effecontrol
effective energy

METAL TATRY, s.r.o.
Hôrka 8, 059 12
Hôrka

Dátum: 15.10.2018

IČO: 48127175

DIČ: 2120060151

SMERNICA GDPR

OCHRANA OSOBNÝCH ÚDAJOV

Tento dokument je duševným majetkom Ing. Matúš Kažimir
Kopírovanie a rozširovanie je zakázané táto verzia je poskytnutá v rámci
služby spracovania GDPR .

Spracoval : Technik BOZP/GDPR

Ing. Matúš Kažimir

Schválil : Konateľ spoločnosti

Michal Baran

.....

Podpis prevádzkovateľa

Úvod

Dokument Smernica na ochranu osobných údajov (GDPR)
Spoločnosť METAL TATRY, s.r.o. / **Ďalej len spoločnosť/**si uvedomuje hodnotu svojich aktív a požiadavky legislatívy na ochranu OÚ a preto formou smernice GDPR prijíma opatrenia na ich ochranu.
Spoločnosť je podľa zákona Prevádzkovateľom, ktorý spracúva OÚ vo vlastnom mene (vymedzuje účel a podmienky spracúvania OÚ).
Smernica - GDPR obsahuje závery vyplývajúce z bezpečnostného zámeru a analýzy bezpečnosti informačného systému v súlade Zákon č. 18/2018 Z. z. Zákon o ochrane OÚ

Úradu na ochranu osobných údajov a v súlade z:
§7 Zásada obmedzenia účelu
Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom; ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom) a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.

§8 Zásada minimalizácie osobných údajov
Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú a v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679

Na ochranu OÚ Slovenskej republiky v znení neskorších predpisov, ktoré obsahujú:

- popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb; ak to automatizované prostriedky spracúvania
- OÚ umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby,miesta a času zabezpečí zaznamenanie každého vstupu oprávnenej osoby do informačného systému,
- rozsah zodpovednosti oprávnených osôb (a zodpovednej osoby),spôsob, formu a periodicitu výkonu kontrolných činností zameraných na
- dodržiavanie bezpečnostných opatrení,postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

Záväznosť

Smernica je vypracovaná pre systémy, v ktorých spoločnosť spracúva OÚ ako prevádzkovateľ. Sú to nasledujúce IS:

č.	Názov informačného systému	Označenie IS
1.	Mzdová a personálna agenda	01
2.	Kamerový informačný systém	03
3.	Agenda BOZP a PO	04
4.	Účtovnícka agenda	05
5.	Agenda zmlúv	06
6.	Zákaznícka agenda	07
7.	Evidencia prijatej a odoslanej pošty	12
8.	Agenda marketingu	13
9.	Agenda evidencie dochádzky	15

Smernica GDPR je záväzná pre všetkých zamestnancov spoločnosti, vrátane pracovníkov externe poskytovaných služieb, ktorí prichádzajú do styku s OÚ
Fyzická osoba sa stáva oprávnenou osobou dňom jej poučenia.
Prevádzkovateľ **spoločnosť** je povinný o poučení oprávnenej osoby vyhotoviť **„Záznam o poučení oprávnenej osoby“,** ktorá spracováva OÚo zmene a doplnení niektorých zákonov. Každý zamestnanec si musí byť vedomý, že ochrana OÚ je súčasťou plneniajeho pracovných povinností

Predmet

Predmetom dokumentu je:

1. popis technických, organizačných a personálnych opatrení pri spracúvaní osobných údajov a ich využitie v konkrétnych podmienkach.
2. rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému.
3. rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov.
4. spôsob, forma a periodicita výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému.
5. postup pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.
6. popis procesov a procedúr súvisiacich so spracúvaním osobných údajov v informačných systémoch prevádzkovateľa.

Použité skratky

AIS - Automatizovaný informačný systém

DO- Dotknutá osoba

EZS- Elektronický zabezpečovací systém

FO- Fyzická osoba

HW- Hardvérové technické vybavenie

BI- Bezpečnostný incident

IS- Informačný systém

OO- Oprávnená osoba

OOÚ- Ochrana osobných údajov

OS- Operačný systém

ŠO- Špeciálne okruhy (ŠO)

OÚ- Osobný údaj

PV- Priestory určené pre styk s verejnosťou, zásobovaním a odberateľmi

PZ- Priestory určené pre prácu zamestnancov

SW- Softvérové vybavenie

VPN- Virtual Private Network – virtuálna privátna sieť

ZEP- Zaručený elektronický podpis

Zákon č. 18/2018 Z. z. – zákon č. 18/2018 Z. z. o ochrane osobných údajov.

