

BEZPEČNOSTNÝ PROJEKT

INFORMAČNÝCH SYSTÉMOV NEŠTÁTNEHO ZDRAVOTNÍCKEHO ZARIADENIA

podľa zákona č. 122/2013 Z.z. o ochrane osobných údajov

pre: **SOFTPROGRES s.r.o.**

adresa: **E. Belluša 4**

mesto: **Piešťany**

PSČ: **921 01**

IČO: **36250163**

Bezpečnostný projekt bol vypracovaný na základe údajov poskytnutých objednávateľom

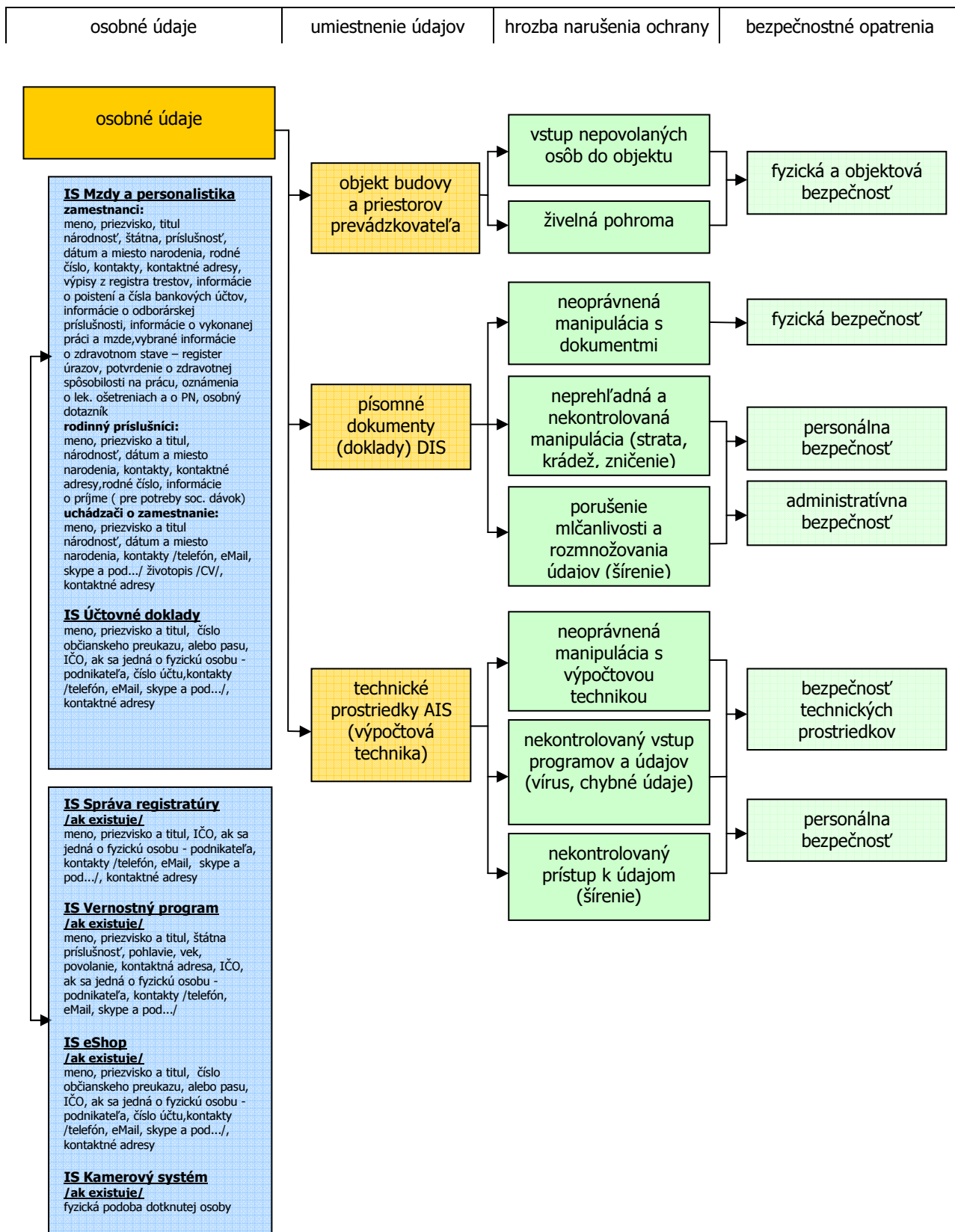
BEZPEČNOSTNÝ PROJEKT INFORMAČNÝCH SYSTÉMOV

podľa zákona č. 122/2013 Z.z. o ochrane osobných údajov

Obsah

1. SCHÉMA BEZPEČNOSTNEJ ŠTRUKTÚRY PREVÁDZKOVATEĽA	2
2. EVIDENCIA INFORMAČNÝCH SYSTÉMOV (IS)	2
3. BEZPEČNOSTNÝ ZÁMER	3
Zoznam informačných systémov podľa spôsobu spracúvania	3
Zoznam osobných údajov spracúvaných v informačných systémoch	3
Stupeň bezpečnosti osobných údajov podľa bezpečnostných štandardov	4
Základné bezpečnostné ciele a minimálne bezpečnostné opatrenia	4
Špecifikácia technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia	4
Vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti.	5
Vymedzenie hraníc určujúcich množinu zvyškových rizík.	5
4. ANALÝZA BEZPEČNOSTI INFORMAČNÉHO SYSTÉMU	6
Kvalitatívna analýza rizík.	10
5. POUŽITIE BEZPEČNOSTNÝCH ŠTANDARDOV.	12
6. VZŤAH BEZPEČNOSTNÝCH OPATRENÍ VYHLÁŠKY č. 164/2013 Z.z. a BPIS	15
7. BEZPEČNOSTNÉ SMERNICE, POUČENIA, ZMLUVY A FORMULÁRE	18

1. SCHÉMA BEZPEČNOSTNEJ ŠTRUKTÚRY PREVÁDZKOVATEĽA



2. EVIDENCIA INFORMAČNÝCH SYSTÉMOV (IS)

Príloha č. 1 obsahuje evidenciu používaných IS v zmysle § 43 zákona 122/2013 Z.z.

(Na každú poslednú stranu evidenčného listu IS je potrebné doplniť dátum začatia spracovania osobných údajov a podpis. Napríklad: v **IS Mzdy a personalistika** to bude dátum vytvorenia prvého pracovnoprávneho vzťahu, alebo dátum začatia prípravy takéhoto vzťahu, v **IS Účtovné doklady** to bude dátum začiatku podnikania.)

3. BEZPEČNOSTNÝ ZÁMER

Zoznam informačných systémov podľa spôsobu spracúvania

Prevádzkovateľ používa na svoju činnosť:

- Automatizovaný informačný systém (ďalej: "AIS") - prostriedky výpočtovej techniky obsahujúce údaje uložené na pamäťových nosičoch.
- Dokumentárny informačný systém (ďalej: "DIS") - manuálne alebo výpočtovou technikou vytvorené písomnosti a listiny používané na spracúvanie osobných údajov.

Zoznam osobných údajov spracúvaných v informačných systémoch

Prevádzkovateľ spracúva v jednotlivých IS nasledujúce osobné údaje:

V **IS Mzdy a personalistika** aj osobitné kategórie osobných údajov a to hlavne z dôvodu evidencie rodných čísel.

U zamestnancov (aj bývalých) sa spracovávajú údaje:

meno, priezvisko a titul, národnosť, štátna príslušnosť, dátum a miesto narodenia, rodné číslo*, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy, výpisy z registra trestov, informácie o poistení a čísla bankových účtov, informácie o odborárskej príslušnosti, informácie o vykonanej práci a mzde, vybrané informácie o zdravotnom stave – register úrazov, potvrdenie o zdravotnej spôsobilosti na prácu, oznámenia o lek. ošetreniach a o PN, osobný dotazník

O rodinných príslušníkoch zamestnancov sa spracovávajú údaje:

meno, priezvisko a titul, národnosť, dátum a miesto narodenia, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy, rodné číslo*, informácie o príjme (pre potreby soc. dávok)

O uchádzačoch o zamestnanie sa spracovávajú údaje:

meno, priezvisko a titul, národnosť, dátum a miesto narodenia, kontakty /telefón, eMail, skype a pod.../, životopis /CV/, kontaktné adresy

V **IS Účtovné doklady** osobné údaje bez osobitných kategórií:

meno, priezvisko a titul, číslo občianskeho preukazu, alebo pasu, IČO, ak sa jedná o fyzickú osobu - podnikateľa, číslo účtu, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy

V **IS Správa registratúry** osobné údaje bez osobitných kategórií: Jedná sa hlavne o evidenciu prijatej a odoslanej korešpondencie:

meno, priezvisko a titul, IČO, ak sa jedná o fyzickú osobu - podnikateľa, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy

V **IS Vernostný program** spracúva aj osobitné kategórie osobných údajov hlavne z dôvodu evidencie pohlavia a veku. **Na spracovanie týchto údajov je nutný súhlas dotknutej osoby:**

meno, priezvisko a titul, štátna príslušnosť, pohlavie, vek, povolanie, kontaktná adresa, IČO, ak sa jedná o fyzickú osobu - podnikateľa, kontakty /telefón, eMail, skype a pod.../

V **IS eShop** osobné údaje bez osobitných kategórií:

meno, priezvisko a titul, IČO, ak sa jedná o fyzickú osobu - podnikateľa, číslo účtu, kontakty /telefón, eMail, skype a pod.../, kontaktné adresy

Infomácia zo stránky úradu:

„Vernostné programy“, ako informačné systémy osobných údajov

Na spracúvanie osobných údajov na účely vernostných programov slúžiacich na odmeňovanie vernosti zákazníkov je potrebný súhlas dotknutej osoby, konkrétneho zákazníka. V tejto súvislosti dávame do pozornosti potrebu registrácie informačného systému osobných údajov, ktorý je prevádzkovaný v súvislosti s vernostným programom podnikateľa v prípade, ak tento nepodlieha dohľadu zodpovednej osoby.

„E - shopy“, ako informačné systémy osobných údajov

Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov neobsahuje náležitosti týkajúce sa spracúvania osobných údajov, a teda nie je naplnená podmienka podľa § 34 ods. 2 písm. d) zákona. E - shop, ako informačný systém osobných údajov, je potrebné prihlásiť na registráciu, ak nepodlieha dohľadu zodpovednej osoby

tieto údaje prevádzkovateľ spracováva v aplikačnom softvéri a v dokumentoch za účelom:

- vedenia účtovníctva
- vedenia personálnej a mzdovej agendy zamestnancov
- vedenia registratúry /najmä evidencia došlej a odoslanej pošty/
- evidencie a správy vernostného programu
- evidencia a správa elektronických objednávok

Stupeň bezpečnosti osobních údajů

Informačné systémy prevádzkovateľa patria medzi systémy, ktoré s nimi prichádzajú do kontaktu, medzi málo ohrozené, pretože s nimi majú osôb a vzhľadom na povinnosti stanovené zákonom č. 180/2018 Z.z. o ochrane.

Pre stupeň bezpečnosti osobných údajov je potrebné sa inšpirovať stupňom ochrany "Vyhradené" pre ochranu osobných údajov a bezpečnosť aplikovať tieto vyhlášky, je to však jediná ucelená koncepcia, ktorá stanoví' rozumný pomer medzi doporučovanými štandardmi a bezpečnosťou.

Bezpečnostný projekt bol zostavený na základe platných a účinných predpisov, nariadení a vyhlášok:

- Metodický pokyn Ministerstva vnútra Slovenskej republiky č. M 1/2004, ktorým sa ustanovujú pravidlá Ministerstva financií Slovenskej republiky č. 132 Z. z. o štandardoch práce v štátnej správe
- STN ISO/IEC 27001 Informačná bezpečnosť, Zabezpečovacie techniky, Informačná bezpečnosť
- STN ISO/IEC 27002 Informačná bezpečnosť, Zabezpečovacie techniky, Informačná bezpečnosť
- Zákon č. 215/2004 Z. z. o štandardoch práce v štátnej správe
- Vyhláška č. 453/2007 Z. z. o štandardoch práce v štátnej správe
- Vyhláška Národného bezpečnostného úradu č. 1/2007 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. 2/2007 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. 3/2007 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti

Základné bezpečnost

Pri stanovení základných prihladnutím na v praxi informačných systémov vyhlášky a medzinárodné predchádzajúcej v

Bezpečnostné ciele pre

- a) zamedziť vstupeň do objektu prevádzkovaného
- b) minimalizovať množstvo údajov, ktoré sa zhromažďujú, alebo znížiť rozsah použitia týchto údajov na účely pohromy
- c) ochrániť osobné údaje, ktoré neoprávneným osobám nemajú byť zverejnené
- d) vytvoriť systém, ktorý zabezpečí, aby údaje boli chránené pred nekontrolovaným používaním údajov
- e) zabezpečiť ochranu osobných údajov pred zneužitím na iný účel, ako boli spracované

Špecifikácia technických opatrení na zabezpečenie ochrany osobných údajov

- a) Fyzická ochrana AIS:
- Realizácia vhodných opatrení na ochranu a monitoringu vstupných dvierok, ktoré umožnia prístup len prevádzkovateľovi.
 - Vymenenie prevádzkovateľa technickými zariadeniami na bezpečnosť a pamäťových nosičov a zabezpečenie ich fyzického ničenia.
- b) Bezpečnosť informácie AIS:
- Použitie vhodných informáčných systémov na ochranu prostriedkov (kľúčov, hesiel, kariet) prístupných k AIS.
 - Ochrana prístupových údajov AIS.
 - Použitie vhodných opatrení na zabezpečenie stability systémov, ako aj na zníženie rizika poruchy elektrickej siete.
 - Použitie vhodných opatrení na ochranu počítačových vírusov.
 - Použitie vhodných opatrení na zabezpečenie prístupových práv k jednotlivým zdrojom AIS.
 - Zabezpečenie AIS riadne ukončený a aby pre ďalšie osoby nebol AIS prístupný.

