNÝ SÚLAD	Riešenie pre vynútenie pravidiel prístupu do verejne počítačovej siete je implementované čiastočne. Neexistujúca smernica. čiastočne filtrované, neudržiavaný, black listy automatizované	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis pre pravidlá používania Internetu a elektronickej pošty
1540	1. Technické opatrenia	1.5 Sieťová bezpečnosť	Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete	SÚLAD	Firewall Fortinet s aktívnou ochranou	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu pravidelnej kontroly a penetračné testy
1610	1. Technické opatrenia	1.6 Zálohovanie	Testovanie funkčnosti záložných dátových nosičov	ČIASTOČNÝ SÚLAD	Vykonávané len pri teste obnovy pri výpadku systémov.	zníženie / ďalšie ošetrovanie rizika	Zvážiť zavedenie procesu overovania integrity vytváraných záloh.
1620	1. Technické opatrenia	1.6 Zálohovanie	Vytváranie záloh s vopred zvolenou periodicitou	ČIASTOČNÝ SÚLAD	Nepravidelné zálohovanie užívateľských dát, Ekon.systém sa zálohuje denne	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu komplexného zálohovacieho riešenia pre súbory užívateľov

Cislo	Kategoria	Oblast	Poziadavka	Stav suladu	Jestvujuci stav	Osetrenie rizika	Navrh opatreni
1630	1. Technické opatrenia	1.6 Zálohovanie	Určenie doby uchovávanie záloh a kontrola jej dodržiavania	ČIASTOČNÝ SÚLAD	Je stanovená retenčná doba záloh, ale nie pre všetky kategórie	zníženie / ďalšie ošetrovanie rizika	Formálne stanoviť retenčnú dobu pre jednotlivé kategórie OÚ a jednotlivé spracovateľské činnosti
1640	1. Technické opatrenia	1.6 Zálohovanie	Test obnovy informačného systému zo zálohy	ČIASTOČNÝ SÚLAD	Vykonávané len pri teste obnovy pri výpadku systémov.	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu zálohovacieho riešenia pre súbory užívateľov
1650	1. Technické opatrenia	1.6 Zálohovanie	Bezpečné ukladanie záloh	ČIASTOČNÝ SÚLAD	Zamykaná serverovňa. Zálohy neopúšťajú budovu	zníženie / ďalšie ošetrovanie rizika	Zvážiť implementáciu zálohovacieho riešenia pre súbory užívateľov a uchovávanie záloh mimo budovy
1710	1. Technické opatrenia	1.7 Likvidácia osobných údajov a dátových nosičov	Technické opatrenia pre bezpečné vymazanie osobných údajov z dátových nosičov	ČIASTOČNÝ SÚLAD	DVD/FDD existujú, používanie USB neriadené a nekontrolované. Vyraďovanie HDD neformálne riešené, HDD sú skladované v trezore bez doterajšej likvidácie.	zníženie / ďalšie ošetrovanie rizika	Zvážiť vydanie interného predpisu o používaní prostriedkov IKT a základných zásadách informačnej bezpečnosti. Poučiť zamestnancov o Best Practice a optimálnej starostlivosti o dáta. Zvážiť implementáciu riešenia pre zaručené vymazávanie osobných údajov. Vyriešiť bezpečnú likvidáciu HDD prípadne iných médií interne alebo dodávateľským spôsobom.
1720	1. Technické opatrenia	1.7 Likvidácia osobných údajov a dátových nosičov	Zariadenie na mechanické zničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií)	SÚLAD	Pracovisko je vybavené skartovacím zariadením Cat3, datové médiá sa neskartujú (neexistujú)	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2110	2. Organizačné opatrenia	2.1 Personálne opatrenia	Poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi	ČIASTOČNÝ SÚLAD	Poučenia oprávnených osôb nie sú vykonávané v plnom rozsahu.	zníženie / ďalšie ošetrovanie rizika	Vykonať a cyklicky opakovať v odpovedajúcom rozsahu poučenia oprávnených osôb.
2111	2. Organizačné opatrenia	2.1 Personálne opatrenia	Poučenie o právach a povinnostiach vyplývajúcich zo zákona alebo osobitného predpisu a zodpovednosti za ich porušenie	ČIASTOČNÝ SÚLAD	Poučenia oprávnených osôb nie sú vykonávané v plnom rozsahu.	zníženie / ďalšie ošetrovanie rizika	Vykonať a cyklicky opakovať v odpovedajúcom rozsahu poučenia oprávnených osôb.
2112	2. Organizačné opatrenia	2.1 Personálne opatrenia	Vymedzenie osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh	ČIASTOČNÝ SÚLAD	Proces nie je dostatočne zavedený.	zníženie / ďalšie ošetrovanie rizika	Formálne definovať proces. Vykonať a cyklicky podľa potrieb realizovať poučenia oprávnených osôb.
2113	2. Organizačné opatrenia	2.1 Personálne opatrenia	Určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov	ČIASTOČNÝ SÚLAD	Proces nie je dostatočne zavedený.	zníženie / ďalšie ošetrovanie rizika	Formálne definovať proces. Vykonať a cyklicky podľa potrieb realizovať poučenia oprávnených osôb.
2114	2. Organizačné opatrenia	2.1 Personálne opatrenia	Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi	ČIASTOČNÝ SÚLAD	Proces nie je dostatočne zavedený.	zníženie / ďalšie ošetrovanie rizika	Formálne definovať proces. Vykonať a cyklicky podľa potrieb realizovať poučenia oprávnených osôb.
2115	2. Organizačné opatrenia	2.1 Personálne opatrenia	Vymedzenie zodpovednosti za porušenie zákona alebo osobitného predpisu	ČIASTOČNÝ SÚLAD	Proces nie je dostatočne zavedený.	zníženie / ďalšie ošetrovanie rizika	Formálne definovať proces. Vykonať a cyklicky podľa potrieb realizovať poučenia oprávnených osôb.
2120	2. Organizačné opatrenia	2.1 Personálne opatrenia	Poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov)	ČIASTOČNÝ SÚLAD	Poučenia oprávnených osôb nie sú vykonávané v plnom rozsahu.	zníženie / ďalšie ošetrovanie rizika	Vykonať a cyklicky opakovať v odpovedajúcom rozsahu poučenia oprávnených osôb.
2130	2. Organizačné opatrenia	2.1 Personálne opatrenia	Určenie zodpovednej osoby	ČIASTOČNÝ SÚLAD	Zodpovedná osoba nie je formálne určená, ale úlohy sú vykonávané	zníženie / ďalšie ošetrovanie rizika	Vymenovať Zodpovednú osobu podľa GDPR
2140	2. Organizačné opatrenia	2.1 Personálne opatrenia	Vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií)	ČIASTOČNÝ SÚLAD	Nie je pravidelne vykonávané, poučenie je vykonávané len na úrovni minimálneho rozsahu pre oprávnené osoby.	zníženie / ďalšie ošetrovanie rizika	Zvážiť zavedenie cyklického vzdelávacieho procesu zvyšovania bezpečnostného povedomia.
2150	2. Organizačné opatrenia	2.1 Personálne opatrenia	Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)	SÚLAD	Exit management proces je formálne definovaný. Zvykové postupy existujú, neexistuje kontrolný mechanizmus.	riziko nie je identifikované	Zvážiť internú smernicu Exit management
2160	2. Organizačné opatrenia	2.1 Personálne opatrenia	Práca na diaľku a pravidlá mobilného spracovania dát	NESÚLAD	Pravidlá pre teleworking nie sú formálne definované.	zníženie / ďalšie ošetrovanie rizika	Zvážiť internú smernicu pre pravidlá vzdialeného prístupu a práce na diaľku
2210	2. Organizačné opatrenia	2.2 Riadenie aktív	Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia	SÚLAD	Vedenie evidencie v SW v obmedznom rozsahu	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2220	2. Organizačné opatrenia	2.2 Riadenie aktív	Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou	SÚLAD	Vedenie evidencie v SW v obmedznom rozsahu	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2230	2. Organizačné opatrenia	2.2 Riadenie aktív	Určenie vlastníctva aktív a zodpovednosti za riziká	SÚLAD	Vedenie evidencie v SW v obmedznom rozsahu	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2240	2. Organizačné opatrenia	2.2 Riadenie aktív	Pravidlá a postupy pre klasifikáciu informácií a súbor postupov na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou	ČIASTOČNÝ SÚLAD	Pravidlá klasifikácie aktív nie sú formálne definované a ani potrebné	akceptácia zvyškového rizika	Klasifikácia aktív je vzhľadom na procesy spracovania OÚ bezpredmetná. Akceptovať zvyškové riziko.
2250	2. Organizačné opatrenia	2.2 Riadenie aktív	Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií	ČIASTOČNÝ SÚLAD	Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií nie sú formálne defnované	zníženie / ďalšie ošetrovanie rizika	Rozšíriť jestvujúcu smernicu o používaní IKT o pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.
2260	2. Organizačné opatrenia	2.2 Riadenie aktív	Opatrenia pre vrátenie aktív patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo prevádzkovej zmluvy	ČIASTOČNÝ SÚLAD	Exit management proces nie je formálne definovaný. Zvykové postupy jestvujú a sú efektívne, nejestvuje kontrolný mechanizmus.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť internú smernicu o Exit managemente, resp. zapracovať povinnosti vyplývajúce z exit management procesu do smernice o IKT
2310	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa	SÚLAD	Vrátnica 11/5, vstupy evidované dochádzkovým systémom na báze čipových kariet, vstup len v sprievode oprávnenej osoby (evidencia vstupov zapisovaním pracovníkom vrátnice)	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení

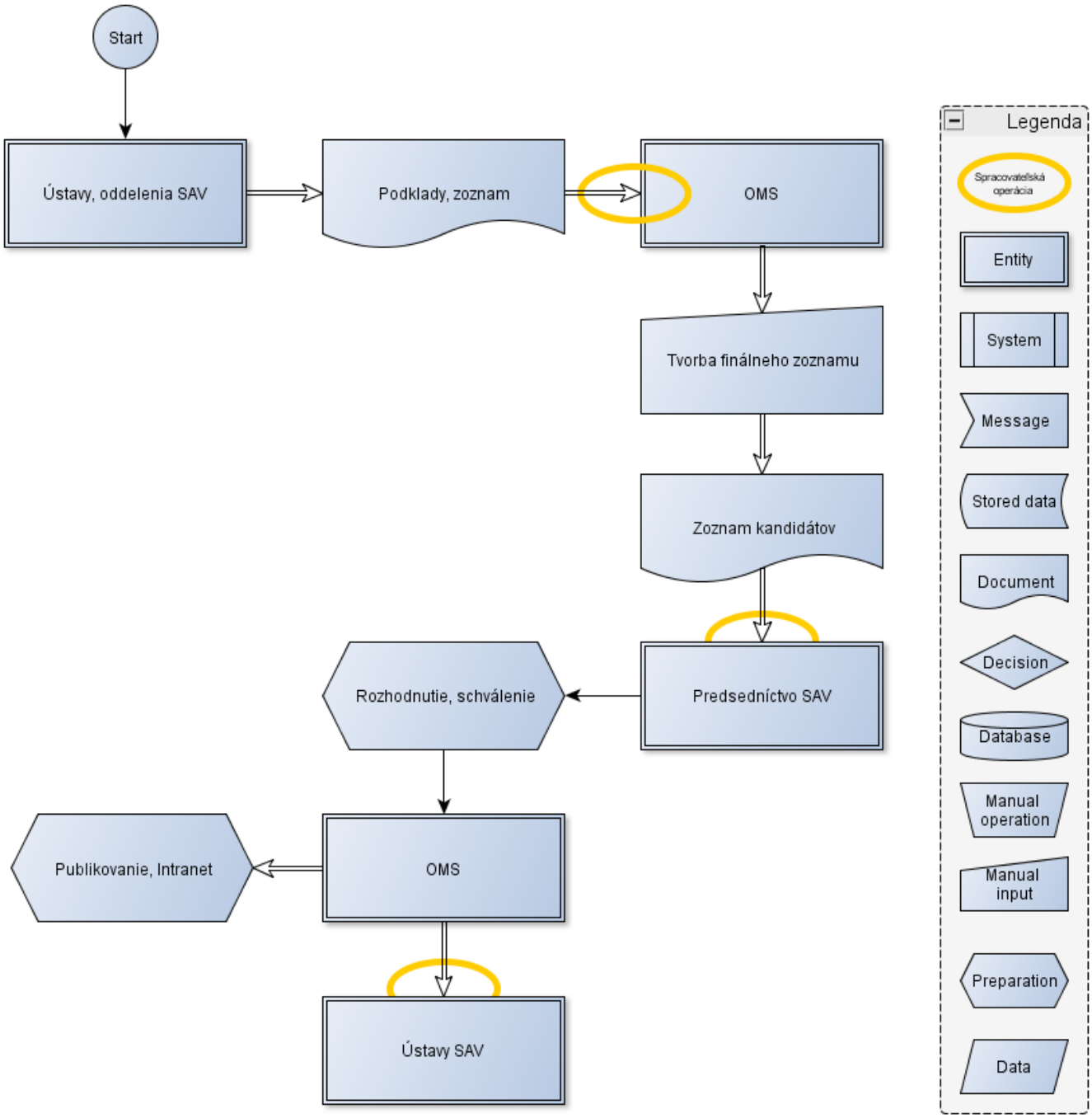
Cislo	Kategoria	Oblast	Poziadavka	Stav suladu	Jestvujuci stav	Osetrenie rizika	Navrh opatreni
2320	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)	SÚLAD	Je definovaná neformálna politika. Záložné kľúče v správe vrátnice	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2330	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Pravidlá pre prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb	ČIASTOČNÝ SÚLAD	Proces nie je formálne definovaný, práva na adresáre prideľuje správca IT na základe inštrukcie vlastníka údajov	zníženie / ďalšie ošetrovanie rizika	Navrhnúť predpis o manažmente identít, resp. zapracovať povinnosti vyplývajúce z procesu riadenia identít do smernice o IKT
2340	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov	NESÚLAD	Proces nie je formálne definovaný.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť predpis o manažmente identít, resp. zapracovať povinnosti vyplývajúce z procesu riadenia identít do smernice o IKT
2350	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Pravidlá pre vzájomné zastupovanie oprávnených osôb	SÚLAD	Zastupovanie je neformálne definované.	riziko nie je identifikované	Zvážiť prijatie Kompetenčného poriadku
2360	2. Organizačné opatrenia	2.3 Riadenie prístupu oprávnených osôb k osobným údajom	Pravidlá pre odstránenie alebo zmenu prístupových práv oprávnených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, prípadne prispôsobenie zmenám rolí	ČIASTOČNÝ SÚLAD	Proces je neformálne definovaný, ale technicky funkčný	zníženie / ďalšie ošetrovanie rizika	Navrhnúť predpis o manažmente identít, resp. zapracovať povinnosti vyplývajúce z procesu riadenia identít do smernice o IKT
2410	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Pravidlá spracúvania osobných údajov v chránenom priestore	ČIASTOČNÝ SÚLAD	Proces nie je formálne definovaný. Politika čistého stola neexistuje.	zníženie / ďalšie ošetrovanie rizika	Rozšíriť jestvujúcu smernicu o používaní IKT o postupy ochrany údajov.
2420	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby	SÚLAD	Návštevy sú vždy sprevádzané Oprávnenou osobou, nie je možný prístup do chránených priestorov bez oprávnenej osoby.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2430	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Režim údržby a upratovania chránených priestorov	SÚLAD	Údržbu vykonáva zmluvne tretia strana. Len v prítomnosti OO.	riziko nie je identifikované	Nie je nutná implementácia ďalších opatrení
2441	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovedností	NESÚLAD	Proces nie je formálne definovaný. Politika čistého stola neexistuje.	zníženie / ďalšie ošetrovanie rizika	Rozšíriť jestvujúcu smernicu o používaní IKT o postupy ochrany údajov.
2442	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Pravidlá používania automatizovaných prostriedkov spracúvania (napr. počítače, notebooky) mimo chránených priestorov a vymedzenie zodpovedností	NESÚLAD	Proces nie je formálne definovaný. Politika čistého stola neexistuje.	zníženie / ďalšie ošetrovanie rizika	Bolo vykonané poučenie oprávnených osôb. Rozšíriť jestvujúcu smernicu o používaní IKT o pravidlá spracúvania OÚ mimo chránených priestorov
2443	2. Organizačné opatrenia	2.4 Organizácia spracúvania osobných údajov	Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností	NESÚLAD	Proces nie je formálne definovaný. Politika čistého stola neexistuje.	zníženie / ďalšie ošetrovanie rizika	Bolo vykonané poučenie oprávnených osôb. Rozšíriť jestvujúcu smernicu o používaní IKT o pravidlá spracúvania OÚ mimo chránených priestorov
2510	2. Organizačné opatrenia	2.5 Likvidácia osobných údajov	Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)	ČIASTOČNÝ SÚLAD	Proces je definovaný, vykonávaný je ad-hoc. Povedomie zamestnancov je dostatočné. Vyraďované pevné disky historicky skladované v trezore.	zníženie / ďalšie ošetrovanie rizika	Zvážiť riešenie bezpečnej likvidácie vyradených pevných diskov.
2610	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Postup pri oznamovaní porušenia ochrany osobných údajov dozornému orgánu a dotknutej osobe na účel včasného prijatia preventívnych alebo nápravných opatrení	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2620	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách	NESÚLAD	Proces je neformálne definovaný, vykonávaný je ad-hoc.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2630	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Evidencia porušení ochrany osobných údajov a použitých riešení	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2640	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Postupy pre identifikáciu a riešenie jednotlivých typov porušení ochrany osobných údajov	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2650	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Postupy pre odstraňovanie následkov porušení ochrany osobných údajov	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2660	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Postupy zaručenia kontinuity činností pri haváriách, poruchách a iných mimoriadnych situáciách	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2670	2. Organizačné opatrenia	2.6 Porušenia ochrany osobných údajov	Postupy pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania	NESÚLAD	Servisné činnosti sú zabezpečované vo firme internými zamestnancami, servisované zariadenia neodchádzajú zo spoločnosti.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o manažmente incidentov. Zaviesť opakovateľný a udržateľný proces manažmentu incidentov.
2710	2. Organizačné opatrenia	2.7 Kontrolná činnosť	Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie	ČIASTOČNÝ SÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o systéme vnútornej kontroly. Zaviesť opakovateľný a udržateľný proces vnútornej kontroly a auditu.
2720	2. Organizačné opatrenia	2.7 Kontrolná činnosť	Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa alebo sprostredkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)	NESÚLAD	Proces nie je zavedený.	zníženie / ďalšie ošetrovanie rizika	Navrhnúť vnútorný predpis o systéme vnútornej kontroly. Zaviesť opakovateľný a udržateľný proces vnútornej kontroly a auditu.