Nariadenie Európskeho parlamentu a Rady (EÚ) **2016/679**

Vymedzenie niektorých pojmov

Osobné údaje sú:

údaje, týkajúce sa identifikovanej fyzickej osoby 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,1) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Súhlas so spracúvaním osobných údajov je:

akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov

Spracúvanie osobných údajov je:

spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so 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 prostriedkami alebo neautomatizovanými prostriedkami.

Poskytovanie osobných údajov je:

osobných údajov na spracúvanie inému prevádzkovateľovi alebo inému zástupcovi prevádzkovateľa, alebo jeho sprostredkovateľovi.

Sprístupňovanie osobných údajov je:

oznámenie osobných údajov alebo umožnenie prístupu k nim inej právnickej osobe, alebo fyzickej osobe s výnimkou dotknutej osoby, alebo oprávnenej osoby, ktorá ich nebude spracúvať ako prevádzkovateľ, zástupca prevádzkovateľa, alebo sprostredkovateľ.

Zverejňovanie osobných údajov je:

publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovo komunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním, alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri, alebo v operáte, ich umiestnením na úradnej tabuli, alebo na inom verejne prístupnom mieste.

Likvidácia osobných údajov je:

zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

Obmedzenie spracúvania osobných údajov je:

označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti.

Informačný systém je:

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

Účel spracúvania osobných údajov je:

vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Cezhraničný tok osobných údajov je:

prenos osobných údajov mimo územia Slovenskej republiky subjektom so sídlom alebo s trvalým pobytom v cudzine, alebo ich výmena s týmito subjektmi.

Adresa je:

súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.

Všeobecne použiteľný identifikátor je:

trvalý identifikačný osobný údaj dotknutej osoby, ktorý zabezpečuje jej rozoznateľnosť v informačných systémoch (rodné číslo).

Genetické údaje sú:

údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby.

Biometrické údaje sú:

osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje.

Údaje týkajúce sa zdravia sú:

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

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 je:

spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia 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 fyzickej osobe alebo identifikovateľnej fyzickej osobe

Logom je:

záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme

Šifrovaním je:

transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo

Online identifikátorom je:

identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu.

Prevádzkovateľ je:

každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky 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.

Prijemcom je:

každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za prijemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov

Treťou stranou je:

každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,

Oprávnená osoba je:

každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, ktorá môže osobné údaje spracúvať len na základe pokynu prevádzkovateľa, zástupcu prevádzkovateľa, alebo sprostredkovateľa, ak tento zákon, alebo osobitný zákon neustanovuje inak.

Porušením ochrany osobných údajov je:

porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

Dotknutá osoba je:

každá fyzická osoba, o ktorej sa spracúvajú osobné údaje.

Zodpovednou osobou je:

osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov.

Zástupcom je:

fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo sprostredkovateľ písomne poveril podľa § 35

Autenticita je:

vlastnosť zaisťujúca, že identita subjektu alebo zdroja je taká, za ktorú sa prehlasuje. Autenticita je aplikovaná na entity, ako sú užívatelia, procesy, systémy a informácie.

Dôvernosť je:

vlastnosť, že aktíva nie sú prístupné neautorizovaným jednotlivcom, entitám alebo procesom.

Integrita je:

vlastnosť, že aktíva nebudú pozmenené, poškodené, narušené neautorizovaným spôsobom.

Dostupnosť je:

vlastnosť zaisťujúca autorizovaným užívateľom prístup k informáciám a aktívam vtedy, keď to potrebujú.

Bezpečnostný incident je:

Udalosť, ktorá spôsobila narušenie dôvernosti, dostupnosti alebo integrity spracúvaných osobných údajov.

Kódexom správania je:

súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať

Osobitné kategórie OÚ

Ide o údaje:

- ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa zdravia alebo pohlavného života, ich spracovanie sa zakazuje (výnimky uvádza § 14),
- všeobecne použiteľný identifikátor ustanovený osobitným zákonom, jeho spracovanie je možné, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania,
- psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti, tieto môže spracovávať len psychológ alebo ten, komu to umožňuje osobitný zákon,
- porušení ustanovení zakladajúcich trestnú zodpovednosť alebo administratívno právnu zodpovednosť, môže ich spracovávať len ten, komu to umožňuje osobitný zákon

- biometrické údaje, ktoré sa môžu spracúvať len ak je to primerané účelu spracúvania a nevyhnutné na jeho dosiahnutie a ak o to prevádzkovateľovi vyplýva výslovne zo zákona, o dotknutá osoba dala na spracúvanie písomný alebo inak hodnoverne preukázateľný súhlas, o spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo o spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany.