4. ANALÝZA BEZPEČNOSTI INFORMÁCIÍ

Hodnotenie stavu bezpečnosti priestorov

FYZIKÉ A ORGANIZAČNÉ PARAMETRE (ďalej len prevádzkovateľ)

SOFTPROGRES, s.r.o. je spoločnosť poskytujúca služby v oblasti počítačových informačných systémov a neštátnych zdravotníckych zariadení. Spoločnosť pôsobí v odbore IT, hlavne na poli informačnej bezpečnosti, zabezpečenia dát a počítačových systémov.

Prevádzkovateľ vykonáva svoju činnosť v priestoroch 4 poschodovej budovy na ulici E. Belluša 4, 921 01 Piešťany.

Priestory sú vo vlastníctve prevádzkovateľa.

Priestory sú umiestnené na prízemí.

Spoločnosť na svoju činnosť využíva priestor o celkovej výmere 150 m².

Pozostáva celkovo z 8 miestností, z ktorých 4 sú vybavené počítačovým systémom s internetom a tiskárkami.

Bezpečnostné dvere priamo z ulice sú vybavené alarmom, ktorý je vybavený telefónnym hlásičom. Alarm nie je pripojený na žiadny centrálny systém.

Spoločnosť je vybavená kamerovým systémom, ktorý sleduje okolia vstupných dverí.

Z pohľadu fyzickej odolnosti priestorov je priestor považovaný za bezpečný priestor.

Priestory spoločnosti sú v podstatnej miere chránené kamerovým systémom.

Majetok je poistený pre prípad požiaru.

Priestory sú vybavené na ochranu pred krádežou počítačového prístroja.

Štruktúra pracovníkov spoločnosti:

Konateľ spoločnosti

Hotline - Konzultant spoločnosti

Programátor spoločnosti

Pomocný pracovník spoločnosti

Mzdový účtovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

Pracovník spoločnosti

AUTOMATIZOVANÝ INFORMAČNÝ SYSTÉM

Spoločnosť neuskutočňuje žiadne automatizované systémy.

Zákazníci spoločnosti majú možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Prevádzkovateľ má možnosť kontaktovať spoločnosť cez e-mail.

Zoznam využívaných IS

Názov IS	Zmena hesla
IS Účtovné daňové	1 rok
IS Mzdy a platby	1 rok
IS Registratúra	1 rok
IS Kamerový systém	1 rok
IS prístupných verejných	1 rok
IS Vernostný program	>6

Údaje do IS sú zasielané elektronicky, alebo sú zasielané poštovou zásilkou.

Prevádzkovateľ používa na svojich počítačoch operačný systém Windows XP, Windows 7 a Linux.

Vstup do operačného systému je chránený heslom.

Počet počítačov s osobnými údajmi v spoločnosti: 4
Počet médií (USB kľúčov, externých pevných diskov) s osobnými údajmi: 4

Prevádzkovateľ má vytvorenú počítačovú sieť.
Ako server je vyčlenený samostatný počítač s dvoma pevnými diskami a dvoma zálohovacími jednotkami.
3 x Linux, 1 x Win XP a 1 x Win7.
Jedno na zálohovanie, druhé na testovacie účely.
Seraery sú umiestnené v samostatnej miestnosti a od siete sú oddelené firewallom.

Pripojenie na internet je zrealizované optickou sieťou, prostredníctvom spoločnosti OTE Slovensko.

V priestoroch prevádzkovateľa je k dispozícii Wi-Fi sieť.

Obsluha informačného systému je zabezpečená v priestoroch spoločnosti.

Seraery, switch a routery vybavené sú zálohovacím zdrojom (UPS - Uninterrupted Power Supply).

Na všetkých počítačoch je nainštalovaný antivírusový program ESET SMART SECURITY, ktorého súčasťou je aj ochrana dát.

Obsluha AIS zálohuje údaje z počítačov a serverov.
Programátori majú povinnosť pravidelne kontrolovať priebeh zálohy.
na externý NAS Synology.
domáceho trezoru konajú sa zálohy.

Zálohové médiá sú uložené v samostatnej miestnosti.

Pri poruche počítačov alebo serverov príde technik do priestorov spoločnosti.
opráv zasielame techniku na opravu.

V prípade potreby likvidácie dokumentov spoločnosť používa bezpečné médiá používa prevádzkovateľ nasledujúcu metódu likvidácie dokumentov.

DOKUMENTÁRNE SPRACOVANIE Zoznam neautomatizovaných

Názov IS	Poznámka
IS Účtovné doklady	
IS Mzdy a personál	
IS Registratúra	
IS Vernostný	Skrinka

Na likvidáciu dokumentov prevádzkovateľ skartovacia metóda likvidácie dokumentov.

Na úschovu dokumentov prevádzkovateľ vyhradzuje priestor, ktorý sú uzamknuté v osobitnej miestnosti.

ZHRNUTIE - OPATRENIA A

Celkový počet oprávnených osôb na prácu s

Spoločnosť nemá 20 a viac oprávnených osôb, ktorých je zodpovednou osobou je štatutár zariadenia /konateľ/ a na zariadenia zodpovednej osoby na úrade. Zároveň podľa informácií zodpovednú osobu dohľadom.

Spoločnosť spracúva osobné údaje a je povinná plniť svoju povinnosť registrovať svoje informačné systémy.

Registrovať musí len IS Vernost
/potrebné formuláre sú súčasťou BPIS/

Spoločnosť má povinnosť, nakladať s informáciami, ktoré sú pripojené k internetu vytvorením a viesť evidenciu svojich informačných

Ďalšou významnou povinnosťou zamestnávateľa sú právnených zmluvných zmluvných agendu, alebo účtovníctvo spracúva externé údaje, ktoré sú súčasťou BPIS/. Činnosťou zmluvy.

Kamerový systém - len pre systém prístupný verejnosti (V prípade, že priestor nie je prístupný verejnosti, nie je potrebné vypracovať zoznam, ale nevzťahujú sa naň ustanovenia zákona 122/2013 Z.z.)

Opatrenie

Pri vstupe do priestorov
Pozor! Priestor je monit

[illegible]

Berieame na vedomie [redacted] priestor pri [redacted] monitorovať len na účely ochrany verejného poriadku, ochrany bezpečnosti štátu, ochrany majetku alebo zdravia, a to len vtedy, ak [redacted] monitorovaný priestor je prevádzkovateľ povinný zreteľne [redacted] zvuk zaznamenaná na nosič informácií. Označenie [redacted] je osobitný zákon. Vyhotovený záznam možno využívať [redacted] o priestupkoch, ak osobitný zákon neustanovuje inak.

Prevádzkovateľ b[redacted]ovaných osôb na 20 a viac podľa §23 odsek 2 zákona 122/2016 o spracúvaní výkonom dohľadu písomne poveriť zodpovednosťou za dodržiavanie zákonných ustanovení pri spracúvaní súkromných údajov inej osoby vzniká povinnosť ohlásenia tejto povinnosť na ochranu osobných údajov.

Berieme na v zásielky, ktoré obsahujú a posilať doporučenou zásielkou.

Berie me na v [redacted] ord bezpečnosti informá [redacted] ch PC zabezpečujú OS na báze
technológie [redacted] 2,Vista,7,8, ktor [redacted] hesla ochranu proti
neoprávnené [redacted]
Žiaľ ani tento sp [redacted] ného PC.
Z týchto skutočnos [redacted] pečiť, len ak sa k IS a jeho
komponentom nedos [redacted] objektová a personálna bezpečnosť
IS ako prioritná.

Opatrenie

Zabezpečení minimální velkosti a

Termin:

podpis

Kvalitatívna analýza rizík.

Zoznam rizík v objektovej bezpečnosti

- a) Strata alebo odcudenie kľúčov od
rozsah rizika: významné
(na hodnotenie rozsahu rizika: významné, 4-veľké)
alternatívne opatrenia:
▪ uzamykanie vstupných dverí
▪ zabezpečenie sebaobmedzenia výmery
b) Neuzamknutie vstupných dverí
rozsah rizika: významné
alternatívne opatrenia:
▪ otváranie dverí z vnútornej strany miestnosti
c) Prekonanie mechanického zabezpečenia
rozsah rizika: ojedinelé
alternatívne opatrenia:
▪ vyšší stupeň ochrany
▪ zálohovanie údajov

Zoznam rizík v dokumentárnom j...

- d) Šírenie informácií poskytnutých v súvislosti s týmto rozhodnutím
rozsah rizika: výzva k šíreniu informácií
alternatívne opatrenia:
▪ záväzok na ochranu informácií
▪ komisiou vykonaná kontrola informácií
- e) Šírenie informácií poskytnutých v súvislosti s týmto rozhodnutím
rozsah rizika: neregulované šírenie nepotrebnými písomnosťami
alternatívne opatrenia:
▪ vyhraď si priestor na nepotrebných písomností a znehodnotenie
dokumentov (zrušenie, zničenie, skartácia) na základe rozhodnutia jednej osoby
▪ vybať a vyhodnotiť potrebné opatrenia na zvládanie rizika
- f) Odcudzenie dôverných informácií poskytnutých v súvislosti s týmto rozhodnutím
rozsah rizika: malé množstvo informácií
alternatívne opatrenia:
▪ uzamykanie písomností
▪ upratovanie informácií osobnými údajmi

Automatizovaný

Riziká prieniku

- a) Prienik do priestoru, v ktorom sa nachádza obrazovka počítača, ak osoba, ktorá má prístup k obrazovke počítača, že nepovolaná osoba má prístup k obrazovke počítača. Rozsah opatrení na zabezpečenie alternatívneho prístupu k obrazovke počítača:
- zabezpečenie prístupu nepovolanej osobe
 - zabezpečenie prístupu mimo zorného poľa
- b) Odcudenie obrazovky počítača. Rozsah opatrení na zabezpečenie alternatívneho prístupu k obrazovke počítača:
- zabezpečenie prístupu nepovolanej osobe
 - uzamknutie obrazovky počítača na to určenej miestnosti
- c) Strata, alebo poškodenie obrazovky počítača alebo na iné pracovisko. Treba vziať na vedomie, že obrazovka počítača obsahuje údaje.

- používanie doporučených postupov
- d) Sprístupnenie pevného disku alebo lokálnej počítačovej siete osobami z vonkajšieho prostredia
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - definovanie prístupových práv
 - definovanie prístupov
- e) Sprístupnenie pevného disku pripojeného na internet osobami, ktoré sú z vonkajšieho prostredia
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - konfigurácia prístupových práv bezpečnostný stupeň
 - použitie antivírusovej ochrany
 - použitie ochrany pred sieťovými útokmi alebo zariadení (FireWall)

Riziká straty osobných údajov

- a) Narušenie objektovej bezpečnosti systémom alebo systémom zvonka
 - rozsah rizika: významne
 - alternatívne opatrenia:
 - zvýšenie objektovej bezpečnosti
 - záloha na prenosnom médiu
- b) Zničením počítača alebo jeho zariadení katastrofou, požiarom alebo zatopením
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - záloha na prenosnom médiu
- c) Odcudzenie počítača alebo jeho zariadení
 - rozsah rizika: veľké
 - alternatívne opatrenia:
 - zvýšenie fyzickej bezpečnosti
 - záloha na prenosnom médiu uložená mimo priestoru počítača
- d) Poškodenie počítača alebo jeho zariadení mechanickou závadou
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - pravidelná kontrola počítača
 - záloha na prenosnom médiu
- e) Poškodenie pevného disku elektrickým napájaním
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - použitie stabilizátorov napájania
- f) Poškodenie počítača alebo jeho zariadení počítačových vírusov
 - rozsah rizika: malé
 - alternatívne opatrenia:
 - pravidelná aktualizácia programov
 - izolácia s podozrivými médiami
- g) Poškodenie počítača alebo údajových štruktúr počítačovej siete neoprávneným prístupom iných používateľov počítačovej siete
 - rozsah rizika: veľké
 - alternatívne opatrenia:
 - definovanie prístupových práv
 - definovanie prístupov
- h) Poškodenie počítača alebo údajových štruktúr počítačovej siete neoprávneným prístupom iných používateľov počítačovej siete
 - rozsah rizika: veľké
 - alternatívne opatrenia:
 - definovanie prístupových práv
 - definovanie prístupov

rozsah rizika: veľký stupeň
bezpečnostný stupeň firewallu

5. POUŽITIE BEZPEČNOSTNÝCH

ŠTANDARDNÉ POŽIADAVKY NA OBJEKTY

Východiskom pre stanovenie štandardov je vyhodnotenie objektivej bezpečnosti a v kapitole 3) uvedené zákony, vyhlášky a schválený kombináciou opatrení fyzickej a objektivej bezpečnosti. Získovateľ a sú čiastočne odvodené od štandardov uvedených v kapitole 3) a od zásad, ktoré používajú poisťovne a verejná správa.