Príloha č. 2a Grafické znázornenie spracovateľských činností

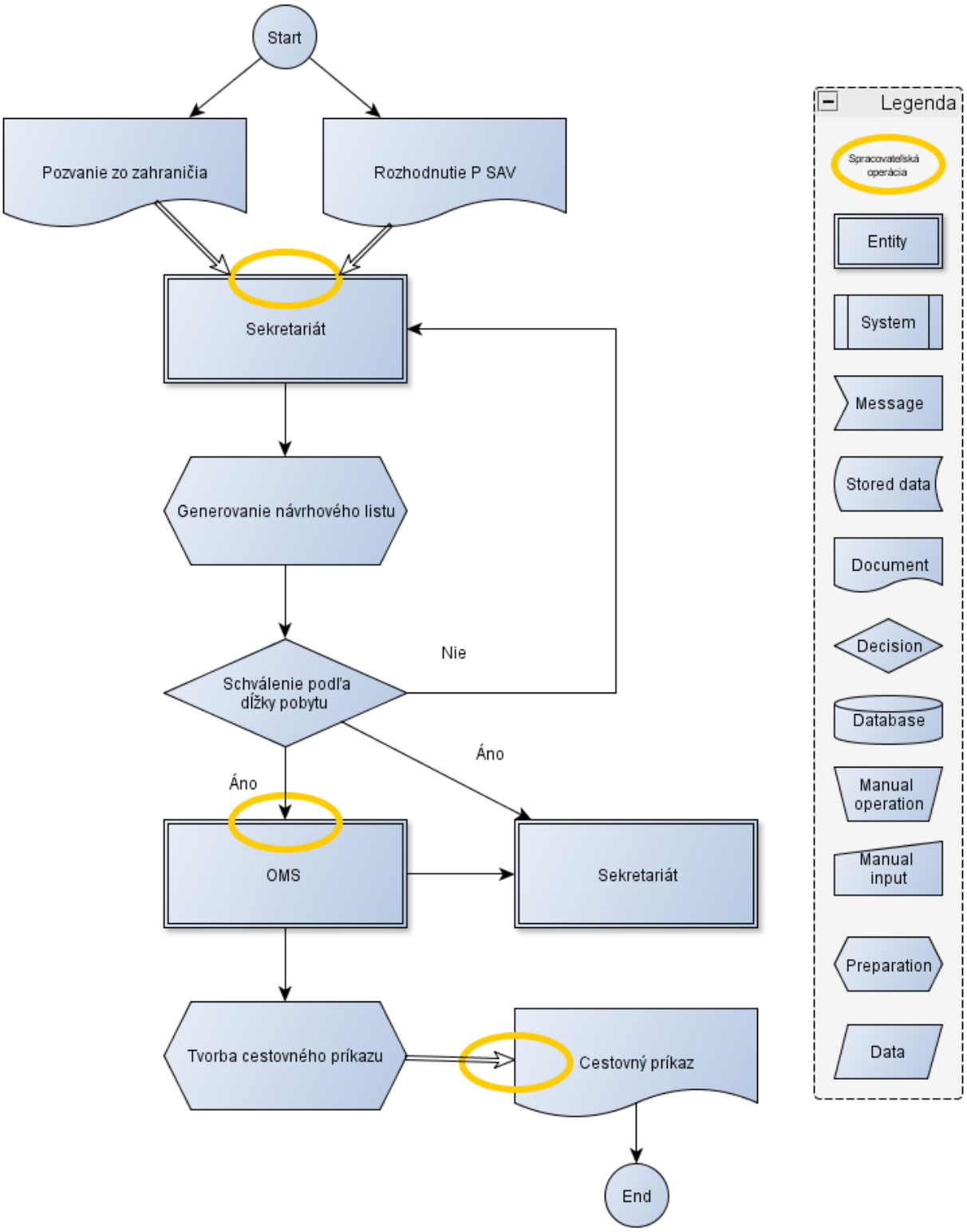
1.1 Schéma procesu MAD - Prijatie



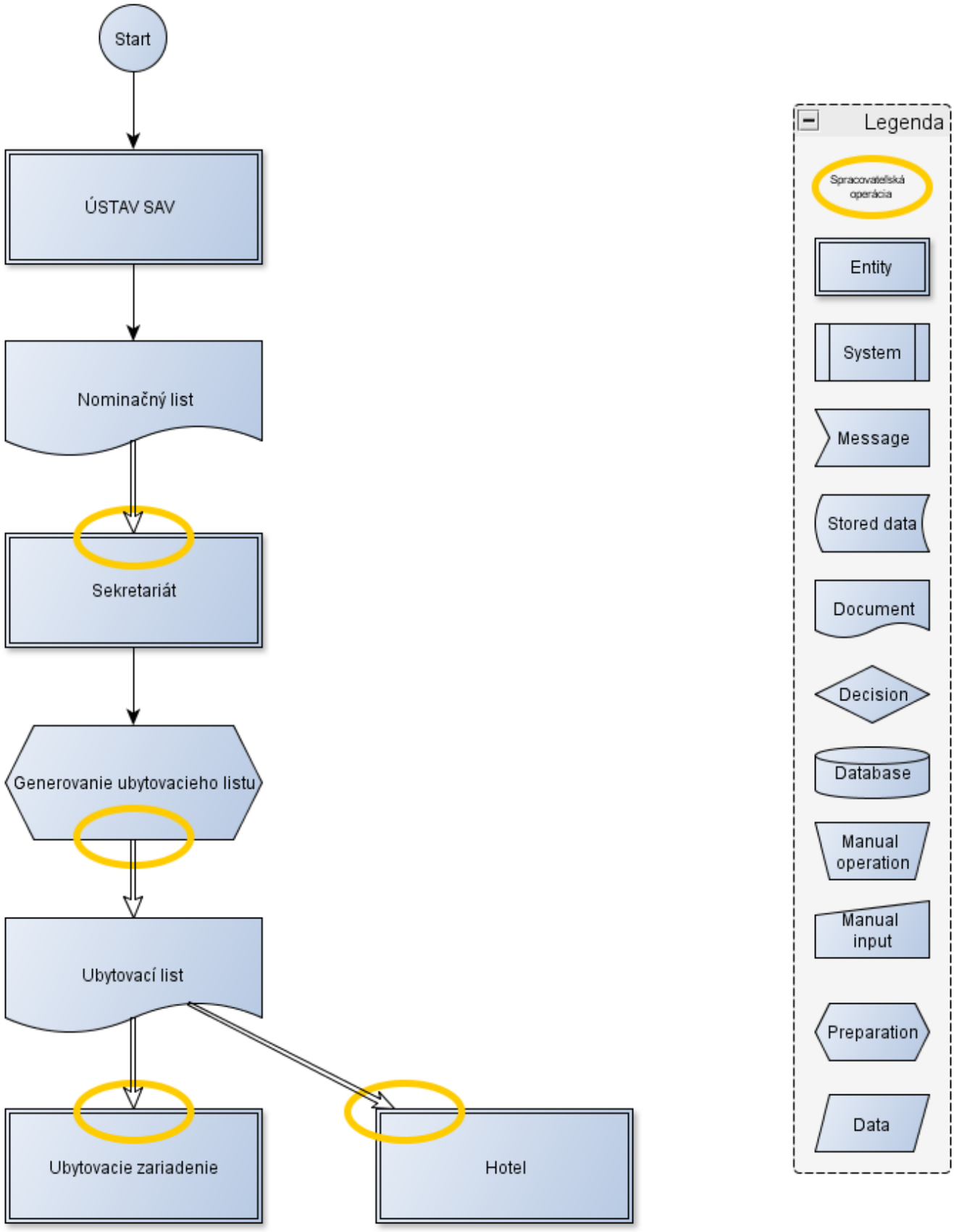
1.2 Schéma procesu MAD - Vyslanie



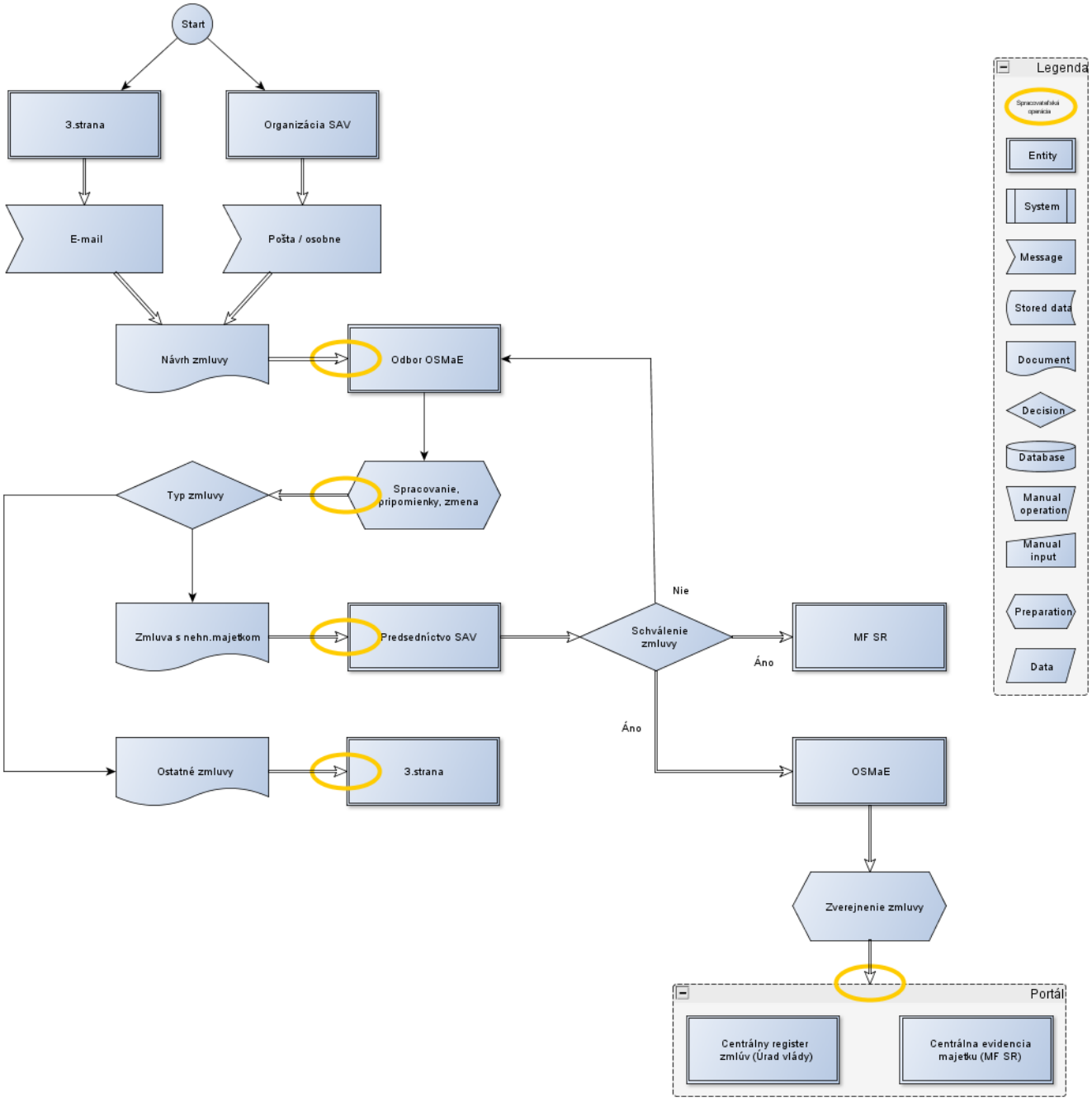
1.3 Schéma procesu Zahraničné cesty



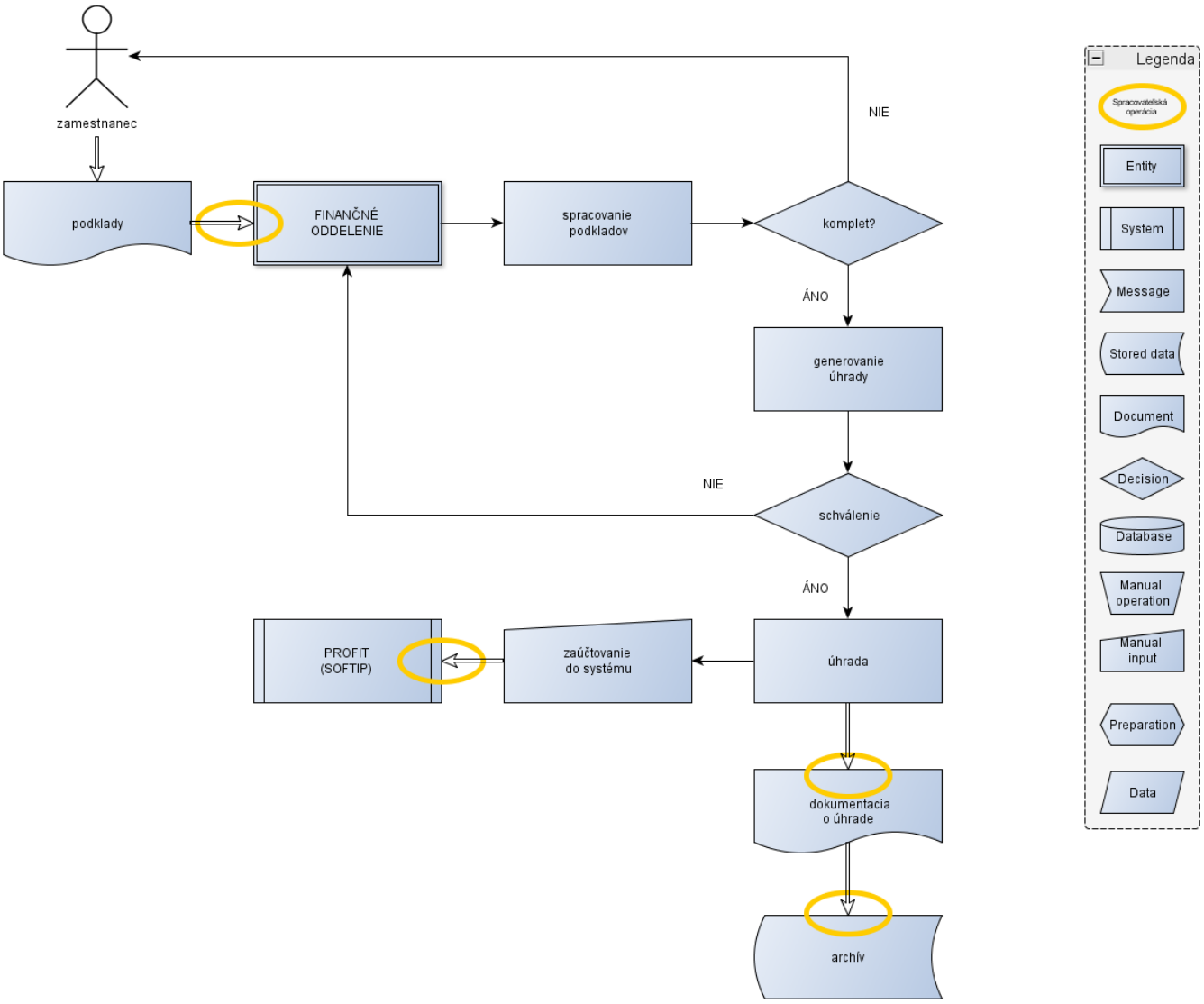
1.4 Schéma procesu Ubytovanie zahraničných hostí



