Bezpečnostná dokumentácia

technických a organizačných opatrení v zmysle požiadaviek
Nariadenia EÚ 2016/679 a zákona č. 18/2018 Z.z.
o ochrane osobných údajov

Prevádzkovateľ:	MTK PLUS s.r.o.
Sídlo:	Stožok 424, 962 12 Detva
IČO:	47 099 283
Prevádzka 1:	Stožok 424 ,962 12 Detva
Prevádzka 2:	Bystrická cesta 5676, 034 01 Ružomberok

Dokumentáciu vypracoval : Mgr. Vladimír Salaj

Informačné systémy : Personálny a mzdový informačný systém
Registratúra
Účtovná agenda
Kamerový systém

Dátum spracovania : 4. mája 2021

.....

Obsah

VŠEOBECNÉ USTANOVENIA ... 3

ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV ... 6

SPRACOVATEĽSKÉ ČINNOSTI V INFORMAČNÝCH SYSTÉMOCH ... 8

- Personálny a mzdový informačný systém ... 8
- Účtovná agenda ... 8
- Správa registratúry ... 9
- Kamerový systém ... 10

METODIKA ANALÝZY ÚROVNE BEZPEČNOSTI ... 10

- Vymedzenie hraníc určujúcich množinu zostatkových rizík ... 11

POŽIADAVKY NA INFORMAČNÚ BEZPEČNOSŤ ... 12

ANALÝZA ÚROVNE BEZPEČNOSTI ... 13

- 1. Politika informačnej bezpečnosti ... 13
- 2. Riadenie aktív ... 13
- 3. Klasifikácia informácií ... 14
- 4. Personálna bezpečnosť ... 14
- 5. Fyzická, objektová bezpečnosť a bezpečnosť prostredia ... 16
- 6. Ochrana proti škodlivému softvéru ... 18
- 7. Zálohovanie ... 18
- 8.Topológia siete - bezpečnosť technických prostriedkov ... 19
- 9. Manipulácia s médiami ... 19
- 10. Služby elektronického obchodu ... 20
- 11. Požiadavky na riadenie prístupu ... 20
- 12. Zodpovednosti používateľov ... 20
- 13. Riadenie prístupu k aplikáciám a informáciám ... 21
- 14. Oznamovanie incidentov informačnej bezpečnosti a bezpečnostných slabín ... 22

SÚLAD SO ZÁKONNÝMI POŽIADAVKAMI ... 23

ZÁVER ... 24

- Existujúce riziká : ... 24
- Použité zdroje ... 24
- Prílohy: ... 25
- P o z n á m k y : ... 29

Všeobecné ustanovenia

Bezpečnostná dokumentácia popisuje prostredie spracúvania osobných údajov, rozsah spracúvania osobných údajov prevádzkovateľa MTK PLUS s.r.o., Stožok 424, 962 12 Detva (ďalej len prevádzkovateľ), identifikuje jednotlivé informačné systémy, hodnotí prijaté technické a organizačné opatrenia k ich ochrane, definuje a analyzuje úroveň bezpečnostných rizík a navrhuje opatrenia pre splnenie zákonných požiadaviek.

Dokumentácia je vypracovaná na základe požiadavky dokumentovania prijatých opatrení v súlade s ustanoveniami § 39 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „Zákon“) a Nariadenia EÚ 2016/679 pre členské štáty Európskej únie.

Predmetom dokumentácie je analýza stavu technických a organizačných opatrení v podmienkach prevádzkovateľa. Cieľom tohto dokumentu je komplexne zhodnotiť informačnú bezpečnosť a konfrontovať ju s požiadavkami medzinárodne uznávaných štandardov pre oblasť informačnej bezpečnosti (predovšetkým ISO/IEC 27002:2005).

Popisná časť analýzy stavu informačnej bezpečnosti je vypracovaná v štruktúre, ktorá reflektuje jednotlivé vytipované požiadavky bezpečnostného štandardu ISO/IEC 27002:2005 v primeranom rozsahu na podmienky prevádzkovateľa.

Predkladaný dokument obsahuje chránené informácie. Všetky informácie v ňom uvádzané slúžia výhradne na internú potrebu prevádzkovateľa alebo kontrolnej činnosti zo strany Úradu na ochranu osobných údajov.

1. Skratky a pojmy

Skratky:

AIS – automatizovaný informačný systém
BOZP – bezpečnosť a ochrana zdravia pri práci
DVR / NVR – záznamové zariadenia pre analógové alebo IP kamerové systémy
EPS – elektrická požiarna signalizácia
EZS – elektrická zabezpečovacia signalizácia
IT - informačné technológie
IS – informačný systém
LAN – Local Area Network (vnútorná sieť výpočtovej techniky)
NBU – Národný bezpečnostný úrad SR
N/A – nehodnotené riziko, nevyskytuje sa
PaM – Práce a Mzdy
PC – pracovná stanica užívateľa (personal computer)
PO – požiarna ochrana
ÚOOÚ – Úrad na ochranu osobných údajov
WAN – Wide Area Network (rozsiahla sieť výpočtovej techniky)

Pojmy :

Osobné údaje – údaje týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje alebo online identifikátor, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, genetickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu .

Spracúvanie osobných údajov – je spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi, alebo súbormi osobných údajov najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to či sa vykonáva automatizovanými alebo neautomatizovanými prostriedkami.

Prevádzkovateľ – je každý, kto sám alebo spoločne s inými vymedzí účel a podmienky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene, prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov.

Sprostredkovateľ – je každý, kto spracúva osobné údaje v mene prevádzkovateľa.

Zodpovedná osoba – je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorý plní úlohy podľa tohto zákona.

Dotknutá osoba – každá fyzická osoba, ktorej sa osobné údaje týkajú.

Informačný systém osobných údajov – je akýkoľvek usporiadaný súbor osobných údajov ktoré sú prístupné podľa určitých kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

Porušenie ochrany osobných údajov – je porušenie bezpečnosti (ďalej aj bezpečnostný incident), ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, alebo neoprávnenému poskytnutiu prenášaných uchovávaných osobných údajov, alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

Profilovanie – je akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.

Pseudonymizácia – spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez požitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej alebo identifikovateľnej fyzickej osobe.

Údaje týkajúce sa zdravia - sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o zdravotnom stave.

Tretia strana- je každý kto nie je prevádzkovateľ, sprostredkovateľ, dotknutá osoba alebo iná osoba, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje.

Aktívom informačnej bezpečnosti hmotný alebo nehmotný objekt, ktorý sa spolupodieľa na fungovaní a vytváraní informačného systému, najmä :
- údajové a dokumentačné aktíva najmä - databázy a dátové súbory, údaje a informácie, systémová dokumentácia, používateľské manuály, zácvikové materiály, prevádzkové alebo podporné procedúry, plány kontinuity, dohody o náhradných postupoch používaných v prípade zlyhania poskytovaných služieb alebo systému, archivované informácie,
- softvérové aktíva najmä - aplikačný softvér, systémový softvér, vývojové nástroje a pomocné programy, zdrojové knižnice programov, knižnice vykonateľných programov,
- fyzické aktíva najmä - počítačové vybavenie (procesory, monitory, modemy), komunikačné vybavenie (smerovače, prepínače, odkazovače), zálohovacie médiá (pásky, pevné disky, kompaktné disky), iné technické vybavenie (napájacie zdroje, klimatizačné jednotky),

Bezpečnostné riziko – je pravdepodobnosť, že existujúca hrozba využije zraniteľnosť aktív IS, čím nepriaznivo ovplyvní dôvernosť, integritu alebo dostupnosť spracúvaných osobných údajov, ako aj vážnosť dopadu využitia takejto zraniteľnosti

Kľúč – mechanický alebo technologický nástroj na zabezpečenie prístupu na pracoviská, do bezpečnostných zón a do ostatných objektov prevádzkovateľa, napr. bezpečnostný kľúč, prístupová karta, čip, prístupový kód

Autentizácia – proces overenia totožnosti oprávnenej osoby podľa požadovanej miery záruky na princípe porovnania identifikátora s hodnotou uloženou v informačnom systéme

Automatizovaný informačný systém – súhrn technických prostriedkov výpočtovej techniky, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením určeným na automatizované spracovanie údajov.

Zamestnanec – osoba v pracovnoprávnom vzťahu s prevádzkovateľom.

Zásady spracúvania osobných údajov

- zákonnosť

V podmienkach prevádzkovateľa sú spracúvané osobné údaje spracúvané výhradne na právnych základoch, napríklad sú nevyhnutné na uzatvorenie pracovnej zmluvy so zamestnancom. Po podpise pracovnej zmluvy v zmysle Zákonníka práce sú od zamestnanca vyžadované ďalšie informácie, napríklad osobné údaje rodinných príslušníkov, pre potreby plnenia požiadaviek ďalších, takzvaných osobitných zákonov, ktoré s pracovnoprávnym vzťahom bezprostredne súvisia (napríklad Zákon o daniach z príjmu. Zákon o sociálnom alebo dôchodkovom zabezpečení....) Prevádzkovateľ je oprávnený vyžadovať len ten rozsah osobných údajov, ktorý určuje konkrétny zákon.