- a) Vstup do objektu a pohyb v ňom musí byť umožnený prevádzkovateľ, alebo vlastník budovy.
- b) Určenie spôsobu a formy ochrany objektu pred poškodením prevádzkovateľom.
- c) Objekt minimálne ľahko prístupný pre porobetonárskych robotníkov.
- d) Okná, zabezpečené mrežami, ochrannou fóliou, ak sú objekt na voľnom terénu, alebo ak sú ľahko prístupné pre robotníkov. Každý z týchto prvkov (strecha, bleskozvod, mreže alebo fólie) je na základe posúdenia bezpečnosti prevádzkovateľa zabezpečením proti preniknutiu do objektu a na okolie a faktory, ktoré môžu vzniknúť.

Napríklad:

- budova je 24-hodinovo obsadená
 - sídlo prevádzkovateľa je v budove
 - okná sú orientované na juhovýchod
- e) Dvere drevené, drevotriekové, s výškou 2,1 m, s hrúbkou 100 mm, s hmotnosťou 150 kg.
- f) Dodržanie zásady, že pri snahe o neoprávnený vstup musí byť použitý špeciálny narušiteľ prekonať dve prekážky.
- Napríklad:
- prekonať dvere priestorov s informačným systémom.
 - preniknúť do priestorov s informačným systémom cez dvere priestorov s informačným systémom.
 - prekonať dvere priestorov s informačným systémom.
- g) Uzamykateľné, ktoré sú na úschovu kľúčov, ktoré sú v nich obsiahnuté, ktoré obsahujú osobné údaje. Kľúče, ktoré nie sú uzamykateľné, musia byť uzamykateľné fyzickej ochrane priestorov strážnou službou. Uzamykateľné dvere do miestností s osobnými údajmi musia byť uzamykateľné bezpečnostným zámkom s osobnými údajmi.
- h) Pridelovanie, ktoré je evidenciou kľúčov do zámkov, ktoré sú v nich obsiahnuté, ktoré stanovuje vlastník (prevádzkovateľ) zariadení.

Nadštandardná

- a) Použitie bezpečnostnej siete.
- b) Použitie bezpečnostných výstražných svetiel so žltou alebo červenou záliatou betónovou zmesou.
- c) Použitie uzamykacieho systému.
- d) EPS (elektrická bezpečnostná sieť).
- e) Monitorovanie priestoru.
- f) Poplašné svetlo, ktoré je viditeľné vo vonkajšom priestore.
- g) EZS (Elektronické zabezpečenie priestoru) s možnosťou náhodného pripojenia na políciu.

ŠTANDARDNÁ BEZPEČNOST DISKOV

Východiskom sú štandardy spracovania písomností podľa zákona č. 453/2007 Z.z. o administratívnej komunikácii, ktorým sa ustanovujú všeobecné štandardy spracovania administratívnej komunikácie. Všeobecné štandardy sú čiastočne od štandardov určených vyhláškou pre písomnosť, ktoré sú čiastočne od zvyklostí vo svojej správe:

Štandardy pe

- a) Pre persónu, ktorá je v pracovnej zmluve viazaná povinnosťou poskytnúť údaje a zmluvne dohodnuté záväzky na ochranu spoločnosti.
- b) Súčasťou výkonu práce je povinnosť zachovávať spoľahlivosť pri dodržiavaní bezpečnostných pravidiel.
- c) Povinnosť zachovávať spoľahlivosť je v pracovnej zmluve viazaný povinnosťou

- d) Všetci zamestnanci majú uloženú povinnosť dodržiavať pravidlá, ktoré zabezpečujú zistení neoprávnenej manipulácie alebo iných porušení bezpečnosti a zistení porušení pravidiel práce.

Nadštandardná personálna bezpečnosť

- a) Pri získavaní osobných údajov sa uplatňuje zásada komisionálnosti (prítomnosť komisie).
- b) Prevádzkovateľ používa bezpečnostný systém na uchovávanie údajov (manuál). Každý zamestnanec písomne potvrdzuje, že dodržiava všetky požiadavky uvedené v bezpečnostnom systéme.
- c) Osoba zodpovedná za ochranu údajov (prevádzkovateľ) vykonáva pravidelné kontroly stavu bezpečnosti a evidencií.

Štandardy administratívnej

Nové záznamy, aktualizácia

- a) Zisťovanie a evidovanie osobných údajov z pohľadu bezpečnosti ukladajú pracovné povinnosti. Pracovník musí byť schopný zistiť a evidovať. Stanovujú sa pravidlá uchovávaní osobných údajov. (Bezpečnostná smernica č.1 b)
- b) Záznamy a zmeny v písomnostiach musia byť iba oprávnené osoby s písomným potvrdením.
- c) Jednotlivé písomnosti musia byť uchované tak, aby bolo ich vypadávanie pri bežnej práci so záznamami jednoduché.

Úschova písomností

- a) Písomnosti obsahujúce údaje o bezpečnosti sa ukladajú do bezpečných (kľúč, kontajnerov, zásuviek kancelárskych alebo do iných uzamykateľných) na uzamykateľnosť zariadení na účely ochrany. Toto je záväzná v prípade zariadení priestorov stráženou službou, alebo v prípade dverí zámkom s bezpečnostným kľúčom a bezpečnostným kovaním.

Prenášanie písomností

- a) Písomnosti je možné prenášať v obale, s otvorom prelepým lepiacou páskou.
- b) Písomnosti prenášajú len oprávnené osoby.
- c) V prípade, že prevádzkovateľ nemá dôvod poškodenia u doručujúcej osoby, musí byť doručenie potvrdené.
- d) Odovzdanie písomností musí byť zaznamenané v príslušnej evidencii.

Preprava písomností

- a) Písomnosti sa môžu prepravovať poštovou zásielkou, alebo kuriérom.
- b) O písomnostiach musí byť zaznamenané v príslušnej evidencii.

Kopírovanie a uchovávanie písomností

- a) Rozmnožovanie opakovaná tlač dokumentu, vytváranie systému, vyhotovovanie fotokopíí písomností.
- b) Rozmnožovanie môže len oprávnená osoba.

Vypožičiavanie

- a) Písomnosti sa môžu vypožičať len oprávnenej osobe.
- b) Záznamy a originály písomností sa môžu vypožičať alebo sprístupniť len osobám a iným subjektom, ktoré sú oprávnené podľa DIS.
- c) Vypožičanie písomností musí byť zaznamenané v príslušnej evidencii.

Evidencie písomností

- a) Prevádzkovateľ eviduje písomnosti, ktoré môžu byť v listinnej alebo počítačovej forme
 - evidencia zamestnancov a ich pracovných pomerov
 - evidencia vypožičiavania a poskytnutia
 - evidencia písomností zaslaných a prijatých
 - evidencia pridelených

Archivácia písomností

- a) Písomnosti, ktoré nie sú určené na okamžitú oddelenie, za podmienok štandardnej

Skartácia písomností (likvidácia)

- a) Písomnosti sa likvidujú spálením, alebo spálením písomností zodpovedných za spracovanie zariadení na médiách.

Zistenie neoprávnenej manipulácie

- a) Osoba zodpovedná za kontrolu písomností v rozsahu stanovenej
- b) Oprávnená osoba poverená za polrok fyzickú inventarizáciu vypožičaných, písomností evidencie.

Nadštandardná administrácia

- a) Na prácu s písomnosťami
- b) Písomnosti sú uschované
- c) Práca s osobnými údajmi stanovuje pravidlá na používanie, odkazovanie a skartáciu

ŠTANDARDNÉ POŽIADAVKY NA BEZPEČNOSŤ AIS

Východiskom pre stanovenie hardvérovej (HW) a softvérovej (SW) bezpečnosti informačných systémov sú overené požiadavky na vyhlášku č. 117/2002 Z. z. a v kapitole 3. - "Stupeň bezpečnosti osobných údajov" a v kapitole 3. - "Stupeň bezpečnosti osobných údajov".

- a) Použitie operacného systému s vyšším stupňom bezpečnosti možného
- b) Použitie antivírusového programu a správne nastavenie brány FireWall.
- c) Použitie bežných databázových systémov (ORACLE, PARADOX, ACCES), pričom za systémy s vyšším stupňom bezpečnosti databázy renomovaných firiem
- d) Štandardné nastavenie počítačového programu zadaním prístupového hesla. Heslo musí obsahovať čísla aj písmená (malé aj veľké) a dĺžka hesla, by sa malo toto v
- e) V prípade potreby pomocou prístupových práv konfigurovať systém k osobným údajom má
- f) Na zabezpečenie integrity databázových systémov je nevyhnutné každé údaje na prenosné médiá. V prípade pamäťových nosičov je vhodné neustále s IS. V prípade pamäťových nosičov je vhodné používať súbory méd. 1 mesiaca formátovať a kontrolovať, že na danom nosiči je permanentne, že v prípade zničenia, alebo neopraveného
- g) V súvislosti s tým minimálne 1x za rok zálohovať všetky databázové nosič (na

- ...e zaden...
nú lokalitu...
tačového...
o urč...
...e užívateľov pomoc...
...ý disk sa uplatň...
...émov voči ekono...
VYHLÁŠKA
...dkami fyzickej povahy
...zábranných prost...
...technických...
...stény, zábr...

VYHLÁŠKA

Príklady fyzickej povahy

- [illegible]

- vaných prostredníctvom
...
... pamäťových nosičov, lebo v prípade
...
...
... prístupu dochádza
...
... IS, pravidla

ch osôb

- autorizácia oprávnených používateľov systému.
 pri prihlasovacom hesle
 jednotlivých oprávnených používateľov systému.
 na úrovni jednotlivých používateľov. Na úrovni
 kolízne stavy.

- elektronickej pošte a v iných súboroch
alebo z dátových nosičov.

- 4.2 Ochrana pred nevyžiadanou komunikáciou
 - => *Riešené v BPIS - Bezpečnostná smernica č.7*
- 4.3 Používanie legálneho a prevádzkového softvéru
 - => *Riešené v BPIS - Bezpečnostná smernica č.7*
- 4.4 Pravidlá sťahovania súborov z verejných zdrojov
 - => *Riešené v BPIS - Bezpečnostná smernica č.7*

5. Siet'ová bezpečnosť

- 5.1 Kontrola, obmedzenie a monitorovanie prístupu k dátam sú spracúvané osobné údaje s verejným prístupom
 - => *Riešené v BPIS*
- 5.2 Evidencia všetkých miest, odkiaľ sa prístup k dátam vrátane verejného prístupu realizuje
 - => *Riešené v BPIS*
- 5.3 Ochrana vonkajšieho siete prostredníctvom nástrojov zabezpečenia (napr. firewall).
 - => *Riešené v BPIS - Bezpečnostná smernica č.7*
- 5.4 Pravidlá prístupu do verejnej siete
 - (napr. zamedzenie pripojenia zo zahraničia)
 - => *Riešené v BPIS + Bezpečnostná smernica č.7*
- 5.5 Ochrana proti iným hrozbám ako sú vírusy, škodlivý softvér (napr. hackerský útok)
 - => *Neriešené v BPIS, riešenie vírusov a hackerov a cenovo únosné sú len štandardné opatrenia*

6. Zálohovanie

- 6.1 Test funkcionality zálohovania
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 6.2 Vytváranie zálohovania s periodicitou
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 6.3 Test obnovy dát z zálohy
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 6.4 Bezpečné uloženie záloh
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*

7. Likvidácia osobných údajov

- 7.1 Bezpečné vymazanie údajov
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 7.2 Zariadenie na likvidáciu údajov
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*

8. Aktualizácia

- 8.1 Aktualizácia softvéru
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 8.2 Aktualizácia hardvéru a aplikačného vybavenia
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*

Organizačné

1. Personál

- 1.1 Písomná informácia o povinnostiach zamestnancov v oblasti prevádzkovej operácie s osobnými údajmi
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 1.1.1. Poučenie zamestnancov o povinnostiach a zodpovednosti za ich porušenie
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*
- 1.1.2. Prístup k dátam musí mať konkrétna oprávnená osoba prístup na účel
 - => *Riešené v BPIS - Bezpečnostná smernica č.8*

- 1.1.3. Určenie postupov, ktorými sa zabezpečí bezpečnosť a uplatňovanie právnych údajov
=> *Riešené v BPIS - Bezpečnosť*
- 1.1.4. Vymedzenie zakázaných postupov
=> *Riešené v BPIS - Bezpečnosť*
- 1.1.5. Vymedzenie zodpovednosti za porušenie
=> *Riešené v BPIS - Bezpečnosť*