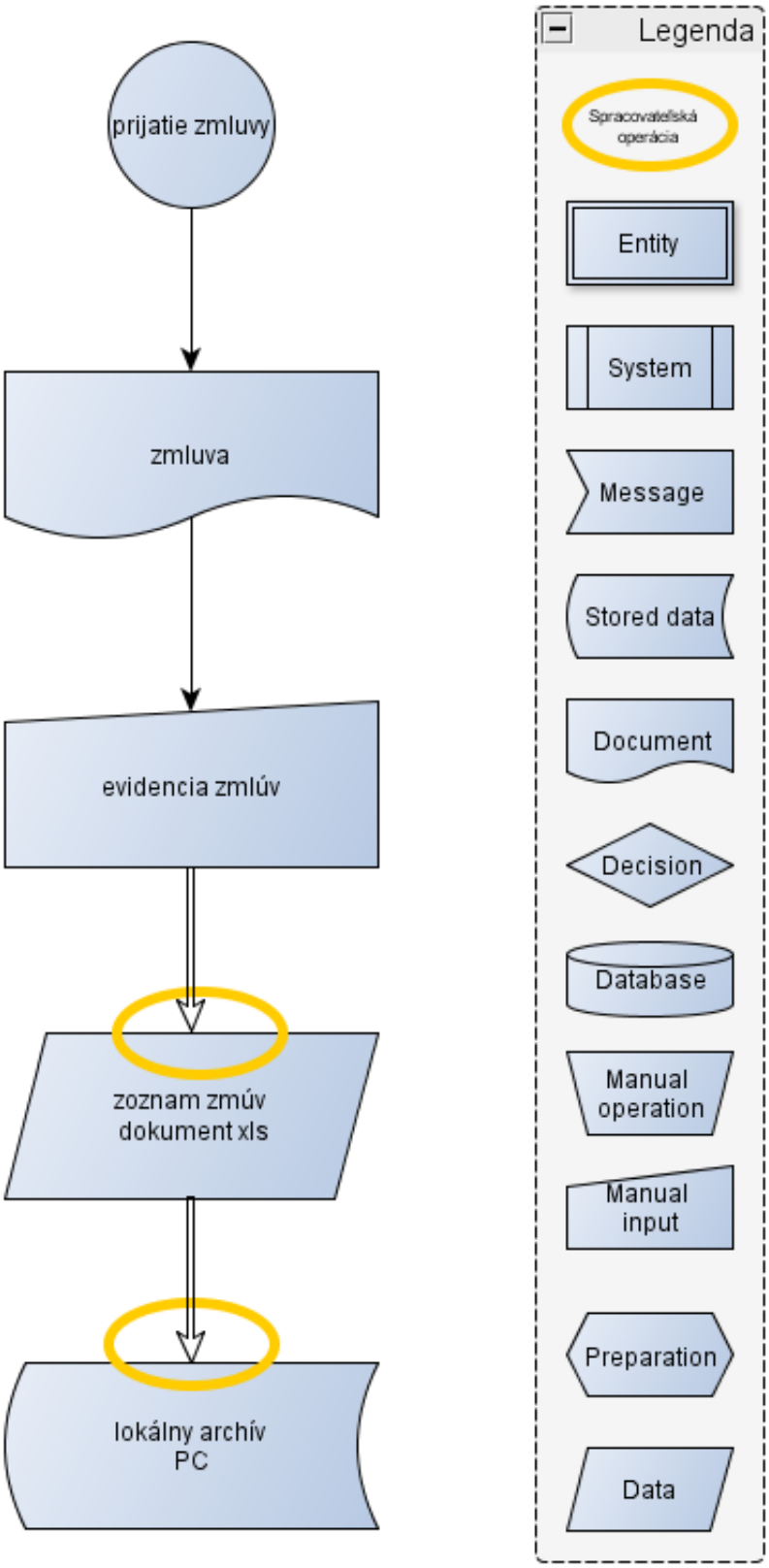
1.5 Schéma procesu OSMaE – Prijatie zmluvy



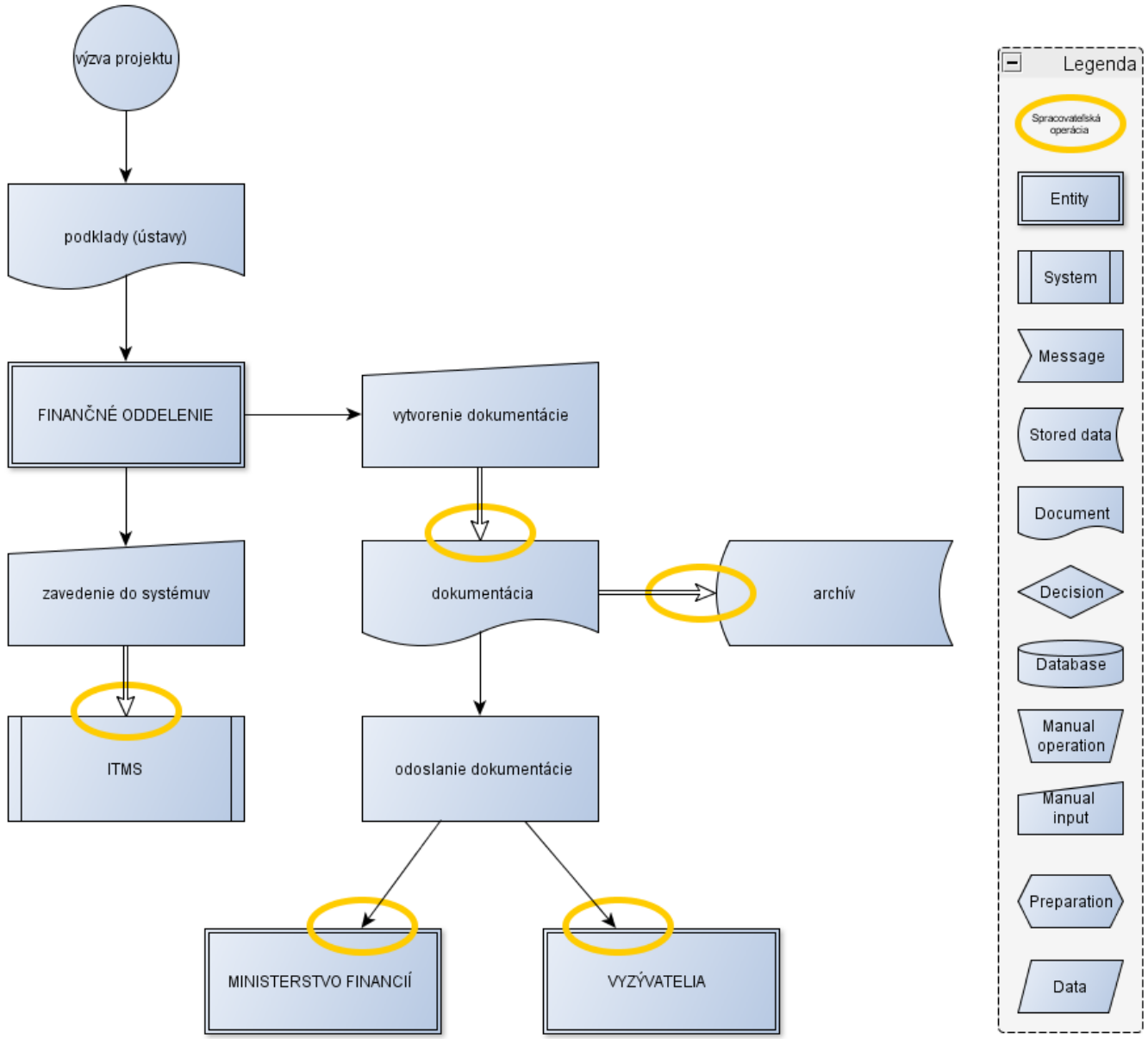
1.6 Schéma procesu Spracovanie podkladov na úhrady



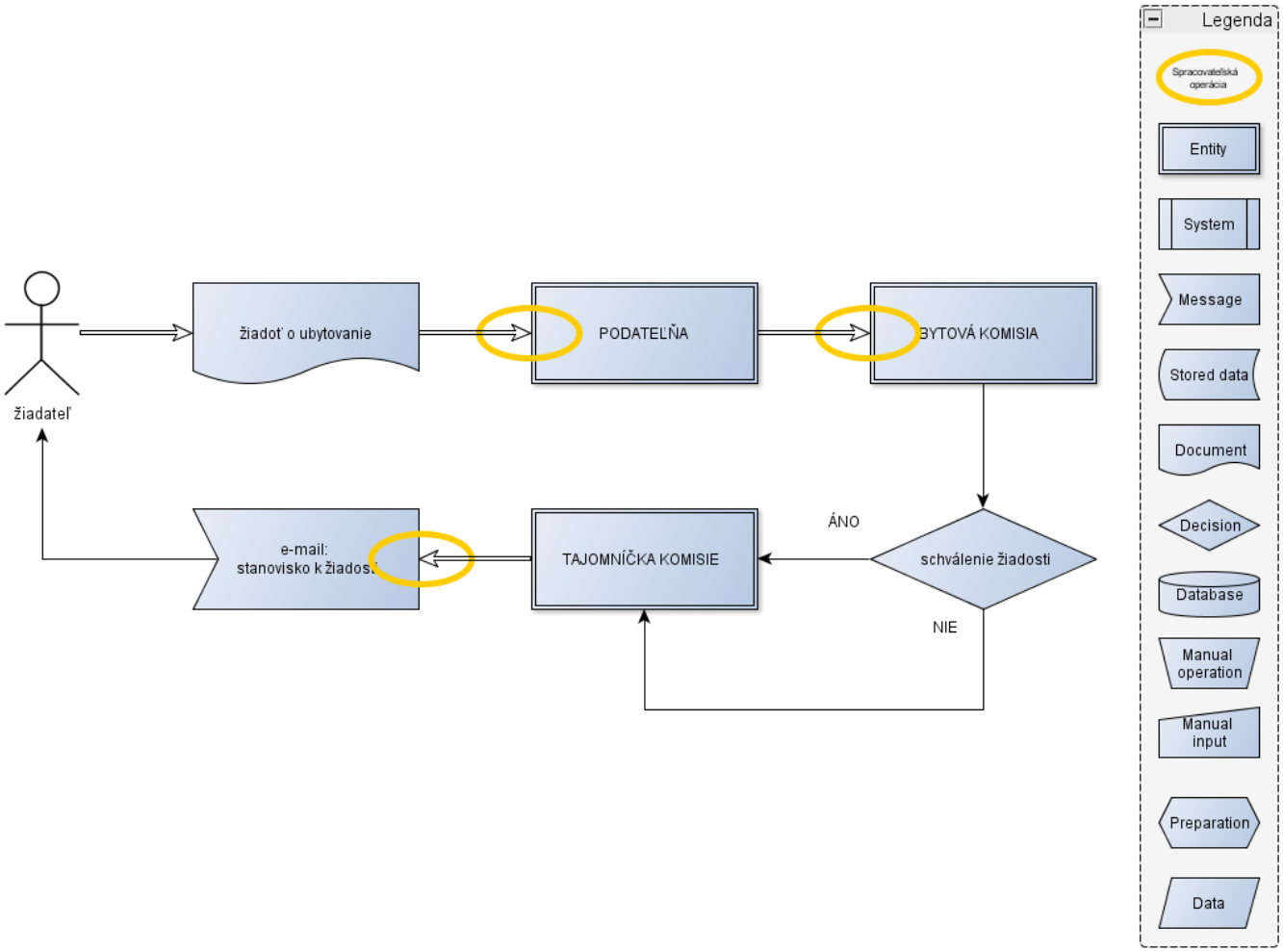
1.7 Schéma procesu Centrálna evidencia zmlúv



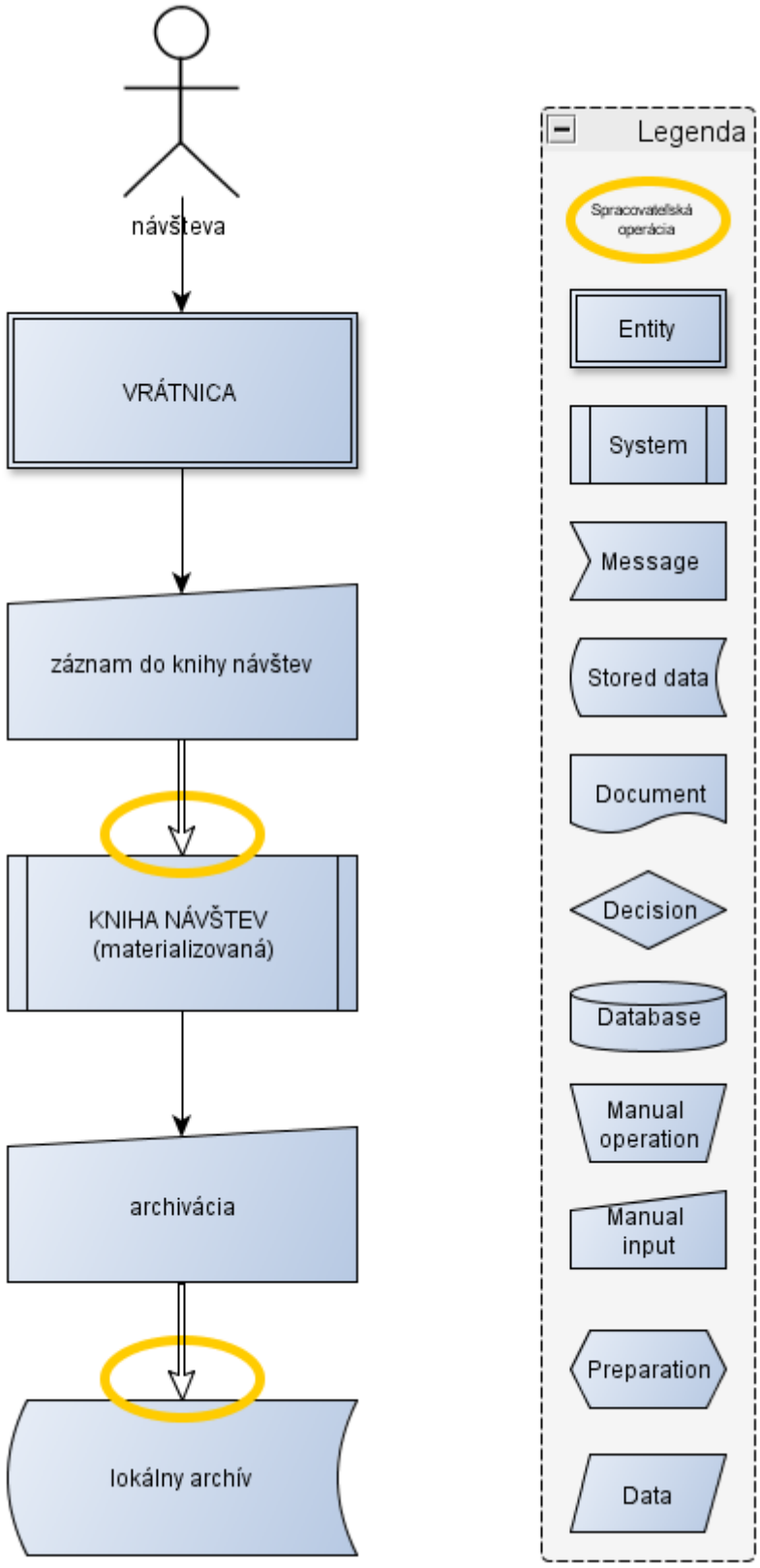
1.8 Schéma procesu Podklady k štrukturálnym fondom



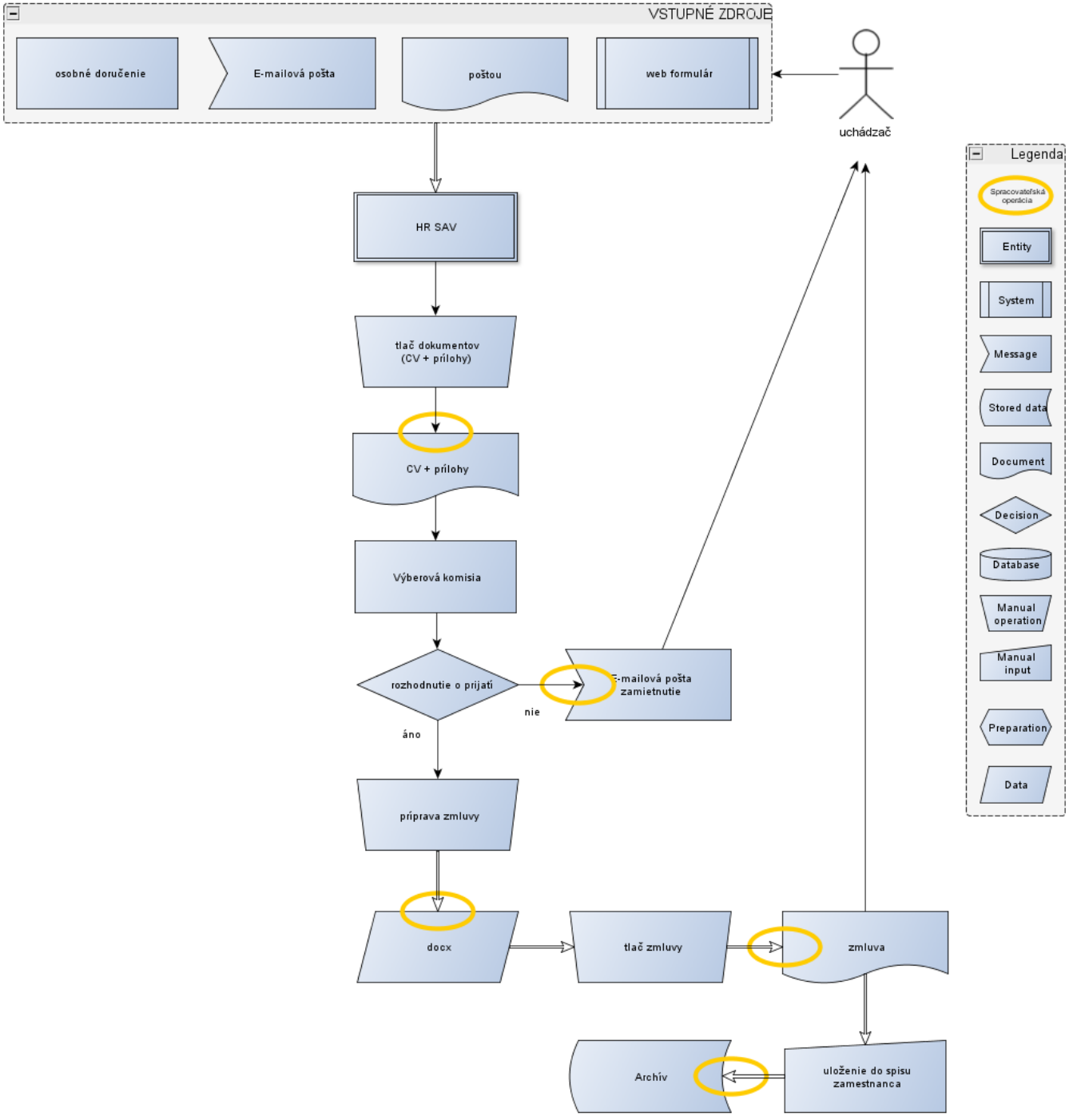
1.9 Schéma procesu Správa ubytovacích zariadení



