Dokumentácia o ochrane osobných údajov

GDPR

prevádzkovateľa

FRADEX, s.r.o.

Továrenská 3682/47, 953 01 Zlaté Moravce

IČO: 46 315 870

Zast. Bc. Denis Francík, konateľ

podľa NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj „nariadenie“, „GDPR“)

a ZÁKONA 18/2018 Z. z. z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „zákon“).

Dokumentácia bola vypracovaná na základe údajov poskytnutých prevádzkovateľom.

Vypracoval: **SOKOL trade s.r.o.**

OBSAH

PRVÁ ČASŤ

Opis spracúvania osobných údajov

Článok I

Personalistika a mzdy

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému je: **Personalistika a mzdy**

Účel spracúvania

Účelom spracúvania osobných údajov **je zabezpečenie plnenia povinností prevádzkovateľa ako zamestnávateľa súvisiace s pracovným pomerom alebo obdobným vzťahom (napr. na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane predzmluvných vzťahov**.

Právny základ spracúvania

Právnym základom spracúvania je **zákon** (Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, Zákon č. 580/2004 Z. z. 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, Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení v znení neskorších predpisov, Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov, Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých, Zákonov v znení neskorších predpisov, Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov).

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **uchádzači o zamestnanie, zamestnanci, manželia alebo manželky zamestnancov, blízke osoby, bývalí zamestnanci.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, priezvisko, rodné priezvisko a titul, rodné číslo, dátum a miesto narodenia, podpis, rodinný stav, štátna príslušnosť, štátne občianstvo, trvalé bydlisko, prechodné bydlisko, pohlavie, údaje o vzdelaní, spôsobilosť na právne úkony, poberanie prídavkov na deti, mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon pracovnej činnosti, údaje o odpracovanom čase, údaje o bankovom účte fyzickej osoby, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, ročný úhrn vyplateného dôchodku, údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zmenenej pracovnej schopnosti, údaje o zamestnávateľoch, pracovné zaradenie a deň začiatku pracovnej činnosti, údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa, údaje z potvrdenia o zamestnaní, údaje o vedení zamestnanca v evidencii nezamestnaných občanov, údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, údaje z dokladu o bezúhonnosti, údaje o priznaní dôchodku, o druhu dôchodku, údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne, osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, fotografia, poradové číslo.**

Príjemcovia

Osobné údaje z informačného systému sa poskytujú:

Sprostredkovatelia- **spoločnosť na spracovanie miezd a účtovníctva,**

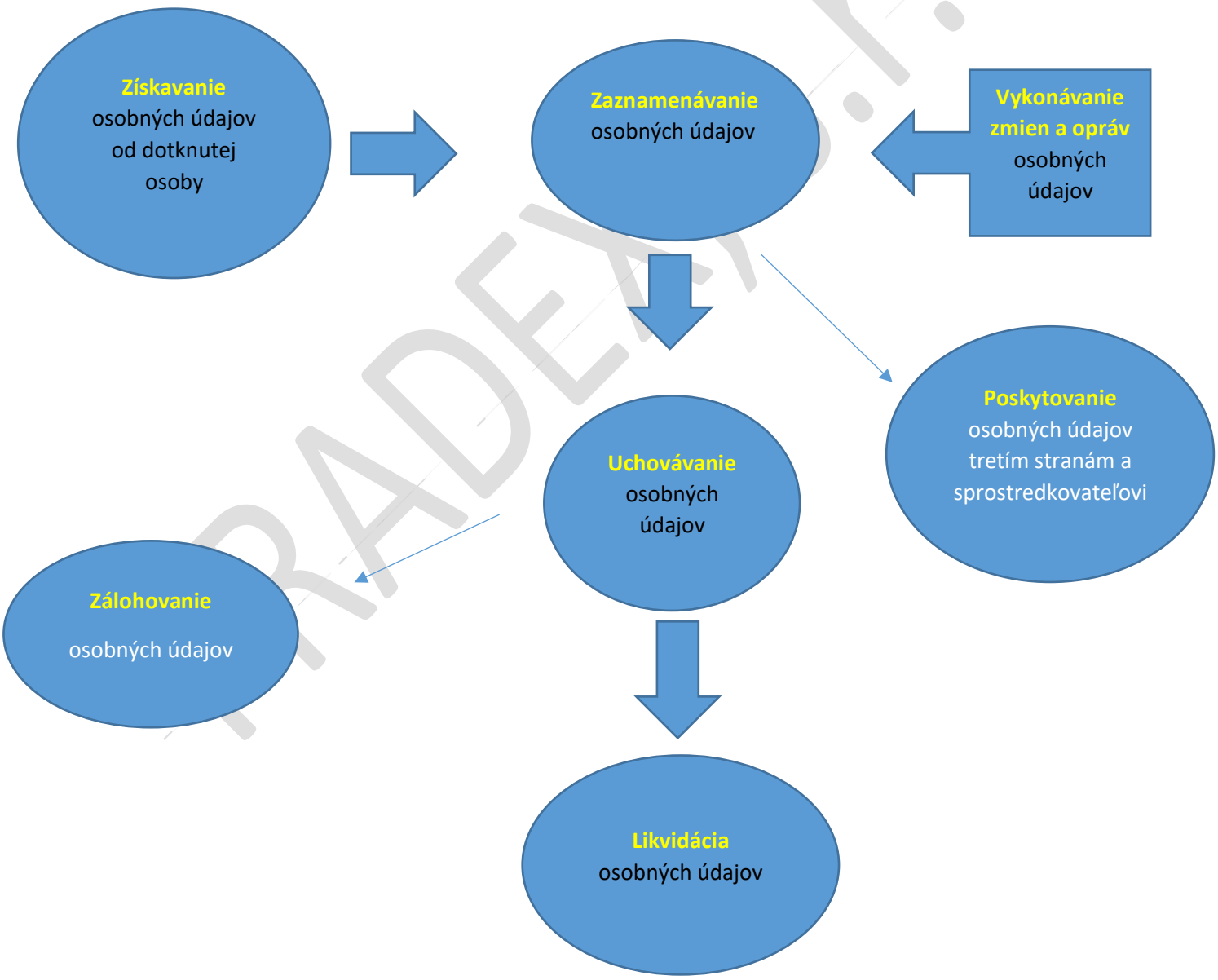
tretie strany- **Sociálna poisťovňa, zdravotné poisťovne, Finančný úrad, doplnkové dôchodkové sporiteľne, dôchodkové správcovské spoločnosti, orgány štátnej správy a verejnej moci na výkon**

kontroly a dozoru, Ústredie práce sociálnych vecí a rodiny, súd a orgány činné v trestnom konaní, exekútor, iný oprávnený subjekt.

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok II

Účtovné doklady

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému je: **Účtovné doklady**

Účel spracúvania

Účelom spracúvania osobných údajov **je vedenie účtovníctva prevádzkovateľa, spracovanie účtovných dokladov.**

Právny základ spracúvania

Právnym základom spracúvania je **zákon** (zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, zákon č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov, zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov, zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov)

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **zamestnanci, klienti, dodávatelia** prevádzkovateľa.

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **titul, meno, priezvisko, adresa, číslo OP, číslo účtu**

Príjemcovia

Osobné údaje z informačného systému sa poskytujú:

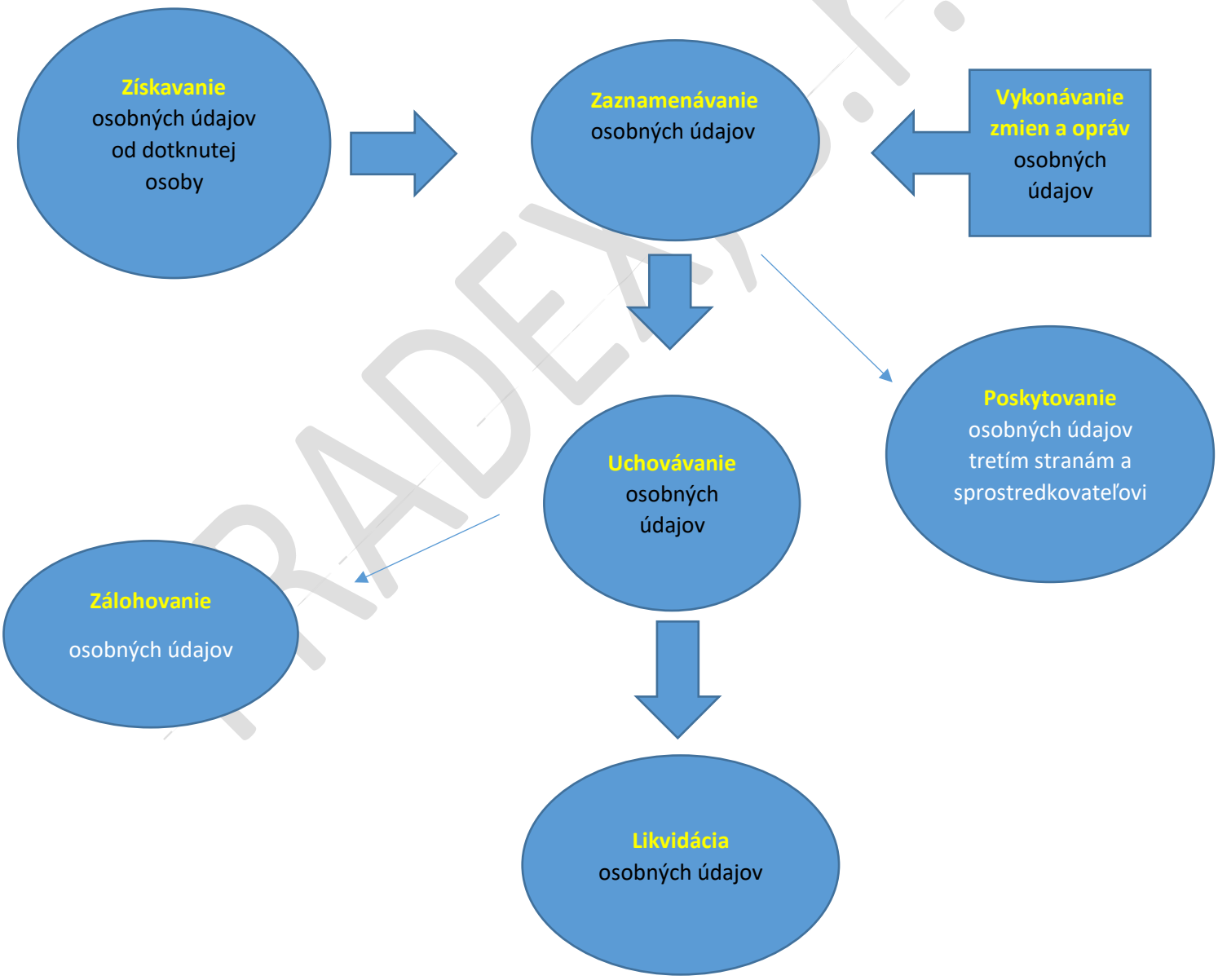
Sprostredkovatelia- **spoločnosť na spracovanie miezd a účtovníctva,**