Legislatíva o ochrane (osobných) údajov

V zmysle Zákona č. 18/2018 Z.z. o ochrane osobných údajov v znení ďalších predpisov všetci zamestnanci spoločnosti (t.j. osoby, ktoré sú v pracovnom pomere alebo obdobnom pracovnom vzťahu), sú povinní dodržiavať nasledujúce ustanovenia:

- Dodržiavať a uplatňovať organizačné a technické opatrenia na zabezpečenie ochrany OÚ pred odcudzením, stratou, poškodením, neoprávneným prístupom,zmenou a rozširovaním.

- Oprávnené osoby sú povinné zachovávať mlčanlivosť o OÚ s ktorými prídu do styku, tie nesmú využiť ani pre osobnú potrebu a bez pokynu vedenia spoločnosti ich nesmú zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po ukončení spracovania.

- Povinnosť mlčanlivosti podľa predchádzajúceho odseku platí aj pre iné osoby, ktoréprídu do styku s osobnými údajmi v priestoroch spoločnosti a trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jeho pracovného pomeru alebo obdobného pracovného vzťahu.

- Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov SR, pri plnení jeho úloh.

- Oprávnená osoba, ktorá nezískava od okruhu dotknutých osôb osobné údaje, ktorýchúčel, zoznam alebo rozsah, prípade ďalšie podmienky spracúvania, sú vymedzené právne záväzným aktom EÚ, medzinárodnou zmluvou alebo zákonom, musí prizískavaní osobných údajov dotknutej osobe podať nasledujúce informácie o identifikačné údaje prevádzkovateľa, resp. sprostredkovateľa o účel spracúvania osobných údajov,o zoznam, rozsah osobných údajov, o poučenie o dobrovoľnosti alebo povinnosti poskytovať požadované osobné údaje, o zákon, ktorý ustanovuje povinnosť poskytnúť požadované osobné údaje a následky odmietnutia poskytnúť osobné údaje, o tretie strany, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje poskytnuté, o okruh príjemcov, ak im budú údaje poskytnuté, o formu

- biometrické údaje, ktoré sa môžu spracúvať len ak je to primerané účelu spracúvania a nevyhnutné na jeho dosiahnutie a ak o to prevádzkovateľovi vyplýva výslovne zo zákona, o dotknutá osoba dala na spracúvanie písomný alebo inak hodnoverne preukázateľný súhlas, o spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo o spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa alebo tretej strany.

Legislatíva o ochrane (osobných) údajov

V zmysle Zákona č. 18/2018 Z.z. o ochrane osobných údajov v znení ďalších predpisov všetci zamestnanci spoločnosti (t.j. osoby, ktoré sú v pracovnom pomere alebo obdobnom pracovnom vzťahu), sú povinní dodržiavať nasledujúce ustanovenia:

- Dodržiavať a uplatňovať organizačné a technické opatrenia na zabezpečenie ochrany OÚ pred odcudzením, stratou, poškodením, neoprávneným prístupom,zmenou a rozširovaním.

- Oprávnené osoby sú povinné zachovávať mlčanlivosť o OÚ s ktorými prídu do styku, tie nesmú využiť ani pre osobnú potrebu a bez pokynu vedenia spoločnosti ich nesmú zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po ukončení spracovania.

- Povinnosť mlčanlivosti podľa predchádzajúceho odseku platí aj pre iné osoby, ktoréprídu do styku s osobnými údajmi v priestoroch spoločnosti a trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jeho pracovného pomeru alebo obdobného pracovného vzťahu.

- Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov SR, pri plnení jeho úloh.

- Oprávnená osoba, ktorá nezískava od okruhu dotknutých osôb osobné údaje, ktorýchúčel, zoznam alebo rozsah, prípade ďalšie podmienky spracúvania, sú vymedzené právne záväzným aktom EÚ, medzinárodnou zmluvou alebo zákonom, musí prizískavaní osobných údajov dotknutej osobe podať nasledujúce informácie o identifikačné údaje prevádzkovateľa, resp. sprostredkovateľa o účel spracúvania osobných údajov,o zoznam, rozsah osobných údajov, o poučenie o dobrovoľnosti alebo povinnosti poskytovať požadované osobné údaje, o zákon, ktorý ustanovuje povinnosť poskytnúť požadované osobné údaje a následky odmietnutia poskytnúť osobné údaje, o tretie strany, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje poskytnuté, o okruh príjemcov, ak im budú údaje poskytnuté, o formu

zverejnenia, ak majú byť osobné údaje zverejnené, o tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov, o poučenie o právach dotknutej osoby.