Inou zákonnou požiadavkou môže byť spracúvanie osobných údajov nevyhnutných na ochranu života alebo zdravia dotknutej osoby (napr. lekári, zdravotná služba), alebo ak je spracúvanie nevyhnutné na splnenie úlohy vo verejnom záujme alebo pri výkone verejnej moci (obecné úrady, školstvo, ozbrojené zbory...), v tomto prípade rozsah osobných údajov určuje osobitný predpis, alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná. Zákonné požiadavky k získavaným a ďalej spracúvaným osobným údajom v podmienkach prevádzkovateľa sú rozpracované v tomto dokumente v časti „Informačné systémy“)

Podmienka zákonnosti je dodržaná aj v prípade, keď dotknutá osoba dobrovoľne poskytne určitý rozsah svojich osobných údajov (napríklad v predzmluvnom vzťahu v žiadosti o prijatie do zamestnania) alebo súhlasí so spracúvaním osobných údajov, na ktoré prevádzkovateľ inak nemá právny nárok (zverejnenie fotografie tváre zamestnanca alebo dotknutej osoby). Súhlas musí byť jednoznačný, slobodne daný a dotknutá osoba má právo tento súhlas kedykoľvek odvolať.

Prevádzkovateľ môže vyžadovať osobné údaje, ak ich spracúvanie je nevyhnutné na účel ochrany oprávnených záujmov prevádzkovateľa alebo tretej strany, napríklad fotografia tváre zamestnanca pre účel zhotovenia identifikačného štítku zamestnanca s povinnosťou viditeľného nosenia (§ 16 ods. 2 písm. b/), alebo inštalácia kamerového systému za účelom ochrany majetku prevádzkovateľa, alebo ochranu verejného poriadku a možnosti dokumentovania vzniknutej škody na živote, zdraví alebo majetku.
Pri požiadavke fotografie tváre je potrebné brať do úvahy aj recitál 51 DPR: *„Spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov , pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby.“*

- obmedzenie účelu a minimalizácia doby spracúvania

Prevádzkovateľ získava osobné údaje len na konkrétne určený oprávnený účel a je povinný ich spracúvať len v súlade s týmto účelom (napríklad personálna a mzdová agenda zamestnancov, agenda pacientov, agenda žiakov, agenda klientov advokátskej kancelárie...)
Pri aktuálnom ukončení spracúvania osobných údajov určuje osobitný predpis lehotu uchovávania osobných údajov (spisový materiál dotknutej osoby a jeho uloženie v registratúre)
Pred uložením do registratúry prevádzkovateľ zhodnotí obsah a rozsah dokumentácie a vyradí materiály, ktorých uchovávanie nie je naďalej nevyhnutné (napríklad fotografie)
Ďalšie spracúvanie osobných údajov na účel archivácie, vedeckého účelu, historického výskumu, alebo na štatistický účel, ak je v súlade s osobitným predpisom (napr. Zákon o štátnej štatistike...) a sú dodržané primerané záruky ochrany práv dotknutej osoby sa nepovažuje za nezlučiteľné s pôvodným účelom.

- minimalizácia rozsahu osobných údajov

Spracúvané osobné údaje musia byť primerané a obmedzené na nevyhnutný rozsah, daný účelom na ktorý sa spracúvajú. Rozsah a účel určuje osobitný zákon (predpis), alebo interný predpis (napr. aj zakladateľská listina).

- správnosť a aktuálnosť osobných údajov

Prevádzkovateľ zaznamenáva osobné údaje u ktorých podľa svojich možností overil ich správnosť (napr. porovnanie s úradným dokladom) pričom tieto údaje podľa potreby aktualizuje. Pri zistení a overení zmeny (adresa, meno, priezvisko, rodinný stav...) túto informáciu bezodkladne spracuje a informuje ďalšieho príjemcu, ak sú osobné údaje ďalej poskytované (sociálna, zdravotná poisťovňa, obchodný partner...)

- integrita a dôvernosť

Prevádzkovateľ prostredníctvom technických a organizačných opatrení zabezpečuje a zaručuje primeranú bezpečnosť spracúvaných osobných údajov, ktorá pozostáva z ochrany proti zámernému ale aj náhodnému poškodeniu alebo zničeniu, zmene, strate, neoprávnenému prístupu, neoprávnenému poskytnutiu, sprístupňovaniu, zverejňovaniu a akýmikoľvek inými neprípustnými formami spracúvania.

Prijaté opatrenia je povinný prevádzkovateľ podľa potreby aktualizovať, s ohľadom na vývoj technických riešení bezpečnosti a organizačných zmien.

Za týmto účelom je nevyhnutné:

- vytvoriť podmienky pre bezpečné umiestnenie dôležitých prvkov informačného systému v elektronickom aj manuálnom spracúvaní
- trvalo udržiavať a zlepšovať technickú a režimovú ochranu, chrániť informačné systémy pred zakázanými činnosťami,
- zaviesť do spracúvania osobných údajov riadiace a kontrolné procesy, spracovať internú dokumentáciu prevádzkovateľa pre činnosť s osobnými údajmi (záväzné vnútorné nariadenie, smernica, poučenie oprávnenej osoby, popis pracovnej činnosti, zmluva so sprostredkovateľom, záznamy o spracovateľských činnostiach...)

Popis zabezpečenia a rozsah prijatých opatrení je ďalej rozpracovaný v časti Analýza úrovne bezpečnosti.

- rozsah zodpovednosti

Prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami ich spracúvania a je povinný tento súlad na požiadanie úradu preukázať.

Vzhľadom k tomu, že každá osoba konajúca za prevádzkovateľa alebo sprostredkovateľa a má prístup k osobným údajom, môže tieto spracúvať len na základe pokynov prevádzkovateľa (alebo iného predpisu), prevádzkovateľ zabezpečí:

- v popise pracovnej činnosti určí rozsah činností, ku ktorým je osoba oprávnená
- v poučení zamestnanca určí požiadavky na spracúvanie osobných údajov, tak aby bola zaručená integrita, dôvernosť a dostupnosť spracúvaných osobných údajov
- definuje zoznam zakázaných činností
- oboznámi zamestnanca s možnosťou právnej zodpovednosti za porušenie stanovených požiadaviek

Spracovateľské činnosti v informačných systémoch.

- **Personálny a mzdový informačný systém**

V spracovateľskej činnosti agendy ľudských zdrojov je Personálny a mzdový informačný systém hlavnou časťou dokumentácie, je spracúvaný v písomnej a elektronickej forme. Elektronické spracúvanie mzdovej agendy je realizované zmluvným sprostredkovateľom. Dochádzka je zaznamenávaná zápisom. Prevádzkovateľ neuchováva agendu uchádzačov o zamestnanie, vzhľadom k minimálnemu počtu zamestnancov.

V rámci Personálnej a mzdovej agendy boli identifikované tieto subsystémy, v ktorých sa spracúvajú alebo môžu spracúvať osobné údaje zamestnancov:

- Prijímacie konanie zamestnancov (viď aj IS „Registratúra“)
- Osobné spisy zamestnancov
- Vzdelávací proces zamestnancov (viď aj IS „Registratúra“)
- Evidencia dochádzky
- Školenia BOZP a ochrany pred požiarmi
- Agenda pracovných úrazov zamestnancov
- Agenda poistných udalostí zamestnancov
- Agenda právnych sporov so zamestnancami

Všetky uvedené subsystémy spracúvajú osobné údaje na základe Zákonníka práce a ďalších zákonov súvisiacich s pracovnoprávnym vzťahom (dane, sociálne a zdravotné poistenie, dôchodkové zabezpečenie atď.) Účelom spracovateľskej činnosti je vytvorenie a dodržanie podmienok pracovnoprávneho vzťahu. Uvedené subsystémy nie je možné prevádzkovať samostatne, sú vždy viazané na PaM agendu.

V priebehu získavania osobných údajov v rámci prijímacieho konania zamestnanca v internom formulári „Osobný dotazník" môže zamestnávateľ požadovať fotografiu dotknutej osoby, napr. pre vyhotovenie identifikačných štítkov zamestnancov. V zmysle definície osobitných kategórií podľa § 16 ods. 1 Zákona je toto zobrazenie biometrickým údajom. Právnym základom a súčasne účelom spracúvania je oprávnený záujem prevádzkovateľa v zmysle §13 ods. 1 písm. f/ Zákona.