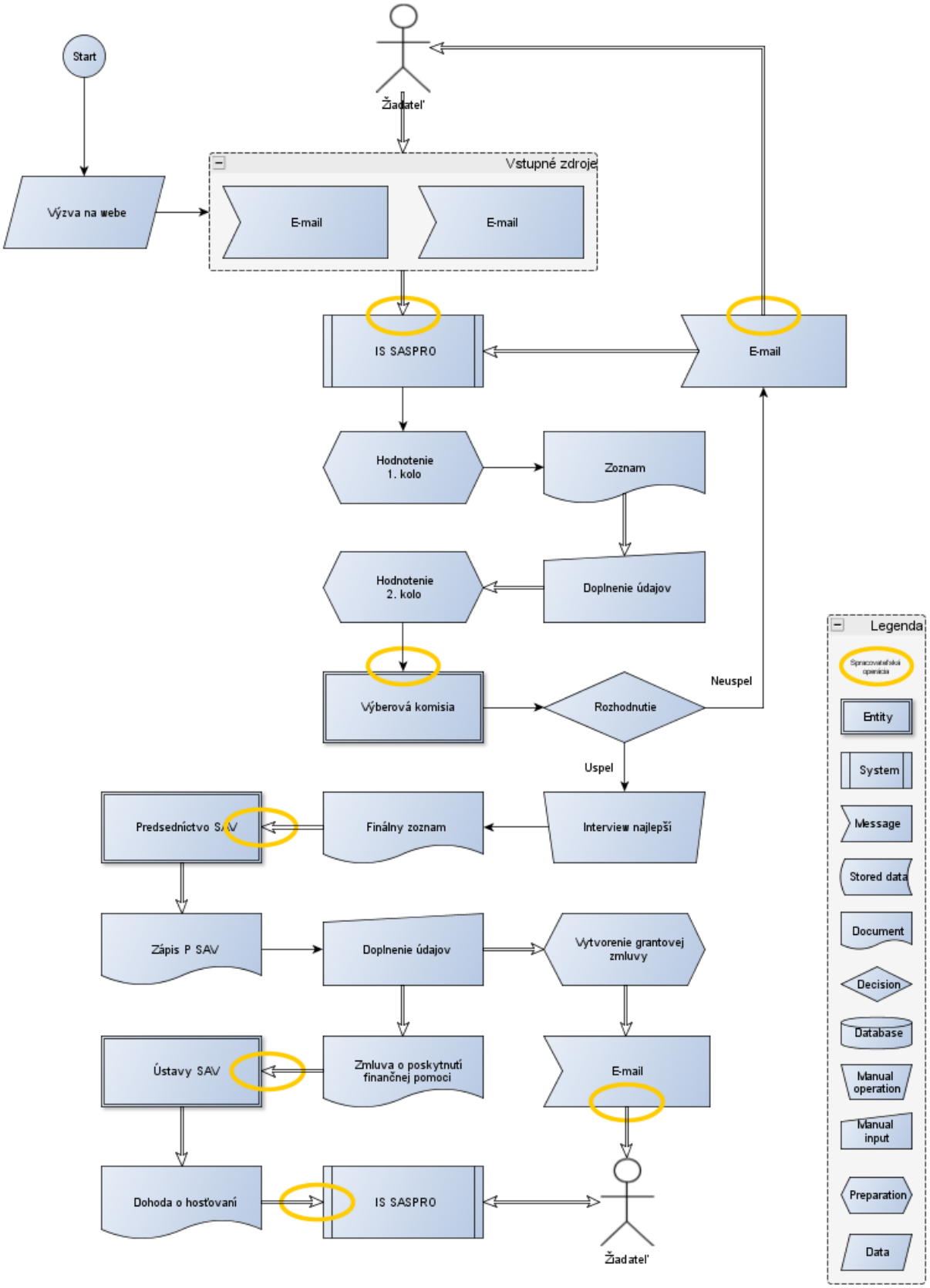
1.10 Schéma procesu Kniha návštev



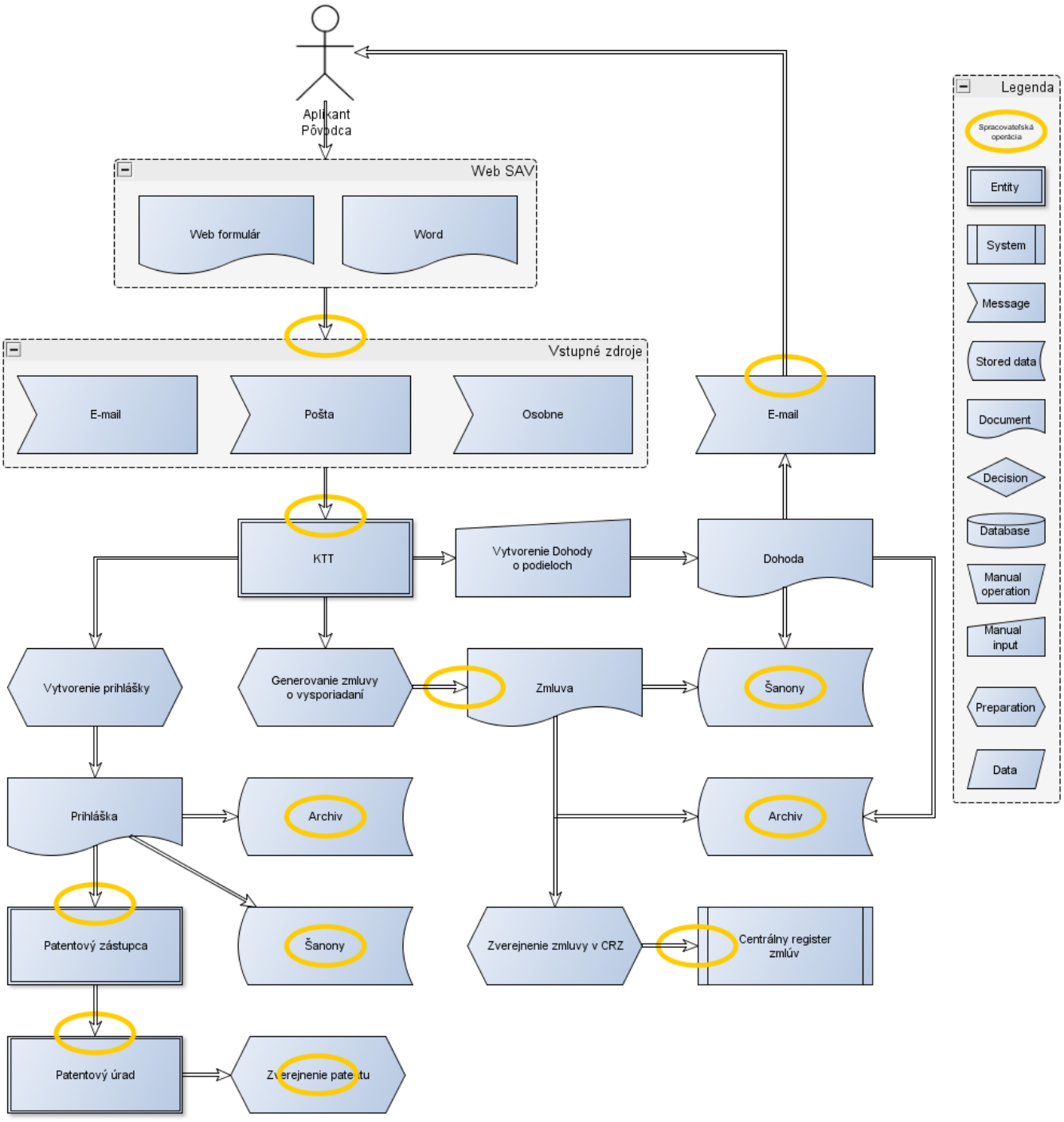
1.11 Schéma procesu HR – výber zamestnanca