- Získavať OÚ nevyhnutné na dosiahnutie účelu spracovania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií je možné len vtedy, ak s tým dotknutá osoba písomne súhlasí alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby. Písomný súhlas dotknutej osoby môže byť priamo na fotokópii dokumentu. To neplatí, ak ide o získavanie OÚ naúčely jednorazového vstupu do priestorov ich zaznamenávaním z úradného dokladu automatizovanými prostriedkami spracúvania.

- Pri získavaní OÚ upozorniť dotknuté osoby na osobnú zodpovednosť za pravdivosť poskytnutých OÚ s možnou sankciou za poskytnutie nepravdivých údajov zo strany Úradu na ochranu osobných údajov SR.

- Zabezpečiť opravu alebo doplnenie tých OÚ, ktoré sa v priebehu spracúvania stanú neaktuálnymi, alebo sa preukáže, že sú nesprávne

- Prevádzkovateľ spracúva OÚ bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie OÚ je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo v predzmluvných vzťahoch s dotknutou osobou alebo pri rokovaní o zmene zmluvy, ktoré sa uskutočňuje na žiadosťdotknutej osoby.

- Na účely identifikácie fyzickej osoby pri jednorazovom vstupe do priestorov možno požadovať iba minimálne údaje postačujúce na identifikáciu osoby. V rámci novej legislatívy môže dotknutá osoba odmietnuť poskytnutie OÚ prípadne ich spracovanie príslušným spôsobom. Ak sa fyzická osoba preukáže podľa osobitného zákona, na účely identifikácie sa použije iba číslo služobného preukazu a názov orgánu, ktorý preukaz vydal.

- Kontrolovaná osoba je povinná:

  a) vytvoriť kontrolnému orgánu primerané podmienky na výkon kontroly a spracovanie kontrolných zistení

  b) poskytnúť kontrolnému orgánu požadovanú súčinnosť a zdržať sa konania, ktoré by mohlo mariť výkon kontroly

  c) dostaviť sa na predvolanie úradu s cieľom podať vysvetlenia v určenom čase na určené miesto

  d) oboznámiť sa s obsahom protokolu a na požiadanie kontrolného orgánu dostaviť sa na jeho prerokovanie

Neplnenie si týchto povinností v oblasti ochrany OÚ zo strany oprávnených osôb ako i iných zamestnancov, ktorí prišli do styku s OÚ spoločnosti sa považuje za závažné porušenie pracovnej disciplíny. Za sledovanie zmien v legislatíve SR,

následné zapracovanie do interných noriem a zabezpečenie zmien vnútorného prostredia tak, aby tejto legislatíve vyhovovali je zodpovedná osoba poverená dohľadom nad ochranou osobných údajov.

Právo dotknutej osoby na prístup k údajom

1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:

   a) účely spracúvania
   b) kategórie dotknutých osobných údajov
   c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie
   d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie
   e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu
   f) právo podať sťažnosť dozornému orgánu
   g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj
   h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu

2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Špecifikácie

Prevádzkovateľ je povinný pred spracúvaním osobných údajov zaviesť a počas spracúvania osobných údajov mať zavedenú špecificky navrhnutú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení, najmä vo forme pseudonymizácie, na účinné zavedenie primeraných záruk ochrany osobných údajov a dodržiavanie základných zásad podľa *§ 6 až 12*.

Prevádzkovateľ je povinný pri špecificky navrhnutej ochrane osobných údajov podľa odseku 1 zohľadniť najnovšie poznatky ochrany osobných údajov, náklady na vykonanie opatrení podľa odseku 1, povahu, rozsah, kontext a účel spracúvania osobných údajov a riziká spracúvania osobných údajov s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie osobných údajov predstavuje pre práva dotknutej osoby.