Ďalším prípadom môže byť požiadavka na zverejnenie fotografie tváre zamestnanca (mediálna prezentácia, web stránka...). V tomto prípade je právnym základom spracúvania súhlas dotknutej osoby.

Formulár súhlasu so zverejnením fotografie tváre zamestnanca musí presne definovať použitie fotografie, miesto zverejnenia a možnosť odmietnutia súhlasu. Formulár sa zakladá do osobného spisu zamestnanca.

Súhlas sa nevzťahuje na situácie dokumentovania aktivít prevádzkovateľa na web stránke prevádzkovateľa, dotknutá osoba je o dokumentovaní aktivít oboznámená.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách.

Vzhľadom na pravidelnosť spracúvania je potrebné v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Personálna a mzdová agenda", ktorý bude opisom spracovateľskej činnosti všetkých uvedených subsystémov ako jedného celku.

- **Účtovná agenda**

Spracovateľská činnosť pri tomto informačnom systéme je vyžadovaná osobitnými zákonmi riadiacimi obeh a uchovávanie účtovných dokladov. Účel spracúvania je daný jednotlivými zákonmi (Zákon o daniach z príjmu, Zákon o vedení účtovníctva...).

Agenda je spracúvaná v elektronickej aj písomnej forme, prevažnú časť agendy tvoria písomnosti dokumentujúce obchodné vzťahy s právnickými osobami. Elektronické spracúvanie je realizované zmluvnou právnickou osobou a uchovávané v zmysle požiadaviek zákona o účtovníctve.
V dokumentácii sa vyskytujú aj fyzické osoby, v rozsahu údajov meno, priezvisko, adresa a súvisiace informácie napr.:

- fakturovaná suma pri odkúpení prebytočného majetku organizácie
- fakturovaná suma za predaj tovaru alebo služby
- náhrady pri pracovných cestách
- náhrady pri používaní súkromného motorového vozidla na pracovné účely
- náhrada škody spôsobenej zamestnávateľovi

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách.

Vzhľadom na pravidelnosť spracúvania je potrebné v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Účtovná agenda", ktorý bude opisom uvedených spracovateľských činností ako jedného celku.

- **Správa registratúry**

Agenda vzniká predovšetkým v zmysle požiadaviek Zákona o archívoch a registratúrach a tiež za účelom plnenia požiadaviek osobitných zákonov, ktoré uchovávanie príslušného rozsahu dokumentácie v rôznych lehotách požadujú. Pošta je zaznamenávaná v písomnej forme, zakladaná chronologicky.
Spracovateľskú činnosť možno rozdeliť do dvoch skupín :

nepravidelne spracúvaná agenda - obsiahnutá v písomnom aj elektronickom spracúvaní

- dokumentácia vzniknutá vybavením došlej a odosielanej pošty obsahujúca osobné údaje (dožiadania orgánov štátnej správy alebo územnej samosprávy týkajúce sa zamestnanca – následne zakladané do osobného spisu)
- dokumentácia obsahujúca osobné údaje poskytnuté uchádzačom o zamestnanie v elektronickej alebo písomnej forme. Poskytnuté materiály (žiadosti, životopisy, priložené dokumenty) prechádzajú do personálnej agendy, alebo sú v režime nevyžiadanej pošty skartované (spravidla rok nasledujúci po roku prijatia žiadosti)
- dokumentácia obsahujúca osobné údaje vzniknutá v procese činnosti prevádzkovateľa (agenda činností prevádzkovateľa, prezenčné listiny, pozvánky, dotazníky...)

pravidelne spracúvaná agenda – obsiahnutá v písomnom aj elektronickom spracúvaní

- účtovné doklady obsahujúce osobné údaje, určené k uloženiu do registratúrneho strediska
- osobné spisy a agenda zamestnancov po ukončení pracovnoprávneho vzťahu, určené k uloženiu do registratúrneho strediska

Nespracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb.

Osobné údaje sa spracúvajú v pravidelných i nepravidelných intervaloch a uchovávajú sa v zákonom stanovených lehotách.

Vzhľadom na pravidelnosť spracúvania je potrebné v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Správa registratúry", ktorý bude opisom spracovateľskej činnosti.

- **Kamerový systém**

Účelom spracúvania je *oprávnený záujem prevádzkovateľa* v zmysle §13 ods. 1 písm.f/ Zákona pričom záznam monitorovaného prostredia môže byť použitý v oblastiach:

- prevencia trestnej a priestupkovej činnosti v monitorovanom prostredí
- možnosť dokumentovania vzniknutej škody na zdraví (dokumentovanie úrazu)
- poskytnutie dôkazného materiálu Policajnému zboru v zmysle Trestného poriadku (dokumentovanie vzniknutej škody)

Záznam je uchovávaný po dobu 5 dní, na vlastnom zálohovacom zariadení NVR.

Rozmiestnenie kamier je schematicky zaznamenané v prílohe internej smernice o používaní kamerového systému.

Kamerový systém nie je určený k monitorovaniu zamestnancov, s ohľadom na §13 Zákonníka práce.

O inštalácii kamerového systému je verejnosť informovaná informačnými tabuľkami na vstupoch do objektu.

Agenda je v elektronickej forme zaznamenávaná na NVR záznamník.

Nespracúvajú sa osobitné kategórie osobných údajov.

Nevykonáva sa profilovanie ani monitorovanie dotknutých osôb, vykonáva sa monitorovanie prostredia v ktorom sa fyzické osoby vyskytujú.

Osobné údaje sa spracúvajú v pravidelných intervaloch – v nepretržitom dátovom toku a následne sú prepisované novými dátami.

Vzhľadom na pravidelnosť spracúvania je potrebné v zmysle §37 ods. 1/ Zákona (čl. 30 GDPR) vytvoriť Záznam o spracovateľskej činnosti "Kamerový systém", ktorý bude popisovať uvedenú spracovateľskú činnosť.

Metodika analýzy úrovne bezpečnosti

Analýza súčasného stavu informačnej bezpečnosti (ďalej len analýza rizík) bola vykonaná formou kvalitatívnej analýzy rizík, a to v rozsahu a v súlade s požiadavkami nasledovných bezpečnostných štandardov:

- ISO/IEC 27001:2005 – Systém manažérstva informačnej bezpečnosti (ďalej len ISO 27001),
- ISO/IEC 27002:2005 – Kódex praxe manažérstva informačnej bezpečnosti (ďalej len ISO 27002),
- ISO/IEC 27005:2011 – Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti (ďalej len ISO 27005).

Pre identifikáciu a ohodnotenie rizík pôsobiacich na jednotlivé aktíva bol zvolený prístup analýzy vytipovaných rizík so zameraním sa najmä na aktíva, ktoré sú identifikované ako významné pre činnosť prevádzkovateľa. Analýza bola vypracovaná kvalitatívnou metódou.

Prehľad úrovne plnenia požiadaviek ISO/IEC 27002:2005 je hodnotený v trojúrovňovej škále:

ÁNO – požiadavka je splnená v plnom rozsahu, nie sú identifikované systémové nezhody, identifikované riziká boli akceptované

ČIASTOČNE – požiadavka je splnená iba čiastočne, nie sú identifikované systémové nezhody, boli identifikované riziká, ktoré neboli akceptované

NIE – požiadavka nie je plnená, resp. existuje systémová nezhoda

- **Vymedzenie hraníc určujúcich množinu zostatkových rizík**

V zmysle požiadaviek Zákona je prevádzkovateľ povinný prijať *vhodné, primerané opatrenia* na ochranu osobných údajov pred ich náhodným ako aj úmyselným poškodením či zničením, pred neoprávneným prístupom alebo akýmikoľvek nezákonnými spôsobmi spracúvania.

V prípade štandardnej ochrany spracúvaných dát je primeraným opatrením zamedzenie bezprostredného prístupu k dátam. Čiže zamestnanec (osoba určená k spracúvaniu údajov) prekonáva reálne prekážky pri prístupe k dátam (napr. deaktivácia poplachového systému, kľúče, prístupové heslá do databáz, prístupové práva...)
Pri vykonávaní analýzy bezpečnosti informačného systému je nutné brať do úvahy všetky faktory, spôsobilé narušiť bezpečnosť alebo funkčnosť IS, pričom sa prihliada na zhodu / nezhodu so stanovenými zásadami spracúvania.
Pri posudzovaní prostredia umiestnenia informačného systému v rôznych úrovniach informačnej bezpečnosti môžu byť zistené bezpečnostné riziká.

Pri hodnotení primeranosti nákladov na pokrytie hodnoteného rizika sa rozhoduje, či je zistené riziko závažné (jeho pokrytie je nevyhnutné), alebo bude akceptovateľné z dôvodu neúmerne vysokých nákladov na jeho pokrytie.
Hodnotenie rizík bude vykonané podľa nasledovných štyroch krokov :

a.) Špecifikácia rizík, z ktorých vyplýva akákoľvek hrozba pre funkčnosť systému v organizačnej alebo technickej oblasti – prevzaté z ISO normy.

b.) Určenie závažnosti rizika a definovanie jeho dopadu pre informačný systém.