1.2 Poučenie oprávnených osôb o pravidlách spracúvania a súvisiacich právach a povinnostiach (v rámci priestorov)
=> *Riešené v BPIS + Bezpečnosť*

1.3 Písomné poverenie zodpovedajúce zákona, ktoré obsahuje osobné údaje prostredníctvom 20 alebo viac osôb
=> *Riešené v BPIS for* *... ktoré sú súčasťou BPIS*

1.4 Oboznámenie oprávnených osôb s bezpečnostnými smernicami
=> *Riešené v BPIS + Bezpečnosť* *... č. 1*

1.5 Vzdelávanie oprávnených osôb v oblasti, oblasti
=> *Riešené v BPIS + Bezpečnosť*

1.6 Postup pri ukončení pracovnej doby, vrátane zodvzdanie pridelených aktív, zrušenie prístupov k informáciám (v rámci priestorov alebo zmluvnej povinnosti mlčanlivosti)
=> *Riešené v BPIS + Bezpečnosť*

2. Vedenie zoznamu aktív

2.1 Pre malých prevádzkovateľov, ktorí majú všetky aktíva, t.j. počítače, iné HW, SW produkty
=> *Neriešené v BPIS*

3. Riadenie prístupu k osobným údajom

3.1 Kontrola vstupov do chránených priestorov prostredníctvom technických a personálnych opatrení
=> *Neriešené v BPIS* *... prevádzkovateľov prívětní*

3.2 Správa kľúčov, vrátane kľúčov, bez kľúčov (v rámci priestorov kľúčov)
=> *Riešené v BPIS* *... smernica č. 6*

3.3 Pridelovanie prístupov
=> *Neriešené v BPIS*

3.4 Správa hesiel
=> *Riešené v BPIS*

3.5 Vzájomné informácie o nehody, dočasnej pracovnej neschopnosti, ukončení
=> *Riešené v BPIS*

4. Organizácia spracúvania údajov

4.1 Pravidlá spracúvania údajov v chránených priestoroch
=> *Riešené v BPIS* *... bezpečnostná smernica*

4.2 Nepriame spracúvanie oprávnenej osoby v chránených priestoroch, v ktorom nachádzajú aj iné ako oprávnené osoby
=> *Riešené v BPIS* *... bezpečnostná smernica č. 1*

4.3 Režim spracúvania údajov
=> *Riešené v BPIS*

4.4 Pravidlá spracúvania údajov, ktoré sa také spracúvanie predpokladá
=> *Riešené v BPIS*

4.4.1. Pravidlá spracúvania údajov (napr. listiny, fotografie) mimo chránených priestorov
=> *Riešené v BPIS* *... č. 1.2.3.4.5.6*

- 4.4.2. Pravidlá používania autentičnej spracúvanej informácie v chránených priestoroch a v chránených zariadeniach
=> *Riešené v BPIS - Bezpečnosť informácií*
- 4.4.3. Pravidlá používania prenosných zariadení a zariadení zodpovednosti
=> *Riešené v BPIS - Bezpečnosť informácií*

5. Likvidácia osobných údajov

- 5.1 Určenie postupov likvidácie osobných údajov jednotlivých oprávnených osôb (bezpečnosť informácií, likvidácia dátových nosičov a fyzických nosičov)
=> *Riešené v BPIS - Bezpečnosť informácií (Bod 2. písm. b) a Smernica č.3 (Bod 3.)*

6. Bezpečnostné incidenty

- 6.1 Postup pri ohlasovaní bezpečnostných incidentov a zistených zranení bezpečnostného systému na účel včasného prijatia nápravných opatrení
=> *Riešené v BPIS - Bezpečnosť informácií (Bod 4. písm. b)*
- 6.2 Evidencia bezpečnostných incidentov
=> *Riešené v BPIS - Bezpečnosť informácií*
- 6.3 Postup pri riešení jednotlivých bezpečnostných incidentov
=> *Riešené v BPIS - Bezpečnosť informácií*
- 6.4 Identifikácia, evidencia bezpečnostných incidentov
=> *Riešené v BPIS - Bezpečnosť informácií*
- 6.5 Postupy pri havárii bezpečnostných incidentov (napr. oznamovanie bezpečnostných incidentov)
=> *Riešené v BPIS - Bezpečnosť informácií*
- 6.6 Postup pri poruche bezpečnostného systému (napr. ochrana osobných údajov, oprava oprávovaného počítača)
=> *Riešené v BPIS - Bezpečnosť informácií (Bod 4. písm. b)*

7. Kontrolná činnosť

- 7.1 Kontrolná činnosť je plánovaná na dodržanie bezpečnostných opatrení s určením spôsobu realizácie (napr. prístupov k informačnému systému)
Nakoľko sa jedná o neustále. Oprávnené osoby robia s informačným systémom, bezpečnosť chodu sú zaznamenávané do pr...
=> *Riešené v BPIS - Bezpečnosť informácií*
- 7.2 Informovanie o bezpečnosti (3) ak je u prevádzkovateľa zavedený (rozsah kontroly)
V malej kolektíve, ktorý poriadok kontrol nakoľko malý
=> *Nemajú sa zavádzať*

7. BEZPEČNOSTNÉ SMERNICE, POUČENIA A INŠTRUKČNÉ MANUÁLARE

súčasťou bezpečnostného systému sú:

- smernice AIS č. 7. a 8
- poučenie o bezpečnosti informácií
- zmluva o spracovaní informácií
- zmluva o spracovaní informácií
- evidencia informácií

Za spracovanie a dodržanie

V.....

Vlastnoručný podpis

PRÍLOHA č.1 - EVIDENCIA INFORMÁČNÉHO SYSTÉMU

podľa § 43
o ochrane osobných údajov

I. NÁZOV INFORMAČNÉHO SYSTÉMU
IS Mzdy a personalistika

II. ÚDAJE O PREVÁDZKOVATEĽovi	
Názov prevádzkovateľa	S. J.
Identifikačné číslo organizácie	183
Obec a PSČ	Veľký Štáň 1, 921 01
Ulica a číslo	Belluša 4
Štát	Slovenská republika
Právna forma	Spoločnosť s ručením
Statutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa	
Počet oprávnených osôb	

III. ÚDAJE O INFORMAČNOM SYSTÉME	
Účel spracúvania osobných údajov	Pracovné činnosti priamo súvisiace s mzdovou, personálnou a
Právny základ spracúvania osobných údajov	Zákon o ochrane osobných údajov Zb. Občiansky 33/2007 Z. z. o minimálnom c. 461/2003 Z. z. o sociálnom p 462/2003 Z. z. o náhrade príjmu plnení niektorých zákonov 2004 Z. z. o zdravotnom poisťovníctve zmene a doplnení niektorých zákonov Z. z. o dani z príjmov neskorších predpisov zmene a doplnení niektorých plnení niektorých zákonov v plnení zákona č. 286/1992 Zb. o rozvoji verejného zdravia a o zmene a doplnení pisov ne zdravia pri práci a o zmene a doplnení e a doplnení niektorých zákonov v znení
Okruh dotknutých osôb	Súčasní a bývalí zamestnanci príslušníci, uchádzači o
Zoznam osobných údajov, ktoré sú spracúvané (alebo rozsah spracúvania)	Súčasní a bývalí zamestnanci meno, priezvisko, titul, národnosť, kontakty, identifikátory bydliska, informácie o odborárskych o zdravotnej spôsobilosti na prácu, le
Označenie opatrení na ochranu osobných údajov	rodenia, kontakty, identifikátory bydliska, (k). esto narodenia, kontakty, identifikátory bydliska, súvisiacich s ich pracovnoprávnym vzťahom.

IV. SPRACOVATEĽSKÉ OPERÁCIE

Posk

Tretie strany(prípadne okruh tr. strán)

Právny základ

Zdravotné poisťovne

Zákon č. 592/1992 Sb., o právním jednáních úředních orgánů, na č.
95/2008 Sb., o právním jednáních úředních orgánů v znění neskorších

Sociálna poisťovňa

...predpisov
...a doplnení niektorých

Daňový úrad

Doplňkové dôchodkové sporiťne

... v súlade s predpisom ...

Dôchodkové správcovské spoločnosti

33 Z. z. o sociálnom poistení
34 Z. z. o starobnom dôchodkovom
... skorších predpisov

Orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)

z. Zákonník práce v znení nes o inšpekcii práce a o zm nom zamestnávate ých v zne	82/2005 Z. z. o avia a o zmene a zmene
---	---

Zástupcovia zamestnancov

Zákon...

Ústredie práce, sociálnych
vecí a rodiny

Závěr vyplnění

**Súd, orgány činné v
trestnom konaní**

znení neskorších predpisov zákon č.
predpisov

Exekútor

činnosti (Exekučný poriadok
šších predpisov

iný oprávnený subjekt

Priloga št. 1 k Zakonu o varstvu osebnih podatkov a Zakonu o dostopu do informacij
zakona č. 122/2013 Z. z. o

prístupovanie osobn

Okruh príjemcov

Právní základ

Osobné údaje sú spracované v súlade s § 6 ods. 1 písm. b) zákona č. 595/2003 Z. z. o dani z príjmov, § 6 ods. 1 písm. c) zákona č. 461/2003 Z. z. o sociálnej poisťovni, § 6 ods. 1 písm. e) zákona č. 323/2004 Z. z. o výkone komerčnej správy výkonom komerčnej správy.

č. 595/2003 Z. z. o dani z príjmov
461/2003 Z. z. o sociálnej poisťovni
3/2004 Z. z. o zrušení zákona
zákon

Spôsob zverejnenia

Priloge

Nástenka, reklamný materiál
v rozsahu titul, meno, priezvisko
útvár, miesto výkonu práce
pracovisko a identifikačný
služobných alebo funkčných

ods. 3 zákona č. 122/2013 Z. z. o
ochrane osobných údajov a o zmene a
doplnení niektorých zákonov

Tretia krajina

Právny základ

Prevádzkovač: [REDACTED] prenos osobných

prenos osobných

V. ZAČIAT

ANALÝZA OSOBNÝCH ÚLOH

Odtlačok pečiatky

m, meno a podpis

Orgánu prevádzkovateľa

I. NÁZOV INFORMÁCIE	
IS Účtovné doklady	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (OZ)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	Spoločnosť s ručením obmedzeným
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	Ing. Juraj ZOŇ
Zástupca prevádzkovateľa (ak nie je vymenovaný)	
Počet oprávnených osôb	1
III. ÚDAJE O INFORMÁCIIACH O OSOBNÝCH ÚDAJOCH	
Účel spracúvania osobných údajov	vykonávanie činnosti súvisiace s prevádzkou
Právny základ sprac. osob. údajov	Zákon o ochrane osobných údajov, Zákon č. 180/2014 Z. z. o ochrane osobných údajov a doplnení niektorých zákonov, Zákon č. 122/2013 Z. z. o ochrane osobných údajov a doplnení zákona č. 286/1992 Zb. o slobode informácií a doplnení niektorých predpisov
Okruh dotknutých osôb	Fyzické osoby, Fyzické osoby - podnikatelia, Fyzické osoby - podnikatelia, Fyzické osoby - podnikatelia
Zoznam osobných údajov (alebo rozsah)	meno a priezvisko a titul, IČO, ak sa predkladá, kontakty /telefón, e-mail, facebook, skype a pod.../, identifikácia, údaje vedené v rozsahu zákona o ochrane osobných údajov a doplnení niektorých zákonov
Označenie bezpečnostných opatrení	
IV. SPRACOVATEĽ	
Tretie strany (prípadne okruh tretích strán)	
Sociálna poisťovňa	Príjemní neschválili neskorších predpisov; zákon o sociálnej poisťovni a o zmene a doplnení niektorých zákonov
Zdravotné poisťovne	Príjemní neschválili neskorších predpisov; zákon o zdravotnej poisťovni a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Daňový úrad	Príjemní neschválili neskorších predpisov
Súd, orgány štátnej trestnej moci	Príjemní neschválili neskorších predpisov
iný oprávnený orgán	Všeobecne záväzný právny predpis, zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

I. NÁZOV INFORMAČNÉHO SYSTÉMU	
Kamerový informačný systém - N	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	SO
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	Juraj ZOŇ
Zástupca prevádzkovateľa	je vymenovaný
Počet oprávnených osôb	
III. ÚDAJE O INFORMACIÁCH A OSOBNÝCH ÚDAJOCH	
Účel spracúvania osobných údajov	bezpečnosť prevádzkovateľa.
Právny základ spracúvania osobných údajov	menne a
Okruh dotknutých osôb	z prevádzkovateľa
Zoznam osobných údajov	Fv
Označenie bezpečnostných opatrení	údajov
IV. SPRACOVATEĽSKÉ POSTUPY	
Tretie strany (prípadne prevádzkovateľ osobných údajov)	Právny základ
Prevedenie účelov spracúvania osobných údajov alebo konania o priebehu zákona neustanovených	č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Okruh príjemcov	Právny základ
Prevedenie účelov spracúvania osobných údajov alebo konania o priebehu zákona neustanovených	č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Spôsob zverejnenia	Právny základ
Prevedenie účelov spracúvania osobných údajov alebo konania o priebehu zákona neustanovených	
Tretia krajina	Právny základ
Prevedenie účelov spracúvania osobných údajov alebo konania o priebehu zákona neustanovených	
V. ZAČIATOK SPRACOVANIA OSOBNÝCH ÚDAJOV	