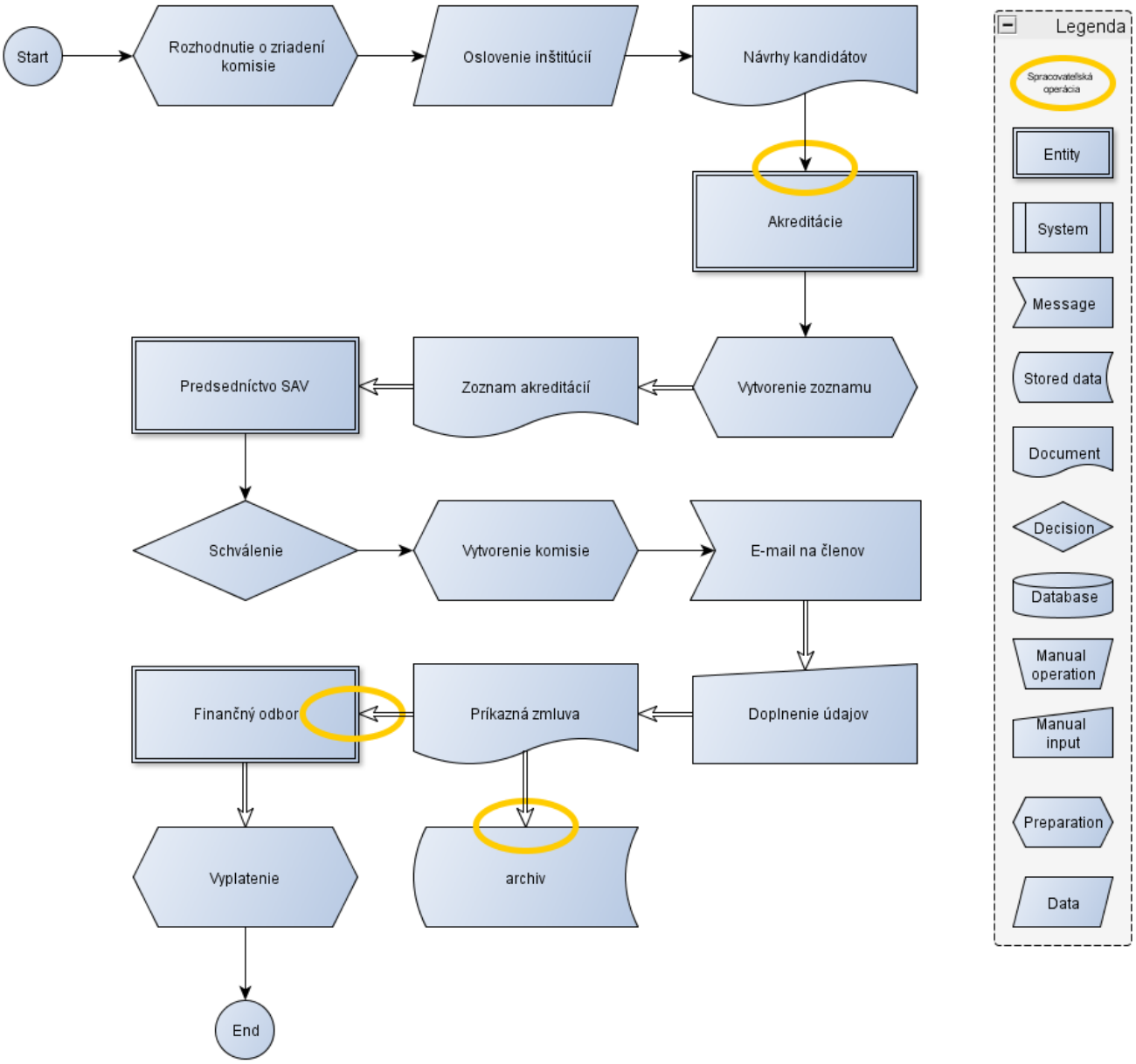
1.12 Schéma procesu SASPRO



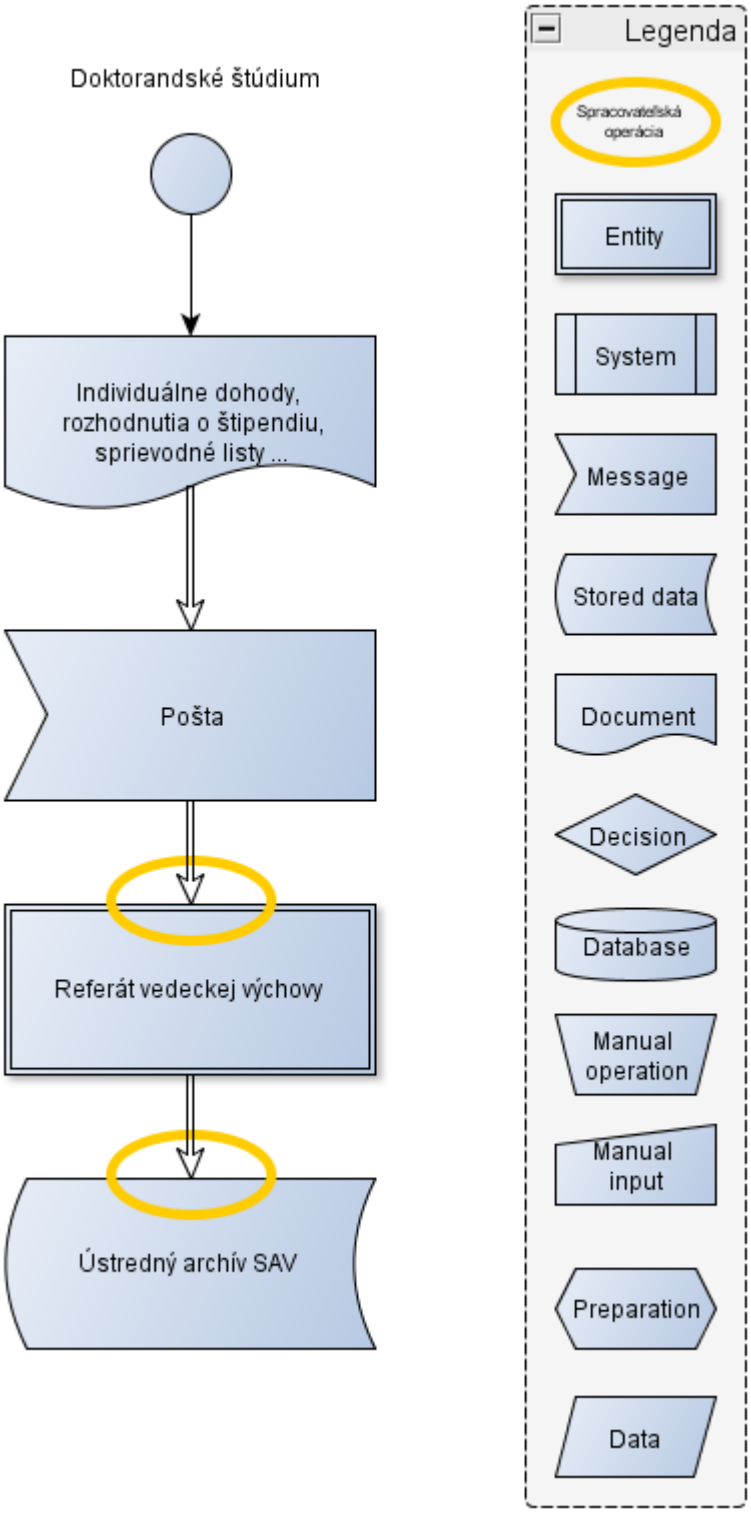
1.13 Schéma procesu KTT



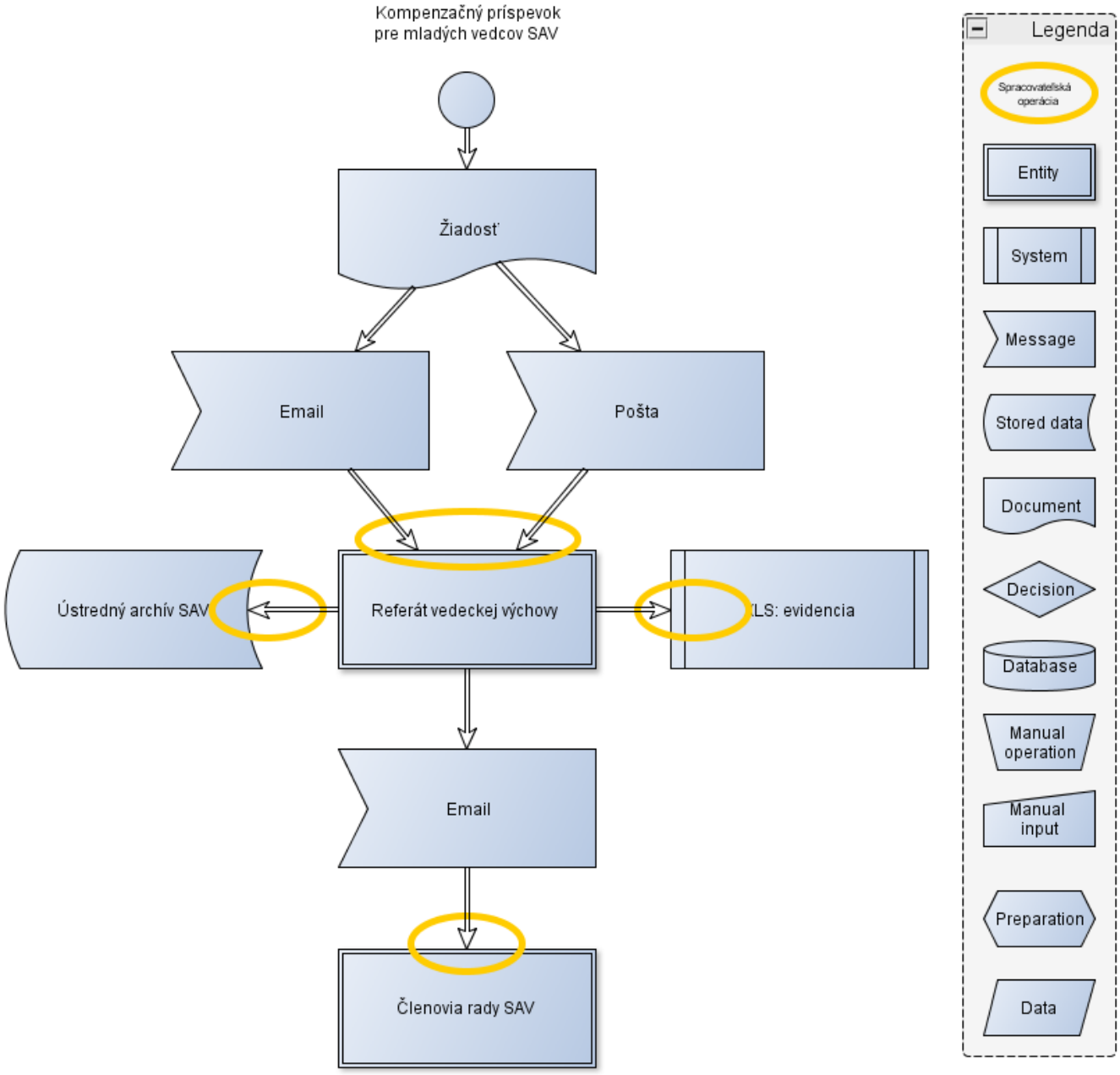
1.14 Schéma procesu Akreditácie



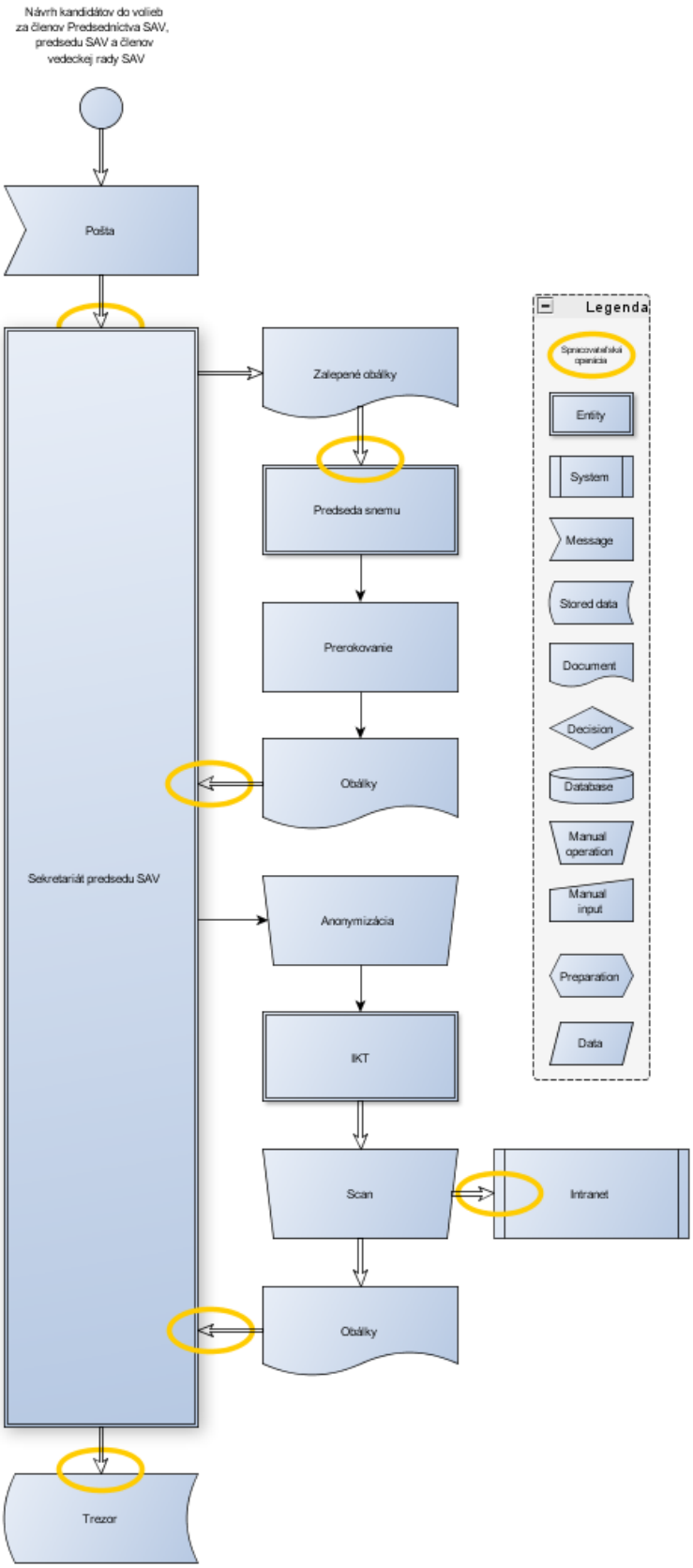
1.15 Schéma procesu Doktorandské štúdium



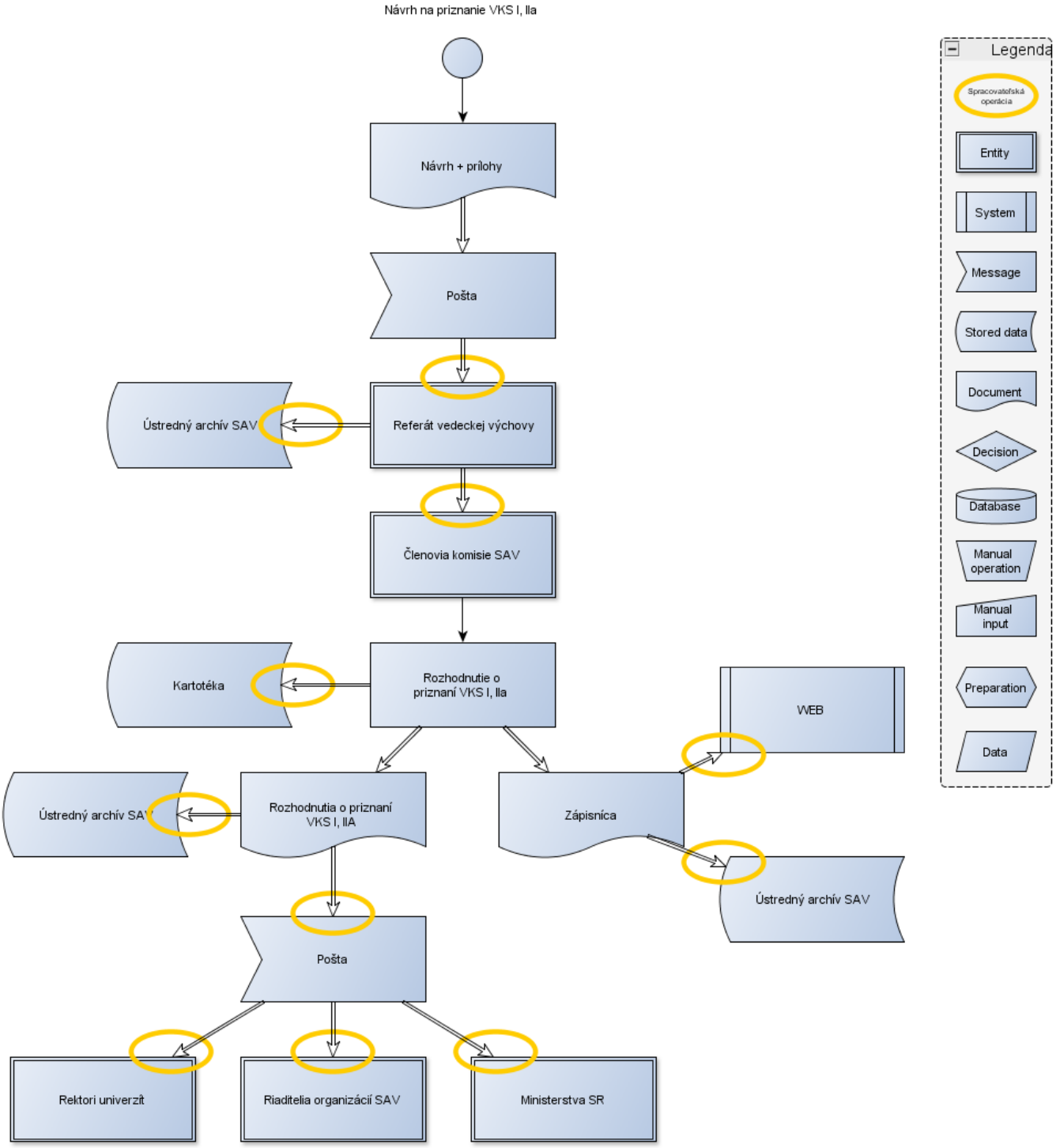
1.16 Schéma procesu Kompenzačný príspevok



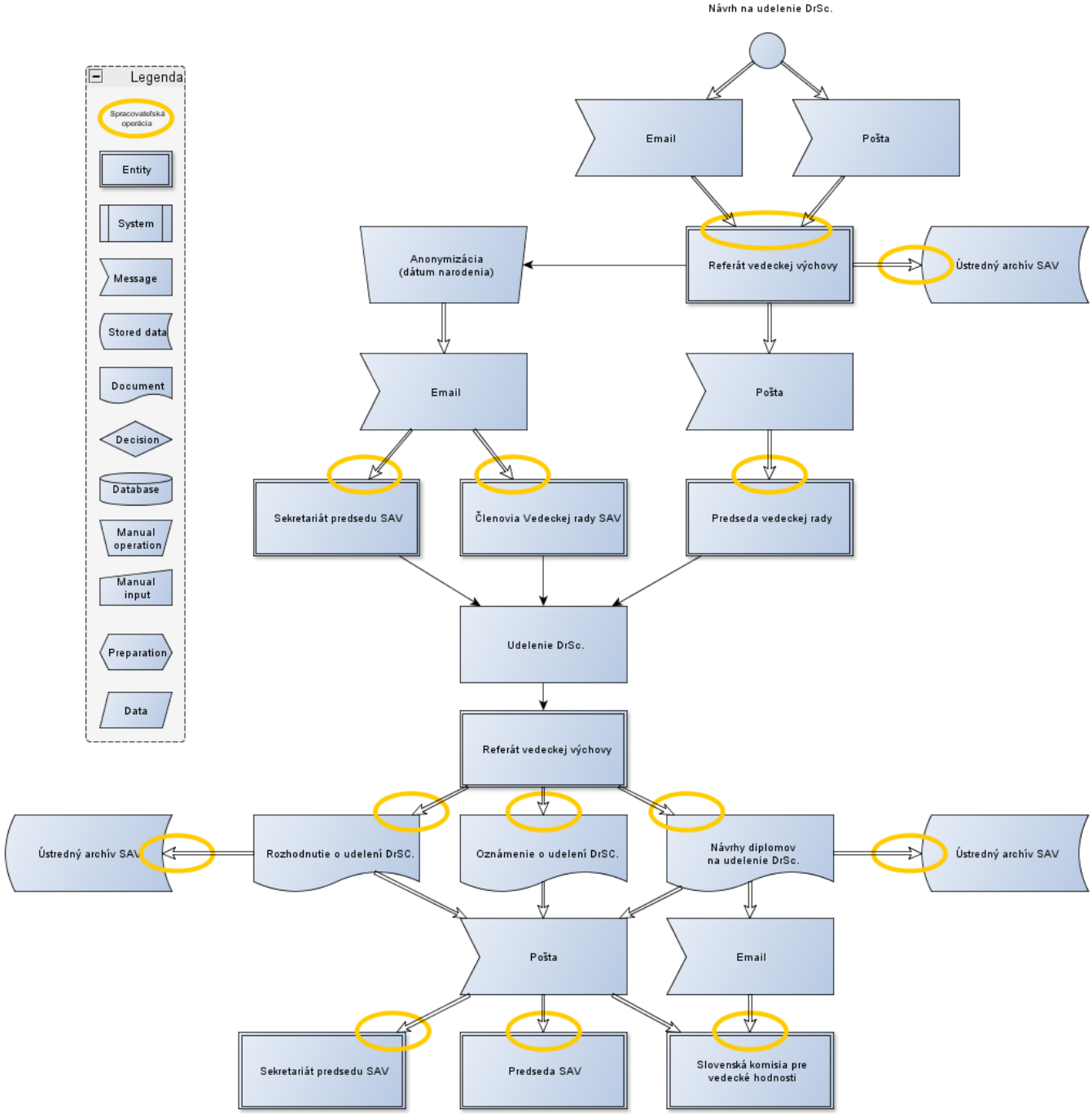
1.17 Schéma procesu Návrh kandidátov do Predsedníctva a VR



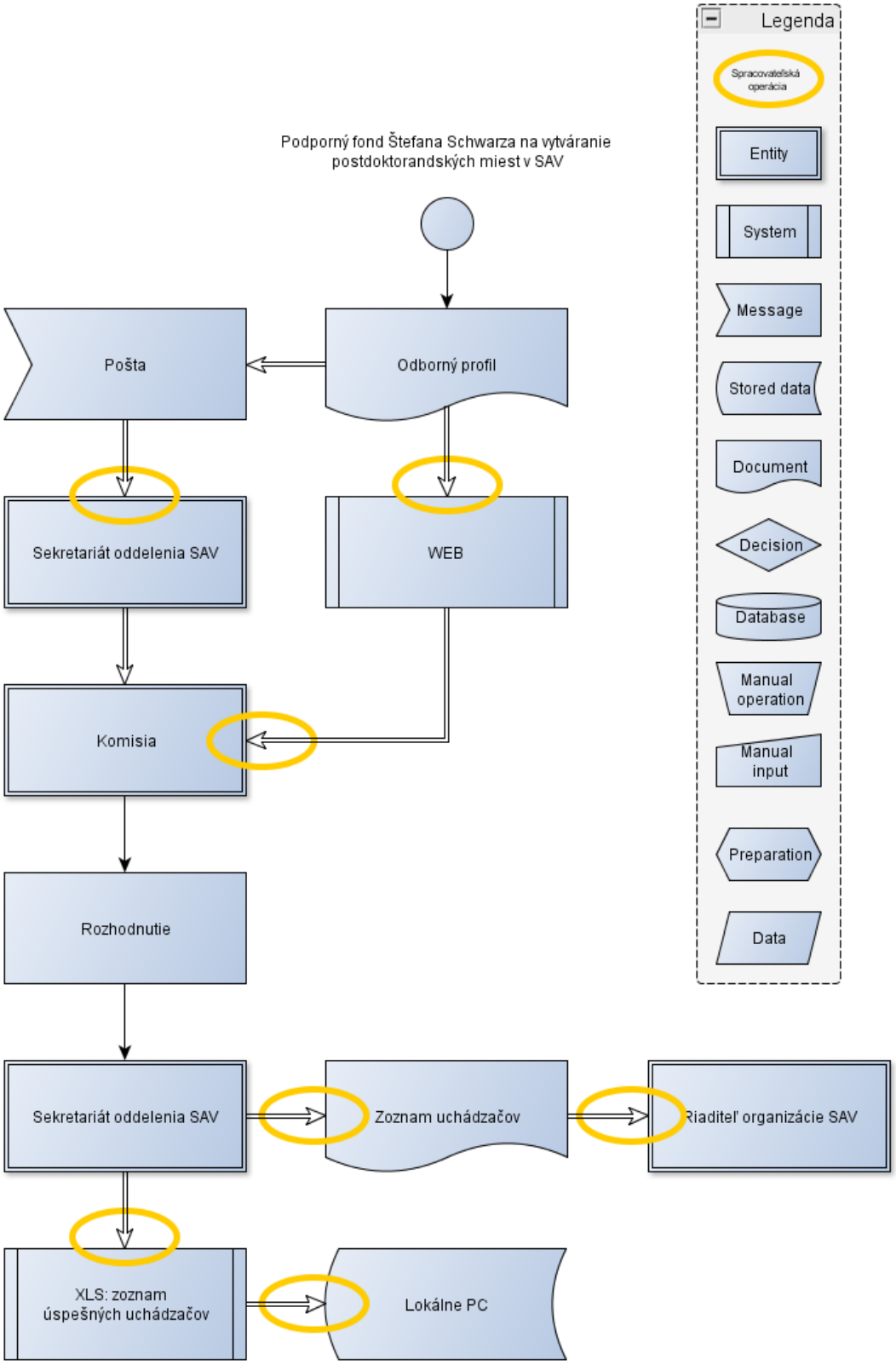
1.18 Schéma procesu Návrh na priznanie VKS



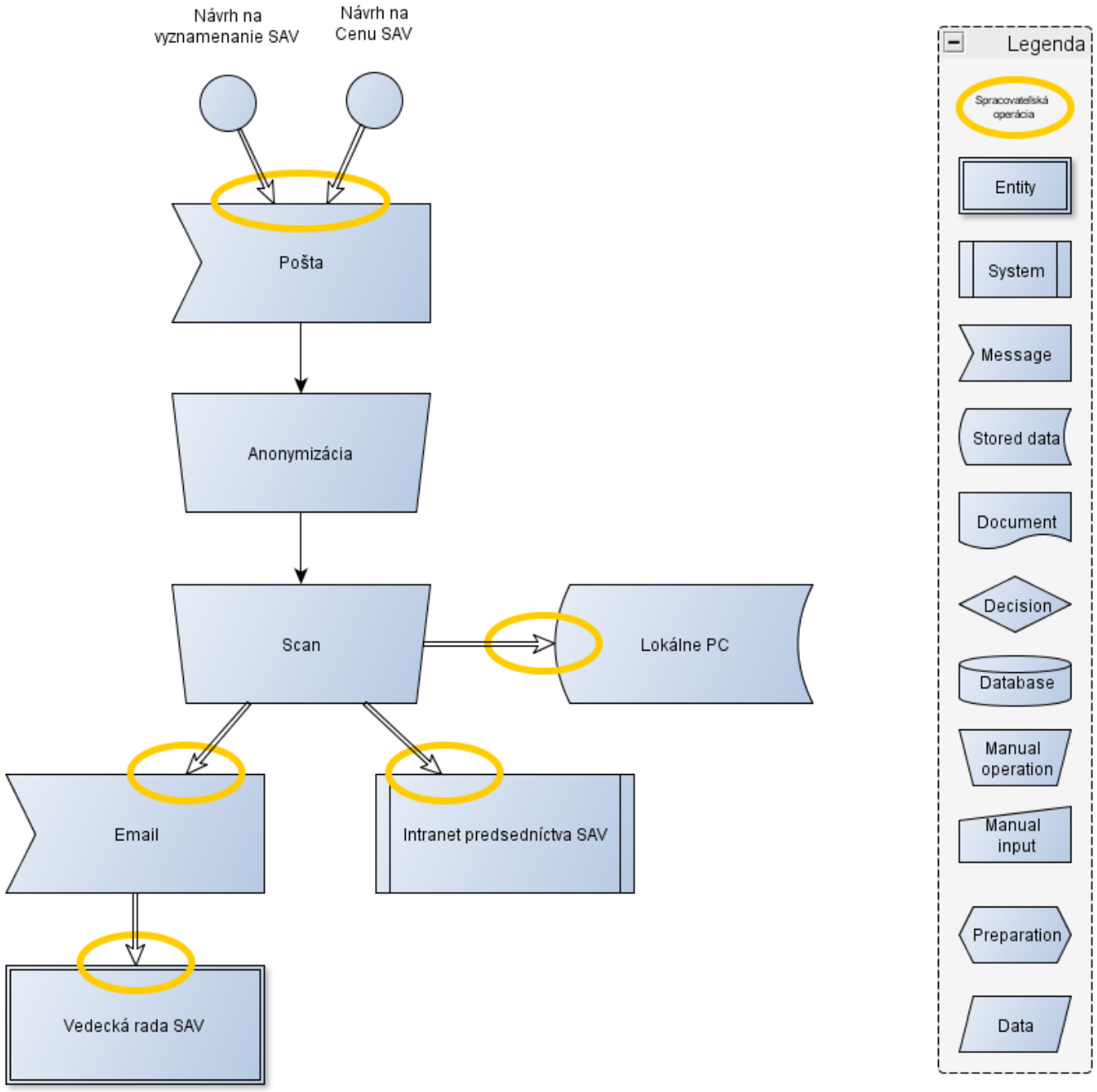
1.19 Schéma procesu Návrh na udelenie DrSc.