tretie strany- **orgány kontroly a dozoru**

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok III

Výkup

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Výkup**

Účel spracúvania

Účelom spracúvania osobných údajov je **poskytovanie služieb prevádzkovateľa- výkup kovového odpadu, evidencia FO zákazníkov.**

Právny základ spracúvania

Právnym základom spracúvania je **zákon** (Zákon č. 79/2015 o odpadoch, Vyhláška č. 366/2015 o evidenčnej a ohlasovacej povinnosti)

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **zákazníci.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu:

titul, meno, priezvisko, adresa, číslo OP

Príjemcovia

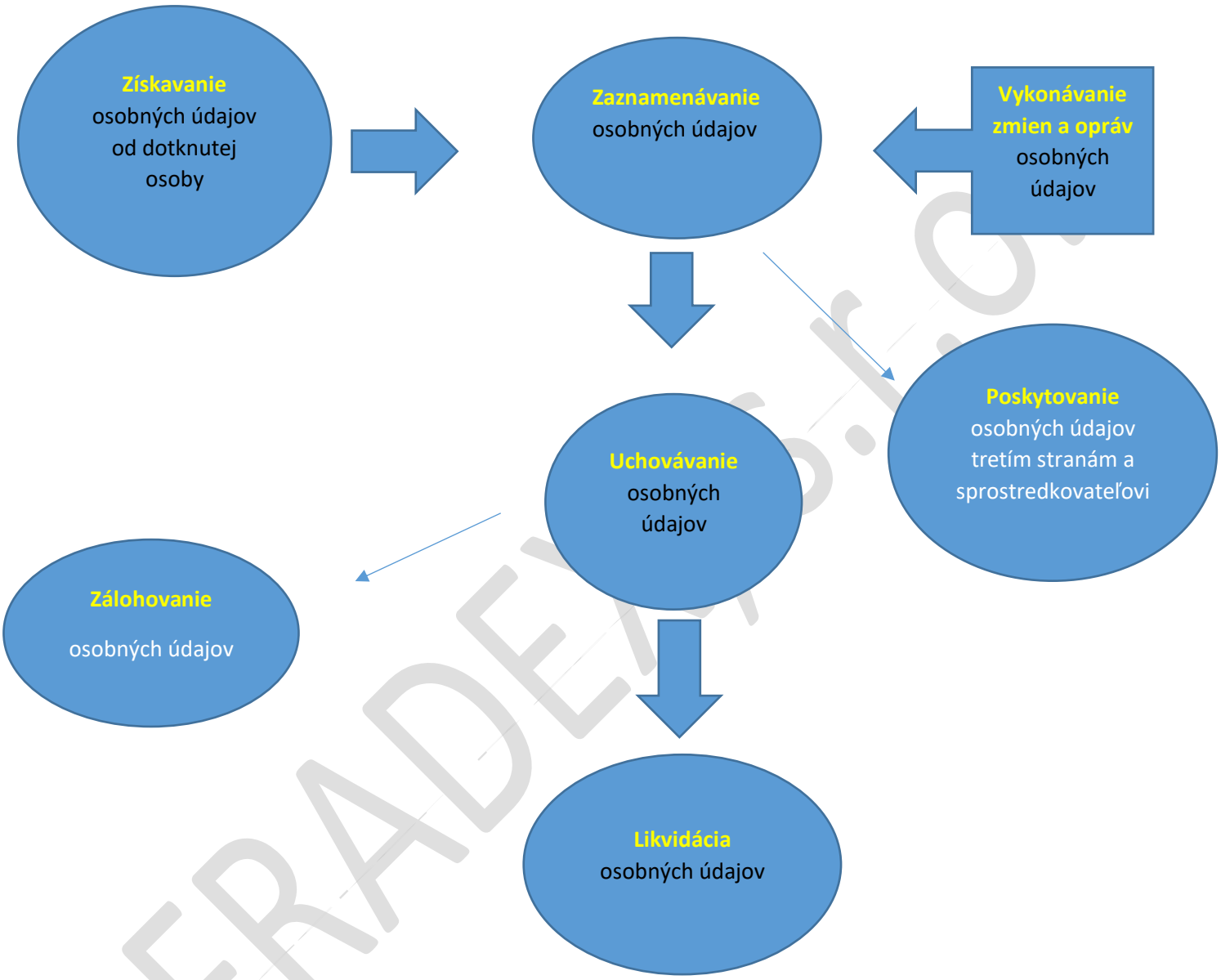
Osobné údaje z informačného systému sa poskytujú

Tretie strany- **štátne orgány kontroly a dozoru**

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok IV

Kamerový systém

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Kamerový systém.**

Účel spracúvania

Účelom spracúvania osobných údajov **je ochrana verejného poriadku a bezpečnosti, odhaľovanie kriminality, narušenia bezpečnosti štátu, alebo ochrana majetku alebo zdravia.**

Právny základ spracúvania

Právnym základom spracúvania je **zákon** (zákon č. 79/2015 o odpadoch, zákon č. 18/2018 o ochrane osobných údajov)

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **zamestnanci, zákazníci iné dotknuté osoby vstupujúce do areálu spoločnosti.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **zachytávanie jednotlivých charakteristík a údajov o dotknutej fyzickej osobe, informácie týkajúce sa fyzickej, psychickej, ekonomickej, sociálnej alebo kultúrnej identity.**

Príjemcovia

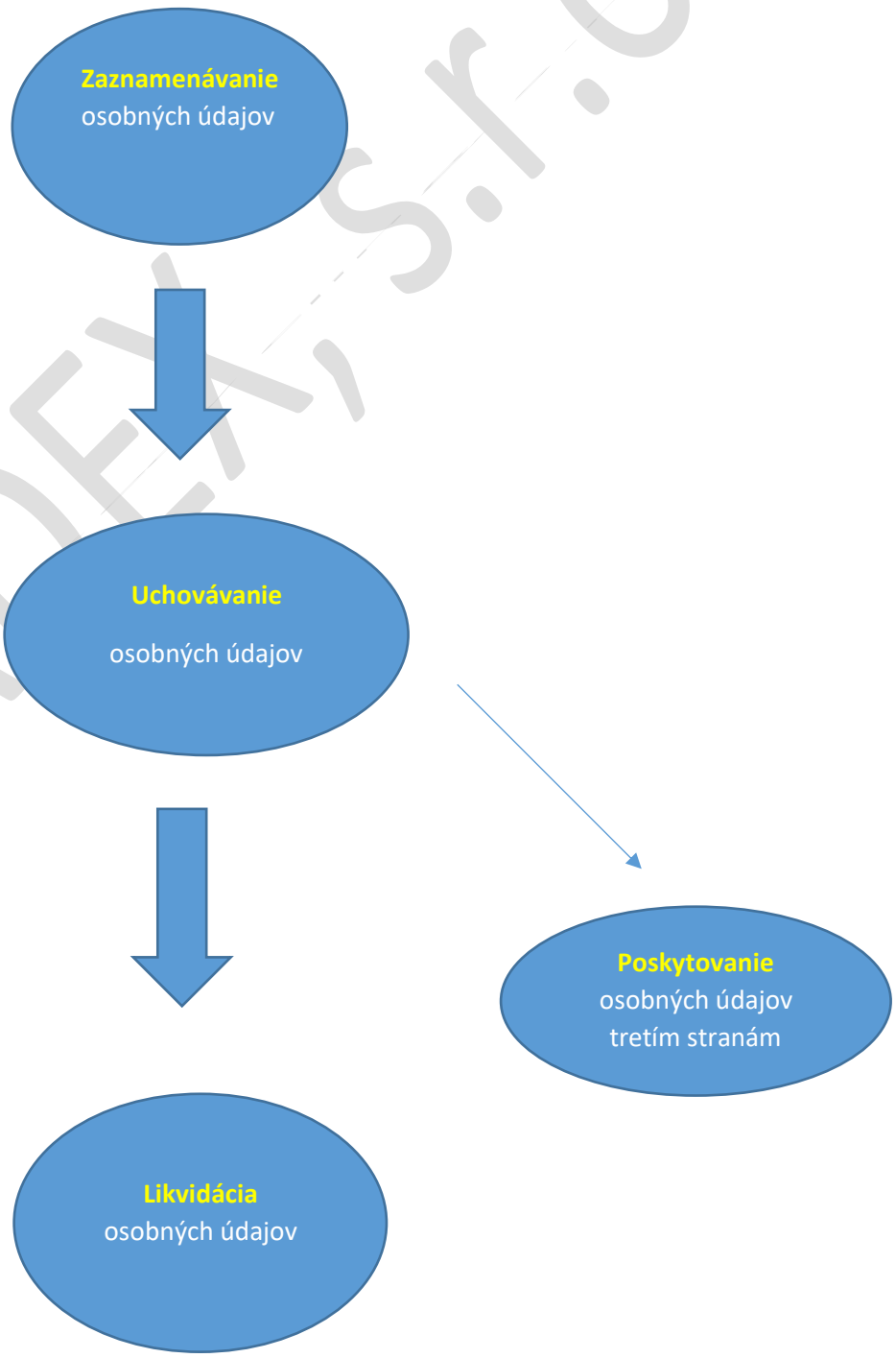
Osobné údaje z informačného systému sa poskytujú príjemcom:

Tretie strany- **orgány štátnej správy odpadového hospodárstva a orgány činné v trestnom konaní a súd.**

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok V

GPS monitoring vozidiel

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je GPS monitoring vozidiel.**

Účel spracúvania

Účelom spracúvania osobných údajov **je ochrana majetku zamestnávateľa pred poškodením, stratou, zničením a zneužitím.**

Právny základ spracúvania

Právnym základom spracúvania je **zákon.**

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **zamestnanci vodiči.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, priezvisko vodiča, poloha vozidla.**

Príjemcovia

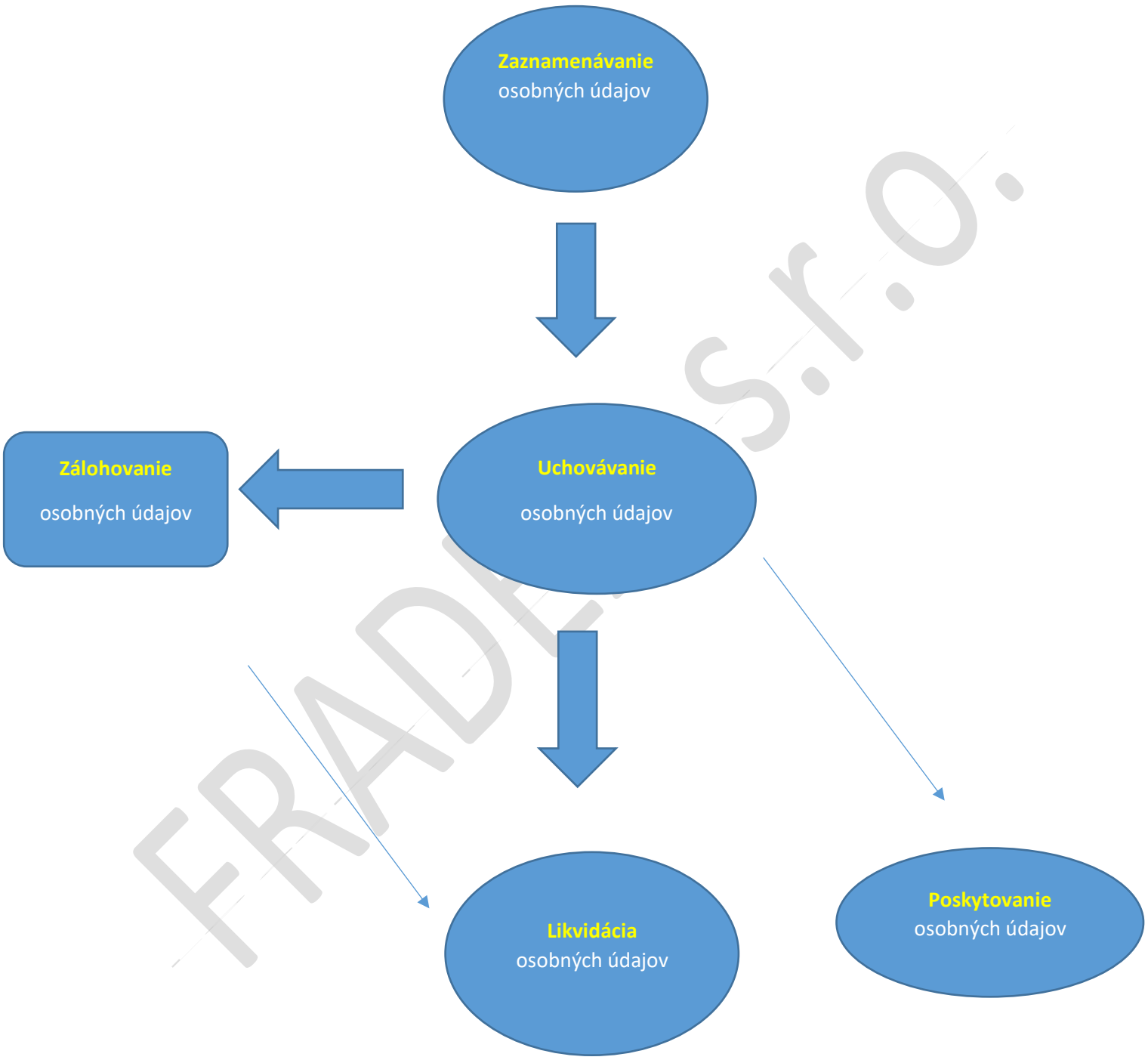
Osobné údaje z informačného systému sa poskytujú príjemcom:

Tretie strany- **orgány činné v trestnom konaní a súd.**

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok VI

Elektronický dochádzkový systém

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Elektronický dochádzkový systém.**

Účel spracúvania

Účelom spracúvania osobných údajov **je elektronická evidencia dochádzky, ako podklad na spracovanie miezd.**

Právny základ spracúvania

Právnym základom spracúvania je **zákon.**

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **zamestnanci.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, priezvisko adresa, fotografia**