Závažné riziko – riziko, ktoré nie je v súčasnosti dostatočne pokryté bezpečnostnými opatreniami a nebezpečenstvo z neho vyplývajúce je veľké (s návrhom nutných okamžitých opatrení na odstránenie rizika),

Pokryté riziko – riziko, ktoré je už inštalovanými bezpečnostnými opatreniami dostatočne pokryté,

Zostatkové riziko – riziko, ktoré po prijatí bezpečnostných opatrení zostalo nepokryté, ale jeho pravdepodobnosť výskytu je veľmi nízka, alebo cena technických opatrení k odvráteniu rizika je vzhľadom k hodnote chránených aktív neprimerane vysoká.

c.) Výber a navrhnutie opatrení, ktoré definované riziká eliminujú, prípadne zmiernia ich dopad.

d.) Posúdenie zostatkových rizík s ohľadom na pomer ceny bezpečnostných opatrení k hodnote, či dôležitosti spracúvaných dát.

K zostatkovým rizikám, ktoré nebudú brané do úvahy pri analýze bezpečnosti IS zaraďujem:

Povodeň – lokalizácia organizácie v záplavovom území môže znamenať vážne ohrozenie bezpečnosti a významné riziko zničenia informačného systému a spracúvaných osobných údajov.

Priestory prevádzkovateľa sú lokalizované mimo záplavových území, informačný systém nie je ohrozený zvýšenou hladinou riek, spodnou vodou ani prípadnou záplavou. Pri sústreďovaní podkladových informácií k spracovaniu bezpečnostnej dokumentácie je pri hodnotení

umiestnenia registratúrneho strediska a serverovej miestnosti braná do úvahy možnosť zaplavenia priestoru vodou z kanalizácie.

Zemetrasenie – môže spôsobiť nedostupnosť prípadne zničenie osobných údajov. V našej zemepisnej oblasti je riziko zemetrasenia zanedbateľné a navrhovanie opatrení k ochrane komponentov IS by bolo cenovo neúmerné k rozsahu a dôležitosti spracúvaných dát.

Terorizmus – cieľom terorizmu je násilné poškodenie prevádzkovateľa, čo najväčšie narušenie jeho činnosti, vznik psychickej nestability medzi zamestnancami. Riešenie hrozieb spojených s terorizmom je možné len v spolupráci s Políciou SR.

Audio a video monitoring priestoru - neoprávnené zaznamenávanie informácií napr. inštalované skryté kamery a mikrofóny v objekte...

Údaje spracovávané v prevádzkovateľa nie sú charakteru stupňa utajenia v zmysle zák. č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov, ktorý by vyžadoval krytie rizík tohto druhu.

Požiadavky na informačnú bezpečnosť

Identifikácia požiadaviek na informačnú bezpečnosť a na ochranu aktív je nevyhnutným predpokladom posúdenia primeranosti bezpečnostných opatrení. Požiadavky na informačnú bezpečnosť sú okrem toho dôležitým predpokladom pre stanovenie vhodnej stratégie obnovy jednotlivých systémov v prípade ich výpadku.
Požiadavky na informačnú bezpečnosť sú tvorené kombináciou troch základných atribútov bezpečnosti:

Dôvernosť *je charakteristika informácií, ktorá znemožňuje ich odhalenie neautorizovaným subjektom. Ide o zabránenie neoprávneného prístupu k informáciám a údajom.*
Potreba dôvernosti informačných aktív vyplýva z nasledovných základných typov požiadaviek:

- požiadavky slovenských, resp. medzinárodných právnych predpisov (najmä zákon o ochrane osobných údajov),
- ochrana oprávnených záujmov tretích strán – ochrana informácií, ktoré by v prípade zverejnenia neoprávneným osobám, mohli poškodiť tretie strany

Dostupnosť *je vlastnosť systému, ktorá zabraňuje neautorizovanému zadržaniu zdrojov alebo údajov. Dostupnosť zaručuje, že informácie budú na správnom mieste v správnom čase alebo, že daná udalosť nastane do určenej doby.*
Požiadavky na dostupnosť informačných aktív a prevádzkovaných systémov a aplikácií prevádzkovateľa vyplývajú najmä:

- z požiadaviek právnych predpisov – dostupnosť systémov vyplývajúca z povinnosti vykonania činností do zákonom stanoveného termínu (zaslanie príslušných informácií štátnym inštitúciám, podanie daňového priznania, úhrada odvodov a pod.),

Integrita *dodržanie tejto požiadavky zaručuje, že objekt(údaje, informácie) bol zmenený len špecifikovaným a autorizovaným spôsobom, bez skrytej manipulácie.*
Pri integrite je dôležité rozlišovať, či je možné modifikácii predchádzať alebo ju len detekovať.

Požiadavky na integritu spracúvaných údajov vyplývajú najmä z:

- požiadaviek právnych predpisov a požiadaviek štátnych orgánov na správnosť a aktuálnosť údajov

- požiadaviek organizácie na predchádzanie možnej škody vzniknutej zničením alebo neautorizovanou zmenou chránených údajov.

Analýza úrovne bezpečnosti

V nasledujúcej časti dokumentu sú popísané výsledky posúdenia úrovne informačnej bezpečnosti relevantných aktív prevádzkovateľa, v oblastiach definovaných bezpečnostným štandardom.

- **1. Politika informačnej bezpečnosti**

V podmienkach prevádzkovateľa sú požiadavky na informačnú bezpečnosť stanovené v internej smernici k ochrane osobných údajov a v poučení zamestnanca.

Pod informačnou bezpečnosťou sa rozumie aktuálny stav plnenia požiadaviek v hodnotených oblastiach fyzickej a objektovej bezpečnosti, organizačnej bezpečnosti, bezpečnosti technických prostriedkov a personálnej bezpečnosti (zvyšovanie úrovne znalostí zamestnancov o definovaných požiadavkách)

Požiadavky na zavádzanie nových prostriedkov na spracúvanie informácií do prostredia vychádzajú od správcu informačných technológií, alebo sú vynútené zmenami v systémoch elektronického spracovania dát (update inštalovaných programov)

Správa informačných technológií je realizovaná zmluvným správcom informačných technológií.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A..1.1 Vedenie organizácie musí aktívne podporovať bezpečnosť vo svojich podmienkach prostredníctvom jasných pokynov, preukazovania angažovanosti, explicitným prideľovaním a uvedomovaním si bezpečnostných zodpovedností.	☒	☐	☐
A..1.2 Všetky bezpečnostné zodpovednosti musia byť definované jednoznačne.	☒	☐	☐
A..1.6 Musia sa udržiavať príslušné kontakty s relevantnými orgánm moci.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **2. Riadenie aktív**

Zodpovednosť za aktíva

Softvérové a hardvérové aktíva prevádzkovateľa tvorí technická infraštruktúra a programové vybavenie. Inventarizácia aktív sa vykonáva predovšetkým vo vzťahu k ekonomike prevádzkovateľa, jednotlivé zodpovednosti a právomoci zodpovedných osôb sú uvedené v popisoch pracovnej činnosti. Aktíva využívané priamo konkrétnymi zamestnancami (notebooky, pracovné stanice, tlačiarne, existujúcu dokumentáciu a iné príslušenstvo) majú konkrétni zamestnanci pridelené. Takýmto spôsobom je určené aj vlastníctvo týchto aktív.
Spôsob prideľovania a presuny HW komponentov zamestnancom nie sú upravené v osobitnom predpise. Evidencia hardveru je vedená v agende majetku. Zamestnanci nemajú povolené svojvoľne presúvať majetok, čím sa má zabrániť vzniku možných rozdielov medzi vedenými evidenciami a skutočnosťou.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.2.1 Všetky aktíva musia byť jednoznačne identifikované a mal by byť zostavený a udržiavaný inventárny zoznam všetkých významných aktív.	☒	☐	☐
A.1.2 Pravidlá pre prijateľné použitie informácií a aktív spojených s prostriedkami na spracúvanie informácií musia byť zdokumentovan a implementované.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **3. Klasifikácia informácií**

Pre osobné údaje sú definované základné pravidlá spracúvania v zákone súvisiacom so spracúvaním, v poučení oprávnených osôb, ako aj v popise pracovnej činnosti zamestnancov.
Pre základné požiadavky ochrany osobných údajov má prevádzkovateľ vypracované poučenie zamestnancov (bližšie informácie o problematike ochrany osobných údajov sa nachádzajú následne v tomto dokumente.