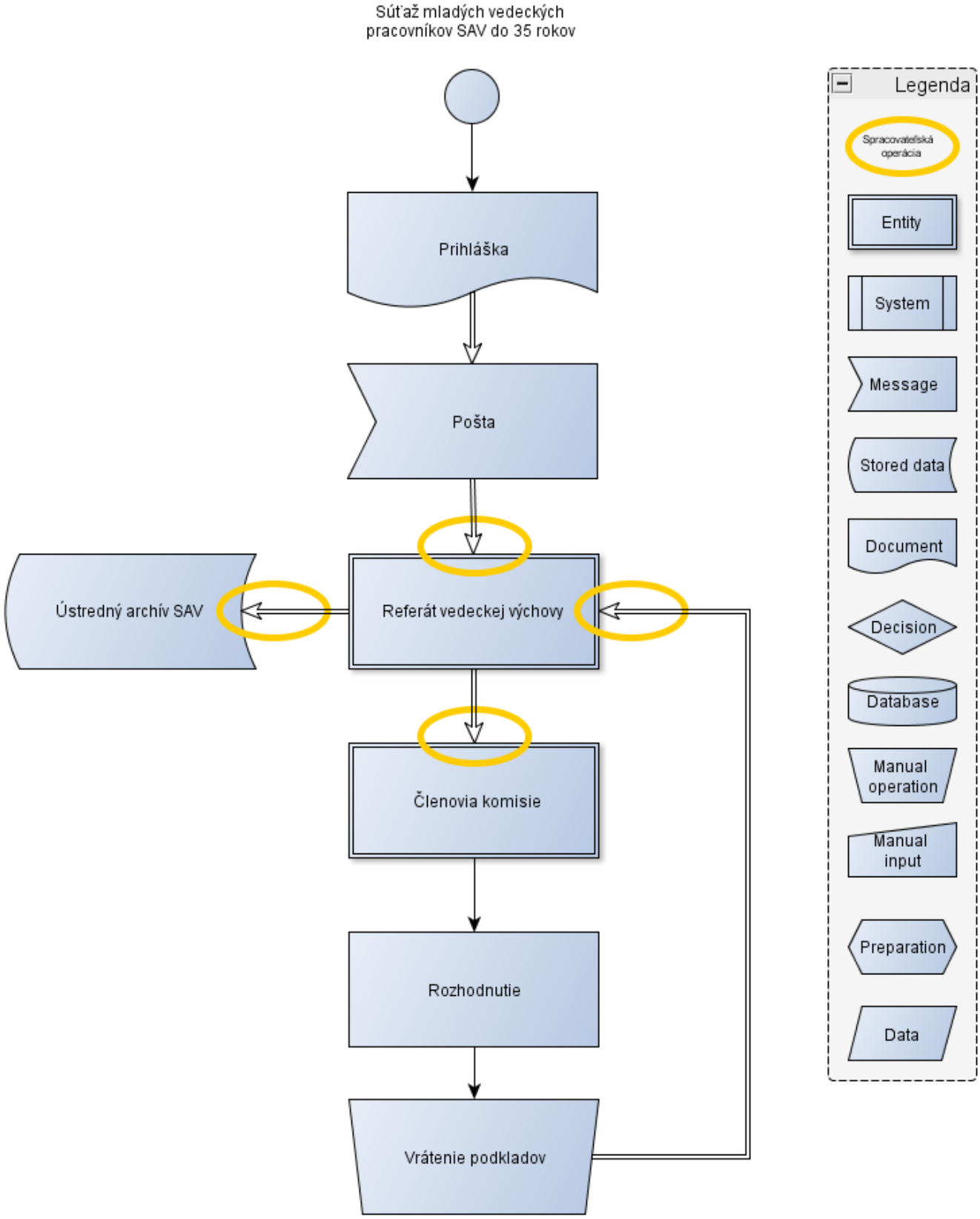
1.20 Schéma procesu Fond Štefana Schwarza



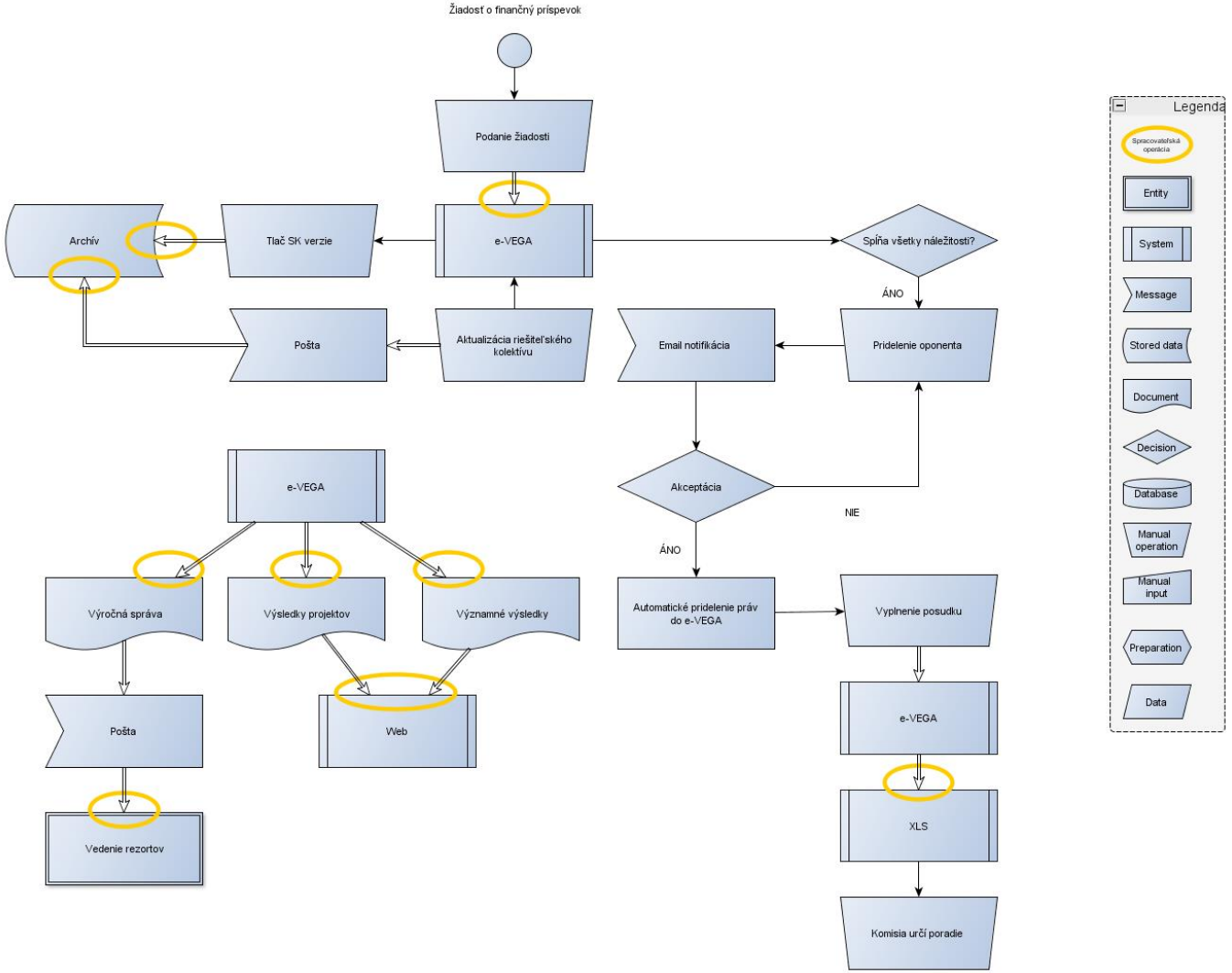
1.21 Schéma procesu Predseda SAV, Cena SAV



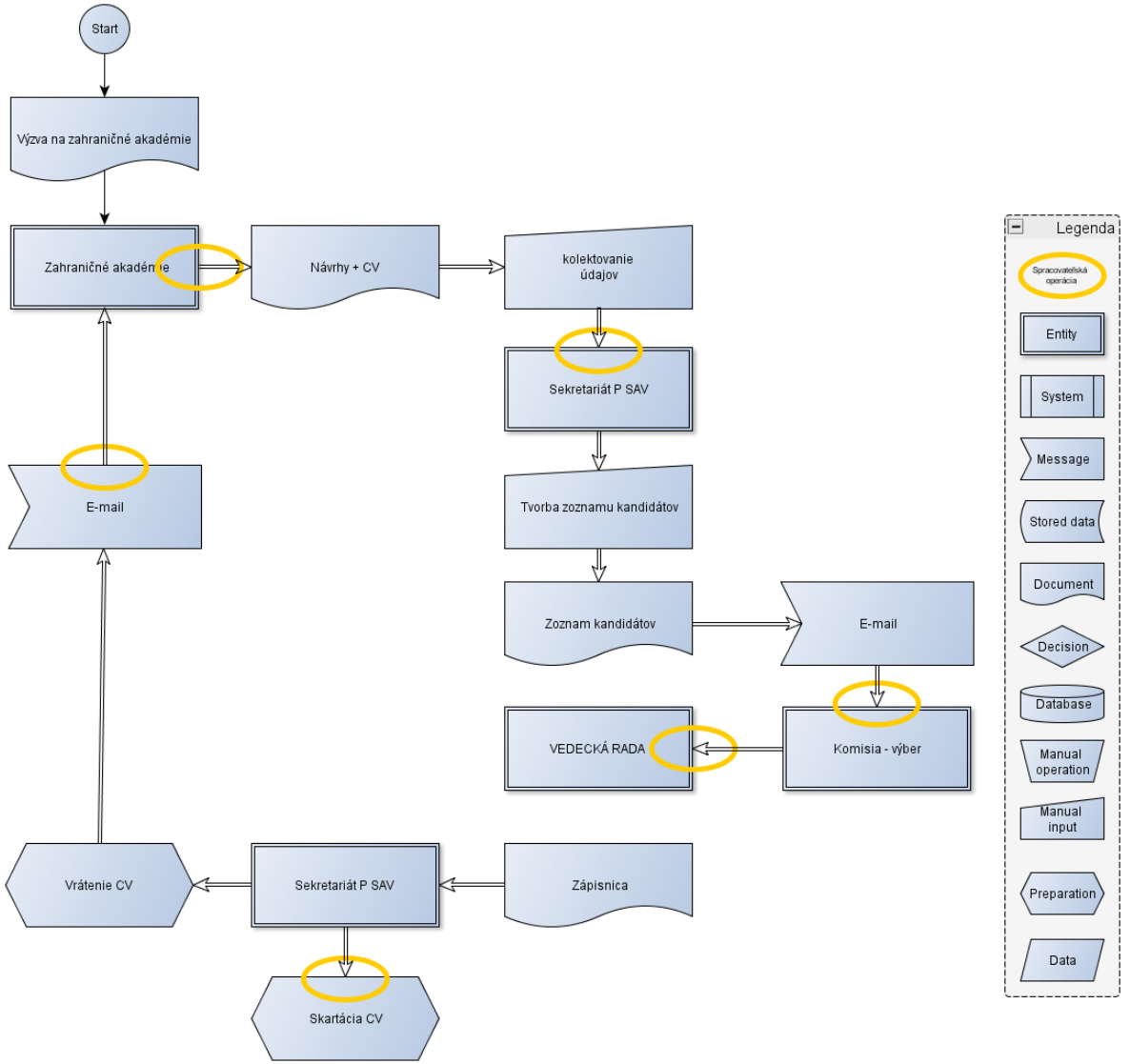
1.22 Schéma procesu Súťaž mladých vedeckých pracovníkov



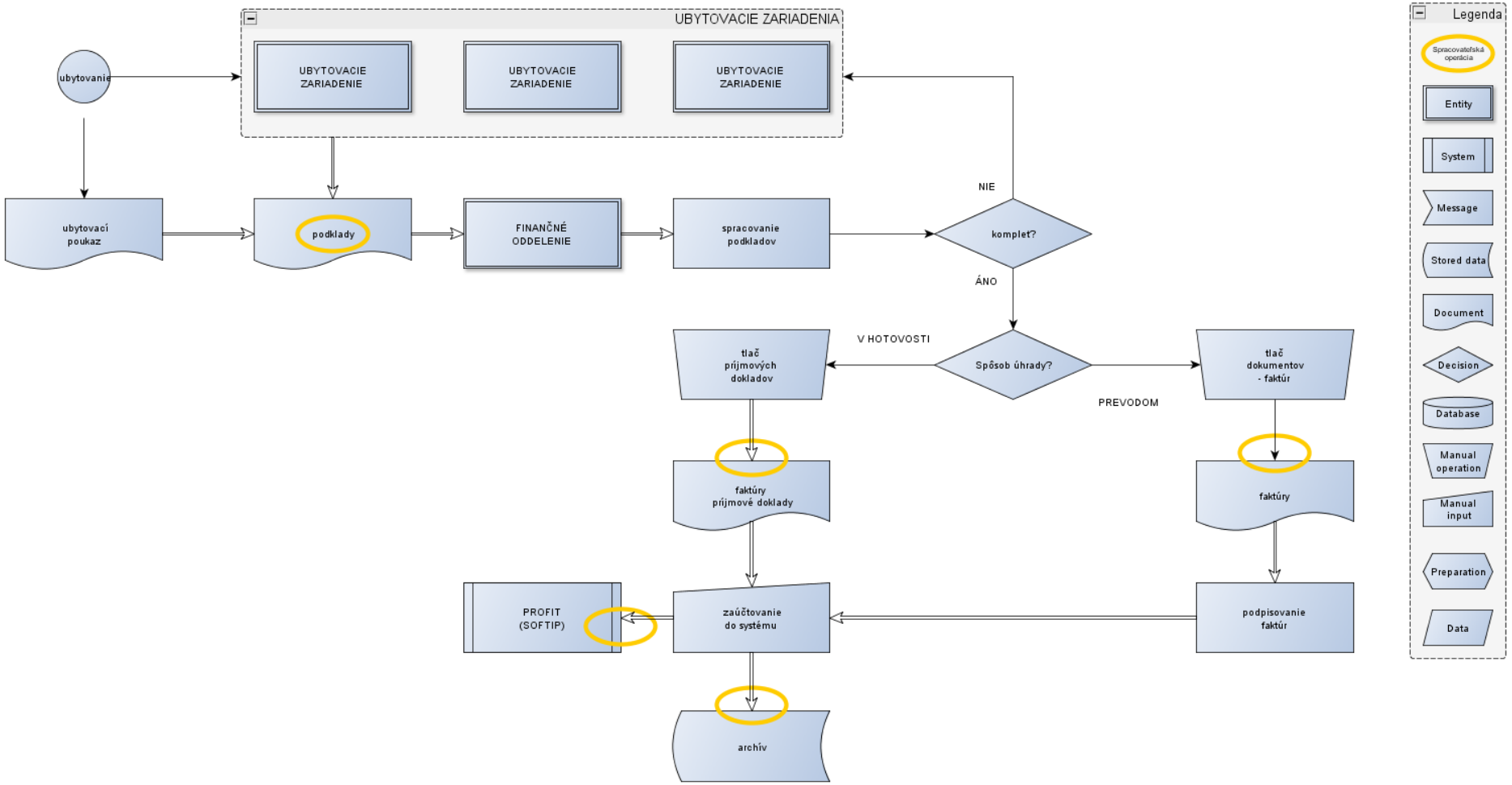
1.23 Schéma procesu Žiadosť o finančný príspevok