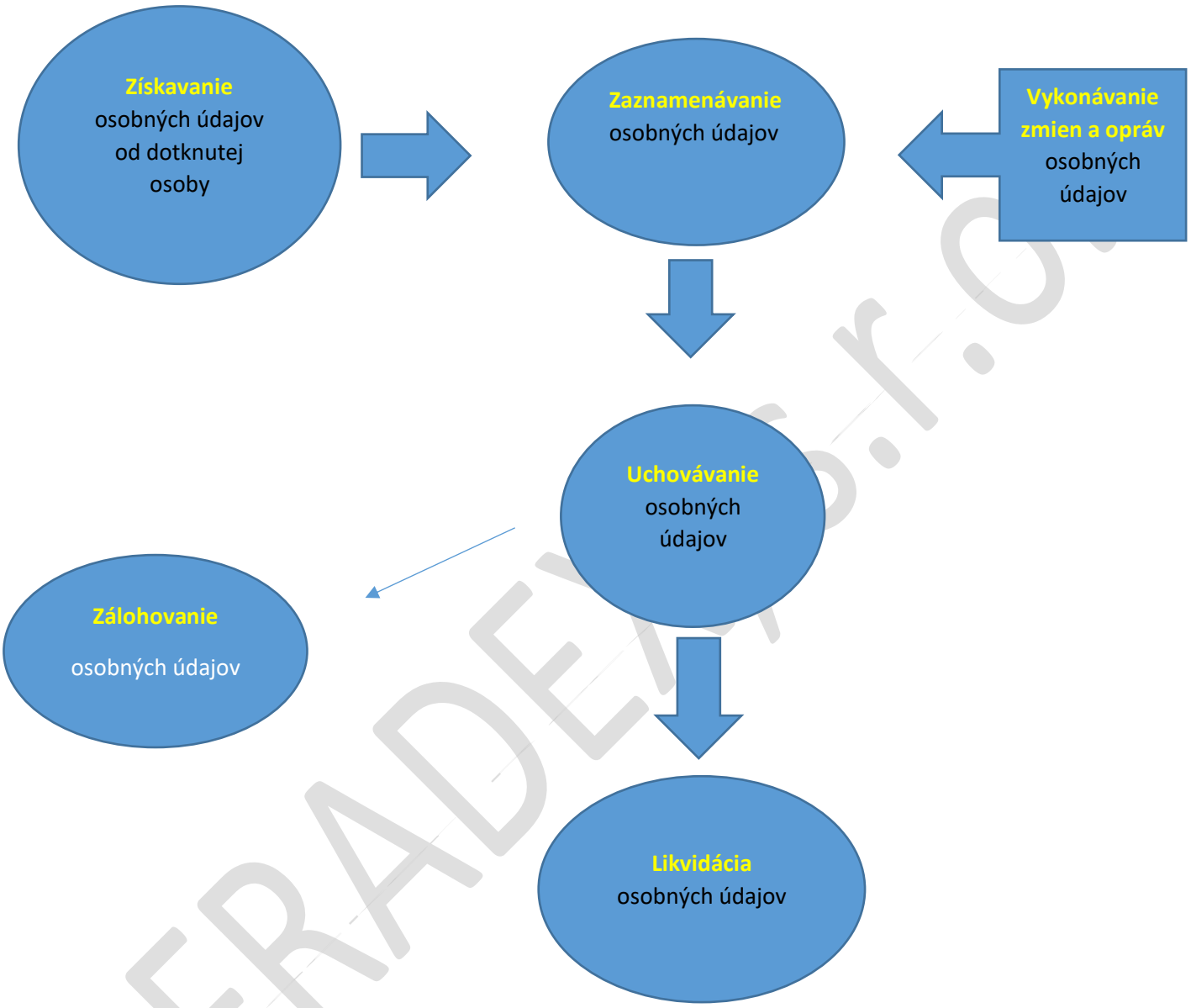
Príjemcovia

Osobné údaje z informačného systému sa neposkytujú príjemcom.

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok VII

Zmluvy s dodávateľmi

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Zmluvy s dodávateľmi.**

Účel spracúvania

Účelom spracúvania osobných údajov **je zmluvný resp. predzmluvný vzťah s dodávateľmi tovarov a služieb.**

Právny základ spracúvania

Právnym základom spracúvania je **zmluva**

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **dodávatelia tovarov a služieb.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, priezvisko adresa, kontaktné údaje, podpis**

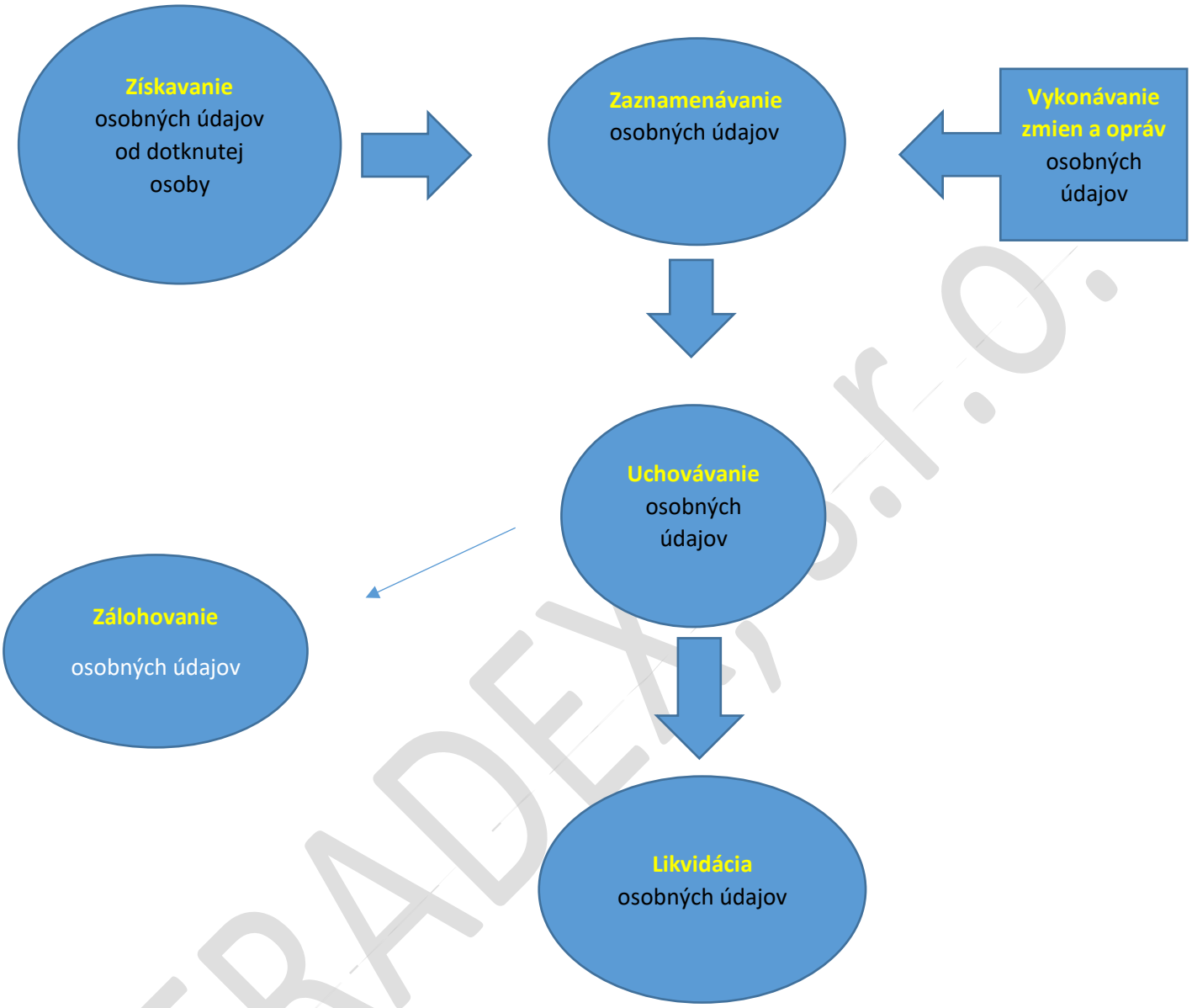
Príjemcovia

Osobné údaje z informačného systému sa neposkytujú príjemcom.

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok VIII

Evidencia došlej a odoslanej pošty

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Evidencia došlej a odoslanej pošty.**

Účel spracúvania

Účelom spracúvania osobných údajov **je evidovanie došlej a odoslanej pošty.**

Právny základ spracúvania

Právnym základom spracúvania je **zmluva a zákon.**

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **dodávatelia tovarov a služieb, klienti, zamestnanci.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, adresa**

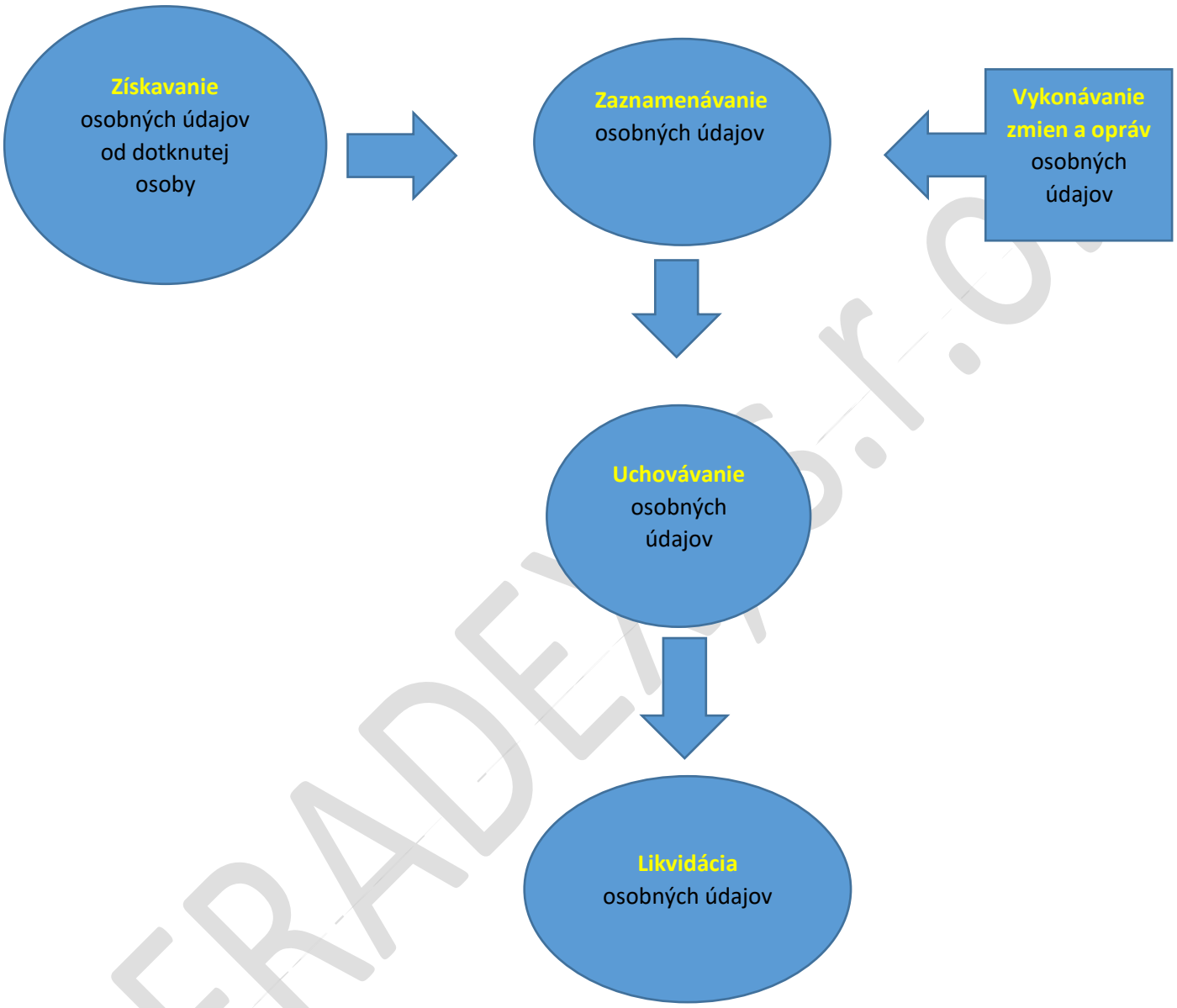
Príjemcovia

Osobné údaje z informačného systému sa neposkytujú príjemcom.