Vzhľadom k charakteru spracúvaných informácií, ktoré nepodliehajú ochrane utajovaných skutočností nie sú prijaté kryptografické opatrenia alebo trezorové úschovné objekty na ukladanie listinnej formy jednotlivých dokumentácií.

Príslušné dokumentácie sú zakladané v kancelárskych zakladačoch s označením. Všetky spracúvané dokumentácie pre organizáciu majú svoj význam daný požiadavkami jednotlivých zákonov podľa ktorých sa spracúvanie realizuje.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.3.1 Informácie musia byť klasifikované na základe ich hodnoty, právnych požiadaviek, citlivosti a významnosti pre organizáciu.	☒	☐	☐
A.3.2 Musí byť zostavená a implementovaná primeraná sada procedúr na označovanie informácií a zaobchádzanie s nimi v súlad s klasifikačnou schémou, ktorú si organizácia osvojila.	☒	☐	☐

Existujúce procesy prebiehajú na základe zákonných požiadaviek.
Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **4. Personálna bezpečnosť**

V nasledujúcom texte sú popísané procesy spojené s prijímaním zamestnancov, s ich hodnotením a ukončením pracovného pomeru.

Informácie o pridelení / odobratí prístupových práv do elektronického spracúvania dát, popisované v nasledujúcej časti sú informatívne, v závislosti od aktuálnej štruktúry zamestnancov pracujúcich s výpočtovou technikou.

Bezpečnostné roly a zodpovednosti zamestnancov sú definované popisom pracovnej činnosti zamestnanca.

/ **PRED NÁSTUPOM DO ZAMESTNANIA**

Proces prijímania nových zamestnancov je realizovaný výberom. Za tento proces zodpovedá konateľ.
Požiadavky na potrebu prijatia nového zamestnanca sú zadávané vedúcim zamestnancom v konkrétnej oblasti výkonu práce.
Vhodný kandidát je hľadaný vyhľadávaním vo verejne dostupných databázach, v databáze uchádzačov, alebo prostredníctvom zverejnenej inzercie. Konečné rozhodnutie o prijatí kandidáta vykonáva konateľ a súčinnosti s personalistom.
Overenie odborných predpokladov podľa predložených kvalifikačných dokumentov uchádzača je súčasťou výberového konania.
Novoprijatý zamestnanec prechádza vstupným oboznámením hlavne s pracovným poriadkom, organizačnými zvyklosťami, požiarnou ochranou a BOZP. Priamo v pracovnej zmluve

zamestnanca nebývajú zakomponované pravidlá informačnej bezpečnosti, ktoré je povinný zamestnanec dodržiavať. Uvedené je riešené poučením zamestnanca.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.4.1 Bezpečnostné role a zodpovednosť zamestnancov, musia byt definované a zdokumentované	☒	☐	☐
A.4.2 Musí byť vykonaná verifikačná previerka personálneho pozadia všetkých uchádzačov o zamestnanie, aj vzhľadom na obchodné požiadavky, klasifikačný stupeň informácií, ku ktorým sa musí pristupovať ako aj na vnímané riziká.	☒	☐	☐
A.4.3 Zamestnanci, musia byť v pracovnej zmluve alebo v samostatnom poučení oboznámení s podmienkami, ktoré musia definovať zodpovednosti za informačnú bezpečnosť v rámci organizácie.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

/ POČAS ZAMESTNANIA

Náležitosti týkajúce sa pracovného pomeru zamestnanca sú dané zákonníkom práce.
Proces vzdelávania pozostáva zo školení podľa osobitných predpisov a odborných školení. U zamestnancov pracujúcich v administratíve sa vykonávajú vstupné školenia pre novoprijatých zamestnancov, poučením, ktoré pokrýva aj oblasť informačnej bezpečnosti.

Cyklické povinné školenia sú realizované pravidelne podľa právnych predpisov. Pravidelné školenia zamestnancov v oblasti informačnej bezpečnosti sa nevykonáva. Bezpečnostné povedomie by malo byť zvyšované prostredníctvom samoštúdia zamestnancov.

Zvyšovanie odbornej kvalifikácie zamestnancov je neustálym procesom vyvolaným zmenami zákonných požiadaviek alebo samotným výkonom práce.
Prípadný disciplinárny proces je realizovaný v zmysle zákonníka práce.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.4.4. Manažment musí od zamestnancov vyžadovať uplatňovanie postupov v zmysle požiadaviek k zabezpečeniu dokumentácií a počítačových komponentov alebo dát.	☒	☐	☐
A.4.5. Všetci zamestnanci a v prípade, že je to potrebné aj zmluvní partneri a používatelia v pozícii tretích strán musia byť poučení o požiadavkách vyplývajúcich z potrieb ochrany osobných údajov a ochrany nosičov údajov.	☒	☐	☐
A.4.6. Musí existovať disciplinárny proces pre zamestnancov, ktorí spôsobili narušenie bezpečnosti.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

/ UKONČENIE ALEBO ZMENA PRACOVNEHO POMERU

Pracovný pomer sa končí v súlade s príslušnými ustanoveniami Zákonníka práce.
Pri ukončení pracovného pomeru alebo v prípade dlhodobej neprítomnosti zamestnanca je odobratie majetku zabezpečené potvrdením na výstupnom liste zamestnanca Na výstupnom liste príslušní zodpovední zamestnanci potvrdia vyrovnanie záväzkov. Výstupný list slúži aj ako podklad pre zrušenie prístupových práv zamestnancov. Správca počítačovej siete zodpovedá za odstránenie prístupových práv pridelených zamestnancovi pre výkon jeho práce.

Pri ukončení pracovného pomeru je zamestnanec upozornený na záväzky, ktoré pre neho naďalej platia, napr. zachovávanie mlčanlivosti o osobných údajov a prípadne o ďalších vybraných skutočnostiach).

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.4.7. Za realizáciu procesu ukončenia pracovného pomeru zodpovedá zamestnanec personalistiky, štatutárny zástupca.	☒	☐	☐
A.4.8. Všetci zamestnanci musia vrátiť akékoľvek aktíva patriace organizácii po zrušení ich pracovného pomeru, resp. po vypršaní uzatvorenej dohody alebo zmluvy.	☒	☐	☐
A.4.9. Prístupové práva všetkých zamestnancov, zmluvných partnerov a používateľov v pozícii tretích strán k informáciám a prostriedkom na ich spracúvanie musia byť po ukončení pracovného pomeru, zmluvy alebo dohody odňaté alebo upravené podľa zmeny	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **5. Fyzická, objektová bezpečnosť a bezpečnosť prostredia**

V kontexte celkovej bezpečnosti informačných technológií a informačných systémov hrá dôležitú úlohu fyzická bezpečnosť jednotlivých zariadení a prostredia, v ktorom sa nachádzajú. V tejto časti je fyzická bezpečnosť rozoberaná hlavne vo vzťahu k bezpečnosti IS a k procesom, ktoré by ju mohli narušiť. Analyzovaný je nielen stav fyzickej bezpečnosti prostredia, ale aj stav fyzickej bezpečnosti komponentov IT infraštruktúry a likvidácia dátových nosičov. Popis aktuálneho stavu je zameraný na priestory, kde sú umiestnené dôležité komponenty informačných technológií.

Prevádzkovateľ sídli v prenajatých priestoroch v stráženom areáli Podpolianských strojární. Ochrana objektu proti neoprávnenému vstupu je zabezpečená inštaláciou poplachového systému. Signál poplachového systému je vedený cestou mobilného operátora odoslaním SMS na telefóny určených zamestnancov.
Osoby oprávnené k samostatnému vstupu do objektu používajú vlastný prístupový kód, systém umožňuje určiť osobu, ktorá aktivovala / deaktivovala poplachový systém.
Výdaj kľúčov nie je vzhľadom k počtu administratívnych zamestnancov evidovaný, kľúče vydáva konateľ.
V poučení zamestnanca pracujúceho v administratíve je stanovená požiadavka, zabezpečenia spracúvaných osobných údajov pred neoprávneným prístupom.
Politika „čistého stola“ je vyžadovaná interným pokynom, podľa aktuálnych podmienok pri odchode z kancelárie (ukončenie pracovnej doby) uložiť spracúvanú dokumentáciu a dátové nosiče do uzamykateľnej skrine.

Upratovací personál nemá prístup k spracúvaným osobným údajom, dokumentácie sú uchovávané uzamknuté, alebo je upratovanie realizované za prítomnosti oprávnených osôb.

Aktívne prvky siete LAN sú uložené v serverovej miestnosti, v technologickej skrini „rack“ zabezpečenej proti prístupu nepovolaných osôb.

/ Registratúrne stredisko

Príručná agenda je uložená v kancelárii spracúvania, uložená v kancelárskych zakladačoch. Agenda uchovávaná v zmysle požiadaviek osobitných zákonov je uchovávaná v registratúrnom stredisku v prízemí budovy.