.....
Odtlačok pečiatky

.....
Meno a podpis
štátneho orgánu prevádzkovateľa

I. NÁZOV INFORMAČNÉHO SYSTÉMU	
Kamerový informačný systém - N	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	SO
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	Juraj ZOŇ
Zástupca prevádzkovateľa	je vymenovaný
Počet oprávnených osôb	
III. ÚDAJE O INFORMACIÁCH A OSOBNÝCH ÚDAJOCH	
Účel spracúvania osobných údajov	amestn
Právny základ spracúvania osobných údajov	
Okruh dotknutých osôb	Z
Zoznam osobných údajov	Fyz
Označenie bezpečnostných opatrení	giov
IV. SPRACOVATEĽSKÉ	
Tretie strany (prípadne	Právny základ
Prevádzkovateľ osobných údajov alebo konania o prie	účely zákona neust
	Prístupňovanie osobných
Okruh príjemcov	Právny základ
Prevádzkovateľ osobných údajov alebo konania o pr	pre účely trestn
	dotkutej osoby
Spôsob zverejnenia	Právny základ
Prevádzkovateľ osobných údajov	
	údajov
Tretia krajina	Právny základ
Prevádzkovateľ osobných údajov	krajín
V. ZAČIATOK SPRACOVANIA OSOBNÝCH ÚDAJOV	

.....
Odtlačok pečiatky

.....
meno a podpis
orgánu prevádzkovateľa

I. NÁZOV INFORMÁCIE	
IS Správa registratúry	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	SO
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	Spoločnosť s ručením obmedzeným
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	Juraj ZOŇ
Zástupca prevádzkovateľa	je vymenovaný
Počet oprávnených osôb	
III. ÚDAJE O INFORMACIACH A OSOBNÝCH ÚDAJOCH	
Účel spracúvania osobných údajov	
Právny základ sprac. osob. údajov	doplnení
Okruh dotknutých osôb	Osobné údaje sú sprístupnené pre: Fyzické osoby -
Zoznam osobných údajov (alebo ich kategórií)	adresa, telefónne číslo
Označenie bezpečnostných opatrení	osobných údajov
IV. SPRACOVATEĽ	
Tretie strany (prípadne okruh príjemcov)	Právny základ
Ministerstvo vnútra	č. 395/2002 Z. z. o archívoch a o zákone o spracúvaní osobných údajov v znení niektorých zákonov
iný oprávnený subjekt	č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Okruh príjemcov	doplnení niektorých
Osobné údaje sú sprístupnené len osobe poverenej orgánom štátnej správy na účely výkonu kontroly..	
Spôsob zverejnenia	Právny základ
Prevádzkovateľ	
Tretia krajina	Právny základ
Prevádzkovateľ	Prenos osobných údajov
V. ZAČIATOK A OSOBNÝCH ÚDAJOCH	

.....
Odtlačok pečiatky

.....
Miesto, meno a podpis
staršieho orgánu prevádzkovateľa

I. NÁZOV INFORMÁCIE	
IS Vernostný program	
II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	Ing. Juraj ZOŇ
Zástupca prevádzkovateľa (alebo osoba vymenovaná)	
Počet oprávnených osôb	
III. ÚDAJE O INFORMÁCIIACH O OSOBNÝCH ÚDAJOCH	
Účel spracúvania osobných údajov	
Právny základ sprac. osob. údajov	Súhlas
Okruh dotknutých osôb	Fyzické osoby, Fyzické osoby -
Zoznam osobných údajov (alebo rozsah)	Miesto narodenia, pohlavie, vek, kontaktné údaje / kontakty / telefón, eMail, facebook, skype
Označenie bezpečnostných opatrení	
IV. SPRACOVATEĽ OSOBNÝCH ÚDAJOV	
Spracovanie osobných údajov	
Tretie strany (prípadne)	
Prevádzkovateľ osobných údajov	
Spracovanie osobných údajov	
Okruh príjemcov	
Prevádzkovateľ osobných údajov	
Spracovanie osobných údajov	
Spôsob zverejnenia	Právny základ
Prevádzkovateľ osobných údajov	
Tretia krajina	Právny základ
Prevádzkovateľ osobných údajov	
V. ZAČIATOK SPRACOVANIA OSOBNÝCH ÚDAJOV	

.....
Odtlačok

.....
, meno a podpis
orgánu prevádzkovateľa

Bezpečnosť**Úlohy a povinnosti pracovníkov s osobnými údajmi****1. Osoby zodpovedné za bezpečnosť**

- Za bezpečnosť osobných údajov zodpovedá pracovník, ktorý osobnými údajmi pracuje 20 a viac pracovných hodín týždenne a ktorému poverenie poskytnúť osobné údaje zodpovednú osobu, ktorá zodpovedá za bezpečnosť osobných údajov, ktorá musí byť kvalifikovaná a nesmie byť mladšia ako 18 rokov (3) zákona 122/2013 Z.z.
- Prevádzkovateľ spravuje osobné údaje prostredníctvom poučených pracovníkov, ktorí musia svojim povolením, znalosťmi a rozsahom práce zodpovedať priloženému formuláru je aj súhlasom s tým, že budú používať osobné údaje v súvislosti s mzdovou agendou.

2. Osoby oprávnené na prácu s osobnými údajmi

- Pracovať s osobnými údajmi v súlade s povolením, a to v rozsahu stanovenom písomne.
- Iné osoby pracujúce s osobnými údajmi alebo spracovávať osobné údaje.

3. Povinnosťou zodpovedných

- Poznať a dodržiavať pravidlá bezpečnosti osobných údajov.
- Kontrolovať prístup k osobným údajom a povolať osoby k osobným údajom.
- Priebežne hodnotiť bezpečnosť osobných údajov a dodržiavať povinnosti oprávnených pracovníkov.
- Zabezpečiť bezpečnosť osobných údajov.
- Najmenej jedna osoba musí dodržiavať skutočnosť, že osobné údaje sú chránené podľa smerniciac.
- Pri výbere pracovníka musí byť zohľadnená jeho kvalifikácia, dôveryhodnosť a schopnosť zachovať bezpečnosť osobných údajov.

4. Povinnosťou oprávnených

- poznať a uplatňovať pravidlá bezpečnosti osobných údajov.
- poznať a dodržiavať pravidlá bezpečnosti osobných údajov.
- používať osobné údaje v súlade s povolením a plnením pracovných povinností a dodržiavať pracovnú disciplínu.
- organizovať osobné údaje v súlade s povolením a dodržiavať bezpečnosť osobných údajov, aby sa zabránilo chybám, ktoré by mohli viesť k poškodeniu alebo zničeniu údajov, ktoré sú chránené, uzamykanie počítačového systému.
- informovať o zistení neoprávnenej osoby, ktorá má prístup k osobným údajom alebo nájdení chránenej písomnosti, ktorá obsahuje osobné údaje.
- viest' osobné údaje v súlade s povolením a dodržiavať bezpečnosť osobných údajov.
- zachovávať bezpečnosť osobných údajov.

5. Osoba poverená získavaním osobných údajov

- a) preukázať na požiadanie svoju spôsobilosť na získavanie osobných údajov požaduje.
- b) bez vyzvania vopred oznámiť dotknutému zamestnávateľ'a, na vykonávanie ich činnosti súvisiacich s informačných systémov: IS Účtovné doklady, IS Informačný systém

Prílohy:

ZÁZNAM O POUČENÍ A OBOZNOMENÍ 22/2013 Z.z.

EVIDENCIA VYPOŽIČIAVANIA VYPISU DOKUMENTOV

Svojím podpisom potvrdzujem že zásad tejto smernice:

V.....

.....
dpis

postupy pri zakladaní nových záznamov

1. Prevádzkovateľ vedie záznamy o dotknutých osobách a písomnostiach.
2. Záznamy a zmeny v záznamoch sú vedené povereným a poučeným.
3. Zisťovanie osobných údajov musí byť v súlade so zákonom a spôsob pri získavaní osobných údajov určuje Bezpečnostný systém, ktorý je určený dotknutej osobou je daný osobitnými zákonmi,
4. Oprávnená osoba zodpovedná za záznamy musí zabezpečiť, aby záznamy boli tak, aby zabránila ich vypadávaniu pri záznamoch (lepením, záznamoch).
5. Osoba, ktorá používa záznamy musí byť informovaná o tom, že obsahujú osobné údaje, aby sa s týmito dokumentmi pracovalo v súlade s tým, ktoré sú v bezprostrednej blízkosti oprávnených na styk s osobnými údajmi.

Svojím podpisom potvrdzujem, že som si prečítal a som s tým súhlasný.

V..... dňa.....
..... pečiatka a podpis

o podmienkach likvidácie písomností obsahujúcich osobné údaje

1. Písomnosti obsahujúce osobné údaje sa skladajú do uzamykateľných zariadení na to určených, uzamykateľných kľúčov, uzamykateľného stola, uzamykateľných zariadení. Požiadavka na uzamykanie písomností musí byť v súlade s požiadavkami na fyzickej ochrany priestoru, v ktorom sa písomnosti nachádzajú, a na dostupných dverí zámkom s bezpečnostnou vložkou.
2. Za úschovu písomností obsahujúcich osobné údaje zodpovedá tá osoba, ktorá písomnosť používa. Táto je povinná po skončení používania písomnosti ju zlikvidovať alebo ju odovzdať osobe, od ktorej písomnosť získala.
3. Likvidáciu nepoužívaných písomností musí zabezpečiť tá osoba. Dokumenty musia byť zlikvidované skartovacím zariadením, ktoré zabezpečuje ich čitateľnosť.

Svojím podpisom potvrdzujem, že som si prečítal a som s tým súhlasný.

V..... dňa:
..... pečiatka a podpis

o podmienkach vypožičania a obsahu

1. Písomnosti, ktoré obsahujú osobné údaje fyzickej osoby.
2. Písomnosti obsahujúcich osobné údaje právnických osôb a inštitúciám v súlade s presnou špecifikáciou.
3. Vypožičanie písomnosti obsahujúcej osobné údaje sa uskutočňuje do evidencie vypožičiavania a poskytnutia písomnosti.
4. Písomnosti s osobnými údajmi sa môžu vybrať výhradne v zalepenom obale, s otvorom prelepeným lepiacou páskou.
5. Písomnosti prenášajú dotknutú činnosť poverený personál alebo zamestnanec.
6. Písomnosti obsahujúce osobné údaje sa môžu vybrať výhradne doporučenou poštou alebo kuriérom.
7. V prípade, že prevádzkovateľ poskytuje písomnosti, musí byť u doručujúcej osoby a odsúhlasí obsah zásielky.
8. Odovzdanie písomnosti na prenos musí byť zaznamenané v evidencii vypožičiavania písomnosti na prenos, pripravuje a balí písomnosti na prenos určená osoba, ktorá musí skontrolovať, či nedošlo k zámene písomností pred zalepením.
9. Písomnosti určené na prenos sa musia zabaliť tak, aby sa zabránilo nekontrolovanej manipulácii.
10. Po vrátení vypožičaných písomností musí byť skontrolovaná celistvosť písomností a či nedošlo k zámene písomností.

Svojím podpisom potvrdzujem vyzdvihnutie a prijatie zásad tejto služby.

V.....
.....
..... pečiatka a podpis

Rozmnožovanie a poskytovanie osobných údajov

1. Rozmnožovanie a poskytovanie informácií z digitizovaného systému, vyhotovovanie fotokópií, odpisovanie.
2. Rozmnožovanie a poskytovanie informácií z fyzických dokumentov.
3. Vydanie tlačenej kópie z počítačového informačného systému, fotokópie alebo inej písomnosti právnickej osoby, ktorá sa eviduje v evidencii vypožičiavania výpisu dokumentov.

Svojím podpisom potvrdzujem vyzdvihnutie a prijatie zásad tejto služby.

V.....
.....
..... pečiatka a podpis

Kľúčový režim zariadenia

Kľúče používané na vstup do priestorov prevádzkovateľa (ďalej len "prevádzkovateľ") sa uchovávajú počítače, počítačové média a písomnosti (ďalej len "dokumenty") sa pridávajú osobám, ktoré určí prevádzkovateľ (ďalej len "osoba ním poverená") zodpovednosťou za ochranu osobných údajov.

Každý evidovaný kľúč musí byť označený a evidovaný v evidencii.

1. Zodpovedná osoba vedie evidenciu kľúčov v evidencii

- identifikačný kód kľúča;
- označenie dverí, zariadenia, ktorým sa kľúčom otvára;
- dátum zariadenia kľúča;
- identifikačné údaje osoby, ktorému kľúč je pridelený;
- dátum pridelenia (vrátane dátumu, keď kľúč bol vydaný).

Osoba, ktorá nie je oprávnená na prácu s kľúčmi, nesmie používať evidované kľúče od priestorov s IS iba s cieľom získať prístup k IS a iné dokumenty obsahujúce osobné údaje sú uzamknuté a držiteľom evidovaných kľúčov.