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Článok VIII

Evidencia prianí a sťažností

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému **je Evidencia prianí a sťažností.**

Účel spracúvania

Účelom spracúvania osobných údajov **je evidencia prianí a sťažností.**

Právny základ spracúvania

Právnym základom spracúvania je **zmluva a zákon.**

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú **dodávatelia tovarov a služieb, klienti, zamestnanci.**

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: **meno, podpis.**

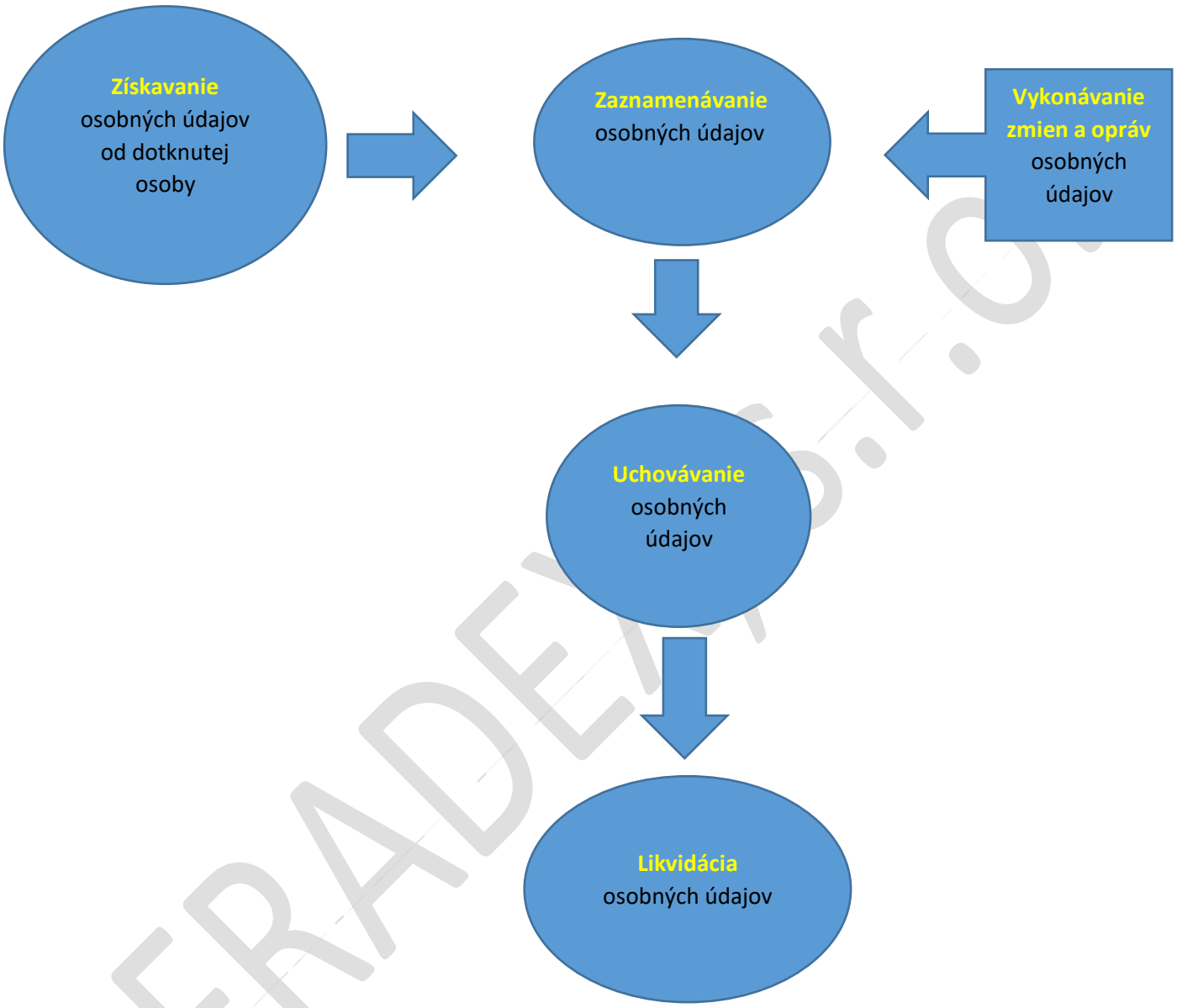
Príjemcovia

Osobné údaje z informačného systému sa neposkytujú príjemcom.

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na dosiahnutie účelu spracúvania.

Funkčný opis spracovateľskej operácie (schéma)



Identifikácia aktív

Neautomatizované aktíva (papierová podoba listín):

- životopisy, pracovné zmluvy, dotazníky, výplatné pásky, korešpondencia- listy a vytlačené e-maily, rôzne poučenia, hlásenia, výkazy, kniha prianí a sťažností, kniha došlej a odoslanej pošty, objednávky, obchodné zmluvy, faktúry, vážne lístky, výdavkové doklady a ďalšie daňové doklady

Automatizované aktíva (elektronická podoba):

- **dokumenty v elektronickej podobe- scany, e-maily, osobné údaje uložené v rámci jednotlivých softvérov**

Výpočtová technika (Hardvér)- **3 ks počítače, 4 ks notebooky**

Softvéry- **Microsoft Office, Adobe Acrobat**

Operačné systémy- **Windows**

Sieťové prepojenie – **vonkajšie- Internet, vnútorné- sieťované PC**

Antivírus- **ESET**

Kódex správania

V rámci primeraných bezpečnostných opatrení sa zavádzajú primerané politiky ochrany osobných údajov prevádzkovateľa alebo kódex správania.

Prevádzkovateľ resp. osoby ním poverené spracúvaním osobných údajov fyzických osôb v rámci prevádzky akceptujú všeobecné pravidla ochrany osobných údajov.

DRUHÁ ČASŤ

Bezpečnosť osobných údajov

Analýza rizík

Identifikácia rizík 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.

Riziká v objektovej bezpečnosti:

- Strata alebo odcudzenie kľúčov od prevádzky,
- Neuzamknutie vstupných dverí do chránených priestorov po odchode z týchto priestorov,
- Prekonanie mechanických zábranných prostriedkov nepovolanou osobou,
- Živelná pohroma.

Riziká v dokumentárnom informačnom systéme:

- Šírenie chránených informácií zamestnancami prevádzkovateľa,
- Šírenie chránených informácií nezlikvidovanými nepotrebnými písomnosťami,
- Cielené získanie informácií o osobných údajoch cudzou osobou,
- Strata alebo odcudzenie dokumentácie obsahujúcej osobné údaje tretími osobami, prípadne zamestnancami prevádzkovateľa.

Riziká v automatizovanom informačnom systéme:

a) Riziká preniknutia osobných údajov k nepovolaným osobám:

- Preniknutie nepovolaných osôb k počítačovému systém,
- Odcudzenie počítačového systému,
- Riziko prieniku do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z lokálnej počítačovej siete, resp. Jeho sprístupnenie týmto osobám,
- Prienik do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z internetu, resp. Jeho sprístupnenie týmto osobám.

b) Riziká straty osobných údajov a narušenia integrity:

- Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom,
- Riziko nezabezpečeného prenosu prostredníctvom aplikácie,
- Riziko poškodenia serverov a aktívnych sieťových prvkov požiarom,
- Poškodenie pevného disku počítača mechanickou závadou,

- Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania,
- Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov,
- Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej siete,
- Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov internetu.

Analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti

Druhým krokom analýzy bezpečnosti je stanovenie rozsahu rizika, že daná hrozba spôsobí narušenie bezpečnosti alebo funkčnosti informačného systému. Riziko sa ohodnocuje podľa nasledovnej tabuľky:

		PRAVDEPODOBNOSŤ		
		Nízka	**Stredná**	**Vysoká**
DOPAD	**Nulový**	nulové	nulové	nulové
	Nízky	nízke	nízke	stredné
	Stredný	nízke	stredné	vysoké
	Vysoký	stredné	vysoké	vysoké

Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti s odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika

Ak je riziko **nulové, nie je potrebné prijať** žiadne opatrenie za účelom eliminácie rizika.
Ak je riziko **nízke, môže byť prijaté** opatrenie za účelom eliminácie rizika.

Ak je riziko **stredné**, opatrenie za účelom eliminácie rizika **by malo byť prijaté**.
Ak je riziko **vysoké**, bezpečnostné opatrenie za účelom eliminácie rizika **musí byť prijaté**.