Vstup do miestností je zabezpečený uzamykateľnými dverami klasickej konštrukcie. Kľúče od miestností má k dispozícií konateľ.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.5.1 Bezpečnostné perimetre (prekážky akými sú steny, vstupné brány ovládané prístupovými kartami alebo recepčná služba na vstupe) musia byť použité na ochranu priestorov, kde sa nachádzajú informácie a prostriedky na ich spracúvanie.	☒	☐	☐
A.5.2 Zabezpečené oblasti musia byť chránené primeranými opatreniami na vstupe, aby sa zabezpečilo, že vstúpiť môžu len autorizované osoby.	☒	☐	☐
A.5.3 Fyzická bezpečnosť pre miestnosti, kancelárie a zariadenia musí byť navrhnutá a aplikovaná.	☒	☐	☐
A.5.4 Prístupové body, akými sú zásobovacie a expedičné priestory ako aj iné body, kde môže neautorizovaná osoba získať prístup do priestorov organizácie musia byť kontrolované a ak je to možné aj izolované od prostriedkov na spracúvanie informácií, aby sa zabránilo neautorizovanému prístupu.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

/ BEZPEČNOSŤ ZARIADENÍ

Aktívne zariadenia (smerovač, prepínače, server a iné) siete LAN sú chránené pred vplyvmi prostredia a neautorizovaným prístupom. Aktívne prvky LAN sú zálohované zdrojmi elektrickej energie UPS.
Osobný počítač sa v prípade jeho odpredaja zamestnancovi softvérovo vymaže, aby sa zabránilo možnému úniku informácii, alebo zneužitiu licencovaného softvéru v prípade vyradenia zariadenia.

Zamestnanci ktorým to vyplýva z pracovných potrieb používajú prenosné zariadenia (notebooky) aj mimo pracoviska.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.5.5. Zariadenia musia byť umiestnené a chránené s cieľom obmedziť riziká vyplývajúce z hrozieb prostredia a príležitosti na neautorizovaný prístup.	☒	☐	☐
A.5.6. Zariadenia musia byť chránené pred výpadkami elektrickej energie a inými anomáliami spôsobenými zlyhaním dodávky podporných služieb.	☒	☐	☐
A.5.7. Elektrická alebo telekomunikačná kabeláž prenášajúca dáta alebo podporné informačné služby, musí byť primerane chránená	☒	☐	☐
A.5.8. Zariadenia musia byť správne udržiavané, aby sa zaistila ich trvalá dostupnosť a integrita.	☒	☐	☐
A.5.9. Všetky prvky zariadení obsahujúce úložné médiá pre dáta musia byť skontrolované, aby sa zabezpečilo, že všetky citlivé dáta licencovaný softvér boli bezpečne zmazané alebo boli prepísané pred vyradením zariadení.	☒	☐	☐
A.5.10. Prístroje, informácie alebo softvér nesmú byť bez predchádzajúceho odsúhlasenia vynášané mimo pracoviska.	☒	☐	☐

Záver: riziká sú pokryté, nie sú vyžadované ďalšie opatrenia

- **6. Ochrana proti škodlivému softvéru**

V LAN prostredí je zabezpečená ochrana proti škodlivému kódu na všetkých dôležitých komponentoch. Na ochranu pracovných staníc proti škodlivým kódom sa používa antivírusová ochrana. Používateľom je znemožnené zasahovať do konfigurácie antivírového riešenia. Databáza vzoriek škodlivých kódov sa pravidelne aktualizuje zo serverov výrobcu. .

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.6.1.1. Musia byť implementované opatrenia detekcie, predchádzania na ochranu pred škodlivým kódom a informovanie používateľov.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **7. Zálohovanie**

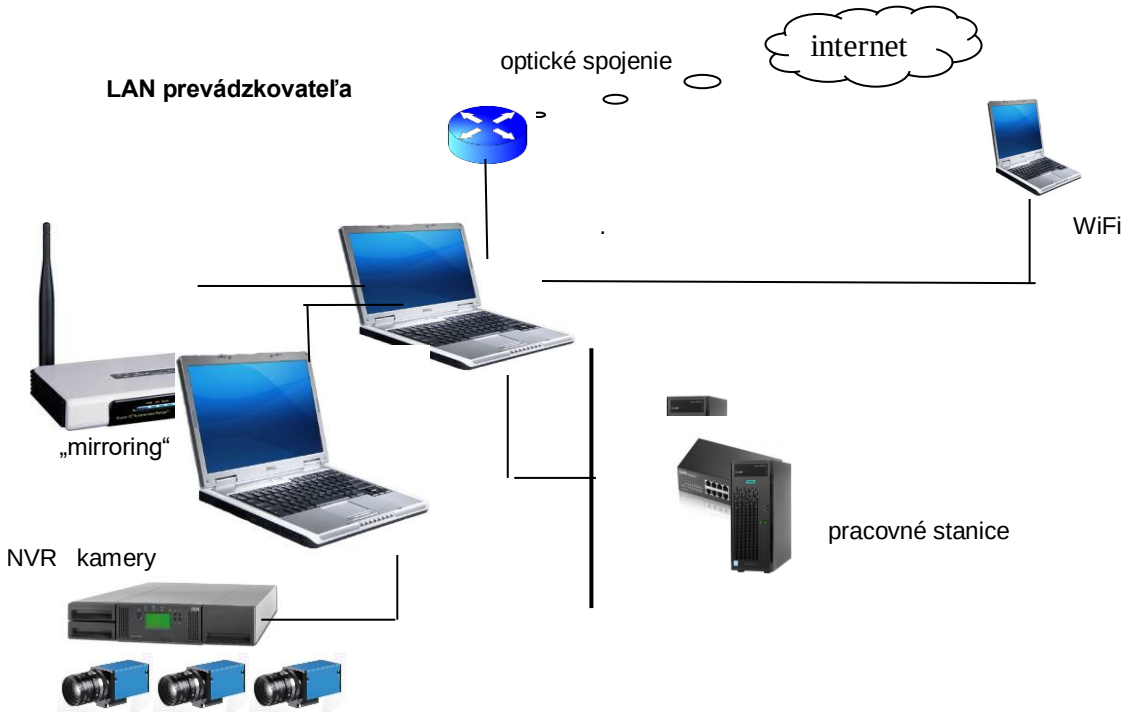
Zálohy spracúvaných osobných údajov sú realizované tzv. „zrkadlovou zálohou“ na dvoch serveroch. Užívateľ si zálohuje potrebné dáta na adresár servera alebo USB médium. Ďalšou zálohou sú písomné výstupy agendy.
Testovanie záloh sa vykonáva podľa potreby po zálohovaní.

Zálohovanie pre jednotlivé dáta bolo zvolené na základe analýzy možných dopadov straty údajov na jednotlivé činnosti a procesy. Elektronické zálohy dát sú pri spracúvaní personálnej, mzdovej a účtovnej agendy taktiež vyžadované zákonom.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.7.1 Pravidelne sa musia robiť záložné kópie dôležitých informácií softvéru v súlade so schválenou politikou zálohovania.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **8.Topológia siete - bezpečnosť technických prostriedkov**



Topológia siete LAN je načrtnutá orientačne so zameraním sa na spracúvané osobné údaje, neobsahuje ďalšie prvky LAN (UPS zálohy el. napätia, optické prevodníky, switche na preklenutie vzdialenosti rozvodu LAN...) Detailný popis siete, konfiguráciu a použité technické prvky uchováva správca informačných technológií.

O topológii siete a jej zmenách a zabezpečení sa rozhoduje na úrovni požiadavky správcu informačných technológií a konateľa.
V rámci sieťového prostredia prevádzkovateľa sa jedná o LAN sieť, v ktorej je prístup k spracúvaným dátam obmedzený úrovňou prístupových práv.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.8.1 Sieť musí byť primerane riadené a spravované, čím sa zabezpečí ochrana pred hrozbami a udržanie primeranej bezpečnosti systémov a aplikácií využívajúcich sieťové prostredie, vrátane prenášaných informácií.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **9. Manipulácia s médiami**

Základné pravidlá pre bezpečnú manipuláciu s médiami, s ohľadom na citlivosť údajov na nich uložených, sú definované v poučení zamestnanca. Súčasťou poučenia sú minimálne požiadavky na ochranu, prenos, likvidáciu. Je zaužívané, že predtým ako je nejaký HW obsahujúci informácie odovzdaný inému zamestnancovi, vyradený alebo odpredaný, tak sú všetky nosiče informácií zmazané (resp. je kompletne preinštalovaný OS).
Média sa vyraďujú a likvidujú spôsobom, ktorý znemožní obnovu ich obsahu. V prípade nadbytočne vytlačeného dokumentu, alebo dokumentu s nesprávnymi údajmi je zamestnanec povinný tento bezodkladne zlikvidovať. Skartovací stroj je dostupný.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.9.1. Médiá, ak už nie sú potrebné, musia byť bezpečne	☒	☐	☐

zlikvidované s uplatnením formálnych procedúr.