2. Držiteľ evidovaných kľúčov

- zaobchádzať s kľúčmi opatrne;
- osobne dohliadať na kľúče (okrem prípadov, keď kľúče sú v ruke personálu) v priestoroch, kde kľúče majú prístup k kľúčom, aby sa v priestoroch, kde kľúče uchovávajú osobné údaje, osoby z iných ako pracovných priestorov;
- uzamykať dvere, od ktorých má prístup, vždy, keď sa vzdáľuje z pracoviska;
- pred uzamknutím kľúčov uschovávať kľúče v priestoroch obsahujúcich osobné údaje;
- bez omeškania oznámiť prevádzkovateľovi kľúčov;
- na výzvu zodpovednú kľúčom.

Svojím podpisom potvrdzuje, že súhlasí s touto zmluvou:

V.....

pečiatka a podpis

B

1. Zodpovedné osoby za bezpečnosť:

- a) Za bezpečnosť osobných údajov zodpovedá osoba s osobnými údajmi pracuje 20 a viac pracovníkov, ktorá musí byť zodpovednú osobu, ktorá musí byť bezúhonná podľa zákona 122/2013 Z.z.)
- b) Za chod automatizovanej spracovávania zodpovedá osoba to určený pracovník, ktorý musí byť bezúhonný a oprávnený na spracovanie údajov.

2. **Zodpovedná osoba (prehľadom oprávnení poverená a úradom určená osoba):**
Určí rozsah oprávnení **pravidiel:**

- Zodpovedná osoba [redacted] celému informovanému subjektu.
- Získavať osobné údaje [redacted] a vydávať ich zodpovednej osobe a prípadne ďalším osobám.
- Osoby oprávnené pracovať s osobnými údajmi ich spracovateľskú činnosť potvrdiť svojím podpisom zodpovednej osoby.
- V súvislosti s možnosťou [redacted] oprávnená osoba prezentuje svojím prístupovým heslom [redacted] osoba.
(dĺžka hesla je [redacted] a obsahuje špeciálne znaky napr. @#%*.)

3. Zodpovedná, alebo

3.1 Technické opatření

- a) Pribežne poskytnúť informácie o činnosti a príležitostiach, ktoré konzultuje s jeho dodávateľom.
- b) Jedenkrát za rok vykonať kontrolu počítačového systému a zabezpečiť servisným technikom, aby sa zabezpečila integrita pevného disku, antivírusový scan a kontrola bezpečných hardwarových komponentov.
- c) Zabezpečiť správu dát.
- d) Zabezpečiť správu aplikácií, ktoré sú poskytované dodávateľskej firme (aplikáciu mzdového systému a aplikáciu na overovanie overeného zdroja).
- e) Zakázať použitie cudzích programov a akýchkoľvek programov z internetu.
- f) Podľa schválených podmienok vykonávať zálohovacích mechaník a nosičov.
- g) V prípade potreby vykonávať monitorovanie priestoru prístupného verejným priestorom, ktoré je dostupné dňa nasledujúceho po dni, v ktorom bolo oznámenie o porušení, alebo ak nie je využitý na účely, ktoré sú určené konaním o porušení, alebo ak nie je využitý na účely, ktoré sú určené konaním o porušení.
- h) V prípade porušenia **informačného systému** s existenciou prevádzkovateľa zabezpečiť zápis o porušení zamestnanca s existenciou prevádzkovateľa.

3.2 Organ

- Pomocou prístupného počítača a iným aktívam IS.
- Pomocou prístupného počítača a iným aktívam IS. V neprítomnosti oprávneného používateľa počítača musí byť chránený heslom.
- Pri krátkodobom prístupe na pokračovanie v programe je potrebné zaviesť heslo.
- Pri prístupe k uloženým zálohám databáz na prenosný nosič.

3.3 Forma a periodicita kontrol

- a) Minimálne jeden krát týždenne skontrolovať bezpečnosť počítačového systému.
- b) V prípade pripájania PC na internet vykonať bezpečnostnú kontrolu.
- c) Pri nekorektnom správaní počítača vykonať technikom zabezpečí kontrolu logových súborov v zohľadnení bezpečnostných opatrení.
- d) V prípade použitia nosiča dát vykonať kontrolu obsahu pred použitím v systéme minimálne rýchlo skontrolovať obsah súborov, ktoré obsahujú neprezerá, nespúšťajú, aby sa zabránilo vniknutiu škodlivých obsahov, prípadnú vírusovú náplň odstrániť.
- e) Minimálne jedenkrát vykonať kontrolu po nekorektnom ukončení počítača vykonať systémovú kontrolu a vykonať kontrolu operačného systému takúto kontrolu.
- f) Minimálne jedenkrát vykonať kontrolu systémového scdisku a defragmentáciu operačného systému takúto voľbu.
- g) Pri údržbe a údržbových prácach vykonať kontrolu stavu hardwaru na použitie (tieto služby, ako aj kontrolu hardwaru sa odporúča vykonať 1x mesačne).
- h) Pri výzve na aktualizáciu systému vykonať aktualizáciu najkratšom termíne s dôrazom na bezpečnosť.

4. Postup pri bezpečnosti

- a) Každý bezpečnostný incident (napr. vírusová infekcia, atď.) poznačí do príslušnej evidencie a podľa potreby vykonať bezpečnostnú kontrolu (Priložený formulár: Záznam o bezpečnostných riešeniach).
- b) Pri havárii, neštandardnom správaní počítača alebo iných problémoch kontaktovať počítačový servis, alebo inštalovať bezpečnostnú ochranu, ktorá počítačový systém ochráni.
- c) Po konzultácii s odborníkom vykonať kontrolu dodávateľskej firmy.
- d) V prípade narušenia databáz v žiadnom prípade nevykonávať opravy. Je bezpodmienečne potrebné kontaktovať odborníka na opravu systému. (Ak po vymazaní súborov nie je dôležitá informácia, napríklad heslo, atď., možno odborným príslušníkom vykonať kontrolu).
- e) Podľa doporučení odborníka vykonať kontrolu databáz a operačného systému.
- f) V prípade nevyhnutnosti vykonať kontrolu počítačového technika, špecializovaná firma) oboznámiť sa s bezpečnostnými opatreniami a zabezpečiť databázy a zabezpečiť vyhotovenie zálohy na vedomie. (Priložený formulár: Záloha podľa §21 ZÁKONA 122/2013 Z.z. O POVINOSTIACH V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV)
- g) V prípade potreby vykonať kontrolu počítačového technika (napr. preberanie reklamácií, kontrola domov, atď.) pokiaľ to jeho stav umožňuje, dáta z počítača bezpečne vymaže bezpečnostnú ochranu, alebo konzultáciu s odborníkom, nakoľko vymazanie súborov je veľmi ľahké a môže byť nebezpečné).

Svojim podpisom potvrdzujem vytvorenie a prijatie zásad.

V.....

pečiatka a podpis

B

Zálohovanie databáz počítačového systému i databázových súborov programu, prípadne len jej časti, v prípade poruchy, alebo odcudzenia počítačového systému, prípadov používajú štandardné komprimačné algoritmy

Táto smernica platí pre každý po

1. Typy zálohovania z hľadiska

pama

- Záloha na ten istý pevný disk je umiestnený najlacnejší a najrýchlejší. Princíp je kópie databáz do iného pevného disku. Zálohovanie databáz, ako aj poškodenie databáz vplyvom výpadku napájania. Zálohovanie údajov spôsobenú poškodením pevného disku alebo odcudzením disku.
- Záloha na iný pevný disk alebo na iný typ sieti je bezpečnejšia, ale stále minuje riziká technickej, alebo inej povahy. Na druhej strane je vyššie riziko na iný pevný disk.
- Záloha na externé nosiče je bezpečnejšia, ale stále platňovať zásadu nezálohovať stále na tie isté nosiče. Zálohovanie na externé nosiče a tieto striedať.
- Záloha na iný pevný disk, floppy disk, prenosný pevný disk, magneto - pásky, alebo na spoľahlivosti je najvýhodnejšou metódou zálohovania. Spoľahlivé je aj napájanie na CD, DVD RW, alebo na iný typ mechaniky a poznať niektoré problémy. Pri zálohovaní lokalizáciu databázových súborov. Tieto sa potom pomocou programu pre napájanie CD/ DVD, alebo prepisovateľ.

2. Zásady, postupy a uspořádání:

- a) Každý deň musí byť vykonaná záloha na pevný disk alebo na iný nosič dát, pričom každý druhý deň (odporúča sa) aj záloha na prenosový nosič dát.
- b) Podľa možnosti sa vykonávajú zálohy na rôznych miestach.
- c) Minimálne raz za mesiac sa vykonávajú zálohy na iný nosič dát s cieľom dôvodu overenia ich funkčnosti.
- d) Minimálne raz za mesiac sa vykonávajú zálohy na iný nosič dát z vykonanej zálohy.
- e) V žiadnom prípade sa zálohy nevykonávajú na pracovisku. Treba si uvedomiť, že v prípade zlyhania počítača alebo zariadenia, na ktorých sa zálohy vykonávajú, V tomto prípade sú údaje nenávratne stratené.
- f) Pri prenosových nosičoch dát sa zálohy vykonávajú iba v bezpečnom prostredí a ani v domácom prostredí ich nenesú.
- g) Nepotrebné zálohy treba vymazať, aby sa zabránilo plneniu kapacity nosiča spálením, mechanickým poškodením alebo použitím špeciálnych nástrojov na likvidáciu pamäťových nosičov.
- h) V systéme s dlhodobým skladovaním databázových dát sa zálohy vykonávajú minimálne 1x za rok. Zálohy sa vykonávajú na iný nosič dát, ktorý sa uloží na "nový" nosič dát. Zálohy počítačového informačného systému sa musia ukladať na "nový" nosič (napr. CD, DVD, Blu-ray). Zálohy je potrebné uložiť na bezpečný nosič (napr. DVD nosič, ktorý je odolný voči mechanickým poškodeniam, a tým aj odolný proti požiaru).

Svojím podpisom po

V.....

pečiatka a podpis

Názov/Obchodné meno:

[illegible]

EVIDENCIA KONTROLNÝCH ČINNOSTÍ - príloha

dátum čas poradové č.	kontrola / popis	Zistené nedostatky	Príčina / meno /
14.06.2013 16.00 001/2013	Kontrola zálohovacích médií Kontrola integrity databázy Defragmentácia		
14.06.2013 14:00 002/2013	Kontrola mzdovej evidencie náhodný výber 1 ks		

Názov / Obchodné meno:

[illegible]

EVIDENCIA BEZPEČNOSTNÝCH INCIDENTOV

dátum čas poradové č.	bezpečnostný incident / popis	použitie	príjmenie / meno / podpis
14.06.2013 16:00 001/2013	program hlási poškodenie databázy nejde spustiť		
12.07.2013 14:00 002/2013	nefunguje obnovenie zo zálohy domácom počítači / OS hlási nemožnosť čítania z média	poškodenie médiu priradené a záloha na znovu na overené médium	
18.07.2013 19:00 003/2013	nejde vykonať UpGrade priamo z programu	navrhovaná firma a problém riešený správnu správu, zlé nastavenie programu, bol pridaný do hodný	

IDENTIFIKOVANÉ TYPY INCIDENTOV A S

Názov/Obchodné meno:

AIS

bezpečnostný incident	typ incidentu
poškodenie databázy	porucha SW/HW
poškodenie databázy	porucha SW/HW
nezálohuje	porucha HW/SW
záloha nejde obnoviť	porucha HW/SW
neštartuje PC, žiadna kontrolka nesvieti	porucha HW
UpGrade priamo z programu nejde	porucha HW
antivírusový program hlási infiltráciu	vírusová nákaza

DIS

bezpečnostný incident	typ incidentu
nevrátenie zapožičanej dokumentácie	normal
odcudzenie dokumentácie	krádež
poškodenie dokumentácie	poškodenie
poškodenie živelnou pohrou	živelná

Názov/Obchodné meno:

[illegible]

EVIDENCIA VYPOŽIČIAVANIA A POSKYTNUTIA

dátum / čas / poradie	dokument	typ	čas poskytnutia	Kto / meno / podpis
14/08/2013 10:00 001/2013	Mzdový list		19.08.2013	
17.08.2013 14:00 002/2013	Zápočet rokov			

ZÁZNAM O POUČENÍ OPRÁVNENEJ OSOBY

podľa § 21 ods. 2 a 3 zákona č. 122/2013 Z. z.

ochrany osobných údajov

IDENTIFIKAČNÉ ÚDAJE

Identifikačné údaje (meno, priezvisko, číslo účtu)

poučená osoba (meno, priezvisko, číslo účtu)

poučenie vykonal/ vykonala (meno, priezvisko, číslo účtu)

POUČENIE OPRÁVNENEJ OSOBY

1. Práva a povinnosti oprávnenej osoby podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení

1.1 Práva oprávnenej osoby

Oprávnená osoba má právo na ochranu osobných údajmi spracúvanými v informačných systémoch osobných údajov, ktoré sú základom, od ktorého prevádzkovateľ odvodzuje oprávnenie spracúvať osobné údaje, ktorý je nevyhnutný na dosiahnutie ustanoveného alebo v zmysle zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení zákona č. 122/2013 Z. z. („zákon č. 122/2013 Z. z.“), inými zákonmi, všeobecne záväznými predpismi prevádzkovateľa.