Riadenie rizík pre práva a slobody dotknutých osôb

Zhodnotil sa pôvod, povaha, osobitosť a závažnosť rizík alebo, konkrétnejšie, každé riziko sa posúdilo z pohľadu dotknutých osôb, ďalej sa zohľadnili zdroje rizík, identifikovali sa prípadné dôsledky resp. dopad na práva a slobody dotknutých osôb v súvislosti s určitými prípadmi vrátane neoprávneného prístupu, neželaných úprav a straty údajov, identifikovali sa hrozby, ktoré by mohli viesť k neoprávnenému prístupu, neželaným úpravám a strate údajov, odhadla sa pravdepodobnosť a závažnosť a stanovili sa opatrenia na riešenie uvedených rizík.
Identifikácia s ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany.

Chránený priestor je priestor prevádzkovateľa, v ktorom dochádza k spracovateľským činnostiam s osobnými údajmi či už automatizovaným alebo neautomatizovanými prostriedkami spracúvania (od získavania cez archiváciu až po ich likvidovanie).

Článok I

Riziká v objektovej bezpečnosti

Strata alebo odcudzenie kľúčov od prevádzky

Prijaté opatrenie

- správa kľúčov prevádzkovateľom,
- kľúčmi od dverí do prevádzky, kancelárií disponujú len prevádzkovateľ a oprávnené osoby.

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko:

Nízke (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby straty alebo odcudzenia kľúčov).

Odporúčané opatrenia:

Zápis o pridelení kľúčov konkrétnej oprávnenej osobe.

Bezpečné uloženie rezervných kľúčov v uzamykateľnej zásuvke alebo trezore, kľúčmi od ktorého disponuje iba prevádzkovateľ.

Neuzamknutie vstupných dverí do chránených priestorov po odchode z týchto priestorov

Prijaté opatrenie

- prevádzkovateľ a oprávnené osoby po tom čo opustia prevádzku vždy uzamknú dvere a okná.

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko

Nízke (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby neuzamknutia dverí).

Odporúčané opatrenia

Písomne poučenie oprávnenej osoby.

Prekonanie mechanických zábranných prostriedkov nepovolanou osobou

Prijaté opatrenie:

- mechanické zabezpečenie chráneného priestoru- uzamykateľné bezpečnostné dvere a uzamykateľné okná do chráneného priestoru,
- elektronické zabezpečenie chránených priestorov- alarm, kamerový systém.

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko

Nízke.

Odporúčané opatrenia

Žiadne.

<u>Živelná pohroma</u>

Prijaté opatrenie:

- zálohovanie dát (server, externý disk)
- záložné nosiče umiestnené mimo chránených priestorov prevádzkovateľa,

Pravdepodobnosť

Nízka

Dopad

Nízky

Vyhodnotené riziko

Nízke.

Odporúčané opatrenia

Bezpečnostné opatrenie- správa kľúčov.

Článok II

Riziká v dokumentárnom informačnom systéme

Šírenie chránených informácií zamestnancami prevádzkovateľa

Prijaté opatrenie

- s listinnými aktívami v rámci chráneného priestoru manipuluje iba prevádzkovateľ a oprávnené osoby,

- prevádzkovateľ a oprávnené osoby spracúvajú listiny s osobnými údajmi v priestore prístupnom tretím osobám iba v ich sprievode,

- záväzok mlčanlivosti prevádzkovateľa oprávnených osôb a zákaz predkladať tretej osobe dokumenty obsahujúce osobné údaje.

Pravdepodobnosť

Nízka

Dopad

Nulový

Vyhodnotené riziko

Nulové

Odporúčané opatrenia

Písomné poučenie oprávnenej osoby.

Šírenie chránených informácií nezlikvidvanými nepotrebnými písomnosťami

Prijaté opatrenie

- prevádzkovateľ a oprávnené osoby všetky nepotrebné listiny s osobnými údajmi bezodkladne zlikvidujú skartovaním,

- nepotrebné listiny s osobnými údajmi prevádzkovateľ a oprávnené osoby nikdy nevyhodia do koša.

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko

Nízke

Odporúčané opatrenia

Písomné poučenie oprávnenej osoby.

Cielené získanie informácií o osobných údajov cudzou osobou

Prijaté opatrenia

- s listinnými aktívami v rámci chráneného priestoru manipuluje iba prevádzkovateľ a oprávnené osoby,
- prevádzkovateľ a oprávnené osoby spracúvajú listiny a ukladajú s osobnými údajmi v priestore prístupnom tretím osobám iba v ich sprievode,
- záväzok mlčanlivosti prevádzkovateľa a oprávnených osôb predkladať a sprístupniť tretej osobe dokumenty obsahujúce osobné údaje,
- dokumenty a dátové nosiče s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom objekte, v uzamykateľnej kancelárií, v uzamykateľnej skrini.
- režim údržby a upratovania chránených priestorov sa vykonáva oprávnenou osobou.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia:

Písomné poučenie oprávnenej osoby.

Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.

Strata alebo odcudzenie dokumentácie obsahujúcich osobné údaje tretími osobami, prípadne zamestnancami prevádzkovateľa

Prijaté opatrenie:

- opatrenia v rámci objektovej bezpečnosti,
- prenos dokumentov mimo chránených priestorov len prevádzkovateľom,
- s listinnými aktívami v rámci chráneného priestoru manipuluje iba prevádzkovateľ a oprávnené osoby,
- dokumenty s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom objekte, v uzamykateľnej kancelárií, v uzamykateľnej skrini,
- režim údržby a upratovania chránených priestorov sa vykonáva oprávnenou osobou.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia:

Písomné poučenie oprávnenej osoby.

Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.

Článok III

Riziká v automatizovanom informačnom systéme

a) Riziká preniknutia osobných údajov k nepovoleným osobám:

Preniknutie nepovolaných osôb k počítačovému systému

Prijaté opatrenie

- rovnako tu platia opatrenia prijaté v objektovej bezpečnosti,
- k počítaču, v ktorom sa spracúvajú osobné údaje má prístup len prevádzkovateľ a oprávnené osoby,
- s aktívami v elektronickej podobe v rámci chráneného priestoru manipuluje iba prevádzkovateľ a oprávnené osoby,
- šetrič obrazovky s heslom, ak sa momentálne na počítači nepracuje.
- prevádzkovateľ a oprávnené osoby vždy používajú prístupové heslo,
- evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou- iba v rámci prevádzky, chráneného priestoru prevádzkovateľa,

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia

Vhodné umiestnenie zobrazovacích jednotiek.

Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.

Odcudzenie počítačového systému

Primerane sa aplikujú opatrenia pre riziko násilného prekonania mechanických zábranných prostriedkov nepovolanou osobou.

Riziko prieniku do pevného disku, v ktorom sú uložené osobné údaje, neoprávnenými osobami z lokálnej počítačovej siete, resp. jeho sprístupnenie týmto osobám

Prijaté opatrenie:

- správa prideľovania jednotlivých prístupom oprávneným osobám,
- definovanie zložitých prístupových práv a hesiel do aplikácií a do sieťových adresárov.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia:

Vykonávať pravidelný upgrade firmware aktívnych sieťových prvkov. Pri zmenách aktívnych sieťových prvkov, inak s periodicitou každých 4-5 rokov vykonávať penetračné testovanie sieťovej infraštruktúry útokom na perimeter zvonku. Primerane renovovať sieťovú infraštruktúru, aktívne prvky vymieňať pravidelne každých 4-5 rokov (preventívny charakter).

<u>Riziko prieniku do pevného disku, v ktorom sú uložené osobné údaje, neoprávnenými osobami z internetu, resp. jeho sprístupnenie týmto osobám</u>

Prijaté opatrenie

- opatrne manipulovať s podozrivými médiami a programami,
- prevádzkovateľ neinštaluje neznáme programy,
- používanie legálneho a prevádzkovateľom schváleného softvéru,
- pravidelná aktualizácia operačného systému a programového aplikačného vybavenia,
- bezpečné a kontrolované sťahovanie súborov z verejne prístupnej počítačovej siete,
- neotváranie podozrivých e-mailov a odkazov,
- definovanie zložitých prístupových práv a hesiel do aplikácií a do sieťových adresárov,
- inštalácia antivírusového programu, a jeho pravidelná aktualizácia,
- firewall na zabezpečenie prvotnej ochrany úniku dát cez internet,
- antispamový systém,
- šifrová ochrana uložených a prenášaných údajov,
- pseudonymizácia osobných údajov.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia

- zamedzenie pripojenia k určitým rizikovým adresám, používanie sieťových protokolov,
- chránenie WiFi silným heslom, zmena prednastavených hesiel od výrobcu.

b) Riziká straty osobných údajov a narušenia integrity

<u>Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom</u>

Primerane sa aplikujú opatrenia pre riziká prekonania mechanických zábranných prostriedkov nepovolanou osobou.

<u>Riziko nezabezpečeného prenosu prostredníctvom aplikácie</u>

Prijaté opatrenia

- definovanie zložitých prístupových práv a hesiel do aplikácií a do sieťových adresárov,
- používanie legálneho a prevádzkovateľom schváleného softvéru,
- inštalácia antivírusového programu, a jeho pravidelná aktualizácia,
- pseudonymizácia osobných údajov.

Pravdepodobnosť

Nízka

Dopad

Nízky.