A.9.2. Musia byť zavedené postupy pre narábanie s informáciami a ich ukladanie, aby sa informácie takto chránili pred neautorizovaným odkrytím alebo zneužitím.	☒	☐	☐
A.9.3.Písomná aj systémová dokumentácia musí byť chránená prec neautorizovaným prístupom.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **10. Služby elektronického obchodu**

Prevádzkovateľ neposkytuje služby elektronického obchodu.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.10.1. Informácie zapojené do elektronického obchodovania prechádzajúce verejne dostupnými sieťami musia byť chránené pre možnosťou podvodných činov, vzniku rozporov so znením uzatvorených zmlúv, neautorizovaným prezradením alebo modifikáciou.		N/A	
A.10.2. Informácie zapojené do on-line transakcií musia byť chránené, aby sa predišlo neúplnosti prenosu, nesprávnemu smerovaniu, nepovolenému skresleniu správ, neautorizovanému prezradeniu, neautorizovanej tvorbe kópii alebo opakovanému prehrávaniu.		N/A	
A.10.3. Integrita informácií, ktoré sa majú sprístupniť prostredníctvom verejne dostupného systému musí byť chránená, aby sa predišlo ich neautorizovanej modifikácii.		N/A	

Záver: riziko nebolo hodnotené

- **11. Požiadavky na riadenie prístupu**

Prístupy do aplikácií obsahujúcich osobné údaje vyplývajú z popisu pracovnej činnosti zamestnanca. Prístupové práva používateľov k spracúvaným dátam sú riadené prostredníctvom nastavení užívateľských práv na základe požiadavky konateľa. Detailnejšie je spôsob riadenia prístupu k zdrojom, informáciám a aplikáciám popísaný v nasledovných kapitolách.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.11.1. Na základe bezpečnostných požiadaviek na prístup musí by definovaný prístup v popise pracovnej činnosti alebo v samostatnom dokumente.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **12. Zodpovednosti používateľov**

Vybrané povinnosti a zodpovednosti používateľov sú popísané v popise pracovnej činnosti a poučení zamestnanca.

K základným zodpovednostiam patrí najmä zachovávanie dôvernosti a ochrana svojich prístupových hesiel a autentizačných predmetov. V zmysle platných pravidiel používatelia zodpovedajú za všetky udalosti, transakcie a činnosti, ktoré sa uskutočnili v prostredí počítačovej siete, s použitím ich užívateľského mena a hesla. V podmienkach prevádzkovateľa je stanovená heslová politika. Užívatelia si volia minimálne osem znakové heslo s obsahom kombinácie veľkých a malých písme, číslic a znakov.

Používatelia tiež zodpovedajú za ochranu aktív IS (napr. údaje, zariadenia, softvér) pred narušením ich bezpečnosti (napr. prezradenie, zničenie, krádež, neautorizované použitie), a to najmä dodržiavaním opatrení a pravidiel stanovených v poučení. Tieto pravidlá sú zamerané najmä na nasledujúce oblasti:

- pravidlo čistého stola a čistej obrazovky,
- pravidlá ochrany proti škodlivému kódu,
- pravidlá práce v internej sieti prevádzkovateľa
- pravidlá pre hlásenie bezpečnostných incidentov.

Používatelia výpočtovej techniky sú o základných pravidlách a povinnostiach poučení pri nástupe do zamestnania.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.12.1. Od používateľov sa musí vyžadovať, aby pri výbere a používaní hesiel dodržiavali potrebné bezpečnostné zásady.	☒	☐	☐
A.12.2. Od používateľov sa musí vyžadovať, aby zaisťovali primeranú ochranu nestrážených prostriedkov.	☒	☐	☐
A.12.3. Musí byť prijatá politika čistého stola pre dokumenty a prenosné médiá a politika čistej obrazovky pre prostriedky spracúvania informácií.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **13. Riadenie prístupu k aplikáciám a informáciám**

Základný prístup k aplikáciám a informáciám je riadený udelením prístupových práv na základe požiadavky konateľa. Pre používané aplikácie sa vyžaduje úroveň identifikácie a autentizácie, pomocou používateľského mena a hesla. Prístup do databáz
V aplikáciách je riadený selektívny prístup k údajom podľa potrieb a popisu pracovnej činnosti.

Požadované opatrenie je splnené	Áno	Čiastočne	Nie
A.13.1. Prístup k informáciám a funkciám aplikačných systémov prostredníctvom používateľov a podporných pracovníkov musí byť obmedzovaný v súlade s politikou riadenia prístupu.	☒	☐	☐
A.13.2. Citlivé systémy musia mať vyhradené (izolované) výpočtové prostredie.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

- **14. Oznamovanie incidentov informačnej bezpečnosti a bezpečnostných slabín**

V podmienkach prevádzkovateľa nie je zavedená samostatná interná smernica, ktorá by upravovala pravidlá súvisiace so správou bezpečnostných incidentov.
V zmysle poučenia jeho zamestnancov sú prípadné bezpečnostné incidenty zistené v prvkoch počítačovej siete, alebo písomnom spracúvaní dát osobne, alebo telefonicky hlásené správcovi informačných technológií, resp. oznámené na kontaktný e-mail, k ďalšiemu zdokumentovaniu.
Výpadky systémov sú obyčajne hlásené priamo zamestnancom, ktorí zodpovedajú za správu daného systému.

A.14.1. Udalosti v prostredí informačnej bezpečnosti, ktoré by mali dopad na zabezpečenie spracúvaných dát, musia byť nahlásené prostredníctvom primeraných riadiacich kanálov tak rýchlo ako je to možné.	☒	☐	☐
A.14.2. Od všetkých zamestnancov využívajúcich informačné systémy a služby sa musí vyžadovať ohlasovanie spozorovaných a potenciálnych bezpečnostných slabín, alebo neštandardné správan aplikácie.	☒	☐	☐

Záver: riziko je pokryté, nie sú vyžadované ďalšie opatrenia

Ak je pravdepodobné, že porušenie ochrany osobných údajov – bezpečnostný incident povedie k riziku ohrozenia práv fyzických osôb, prevádzkovateľ je povinný tento bezpečnostný incident oznámiť Úradu na ochranu osobných údajov najneskôr do 72 hodín, prípadné nedodržanie povinnosti do stanovenej lehoty je povinný náležite zdôvodniť.

V oznámení prevádzkovateľ uvádza:

- popis bezpečnostného incidentu
- kontaktné údaje osoby u ktorej je možné získať detailnejšie informácie
- popis pravdepodobných následkov bezpečnostného incidentu
- popis prijatých opatrení na nápravu alebo zmiernenie dopadu bezpečnostného incidentu

Ak prevádzkovateľ neoznámil bezpečnostný incident dotknutým osobám, Úrad môže po zvážení dôsledkov bezpečnostného incidentu splnenie tejto požiadavky od prevádzkovateľa požadovať.

Súlad so zákonnými požiadavkami

Zhodnotenie stavu spracúvania osobných údajov v informačných systémoch prevádzkovateľa je riešené súhrnne, vzhľadom k tomu že pre všetky informačné systémy a prebiehajúce procesy spracúvania platia určené zásady rovnako.

Súlad / nesúlad je zisťovaný porovnaním skutkového stavu s požiadavkami jednotlivých zásad.

Zásada zákonnosti

Osobné údaje zamestnancov sú získavané a spracúvané v dvoch úrovniach:
V predzmluvnom vzťahu sú vyžadované výlučne osobné údaje a informácie pre posúdenie kvalifikačných predpokladov uchádzača. Po splnení podmienok výberu sú vyžadované následné informácie v rozsahu určenom Zákonníkom práce a osobitnými zákonmi v priamej súvislosti s pracovnoprávnym vzťahom.
Ďalšie spracúvanie osobných údajov v popisovaných subsystémoch agendy ľudských zdrojov je z uvedených dôvodov zákonné.

Osobné údaje dotknutých osôb (obchodná činnosť), vyskytujúcich sa v účtovnej agende sú získané a uchovávané v zmysle zákonov súvisiacich s vedením účtovníctva a dokumentovaní finančných tokov (zákon o daniach, zákon o účtovníctve...).

Osobné údaje klientov Stanice technickej a emisnej kontroly sú vyžadované zákonom.

Zásada obmedzenia účelu

Osobné údaje sú spracúvané výhradne za účelom plnenia požiadaviek vyplývajúcich z osobitných zákonov, alebo zámeru prevádzkovateľa.

Zásada minimalizácie osobných údajov

Rozsah spracúvaných osobných údajov je nevyhnutný a primeraný danému účelu.