Oprávnená osoba má

- pridelenie prístupu k osobným údajom prevádzkovateľa v rozsahu nevyhnutnom na plnenie jeho úloh; prevádzkovateľ určí pracovné zaradenie oprávnenej osoby a povinnosti jej pracovného zaradenia (miesta),
- opätovné poučenie o podstatnej zmene jej pracovného zaradenia, a tým sa významne zmení jej pracovných činností, ktoré podstatne zmenili podmienky spracúvania osobných údajov v rozsahu spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia,
- porušenie povinností oprávnenej podľa zákona č. 122/2013 Z. z., ak je to nevyhnutné na plnenie jeho úloh podľa zákona č. 122/2013 Z. z. (ak je to podľa osobitného zákona alebo vo vzťahu k Úradu verejného ochranku, ktorý je len „úrad“) pri plnení jeho úloh podľa zákona č. 122/2013 Z. z. (ak je to podľa osobitných predpisov),
- vykonávanie spracúvania osobných údajov prevádzkovateľa, vrátane osobitnej kategórie osobných údajov, ktoré sú spracúvané pracovných úloh určených opisom pracovného zaradenia,
- odmietnuť vykonávanie spracúvania osobných údajov, ktorý je v rozpore so všeobecne záväznými právnymi predpismi,
- na vydanie stanoviska k svojej pracovnej príslušnosti k zamestnávateľovi.

Vo vzťahu k oprávnenej podľa zákona č. 122/2013 Z. z. oprávnená osoba kontrolovanej osoby má právo na kontrolu osobných údajov.

- na prístup k osobným údajom kontrolného orgánu pri vykonávaní kontroly,
- vyžadovať kontrolnému orgánu preukázať sa podľa osobitných predpisov, ktoré oprávnená konať v mene štatutárneho orgánu, ak je oprávnenou osobou,
- oboznať kontrolnému orgánu, ak je oprávnenou osobou,
- podávať písomné stanoviska, ak je oprávnenou osobou,
- vyžadovať kontrolu podľa § 55 zákona č. 122/2013 Z. z., ak je oprávnenou osobou oprávnená konať v mene štatutárneho orgánu.

Rozsah oprávnení oprávnenej osoby vykonávať, je definovaný úradom, ktorý osobné údaje v bode č. 2 tohto záznamu o

1.2 Povinnosti oprávnenej os

Oprávnená osoba je v súvislosti so [REDACTED] é povinnosti
formulované prevádzkovateľom [REDACTED]

- a) bezpečnostnej dokumentácie informácií podľa bezpečnostnými
smernicami 1 – 8, ktoré sú súčasťou PR
- b) dodržiavania pravidiel etiky.

Oprávněná osoba je dále po

- [illegible]

Vo vzťahoch plynúcich z konštatovanej podľa zákona č. 180/2014 Z.z. o ochrane osobných údajov a o spôsobe vykonávania kontroly osobných údajov, plynúcej z konštatovanej osoby kontrolovanej osoby je povinná

- a) poskytnúť súčinnosť pri výkone jeho právomocí podľa zákona č. 122/2013 Z. z.,
- b) strpieť preukázanie jeho právomocí inej osobe kontrolným orgánom pri výkone jeho právomocí podľa zákona č. 122/2013 Z. z.,
- c) zdržať sa výkonu svojich právomocí, ak je to potrebné,
- d) dostaviť sa na jeho pozvánku v určenom čase na určené miesto, ak je oprávnenou osobou konať v mene štatutárneho orgánu,
- e) umožniť kontrolu jeho právomocí kontrolným orgánom podľa § 56 zákona č. 122/2013 Z. z., ak je osoba oprávnená konať v mene štatutárneho orgánu,
- f) umožniť kontrolnému orgánu dostaviť sa na jeho prerokovanie, ak je osoba oprávnená konať v mene štatutárneho orgánu.

Opis: [redacted] s cieľom využiť pre osobnú potrebu, či potrebu iných [redacted] z služobnej funkcie [redacted]

2. Rozsah a popis povolených činností

Rozsah oprávnení a povolených činností zameraných na spracovanie údajov je vymedzený týmto poučením, opisom pracovných podmienok, pracovnej zmluvy, všeobecne záväznými právnymi predpismi, ako aj inštrukciami spracovateľa. Úroveň prístupových práv k jednotlivým informačným systémom a pracovateľských operácií, ktoré môže oprávnená osoba v rámci týchto systémov vykonávať je predmetom bodov 2.1 a 2.2 tohto záznamu. Spracovateľské operácie sú súvisiace s právami a oprávneniami na vykonávanie iných spracovateľských činností uvedených v bodoch tohto záznamu.

2.1 Rozsah povolených činností

Rozsah povolených činností: [REDACTED] spracúvaní osôb [REDACTED] h systémoch
osobných údajov prevádzkovateľa [REDACTED] č. 2.2 tohto záznamu [REDACTED] hnutnom
na zabezpečenie účelu plnenia úlohy [REDACTED]

- mzdovej a personálnej
- účtovných dokladov
- registratúrnych záznamov
- vernostného programu

2.2 Popis povolených činností

- a) ***IS Mzdy a personalistika***

Spracovateľské operácie s údajmi: prístupnosť, prístupnosť, usporiadávanie, vyhlásenie, oboznamovanie, uchovávanie
Právny základ: O

- b)
- IS Účtovné da**

Spracovateľské ... prístupňovanie,
usporadúvanie ..., poskytnutie, uchovávanie
Právny základ ... vedené v evidencii

- c) ***IS Registrations***

Spracovateľ/sa spracováva osobné údaje: získavanie, zisťovanie, uchovávanie, usporadúvanie, vyhodnotenie, poskytovanie, odovzdávanie, zverejňovanie, namovanie, uchovávanie

- d) **IS Vernostný p**

Spracovateľské operácie, sprístupňovanie,
usporadúvanie, vyhľadanie, oznamovanie, uchovávanie
Právny základ: Súhlas

Iné spracovanie údajov: [redacted] osoba oprávnená vykonať len na základe predchádzajúceho súhlasu, ktorý je v súlade so zákonom č. 122/2013 Z. z., inými zákonmi a [redacted] s inými aktmi prevádzkovateľa.

3. Podmienky poskytnutia osobných údajov

Podmienky poskytnutia týchto údajov prostredníctvom elektronických prostriedkov spracúvania (listová forma poskytnutia týchto údajov) sú vymedzené v prílohe 1 a 2 k smerniciach 1 až 6.

4. Zodpovednosť

Oprávnenosť Z. z. povinná zachovávať mlčanlivosť o osobných údajoch, ktorých spracúvanie súvisí s trestným konaním, mlčanlivosti trvá aj po ukončení spracúvania osobných údajov. Povinnosť mlčanlivosti sa vzťahuje na sudcov, sudkyň, úložíkov úloh súdu a orgánov činných v trestnom konaní podľa osobitných predpisov, ktorými sa ustanovujú úlohy podľa zákona č. 122/2013 Z. z.; ustanovenia o povinnosti mlčanlivosti podľa zákona č. 122/2013 Z. z. ustanovenia o povinnosti mlčanlivosti podľa zákona č. 122/2013 Z. z.

Porušením povinností alebo znepokojením súkromia súkromných osôb oprávnená osoba naplniť skutkovú podstatu správnych delík podľa § 180 až 183 Z. z., a to nasledovným konaním

- a) poskytnutím osobných údajov v rozpore s § 122/2013 Z. z.,
- b) poskytnutím nepravdivých osobných údajov v rozpore s § 122/2013 Z. z.,
- c) nepostupovaním v súlade s technickými opatreniami prijatými prevádzkovateľom alebo sprostredkovateľom v rozpore s § 122/2013 Z. z.,
- d) porušením svojich povinností podľa § 122/2013 Z. z.,
- e) porušením povinnosti mlčanlivosti podľa § 122/2013 Z. z.,
- f) neposkytnutím úradu podľa § 122/2013 Z. z.

Oprávnená osoba môže v súvislosti s týmto konaním byť trestným stíhaním za trestné činy podľa § 247 a § 374 Z. z. Trestný zákon nie je v tomto prípade voči nej byť vedené disciplinárne konanie.

OBOZNÁMENIE OPRÁVNENEJ OSOBY

Oprávnená osoba svojimi právami a povinnosťami bola osobou, ktorá je v plnom rozsahu oboznámená s platnými internými opatreniami prevádzkovateľa a s právami oprávnených osôb v procese spracúvania osobných údajov.

- a) bezpečnostnými smernicami zameranými na ochranu osobných údajov,
- b) prijatým bezpečnostným projektom,
- c) prijatou bezpečnostnou politikou.

ktoré sú jej kedykoľvek dostupné.

Oprávnená osoba je s obsahom týchto opatrení a povinností vymedzeným v rozsahu tohto záznamu v oblasti spracúvania osobných údajov v plnom rozsahu porozumela.

V, dňa

.....
podpis oprávnenej osoby,
..... vykonala

Dátum ukončenia činnosti oprávnenej osoby

POUČENIE SERVISNEHO ZÁKAZNÍKA O POUŽITÍ SERVISNÝCH SLUŽIEB
O POVINNOSTIACH A PRÁVAH

poučená osoba

poučenie vykoná

Poučená osoba potvrdzuje,

- ☐ vykoná servis na informačnom systéme
- ☐ prevezme počítač, prepraví na externé miesto, prípadne prevádzkovateľa

Poučená osoba sa zaväzuje

1. sa v žiadnom prípade neoprávňuje k zisťovaniu údajov z ostatných evidencií obsiahnutých v informačných systémoch
2. po vykonaní servisu neoprávňuje k zisťovaniu údajov z evidencií servisovaného zariadenia,
3. údaje zo servisovaného zariadenia poskytnúť žiadnej tretej strane
4. zabráni prístupu tretej osoby k informačnému systému.

Poučená osoba berie na vedomie

1. servisované zariadenie môže obsahovať osobné údaje, patriace do kategórie osobitných údajov
2. preberá právne dôsledky zneužitia údajov, prípadne zneužitiu osobných údajov a týkajúce sa

podpis po

podpis vykonávateľa poučenia

ZMLUVA SO SPROSTREDKOVATEĽOM O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Článok 1

1. Prevádzkovateľ

(ak ste právnická osoba napr. s.r.o. alebo a.s.)

Názov:			
Adresa sídla:			
V zastúpení:		Tel.:	

(ak ste fyzická osoba – podnikateľ)

Obchodné meno:	IČO:		
Adresa miesta podnikania:			
V zastúpení:			

2. Sprostredkovateľ

(ak je sprostredkovateľ fyzická osoba)

Titul:			
Meno:			
Adresa trvalého pobytu:			
		Email:	

(Ak je sprostredkovateľ právnická osoba)

Názov:	IČO:		
Adresa sídla:			
V zastúpení:	Tel.:		

(ak je sprostredkovateľ fyzická osoba)

Obchodné meno:			
Adresa miesta podnikania:			
V zastúpení:		Email:	

Dátum začatia spracúvania osobných údajov: _____

1. Dátum:

Článok 2

Účel spracúvania osobných údajov

1. Účelom spracúvania osobných údajov podľa tejto zmluvy je poskytovanie služieb z oblasti mzdovej a personálnej agendy pracovníkom zamestnávateľa s platnými právami Slovenskej republiky.

1. Mzdová a personálna

Článok 3

Podmienky spracúvania osobných údajov

1. Zoznam osobných údajov, ktoré presne špecifikujú osobitné zákony, podľa ktorých postupuje zamestnávateľ a mzdovej agendy. Jedná sa hlavne o identifikačné údaje, údaje o mieste pobytu. Z osobitných kategórií osobných údajov sú spracúvané údaje o zdravotnom stave, o rodinnej situácii, o

1. Dotknuté osoby podľa tejto zmluvy sú priamo alebo nepriamo ovplyvnené a tiež uchádzači o zamestnanie.

Podmienky spracovania osobných údajov

1. Sprostredkovateľ zabezpečí ochranu osobných údajov pred stratou, poškodením, neoprávneným prístupom, zneužitím, zverejnením, šírením, možnými kópiami a inými opatreniami.
2. Po ukončení spracovania osobných údajov prevádzkovateľ zabezpečí, aby boli odstránené všetky kópie a informácie z databáz na prenosných médiách, ktoré sú potrebné na pracovnú a personálnu potrebu.
3. Nepotrebné dokumenty zlikviduje, alebo ich uloží v bezpečnom prostredí, alebo ich vymaže z počítača, alebo iným bezpečným spôsobom.
4. Zo svojho automatizovaného systému odstráni všetky údaje z databázy s osobnými údajmi, ktoré sú potrebné na pracovnú a personálnu potrebu, alebo ich vymaže z počítača, alebo iným bezpečným spôsobom.