Vyhodnotené riziko

Nízke.

Odporúčané opatrenia

Žiadne.

<u>Riziko poškodenia serverov a aktívnych sieťových prvkov požiarom</u>

Prijaté opatrenie

- prevádzkovateľ neprevádzkuje server vo svojich priestoroch,
- protipožiarne opatrenie- hasiace prístroje.

Pravdepodobnosť

Nízka

Dopad

Nízky

Vyhodnotené riziko

Nízke

Odporúčané opatrenia:

Žiadne.

<u>Poškodenie pevného disku počítača mechanickou závadou</u>

Prijaté opatrenia

- prevádzkovateľ minimálne jedenkrát mesačne, alebo po nesprávnom ukončení alebo výpadku energie zabezpečiť systémovú kontrolu disku (scandisk).

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko

Nízke.

Odporúčané opatrenia

Žiadne.

<u>Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania</u>

Prijaté opatrenia:

- prevádzkovateľ používa nepretržitý zdroj napájania,

- prevádzkovateľ po nesprávnom ukončení alebo výpadku energie zabezpečiť systémovú kontrolu disku (scandisk).

Pravdepodobnosť

Nízka

Dopad

Stredný

Vyhodnotené riziko

Nízke

Odporúčané opatrenia

Žiadne.

Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov

Prijaté opatrenia

- opatrne manipulovať s podozrivými médiami a programami,
- prevádzkovateľ neinštaluje neznáme programy,
- bezpečné a kontrolované sťahovanie súborov z verejne prístupnej počítačovej siete,
- inštalácia antivírusového programu, a jeho pravidelná aktualizácia,
- neotváranie podozrivých e-mailov a odkazov.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia

- zamedzenie pripojenia k určitým rizikovým adresám, používanie sieťových protokolov.

Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej siete

Prijaté opatrenie:

- správa prideľovania jednotlivých prístupom oprávneným osobám,
- definovanie zložitých prístupových práv a hesiel do aplikácií a do sieťových adresárov.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia:

Vykonávať pravidelný upgrade firmware aktívnych sieťových prvkov. Pri zmenách aktívnych sieťových prvkov, inak s periodicitou každých 4-5 rokov vykonávať penetračné testovanie sieťovej infraštruktúry útokom na perimeter zvonku. Primerane renovovať sieťovú infraštruktúru, aktívne prvky vymieňať pravidelne každých 4-5 rokov (preventívny charakter).

Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov internetu

Prijaté opatrenie

- opatrne manipulovať s podozrivými médiami a programami,
- prevádzkovateľ neinštaluje neznáme programy,
- používanie legálneho a prevádzkovateľom schváleného softvéru,
- pravidelná aktualizácia operačného systému a programového aplikačného vybavenia,
- bezpečné a kontrolované sťahovanie súborov z verejne prístupnej počítačovej siete,
- neotváranie podozrivých e-mailov a odkazov,
- definovanie zložitých prístupových práv a hesiel do aplikácií a do sieťových adresárov,
- inštalácia antivírusového programu, a jeho pravidelná aktualizácia,
- firewall na zabezpečenie prvotnej ochrany úniku dát cez internet,
- šifrová ochrana uložených a prenášaných údajov,
- pseudonymizácia osobných údajov,
- antispamový systém.

Pravdepodobnosť

Nízka

Dopad

Vysoký

Vyhodnotené riziko

Stredné.

Odporúčané opatrenia

- zamedzenie pripojenia k určitým rizikovým adresám, používanie sieťových protokolov,
- chránenie WiFi silným heslom, zmena prednastavených hesiel od výrobcu.

TRETIA ČASŤ

Primerané bezpečnostné opatrenia

Prevádzkovateľ príjme so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku, pričom uvedené opatrenia prípadne zahŕňajú aj:

a) pseudonymizáciu a šifrovanie osobných údajov;

b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;

c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;

d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Prevádzkovateľ pri prijímaní primeraných bezpečnostných opatrení a záruk dodržiava nasledujúce **zásady spracúvania osobných údajov:**

zákonnosť, spravodlivosť, transparentnosť, obmedzenie a kompatibilita účelov spracúvania, minimalizáciu údajov, pseudonymizáciu alebo šifrovanie, minimalizáciu uchovávania údajov, správnosť údajov, integrita, dôvernosť, dostupnosť údajov, nevyhnutnosť a primeranosť spracúvania s ohľadom na účel spracovateľskej operácie.

Prevádzkovateľ príjme technické a organizačné opatrenia na elimináciu rizík pre práva fyzických osôb.

Článok I

Technické opatrenia

1. Technické opatrenie realizované prostriedkami fyzickej povahy

Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).

Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, mreže alebo presklenia).

Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.

Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.

Opatrenie pre zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).

2. Ochrana pred neoprávneným prístupom

Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia.

Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

3. Riadenie prístupu poverených osôb

Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme).

Riadenie privilegovaných prístupov v informačných systémoch.

Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.

4. **Riadenie zraniteľností**

Opatrenia pre detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu.

Ochrana pred nevyžiadanou elektronickou poštou.

.

Používanie legálneho a prevádzkovateľom schváleného softvéru.

Opatrenia pre zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia.

Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie.

Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík.

5. **Sieťová bezpečnosť**

Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.

Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.

Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia pre zamedzenie pripojenia k určitým adresám, pravidlá pre používanie sieťových protokolov.

Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).

Aktualizácia operačného systému a programového aplikačného vybavenia.

6. Zálohovanie

Test funkčnosti záložných dátových nosičov.

Vytváranie záloh s vopred zvolenou periodicitou.

Určenie doby uchovávania záloh a kontrola jej dodržiavania.

Test obnovy informačného systému zo zálohy.

Bezpečné ukladanie záloh.

7. Likvidácia osobných údajov a dátových nosičov

Technické opatrenia pre bezpečné vymazanie osobných údajov z dátových nosičov.

Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií).

- *Príloha č. 1 TECHNICKÉ OPATRENIA*

Článok II

Organizačné opatrenia

1. Personálne opatrenia

Poverenie osoby prevádzkovateľom alebo sprostredkovateľom, ktorá má prístup k osobným údajom.

Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä

vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh,

určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov,

vymedzenie základných postupov alebo operácií s osobnými údajmi,

vymedzenie zodpovednosti za porušenie zákona alebo osobitného predpisu[1)].

Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov).

Určenie zodpovednej osoby.

Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií).

Postup pri ukončení pracovného alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti).

Práca na diaľku a pravidlá mobilného spracovania dát.

2. Riadenie aktív

Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.

Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.

Určenie vlastníctva aktív a zodpovednosti za riziká.

Pravidlá a postupy pre klasifikáciu informácií.

Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.

Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.

Opatrenia pre vrátenie aktív (napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia a pod.

3. **Riadenie prístupu osôb k osobným údajom**

Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa.

Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov).

Pravidlá pre prideľovanie prístupových práv a úrovní prístupu (rolí) povereným osobám.

Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov.

Pravidlá pre vzájomné zastupovanie poverených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru).

Pravidlá pre odstránenie alebo zmenu prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, prípadne prispôsobenie zmenám rolí.

4. **Organizácia spracúvania osobných údajov**

Pravidlá spracúvania osobných údajov v chránenom priestore.

Nepretržitá prítomnosť poverenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako poverené osoby.

Režim údržby a upratovania chránených priestorov.

Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá

1. pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovedností,
2. pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovedností,
3. pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností.

5. Likvidácia osobných údajov

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

6. Porušenia ochrany osobných údajov

Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na účel včasného prijatia preventívnych alebo nápravných opatrení.

Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.

Evidencia porušení ochrany osobných údajov a použitých riešení.

Postup pre identifikáciu a riešenie jednotlivých typov porušení ochrany osobných údajov.

Postup pre odstraňovanie následkov porušení ochrany osobných údajov.

Postupy zaručenia kontinuity pri haváriách, poruchách a iných mimoriadnych situáciách.

Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania.

7. Kontrolná činnosť

Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov).

Informovanie osôb o kontrolnom mechanizme, ak je u prevádzkovateľa alebo sprostredkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).

Postupy pre monitorovanie súladu spracúvania osobných údajov.

8. Dodávateľské vzťahy

Postup pre overenie dostatočných záruk.

Začlenenie požiadaviek na ochranu údajov do požiadaviek pre nové systémy a do pravidiel pre vývoj a nákup systémov.

Začlenenie požiadaviek na ochranu údajov do zmluvných vzťahov s dodávateľmi a tretími stranami.

Testovanie bezpečnostných funkcií počas vývoja systémov.

Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi.

- *Príloha č. 2 ORGANIZAČNÉ OPATRENIA*

ŠTVRTÁ ČASŤ

Posúdenie vplyvu na ochranu osobných údajov

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. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.

Prevádzkovateľ sa počas vykonávania posúdenia vplyvu na ochranu údajov radí so zodpovednou osobou, pokiaľ bola určená.

Posúdenie vplyvu na ochranu údajov sa vyžaduje najmä v prípadoch:
a) systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
b) spracúvania vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky, alebo
c) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Dozorný orgán vypracuje a zverejní zoznam tých spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov

.Dozorný orgán môže stanoviť a zverejniť aj zoznam spracovateľských operácií, v prípade ktorých sa nevyžaduje posúdenie vplyvu na ochranu údajov.