Zásada správnosti

Pravdivosť a správnosť osobných údajov je overovaná bezprostredne pri ich získavaní a zaznamenávaní do informačného systému, porovnaním poskytnutých údajov s úradným dokladom. Požiadavka aktuálnosti je delegovaná na dotknuté osoby, ktoré sú povinná bezodkladne oznámiť akúkoľvek zmenu spracúvaných osobných údajov (zmena priezviska, adresy...)

Zásada minimalizácie uchovávania

Po ukončení aktuálneho spracúvania pre daný účel sú dokumenty obsahujúce osobné údaje uchovávané v registratúrnom stredisku, v zmysle požiadaviek zákonov súvisiacich so spracúvaním. Tieto zákony (napr. zákon o daniach...) priamo určujú lehotu uchovávania.

Zásada integrity a dôvernosti

Integrita spracúvaných osobných údajov je zabezpečená prijatím opatrení v nasledujúcich hodnotených oblastiach:

- *V oblasti objektovej bezpečnosti* zamedzením vstupu neoprávnených osôb do objektu a priestorov prevádzkovateľa obsahujúcich osobné údaje v písomnej alebo elektronickej forme uzamknutím priestorov,
- *V oblasti organizačnej bezpečnosti* pridelením kľúčov, resp. prístupových kariet, skartáciou nadbytočne vyhotovených dokumentov obsahujúcich osobné údaje, vydaním interných pokynov, smerníc.

- *V oblasti personálnej bezpečnosti* výberom zamestnanca na pracovnú pozíciu, popisom pracovných činností a poučením.
- *V oblasti bezpečnosti technických prostriedkov* prijatím opatrení proti škodlivým kódom (antivírus, antispam...), určením prístupových práv do databáz a aplikácií, používaním prístupových hesiel, bezpečnostnými nastavenia a zálohovaním dát, bezprostredným odstránením prístupových práv zamestnanca pri ukončení pracovného pomeru...

Zásada zodpovednosti

Prevádzkovateľ zodpovedá za dodržiavanie uvádzaných zásad spracúvania osobných údajov vo všetkých podmienkach, oblastiach a okolnostiach spracúvania. Túto zodpovednosť deleguje aj na zamestnancov formou popisov pracovných činností, smernicami a internými pokynmi, poučením zamestnanca. Čiastkovou zodpovednosťou je v prípade potreby viazaný sprostredkovateľ tak, ako im to definuje zmluva alebo požiadavky osobitných zákonov, v zmysle ktorých je spracúvanie vykonávané.

Záver**:** Po vyhodnotení požiadaviek pokrytia bezpečnostných rizík a porovnanie stavu a prostredia spracúvaných osobných údajov v elektronickej aj písomnej forme konštatujem, že prebiehajúce spracovateľské operácie a vykonané opatrenia sú v s ú l a d e s definovanými zásadami spracúvania.

- **Existujúce riziká :**

Neboli zistené

- **Použité zdroje**

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane osobných údajov „General Data Protection Regulation“
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
STN ISO/IEC 27001, 27002 – Bezpečnostný zámer
Národná stratégia pre informačnú bezpečnosť v Slovenskej republike
Výnos Ministerstva financií SR 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy
Občiansky zákonník a Zákonník práce v aktuálnom znení
Analýza materiálov získaných od zadávateľa projektu

- **Prílohy:**

Záznam o spracovateľských činnostiach prevádzkovateľa
v informačnom systéme „Personálna a mzdová agenda“

N á z o v prevádzkovateľa	MTK PLUS s.ro., IČO: 47 099 283
A d r e s a :	Stožok 424, 962 12 Detva

———————————————————————————————————————-

Štatutárny zástupca :	Mária Murínová
Tel. kontakt, e-mail :	mtkdetva@gmail.com 0907 840 534
Zodpovedná osoba :	nie je poverená
Tel. kontakt, e-mail :	
Účel spracúvania osobných údajov:	plnenie požiadaviek Zákonníka práce a ďalších zákonov súvisiacich s pracovnoprávnym vzťahom
Opis kategórií dotknutých osôb:	zamestnanci (aj vyživované a blízke osoby)
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi s pracovnoprávnym vzťahom Nie sú spracúvané osobitné kategórie OÚ Môže byť spracúvaná fotografia zamestnanca na základe jeho súhlasu
Kategórie príjemcov:	Sociálna poisťovňa, Zdravotná poisťovňa, Daňový úrad
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	vek 70 rokov zamestnanca
Všeobecný opis technických a organizačných opatrení:	opatrenia sú popísané v bezpečnostnej dokumentácii a v analýze bezpečnostných rizík

Záznam o spracovateľských činnostiach prevádzkovateľa v informačnom systéme „Registratúra“

N á z o v prevádzkovateľa	MTK PLUS s.r.o,. IČO: 47 099 283
A d r e s a :	Stožok 424, 962 12 Detva

Štatutárny zástupca :	Mária Murínová
Tel. kontakt, e-mail :	mtkdetva@gmail.com 0907 840 534
Zodpovedná osoba :	nie je poverená
Tel. kontakt, e-mail :	
Účel spracúvania osobných údajov:	uchovávanie dokumentácie podľa požiadaviek osobitných zákonov v súvislosti s činnosťou Úradu (napr. Zákon o archívoch a registratúrach, Zákon o daniach, Zákon o účtovníctve, Zákon dôchodkovom zabezpečení...)
Opis kategórií dotknutých osôb:	napr. osoby zúčastnené v konaní prevádzkovateľa, zamestnanci, odosielatelia nevyžiadanej pošty ...
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi so spracúvaním pred uložením do registratúry... Uchovávaná je tiež nevyžiadaná pošta a agenda vzniknutá pri obchodnej činnosti Nie sú spracúvané osobitné kategórie OÚ
Kategórie príjemcov:	OÚ nie sú poskytované
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	doba uloženia je daná osobitnými zákonmi, nevyžiadaná pošta 1 rok po roku prijatia pošty
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnej dokumentácii a v analýze bezpečnostných rizík

Záznam o spracovateľských činnostiach prevádzkovateľa v informačnom systéme „Účtovná agenda“

N á z o v prevádzkovateľa	MTK PLUS s.r.o., IČO: 47 099 283
A d r e s a :	Jesenského 6, 962 12 Detva

Štatutárny zástupca :	Mária Murínová
Tel. kontakt, e-mail :	mtkdetva@gmail.ocm 0907 840 534
Zodpovedná osoba :	nie je poverená
Tel. kontakt, e-mail :	
Účel spracúvania osobných údajov:	plnenie požiadaviek Zákona o účtovníctve a ďalších zákonov (napr. Zákon o daniach...)
Opis kategórií dotknutých osôb:	prevažne právnické osoby, ale aj zamestnanci (napr. výživné, splátky exekúcií ...)
Opis kategórií osobných údajov:	rozsah osobných údajov je daný osobitnými zákonmi súvisiacimi so spracúvaním účtovnej agendy
Kategórie príjemcov:	Daňový úrad
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	5 až 10 rokov od doby zaúčtovania
Všeobecný opis technických a organizačných opatrení:	prijaté opatrenia sú popísané v bezpečnostnej dokumentácii a v analýze bezpečnostných rizík

Záznam o spracovateľských činnostiach prevádzkovateľa v informačnom systéme „Kamerový systém“

N á z o v prevádzkovateľa	MTK PLUS s.r.o., IČO: 47 099 283
A d r e s a :	Stožok 424, 962 12 Detva

Štatutárny zástupca :	Mária Murínová
Tel. kontakt, e-mail :	mtkdetva@gmail.com 0907 840 534
Zodpovedná osoba :	nie je poverená
Tel. kontakt, e-mail :	
Účel spracúvania osobných údajov	§16 ods.2 písm.f/ uplatnenie právneho nároku prevádzkovateľa pri dokumentovaní škody §13 písm.f/ oprávnený záujem prevádzkovateľa
Opis kategórií dotknutých osôb:	osoby v zábere kamery
Opis kategórií osobných údajov:	záznam o pohybe osoby v zábere kamery z monitorovaného prostredia
Kategórie príjemcov:	podľa potreby dokumentovania vzniknutej škody na zdraví alebo majetku (Polícia, poisťovne...)
Príjemca v medzinárodnej organizácii:	prenos sa nevykonáva
Príjemca v tretej krajine:	prenos sa nevykonáva
Označenie tretej krajiny:	prenos sa nevykonáva
Predpokladané lehoty na vymazanie OÚ:	automaticky po zaplnení pamäte DVR/NVR zariadenia
Všeobecný opis technických a organizačných opatrení:	opatrenia sú popísané v bezpečnostnej dokumentácii a v analýze bezpečnostných rizík

- **P o z n á m k y :**