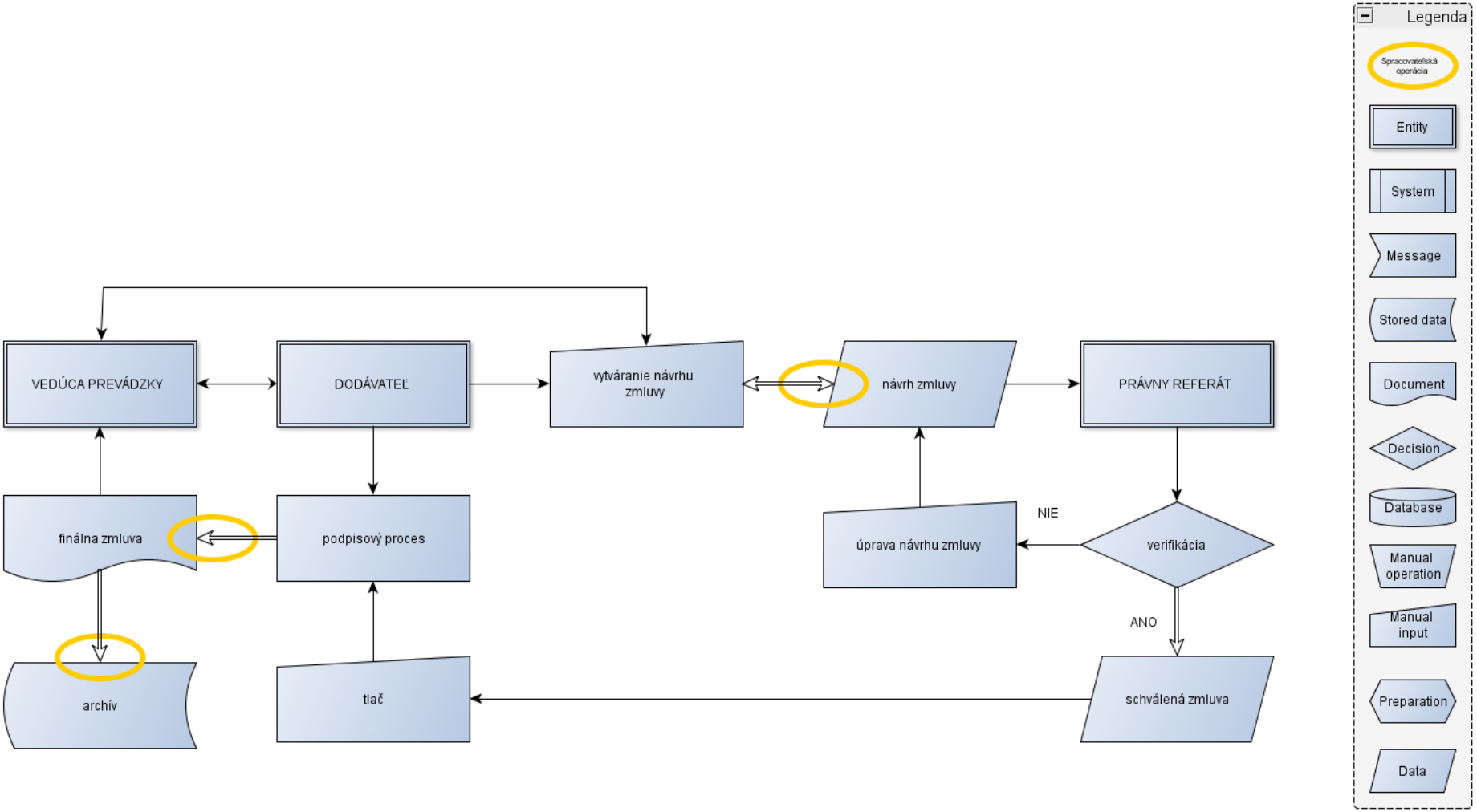
1.24 Schéma procesu Medzinárodná cena SAV



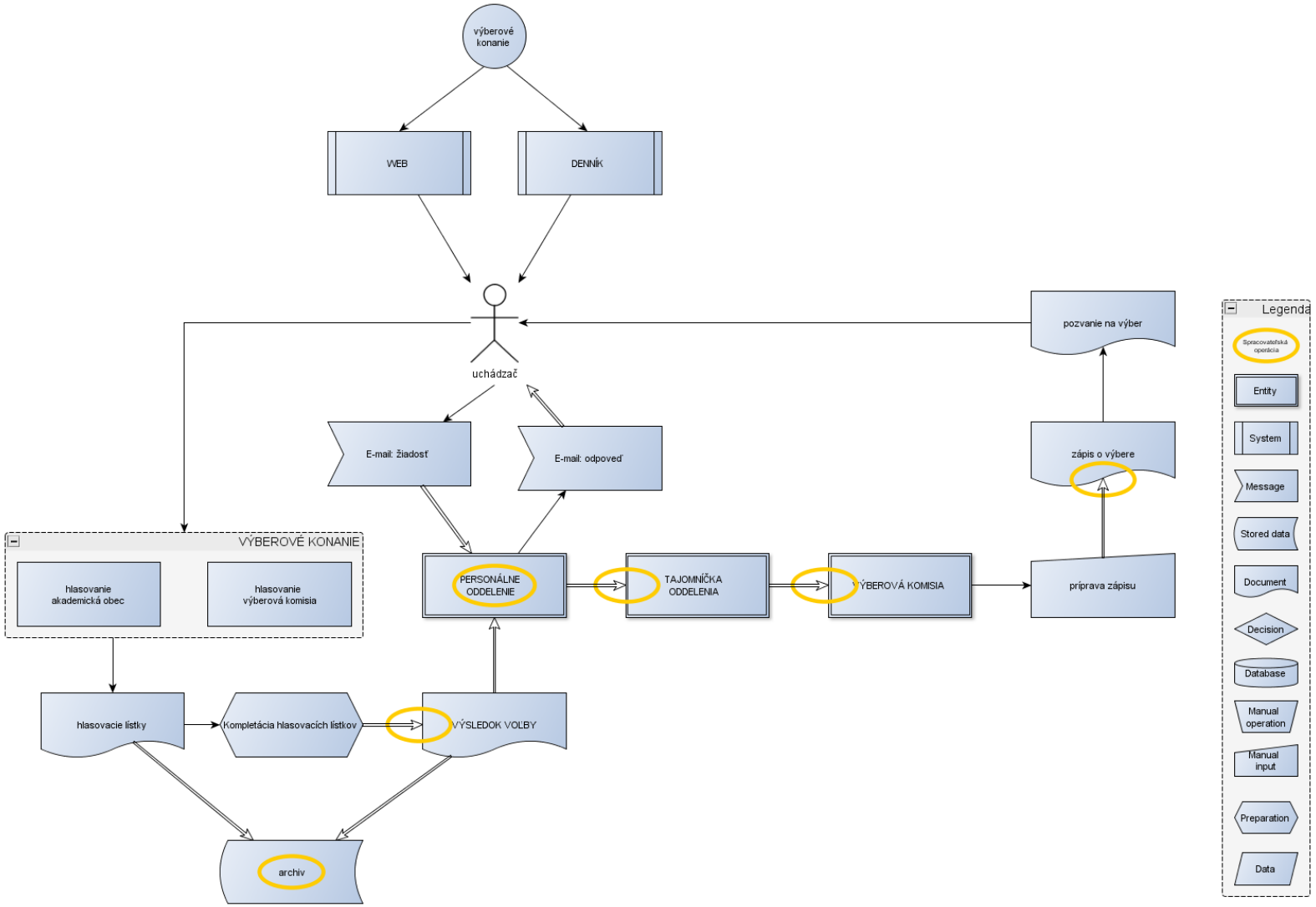
1.25 Schéma procesu Fakturácia



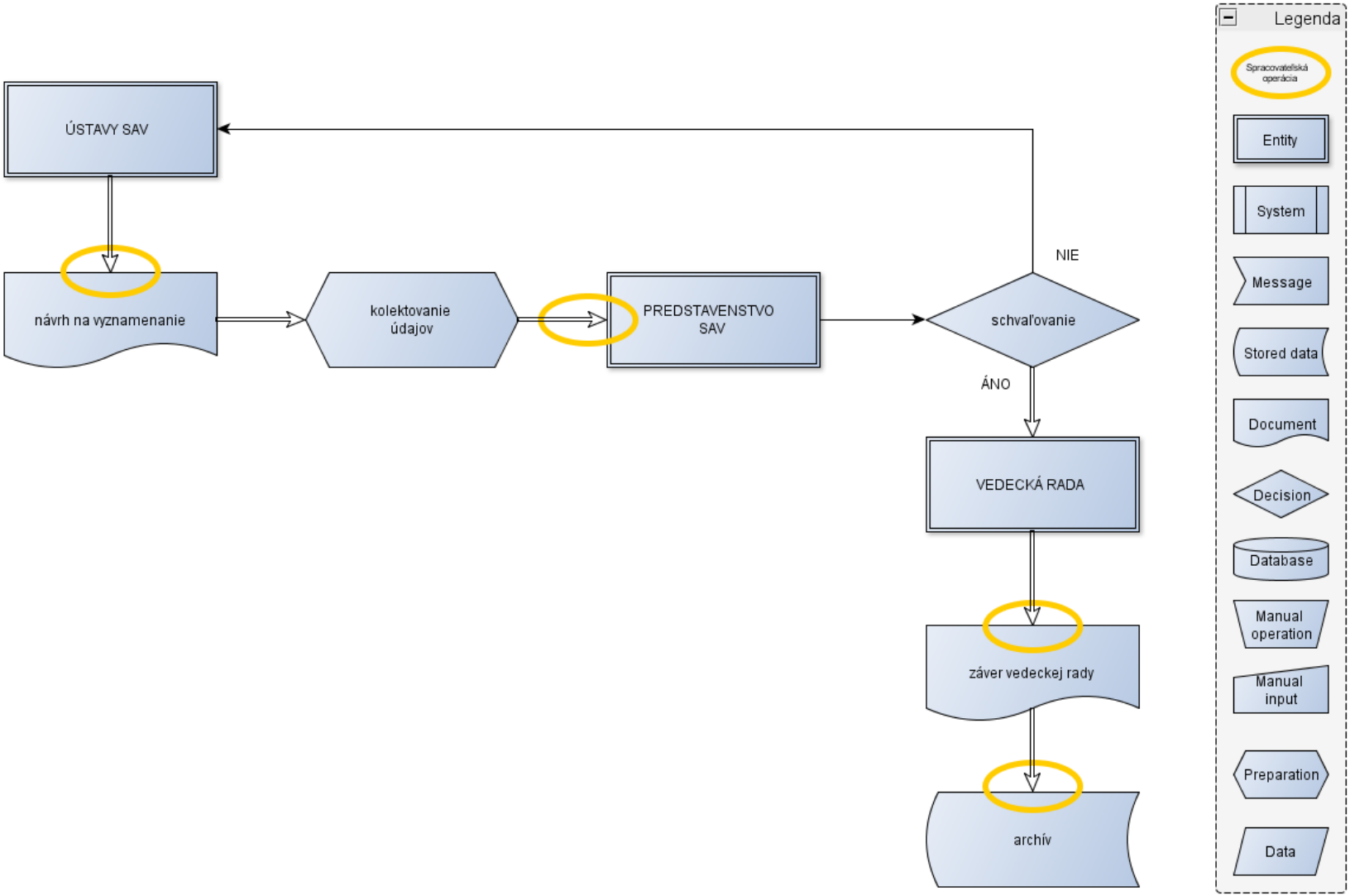
1.26 Schéma procesu Dodávateľské zmluvy



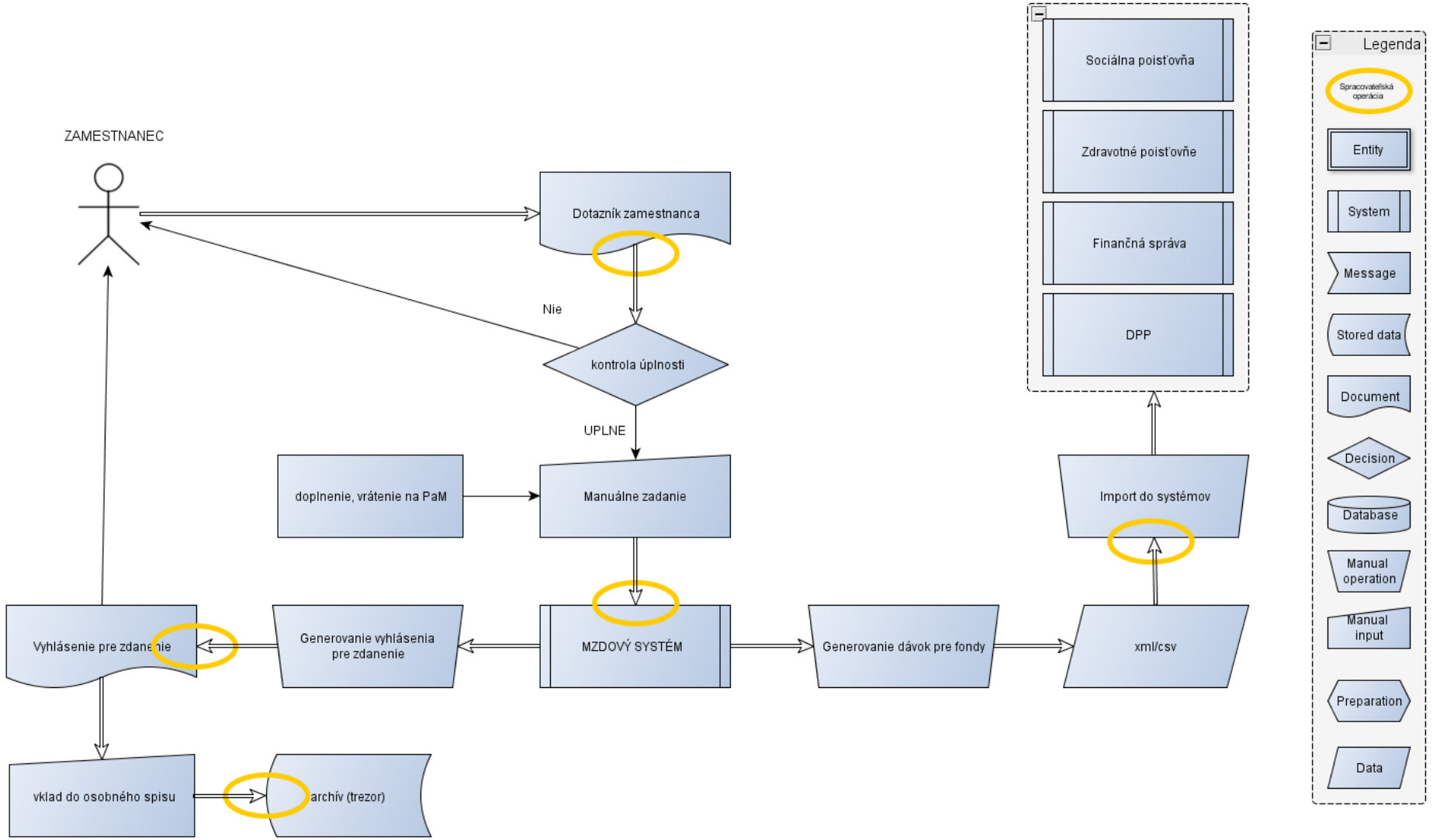
1.27 Schéma procesu Výberové konanie na riaditeľa



1.28 Schéma procesu Vyznamenania



1.29 Schéma procesu HR - mzdy



Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Fyzické poškodenie	Bombový útok a použitie zbraní	Bombový útok, teroristické útoky, vojna, občianske nepokoje, použitie zbraní	A, D, E	A	Veľmi malá	značný vplyv, strata	16	Zanedbateľné
Fyzické poškodenie	Poškodenie vodou	Záplava, vytopenie, poškodenie (typicky nosičov údajov, alebo IT zariadení) vodou	A, D, E	A	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Fyzické poškodenie	Požiar	Poškodenie (typicky nosičov údajov, alebo IT zariadení) požiarom	A, D, E	IA	Veľmi malá	značný vplyv, strata	16	Zanedbateľné
Fyzické poškodenie	Znečistenie - prach, korózia, mráz	Poškodenie (typicky nosičov údajov, alebo IT zariadení) prachom, koróziou, mrázom, snehom	A, D, E	A	Veľmi malá	stredný vplyv, strata	12	Zanedbateľné
Fyzické poškodenie	Zničenie zariadenia, alebo médií	Zničenie zariadení, alebo médií napr. vodou, požiarom, vandalizmus, zlyhanie úložného zariadenia, atď.	A, D, E	A	Malá	malý vplyv, strata	16	Zanedbateľné
Interferencia žiarením	Elektromagnetické impulzy	Poškodenie údajov (typicky na nosičoch) elektromagnetickými impulzmi, resp. kolísaním napájania.	A, D, E	IA	Malá	malý vplyv, strata	16	Zanedbateľné
Interferencia žiarením	Elektromagnetické žiarenie	Poškodenie údajov (typicky na nosičoch) elektromagnetickým žiarením, radiáciou	A, D, E	IA	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Interferencia žiarením	Tepelné žiarenie	Poškodenie údajov (typicky na nosičoch) tepelným žiarením, infračerveným žiarením, neprimeranou teplotou	A, D, E	IA	Malá	malý vplyv, strata	16	Zanedbateľné
Kompromitácia funkcií	Chyby používateľov	Nechcená modifikácia údajov v databázach, zmazanie súborov, potrebných pre chod softvéru, chyba operátora, ktorý modifikuje údaje, vysoké pracovné zaťaženie, stres alebo negatívne zmeny pracovných podmienok, zadanie úlohy nad rámec schopností zamestnanca, slabé znalosti a zručnosti, atď.	A	CIA	Stredná	stredný vplyv, strata	42	Stredné
Kompromitácia funkcií	Maskovanie identity	Sledovanie softvérovým keyloggerom, infekcia škodlivým kódom, inštalácia nástroja na vzdialenú správu, výmena pôvodných komponentov, atď.	D	CIA	Stredná	stredný vplyv, strata	42	Stredné

Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Kompromitácia funkcií	Nedostupnosť personálu	Preloženie, ukončenie kontraktu alebo zrušenie, prevzatie firmy alebo jej časti, prevzatie zamestnanca, zmena zaradenia, ukončenie procesu po organizačnej zmene, doručenie pošty zrušené štrajkom, atď.	A, D	A	Malá	stredný vplyv, strata	24	Malé
Kompromitácia funkcií	Odmietnutie činností	Odmietnutie vykonania pracovnej aktivity, odopretie pracovnej zodpovednosti v procese, štrajk, atď.	D	A	Stredná	stredný vplyv, strata	42	Stredné
Kompromitácia funkcií	Používanie softvéru neoprávneným spôsobom	Skenovanie obsahu, nelegálne spájanie údajov, nepovolené získanie vyšších oprávnení, mazanie stôp po použití, posielanie spamu cez email, zneužite sieťových funkcií, atď.	A, D	CIA	Stredná	stredný vplyv, strata	42	Stredné
Kompromitácia funkcií	Zhoršovanie stavu pamäťových médií	Starnutie archivovaných dokumentov, postupné prepisovanie obsahu v čase, dobrovoľné vymazanie častí dokumentu, zničenie médií napr. pri požiari, záplave atď.	A, D	IA	Malá	zanedbateľný vplyv, strata	8	Zanedbateľné
Kompromitácia funkcií	Zneužitie práv	Zneužitie práv, ovplyvňovanie (phishing, sociálne inžinierstvo, podplácanie, a pod.), nátlak (výhražné emaily, psychologické obťažovanie) atď.	A, D	CI	Stredná	stredný vplyv, strata	42	Stredné
Kompromitácia informácií	Detekcia polohy	Zistenie údajov o geografickej polohe	D	C	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Kompromitácia informácií	Infiltrácia komunikácie (vrátane presmerovania správ)	Reorganizácia kanálov na prenos papiera; zmena pracovného jazyka, zmeny v doručovaní pošty. atď.	D	CIA	Malá	stredný vplyv, strata	24	Malé
Kompromitácia informácií	Krádež médií alebo dokumentov	Krádež dokumentov, krádež súboreov, strata súborov počas sťahovania, krádež emailu z maiboxu, rozmnožovanie dokumentov počas prenosu, nájdenie stratených dokumentov, atď.	D	C	Malá	malý vplyv, strata	16	Zanedbateľné
Kompromitácia informácií	Krádež zariadení	Krádež notebooku, alebo mobilu, strata zariadenia, nájdenie strateného zariadenia, strata úložného zariadenia, atď.	D	CA	Malá	malý vplyv, strata	16	Zanedbateľné
Kompromitácia informácií	Odpočúvanie (vrátane analýzy dátovej prevádzky)	Sledovanie cudzej obrazovky, odfotenie cudzej obrazovky, GPS sledovanie zariadenia, vzdialená detekcia elektromagnetického signálu, atď.	D	C	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné

Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Kompromitácia informácií	Popretie	Popretie pôvodu informácie (neoprávnené popieranie pravdivej informácie)	A, D	I	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Kompromitácia informácií	Údaje z nedôveryhodných zdrojov	Údaje získané z nedôveryhodných zdrojov, kompromitácia údajov, atď. (Napr. prezenčná listina bez súhlasov, používanie mailinglistu s neoprávnene získanými, alebo chybnými adresami)	A, D	I	Malá	malý vplyv, strata	16	Zanedbateľné
Kompromitácia informácií	Vzdialené špehovanie	Špehovanie sieťovej prevádzky, získavanie dát posielaných cez Wi-Fi, atď.	D	CIA	Malá	malý vplyv, strata	16	Zanedbateľné
Kompromitácia informácií	Získavanie recyklovaných alebo vyradených médií	Nedostatočné zmluvy o vyradení alebo údržbe zariadení môžu viesť k neoprávnenému prístupu k OÚ	D	C	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Neautorizované činnosti	Nelegálne spracovanie dát	Neoprávnené použitie údajov, ovplyvňovanie (klebety, dezinformácie), atď.	D	CIA	Malá	malý vplyv, strata	16	Zanedbateľné
Neautorizované činnosti	Nelegálny import / export softvéru (podvodné kopírovanie sw, použitie kopírovaného sw)	Chyby počas aktualizácie, konfigurácie alebo údržby, výmena komponentov, atď.	A, D	CIA	Malá	stredný vplyv, strata	24	Malé
Neautorizované činnosti	Neoprávnené používanie zariadenia	Pridanie nekompatibilnej časti zariadenia, ktoré vedie k nefunkčnosti, odobratie komponentov, potrebných pre správne fungovanie systému, sledovanie hardvérovým keyloggerom, odstránenie komponentov zariadenia, pripojenie zariadení (napr: USB diskov) pre štart OS alebo získanie dát, použitie USB kľúčov alebo diskov, ktoré nie sú vhodné pre danú citlivosť	D	CIA	Malá	malý vplyv, strata	16	Zanedbateľné
Neautorizované činnosti	Poškodenie dát	Poškodenie / vymazanie dát, použitie nelegálneho alebo kopírovaného softvéru, chyby používateľov, ktoré spôsobia stratu údajov, atď.	D	CIA	Stredná	stredný vplyv, strata	42	Stredné
Neautorizované činnosti	Používanie sieťových zariadení neoprávneným spôsobom	Skenovanie sieťových adries a portov, zbieranie konfiguračných dát, analýza zdrojového kódu za účelom lokalizovať slabé miesta, testovanie databáz na reakciu na poškodzujúce dotazy, atď.	D	CIA	Malá	malý vplyv, strata	16	Zanedbateľné
Neautorizované činnosti	Prístup neoprávneného používateľa k sieti	Skenovanie sieťových adries a portov, hľadanie zraniteľností pri počúvaní, analýze, reportovaní alebo sprostredkovacie porty a služby	A, D	CIA	Veľmi malá	malý vplyv, strata	8	Zanedbateľné

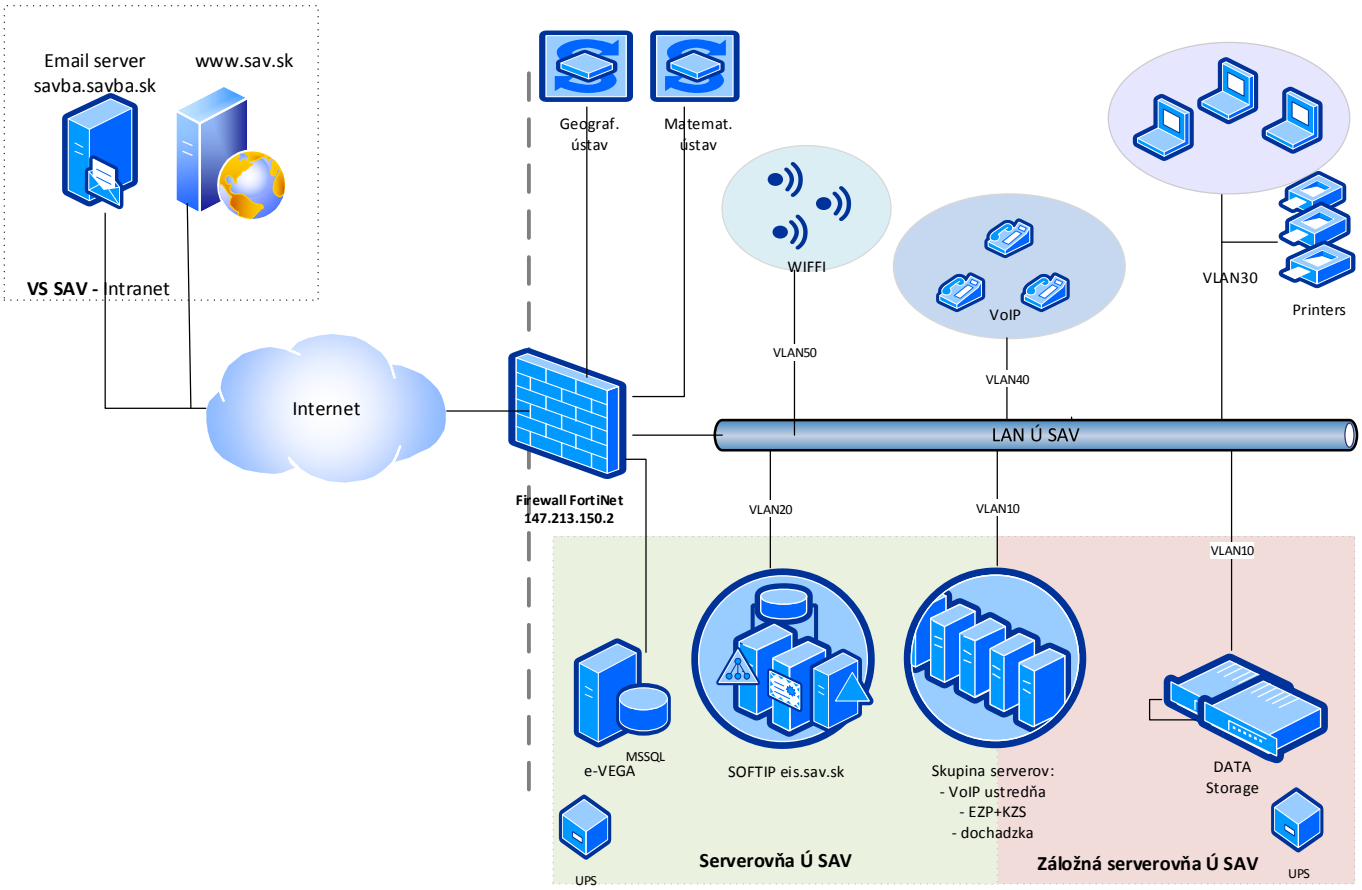
Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Neautorizované činnosti	Škodlivý softvér	Infiltrácia škodlivým kódom, výmaz spúšťacích súborov alebo zdrojového kódu, atď.	A, D	CIA	Stredná	stredný vplyv, strata	42	Stredné
Neautorizované činnosti	Zmena obchodných dát zlomyseľným užívateľom	Zmena hodnôt v súbore, nahradenie originálnych hodnôt falšovanými, zmeny údajov bez vedomia autora, odosielanie viacerých konfliktných dokumentovútoky "man-in-the-middle" alebo "man in the browser" pre zmenu alebo pridanie dát do sieťovej prevádzky, atď.	D	CIA	Malá	značný vplyv, strata	32	Malé
Prírodné udalosti	Blesk	Poškodenie (typicky nosičov údajov a IT zariadení) úderom blesku	E	A	Veľmi malá	malý vplyv, strata	8	Zanedbateľné
Prírodné udalosti	Klimatický jav	Klimatické javy, vis maior	E	A	Veľmi malá	stredný vplyv, strata	12	Zanedbateľné
Prírodné udalosti	Záplavy	Poškodenie (typicky nosičov údajov) záplavou	E	A	Veľmi malá	malý vplyv, strata	8	Zanedbateľné
Prírodné udalosti	Zemetrasenie (alebo vulkanický jav)	Škody spôsobené zemetrasením, výbochom sopky alebo iným javom vulkanického pôvodu	E	A	Veľmi malá	značný vplyv, strata	16	Zanedbateľné
Súkromie	Detekovateľnosť	(1) Potenciál, že útočník dokáže z uložených údajov dostatočne rozlíšiť, či predmet záujmu, resp. položka množiny jestvuje alebo nie. (napr. schopnosť rozpoznania súborov obsahujúcich osobné údaje od iných typov údajov)	A, D	P	Stredná	stredný vplyv, strata	42	Stredné
Súkromie	Identifikovateľnosť	(3) Potenciál, že útočník dokáže priamo identifikovať dotknuté osoby asociované na predmety záujmu (napr. v súbore osobných údajov rozpoznať osobné údaje konkrétnej dotknutej osoby. napr. konkrétneho odosielateľa správy medzi mnohými správami elektronickej pošty). Identifikovateľnosť je špeciálny typ spojiteľnosti, kde sú zahrnuté aj atribúty dotknutých osôb.	A, D	P	Stredná	značný vplyv, strata	56	Vysoké
Súkromie	Nepopierateľnosť	Potenciál, že útočník dokáže z podstaty procesu zhromaždiť dôkazy proti nárokom odporujúcej strany a dokázať, že používateľ vie, že niečo urobil, alebo že niečo povedal. Opakom je Plausible deniability (tzv. prijateľné popretie) . (T.j. neoprávnené zverejňovanie pravdivej informácie, resp. pôvodu informácie - napr. dotknutá osoba nechce, aby bolo jasné, komu dala	A, D	P	Stredná	malý vplyv, strata	28	Malé
Súkromie	Nesúlad systému s politikami a poskytnutým súhlasom	Nesúlad spracovania s politikami a poskytnutým súhlasom je hrozba, ktorá znamená, že napriek deklarácii súladu spracovania s politikami, neexistuje záruka, že systém skutočne vyhovuje prijatým pravidlám. Tým následne môže nastať porušenie práv dotknutej osoby.	A, D	P	Stredná	malý vplyv, strata	28	Malé

Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Súkromie	Neznalosť obsahu	Neznalosť obsahu je hrozba, ktorá indikuje, že používateľ si neuvedomuje citlivosť informácie spracovanej v systéme a následne napr. zverejňuje príliš veľa informácií, ktoré umožnia potenciálnemu útočníkovi zistiť napr. identitu používateľa. Alebo naopak - používateľ poskytuje nepresné informácie, ktoré môžu následne spôsobiť nesprávne rozhodnutia alebo akcie. (napr. nechcené	A	P	Stredná	značný vplyv, strata	56	Vysoké
Súkromie	Prezradenie informácie	Neoprávnené sprístupnenie citlivých informácií v rámci pracovného procesu osobám, ktoré k nim nemajú mať prístup. (Neoprávnené prečítanie, kopírovanie, fotografovanie, použite odpočúvacích zariadení na stretnutiach, atď.)	A, D	P	Stredná	značný vplyv, strata	56	Vysoké
Súkromie	Spojiteľnosť, linkovateľnosť	(2) Spojiteľnosť (linkovateľnosť) je hrozba, že útočník dokáže aj nepriamo rozpoznať podstatu entity, alebo vzájomné vzťahy entít. (napr. odosielateľa podľa domény, aktivity, alebo podľa predmetu správy)	A, D	P	Stredná	malý vplyv, strata	28	Malé
Výpadok základných služieb	Chyby prenosu (vrátane nesprávneho smerovania správ)	Reorganizácia kanálov na prenos papierových dokumentov, zmena pracovného jazyka, zmeny v doručovaní pošty. atď.	A, D	IA	Malá	malý vplyv, strata	16	Zanedbateľné
Výpadok základných služieb	Nedostatok personálu	Pracovný úraz, choroba z povolania, iné zranenie alebo choroba, smrť, neurologická, psychologická alebo psychiatrická diagnóza, atď.	A, D, E	A	Malá	stredný vplyv, strata	24	Malé
Výpadok základných služieb	Porucha klimatizácie alebo prívodu vody	Porucha klimatizácie alebo prívodu vody ktoré môže spôsobiť výpadky systémov a následne zníženie úrovne dostupnosti údajov	A, D	A	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Výpadok základných služieb	Poškodenie liniek	Poškodenie telekomunikačného spojenia, zničenie kabeláže, výpadok komponentov optického spojenia, nedostupné WiFi pripojenie, atď.	A, D	A	Malá	zanedbateľný vplyv, strata	8	Zanedbateľné
Výpadok základných služieb	Preťaženie dopravy	Preťaženie kapacity prevádzky - preťaženie pošty, preťaženie procesov overovania, prekročenie veľkosti databázy, vkladanie dát mimo normálny rozsah hodnôt, zneužite šírky pásma, neoprávnené sťahovanie, strata internetovej konektivity, atď.	A	A	Veľmi malá	zanedbateľný vplyv, strata	4	Zanedbateľné
Výpadok základných služieb	Strata napájania alebo kolísanie výkonu	Strata zdroja napájania alebo kolísanie výkonu napájania zariadení	A, D, E	A	Malá	stredný vplyv, strata	24	Malé
Výpadok základných služieb	Zlyhanie telekomunikačných komponentov	Prerušenie kabeláže, slabý príjem Wi-Fi, atď.	A, D	CIA	Malá	malý vplyv, strata	16	Zanedbateľné

Kategória hrozby	Hrozba	Príklad hrozby	Zdroj hrozby	Ovplyvnené atribúty	Pravdepodobnosť	Dopad	RiskRating	Kvantifikácia rizika
Zlyhania techniky	Porucha softvéru	Chyby počas aktualizácie, konfigurácie alebo údržby, infekcia škodlivým kódom, výmena komponentov, neobnovenie licencie na softvér používaný na prístup k údajom, atď.	A	CIA	Stredná	stredný vplyv, strata	42	Stredné
Zlyhania techniky	Zahltenie informačného systému	Plná úložná jednotka, výpadok el.energie, preťaženie systému, prehriatie, výnimočné teploty, atď.	A, D	IA	Malá	malý vplyv, strata	16	Zanedbateľné
Zlyhania techniky	Zlyhanie alebo porucha zariadenia	Náhle a neplánované zlyhanie alebo porucha IT zariadenia, alebo akéhokoľvek HW komponentu, ktoré môže spôsobiť zníženie úrovne dostupnosti údajov	A	IA	Malá	stredný vplyv, strata	24	Malé
Zlyhania techniky	Zníženie úrovne údržby, chyba údržby informačného systému	Neplánované zníženie úrovne údržby systémov, chyba údržby informačného systému, alebo IT zariadení	A, D	IA	Malá	stredný vplyv, strata	24	Malé

Príloha č. 1 Schémy IT infraštruktúry

1.1 Schéma IT infraštruktúry



1.2 Schéma aplikačnej infraštruktúry