Článok I

Kritéria posúdenia vplyvu

Prevádzkovateľ s ohľadom na povahu, rozsah, kontext a účely spracúvania osobných údajov (PRVÁ ČASŤ) s cieľom zistiť, či niektorý z typov spracovateľských činnosti prevádzkovateľa nepredstavuje vysoké riziko pre práva a slobody dotknutých osôb zohľadnil nasledujúce kritéria:

1. **Hodnotenie alebo prideľovanie bodov** vrátane profilovania a predpovedania, najmä z „aspektov súvisiacich s výkonnosťou dotknutej osoby v práci, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom“ .

Príkladom tohto postupu by mohla byť finančná inštitúcia, ktorá preveruje svojich klientov prostredníctvom v databáze obsahujúcej informácie o úveroch alebo v databáze obsahujúcej informácie o praní špinavých peňazí a financovaní terorizmu alebo v databáze s informáciami o podvodoch, alebo v prípade biotechnologickej spoločnosti by mohlo ísť o ponuku genetických testov priamo spotrebiteľom s cieľom posúdiť a predvídať riziká ochorenia a zdravotné riziká, alebo by mohlo ísť o spoločnosť, ktorá vytvára behaviorálne alebo marketingové profily založené na používaní jej webovej stránky alebo navigácii na nej.

NEVYKONÁVA SA

2. **Automatizované rozhodovanie s právnym alebo podobne závažným účinkom**: spracúvanie, ktorého cieľom je prijatie rozhodnutí o dotknutých osobách „s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu“ . Spracúvanie môže napríklad viesť k vylúčeniu jednotlivcov alebo k diskriminácii voči nim. Spracúvanie s malým alebo žiadnym vplyvom na jednotlivcov nespĺňa toto špecifické kritérium:

NEVYKONÁVA SA

3. **Systematické monitorovanie:** spracúvanie používané na pozorovanie, monitorovanie alebo kontrolu dotknutých osôb vrátane údajov získaných prostredníctvom sietí alebo „systematického monitorovania verejne prístupných miest“ Tento typ monitorovania je kritériom, pretože osobné údaje sa môžu získavať za okolností, keď dotknuté osoby nemusia

vedieť, kto zbiera ich údaje a ako sa budú používať. Okrem toho, pre jednotlivcov sa môže ukázať ako nemožné zabrániť tomu, aby sa stali predmetom takéhoto spracúvania na verejnom (alebo verejne prístupnom) mieste (-ach).

NEVYKONÁVA SA

4. **Citlivé údaje alebo údaje veľmi osobnej povahy:** zahŕňa to osobitné kategórie osobných údajov (napr. informácie o politických názoroch jednotlivcov), ako aj osobné údaje týkajúce sa uznania viny za trestné činy a priestupky.

Príkladom by mohla byť všeobecná nemocnica, ktorá uchováva lekárske záznamy pacientov, alebo súkromný detektív uchovávajúci podrobné informácie o páchateľoch trestnej činnosti. Nad rámec ustanovení všeobecného nariadenia o ochrane údajov sa niektoré kategórie údajov môžu považovať za také, ktoré zvyšujú možné riziko pre práva a slobody jednotlivcov. Tieto osobné údaje sa považujú za citlivé (ako sa tento pojem bežne chápe), pretože sú prepojené na domácnosť a súkromné aktivity (napr. elektronická komunikácia, ktorej dôvernosť by mala byť chránená) alebo preto, že vplývajú na výkon určitého základného práva (napr. údaje o polohe, ktorých získavanie spochybňuje slobodu pohybu), alebo preto, že ich porušenie jednoznačne zahŕňa závažné dôsledky na každodenný život dotknutej osoby (napr. finančné údaje, ktoré by sa mohli použiť na platobné podvody). V tejto súvislosti môže byť relevantné, či už dotknutá osoba alebo tretie strany údaje zverejnili. Skutočnosť, že osobné údaje sú verejne prístupné, sa môže zohľadniť ako faktor pri posudzovaní, ak sa v súvislosti s týmito údajmi očakávalo, že sa budú ďalej používať na isté účely. Toto kritérium môže zahŕňať aj také údaje, ako sú osobné dokumenty, emaily, denníky, poznámky z elektronických čítačiek vybavených prvkami na zapisovanie poznámok a veľmi osobné informácie, ktoré sa nachádzajú v aplikáciách na zaznamenávanie udalostí v rôznych oblastiach života (life-logging applications).

NEVYKONÁVA SA

5. **Údaje spracúvané vo veľkom rozsahu**: Pri posudzovaní toho, či sa spracúvanie vykonáva vo veľkom rozsahu, treba zvážiť predovšetkým tieto faktory:

a. počet dotknutých osôb, ktorých sa to týka, buď ako konkrétne číslo alebo ako podiel relevantnej populácie;

b. objem údajov a/alebo rozsah rôznych údajových položiek, ktoré sa spracúvajú;

c. dĺžka trvania alebo nemennosť činnosti spracúvania údajov;

d. geografický rozsah činnosti spracúvania.

NEVYKONÁVA SA

6. **Spájanie alebo kombinovanie súborov údajov**, napr. údajov pochádzajúcich z dvoch alebo viacerých operácií spracúvania údajov vykonaných na rozdielne účely a/alebo rozličnými prevádzkovateľmi údajov takým spôsobom, ktorý by prekročil rozumné očakávania dotknutej osoby.

NEVYKONÁVA SA

7. **Údaje týkajúce sa zraniteľných dotknutých osôb:** spracúvanie tohto druhu údajov je kritériom z dôvodu zvýšenej nerovnováhy moci medzi dotknutými osobami a prevádzkovateľom, čo znamená, že jednotlivci sa môžu nachádzať v pozícii, že nemôžu jednoduchým spôsobom vyjadriť súhlas so spracúvaním svojich údajov, namietať voči nemu ani vykonávať svoje práva. Zraniteľné dotknuté osoby môžu zahŕňať deti (možno ich považovať osoby, ktoré nie sú schopné vedome a na základe uváženia namietať voči spracúvaniu svojich údajov alebo s ním súhlasiť), zamestnanci, zraniteľnejšie časti obyvateľstva vyžadujúce si osobitnú ochranu (mentálne postihnuté osoby, žiadatelia o azyl, staršie osoby, pacienti atď.) a v každom prípade také osoby, v súvislosti s ktorými možno identifikovať nerovnováhu vo vzťahu medzi postavením dotknutej osoby a prevádzkovateľa.

VYKONÁVA SA – dotknuté osoby zamestnanci.

8. **Inovačné využitie alebo uplatňovanie nových technologických alebo organizačných riešení**, napr. kombinácia využitia odtlačkov prstov a rozpoznávania tvárí pre lepšiu kontrolu fyzického prístupu atď. Vo všeobecnom nariadení o ochrane údajov sa jednoznačne uvádza, že využitie novej technológie vymedzenej v „súlade s dosiahnutým stavom technologických znalostí“, môže viesť k tomu, že bude potrebné vykonať posúdenie vplyvu na ochranu údajov. Je to z toho dôvodu, že využitie takejto technológie môže zahŕňať nové formy získavania a využívania údajov, ktoré môžu byť spojené s vysokým rizikom pre práva a slobody jednotlivcov. Osobné a sociálne dôsledky zavedenia novej technológie môžu byť naozaj neznáme. Posúdenie vplyvu na ochranu údajov pomôže prevádzkovateľovi pochopiť a

riešiť tieto riziká. Napríklad určité aplikácie „internetu vecí“ by mohli mať výrazný vplyv na každodenné životy jednotlivcov a ich súkromie, a preto si vyžadujú posúdenie vplyvu na ochranu údajov.

NEVYKONÁVA SA

9. **Keď samotné spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu**. Zahŕňa to spracovateľské operácie, ktorých cieľom je umožniť, upraviť alebo odmietnuť prístup dotknutých osôb k službe alebo uzavretiu zmluvy. Príkladom tohto postupu by mohla byť situácia, keď banka preveruje svojich klientov v databáze obsahujúcej informácie o úveroch s cieľom rozhodnúť o tom, či im poskytne úver.

NEVYKONÁVA SA

Článok II

Závery k posúdeniu vplyvu

1. **systematické a rozsiahle hodnotenie osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu**

   Záver s ohľadom na vyššiu uvedené kritéria:
   NEVYKONÁVA SA

2. **spracúvanie vo veľkom rozsahu osobitných kategórií údajov alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky**

   Záver s ohľadom na vyššiu uvedené kritéria:
   NEVYKONÁVA SA

3. **systematické monitorovanie verejne prístupných miest vo veľkom rozsahu**

   Záver s ohľadom na vyššiu uvedené kritéria:
   NEVYKONÁVA SA

ZÁVER:

S ohľadom na rozsah naplnených kritérií a vyššie uvedených bodov prevádzkovateľ v konkrétnych podmienkach rozhodol, že k vykonaniu posúdenie vplyvu na ochranu osobných údajov

NEPRISTUPUJE

Žiadna zo spracovateľských činností s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel spracúvania pravdepodobne v konkrétnych podmienkach prevádzkovateľa pravdepodobne nepovedie k vysokému riziku pre práva a slobody dotknutých osôb.

PIATA ČASŤ

Prílohy