1. Prevádzkovateľ vyhlasuje, že pri vykonávaní svojich činností, organizačnú a personálnu spôsobilosť a jeho schopnosť zabezpečiť ochranu osobných údajov v súlade s opatreniami podľa § 19 ods. 1, zariadenia, ktoré sú potrebné na pracovnú a personálnu potrebu.
2. Prevádzkovateľ berie na zreteľ, že osobné údaje sú spracovávané sprostredkovateľovi, a že sú spracovávané v súlade s osobnými záujmami dotknutých osôb.

Ustanovenia

1. Sprostredkovateľ vyhlasuje, že osobné údaje sú spracovávané v súlade s ustanoveniami zákona o ochrane osobných údajov.
2. Sprostredkovateľ berie na zreteľ, že ak chce spracovanie osobných údajov uskutočniť prostredníctvom inej osoby (ďalej len „subdodávateľ“), musí mať písomný súhlas prevádzkovateľa.
3. Subdodávateľ spracováva osobné údaje v súlade s ustanoveniami zákona o ochrane osobných údajov a v súlade s opatreniami prevádzkovateľa. Na subdodávateľa úrad nahliada ako na prevádzkovateľa.
4. Súhlas prevádzkovateľa s tým, že osobné údaje sú spracovávané prostredníctvom inej osoby.

súhlasím so spracovaním osobných údajov v súlade s ustanoveniami zákona o ochrane osobných údajov a v súlade s opatreniami prevádzkovateľa.

Podpis

Táto zmluva sa uzatvára medzi:

Článok 2. Zmluva o spracovaní osobných údajov

Dňa: Prevádzkovateľ:

Dňa: Prevádzkovateľ¹:

¹ pečiatka nie je

ZMLUVA SO SPROSTREDKOVATEĽOM O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Článok 1

1. Prevádzkovateľ

(ak ste právnická osoba napr. s.r.o. alebo a.s.)

Názov:			
Adresa sídla:			
V zastúpení:		Tel.:	

(ak ste fyzická osoba – podnikateľ)

Obchodné meno:		IČO:	
Adresa miesta podnikania:			
V zastúpení:			

2. Sprostredkovateľ

(ak je sprostredkovateľ fyzická osoba)

Titul:			
Meno:			
Adresa trvalého pobytu:			
		Email:	

(Ak je sprostredkovateľ právnická osoba)

Názov:		IČO:	
Adresa sídla:			
V zastúpení:		Tel.:	

(ak je sprostredkovateľ fyzická osoba)

Obchodné meno:			
Adresa miesta podnikania:			
V zastúpení:		Email:	

Dátum podpísania a začiatku spracúvania osobných údajov

1. Dátum:

Článok 2

Účel spracúvania osobných údajov

1. Účelom spracúvania osobných údajov podľa tejto zmluvy je poskytovanie obchodnej agentúry prevádzkovateľa v súlade s požiadavkami zákona o ochrane osobných údajov Slovenskej republiky.

1. IS Účtovné doklady

Článok 3

Prístup k údajom

1. Zoznam osobných údajov, ktoré sú spracúvané, presne špecifikujú osobitné zákony, podľa ktorých sa postupuje. Jedná sa hlavne o identifikačné a kontaktné údaje, ktoré sú potrebné na poskytovanie obchodnej agentúry prevádzkovateľa a zástupcov obchodných partnerov, ako aj na poskytovanie účtovných dokladov.

Okrem

1. Dotknuté osoby sú zástupcovia obchodných partnerov a obchodní partneri.

Podmienky spracovania osobných údajov

1. Sprostredkovateľ zabezpečí ochranu osobných údajov pred stratou, poškodením, neoprávneným prístupom a v súlade s požiadavkami.
2. Po ukončení spracovania osobných údajov prevádzkovateľ prevádzkovateľ odstráni všetky kópie databáz na prenosných médiách a informaciami v informačnom systéme IS.
3. Nepotrebné dokumenty zlikviduje alebo iným bezpečným spôsobom odstráni.
4. Zo svojho automatizovaného systému odstráni všetky databázy s osobnými údajmi a vymazaním z média.

1. Prevádzkovateľ vyhlasuje, že pri výbere a výkone svojich povinností, organizačnú a personálnu spôsobilosť a jeho opatrenia na ochranu osobných údajov v súlade s opatreniami podľa § 19 zákona.
2. Prevádzkovateľ berie na zreteľ osobné údaje spracovávané sprostredkovateľovi, a záujmy dotknutých osôp.

Článok IV Ďalšie ustanovenia

1. Sprostredkovateľ vyhlasuje, že zabezpečí ochranu osobných údajov osôb.
2. Sprostredkovateľ bude spracovávať osobné údaje, ak chce spracovanie osobných údajov vykonať prostredníctvom inej osoby (ďalej len „subdodávateľ“), musí mať písomný súhlas prevádzkovateľa.
3. Subdodávateľ spracováva osobné údaje a zabezpečuje ich ochranu prostredníctvom sprostredkovateľa. Ustanovenia zákona o ochrane osobných údajov sa na subdodávateľa. Na subdodávateľa úrad nahliada ako na prevádzkovateľa.
4. Súhlas prevádzkovateľa na spracovanie osobných údajov prostredníctvom inej osoby.

súhlasím so spracovaním osobných údajov
.....

Táto zmluva sa uzatvára v
.....

Článok XI Záver zmluvy a počet strán.

Dňa: Prevádzkovateľ:

Dňa: Prevádzkovateľ¹:

¹ pečiatka nie je

ŽIADANIE O REGISTRÁCIU

informačného systému osvedčenia
podľa § 35 ods. 2 zákona č. 122/2013 Z. z. o elektronizácii súdnych konaní

a) Identifikačné údaje prevádzkovateľa

Identifikačné číslo organizácie (IČO)

36250163

Názov prevádzkovateľa (obchodné meno)

SOFTPROGRES s.r.o.

PSČ

921 01

Obec

Pí

Ulica

E. Belluša 4

Štát

Slovenská republika

Právna forma

spoločnosť s ručením

b) Štatutárny orgán prevádzkovateľa

Priezvisko

ZOŇ

Titul

Ing.

c) Identifikačné údaje

Identifikačné číslo organizácie

Názov (obchodné meno)

Ulica

číslo

PSČ

Obec

Právna forma

d) Štatutárny orgán prevádzkovateľa

Priezvisko

Titul

nenej konať v mene zástupcu

e) Počet oprávnených osôb prevádzkujúcich

6

f) Názov informačného systému

IS Vernostný program

g) Účel spracúvania osobných údajov

Evidencia a správa zamestnancov a vernostného programu

h) Právny základ spracúvania osobných údajov

Súhlas dotknutej osoby

e) Okruh dotknutých osôb

Zákazníci, ktorí majú zmluvu s našou spoločnosťou a zmluvu s našimi partnermi spoločnosti a za sponzorovania iné benefity.

e) Zoznam osobných údajov, ktoré sú spracovávané podľa §. 4 prvej vety

meno, priezvisko a dátum narodenia, pracovná príslušnosť, dátum nástupu do práce, adresa, pohlavie, vek, kontaktné údaje, e-mail, IČO, ak sa jedná o podnikateľa, kontakty /telefón, fax, mobilný telefón, skype a pod.../ a iné osobné údaje bydliska

e) Tretie strany, prípadne tretia krajina, ktorým budú osobné údaje poskytnuté a právny základ ich poskytnutia

Tretie strany **Právny základ**

Prevádzkovateľ osobných údajov

f) Okruh príjemcov osobných údajov, ktorým budú osobné údaje sprístupnené a právny základ ich poskytnutia

Okruh príjemcov **Právny základ**

Prevádzkovateľ osobných údajov

nesprístupní

g) Spôsob zverejňovania osobných údajov prevádzkovateľ osobných údajov a právny základ ich zverejnenia

Spôsob zverejňovania **Právny základ**

Prevádzkovateľ osobných údajov nezverejňuje

h) Tretie strany, prípadne tretia krajina, ktorým budú osobné údaje poskytnuté a právny základ ich poskytnutia

Tretia krajina **Právny základ**

Prevádzkovateľ osobných údajov poskytnúť údaje do tretích krajín

i) Označenie bezpečnostných opatrení podľa prílohy č. 2

Bezpečnostný projekt informačnej

j) Deň, kedy sa začnú spracúvať
údaje v informačnom systéme

--	--	--	--	--

Spôsob platby:

- ☐ Prevodomuve
- ☐ poštovoukópiu ústrižku
- ☐ v hotovosť
- ☐ oslobodené od p

Uvedte číslo účtu na ktorý Vášpodnutia o vrátení
správneho poplatku

.....
Pečiatka prevádzkova

.....
Dátum,
štatutárneho orgaeľa

Kontaktné údaje:

.....

.....

Popis podmienok spracúvania osobných údajov:

Osobné údaje sú spracúvané v informačnom systéme aj v informačnom systéme.

Potenciálnym klientom vernostného programu vyplývajú z registrácie.

Klientom vernostného programu je následne vyplnenie jeho osobných údajov, ktoré obsahuje rubriky na meno, priezvisko a titul, štátna príslušnosť, vek, kontaktné údaje, IČO, ak sa jedná o fyzickú osobu - podnikateľa, IČO, ak sa jedná o právnickú osobu, identifikačné číslo, identifikačné číslo bydliska

Údaje z formuláru sú následne uložené v informačnom systéme a kontaktný formulár odložený do papierového archívu.

Klient - Obchodný partner spoločnosti je informovaný o spracúvaní všetkých údajov, ktoré obsahuje formulár.

Klient následne potvrdzuje spracúvanie osobných údajov a prípadne súhlas so zasielaním informácií o spracúvaní osobných údajov.

POLITIKA INFORMACÍ A BEZPEČNOSTI

Vyhlásenie prevádzkovateľa:

Vzhľadom na zákon o ochrane osobných údajov č. 122/2001 Z.z. a príslušné normy informačnej bezpečnosti, nasledujúci dokument:

Zabezpečíme, aby osobné údaje obsiahnuté v našich informačných systémoch boli chránené pred zničením, stratou, neoprávnenému prístupu a sprístupneniu, iným než určeným, alebo iným než inému neprípustnému spôsobu spracovania. Zabezpečíme, aby boli spracúvané v súlade s Evidenciou informačných systémov, bezpečnosti, registratúry a so spracovaním osobných údajov.

Vyhlasujeme, že na zabezpečenie organizačné, personálne a informačné možnosti budú zodpovedať úrovni nákladovosti.

Zaväzujeme sa pracovať v súlade s ústavnými zákonmi Slovenskej republiky a platnými zákonmi a nariadeniami, ktoré majú na úmysle chrániť osobné údaje v našom systéme.

Všetky zlepšenia informačnej bezpečnosti budú zavádzať v súlade s medzinárodnými normami ISO 27001.

Za účelom podpory ochrany osobných údajov informačného systému a zdokonaľovania našej práce.

Projekt je koncipovaný v súlade s Zákonom 164/2013 Z.z. a je aplikovaný §7.8. Opis opatrení a to tak, že pre všetky informácie bezpečnostný projekt, pričom je zreteľne označený.

Za ochranu osobných údajov zodpovedá príslušný oprávnený personál.

Dňa:

.....

Vážený zákazník,

ďakujeme za prejavenu dôveru v Softprogres a Bezpečnostného projektu.

Dostávate do rúk Bezpečnostného projektu Informáciu z dotazníka, ktoré ste nám poskytli. Táto informácia sa prihladiť na skôr laické ako odborné znalosti, ktoré sú potrebné, aby projekt nebol len odborným, ale aj praktickou pomôckou počítačových systémov a počítačov.

Samotný projekt musí byť prečítaný a na vyznačenie zodpovedná osoba (pre ktorú je projekt určený) musí podpísať a podpísať projekt, prijatie a prechod.

Na konci projektu sú všetky dokumenty, ktoré sú Vašho pracoviska (Evidencie, Poučenia, Zmluvy, atď.) a ktoré sa stávajú neoddeliteľnou súčasťou projektu. Sú aj zmluvy o spracovaní osobných údajov, ktoré sú aj účtovníctva.

Nezabudnite registrovať na úrade a zaplatiť správny projekt/

Súčasťou dokumentu je Evidencia, kde je dokument pre Kamerový informácijský systém. Ak do budúcnosti kamerový systém, priložte po zavedení tohto dokumentu prílohy č.1 – EVIDENCIA SYSTÉMOV OSOBNÝCH ÚDAJOV. Ak kamerový systém neplánujete, môže byť hodnotiť.

Zároveň Váš projekt musí byť súčasťou zodpovednej osoby dohľadom nad spracovaním údajov. Nemusíte mať žiadne oznamovacie povinnosti voči štátu, ale zodpovednú osobu, ktorá musí prejsť štátom. Údajom majú len pracoviská s počítačom. Starému zákonu je aj skutočnosť, že ak máte možnosť overiť žiadnu inú osobu.

Sledujte projekt, ktorý nás budeme priebežne informovať o jeho priebehu.

V prípade dotazov konzultujte problémy s softprogres, alebo priamo cez úrad.

Úrad na ochranu osobných údajov, Hraničná 12, 820 01 Bratislava
e-mail: info@softprogres.sk

Ing. Juraj ZON

IČO: 14123738

tel.: 033/774361

info@softprogres.sk