Prevádzkovateľ je povinný zaviesť štandardnú ochranu osobných údajov, ktorá spočíva v prijatí primeraných technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov len na konkrétny účel, minimalizácie množstva získaných osobných údajov a rozsahu ich spracúvania, doby uchovávania a dostupnosti osobných údajov. Prevádzkovateľ je povinný zabezpečiť, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

I. Popis bezpečnostných opatrení a spôsob ich uplatňovania v podmienkach prevádzkovateľa

1.1Technické opatrenia

1.1.1 Technické opatrenia realizované prostriedkami fyzickej kontroly

1.1.1.1 Zabezpečenie objektu pomocou mechanických a technických zábranných prostriedkov:

- Zoznam areálov, budov a fyzických miestností, kde sa spracúvajú OÚ je detailne popísaný v samostatnom dokumente.
- Vstupy do budovy a vnútorných priestorov prevádzkovateľa musia byť vybavené mechanickými zámkami.
- Prístup do budovy prevádzkovateľa musí byť 24 hodín chránený v riadenom režime.
- Vstupný priestor do budovy prevádzkovateľa musí byť chránený kamerovým monitorovacím systémom.
- Priestory prevádzkovateľa musia byť vybavené elektronickým zabezpečovacím systémom, snímače musia byť umiestnené minimálne v priestoroch, v ktorých sa nachádzajú citlivé OÚ podľa §13 zákona č. 18/2018 Z. z. (serverovňa, personálne, archív...).

- Kancelárie a miestnosti, v ktorých sa nachádzajú IS s OÚ, je potrebné vybaviť na vstupoch uzamykacími mechanizmami. Prístup do kancelárií musí byť riadený a manipulácia s kľúčmi zdokumentovaná v kľúčovom poriadku.
- Zámkový systém do miestností v ktorých sa spracúvajú OÚ nesmie používať skupinový, alebo univerzálny kľúč.
- Okná do miestností, v ktorých sa spracúvajú OÚ musia byť pevné, nesmú sa dať otvoriť bez použitia násilia.
- Úschovné objekty musia mať zámkové systémy min. triedy 2.
- Ak sa na úschovu údajov používajú police, dvere do miestností musia byť vybavené systémom guľa – kľučka.

Priestory určené pre serverovne vybaviť nasledovne:

- klimatizáciou pre zabezpečenie klimatických podmienok vyžadovaných výrobcami inštalovaných technológií. Inštalácia klimatizácie musí byť vykonaná tak, aby neumožňovala zatečenie aktívnych prvkov IT unikajúcou chladiacou tekutinou.
- Elektronickým zabezpečovacím systémom (EZS) s nadefinovanou samostatnou bezpečnostnou zónou pre priestor miestnosti serverov. EZS musí byť pripojená na pult centrálnej ochrany so stálou (24 hodinovou) službou (PCO), funkčnosť EZS musí byť pravidelne kontrolovaná, zóna musí byť trvale aktívna. K deaktivácii môže dôjsť len pri odôvodnenom vstupe do priestoru serverovne.
- Elektronickou požiarnou signalizáciou (EPS) pripojenou na PCO, funkčnosť EPS musí byť pravidelne kontrolovaná.
- Snímačom teploty pracovného prostredia s akustickou signalizáciou prekročeného rozsahu a zabezpečením odoslania informácie zodpovednému zamestnancovi.
- Snímačom relatívnej vlhkosti prostredia s akustickým výstupom signalizácie prekročenia rozsahu a zabezpečením odoslania informácie zodpovednému zamestnancovi.
- Okná v miestnosti, kde je umiestnený server, v prípade prístupu z vonkajšej strany, chrániť proti vniknutiu nepovolanej osoby (bezpečnostnou mrežou) a v prípade, ak to umiestnenie miestnosti servera vyžaduje (okno smerujúce do verejne prístupného priestoru, vzdialené menej ako 40 m od hranice verejne prístupného priestoru, resp. na 3. a nižšom nadzemnom podlaží) chrániť tiež proti vhodeniu zápalného predmetu (bezpečnostnou fóliou zabraňujúcou rozbitiu okennej tabule).
- Serverovňu chrániť proti zatopeniu z okolitých miestností, ale aj z podlaží nachádzajúcich sa nad serverovňou. Miestnosť nesmie byť umiestnená na miestach, ktoré sa nachádzajú v priestore pod sociálnymi zariadeniami budovy. Miestnosť musí byť vybavená havarijným odtokom tekutiny z podlahy.

- Dvere do serverovne vybaviť bezpečnostnou zámkou a bezpečnostným kovaním, s guľou namiesto kľučky na vonkajšej strane a s automatickým zatváraním (Brano alebo podobné zariadenie).
- Ak to konštrukcia budovy umožňuje, v miestnosti serverovne sa nesmú nachádzať žiadne prvky infraštruktúry budovy ako sú kanalizačné zvody odkvapové zvody, vykurovacie telesa a pod...
- Ak je v miestnosti servera umiestnený radiátor, vodovodné alebo vykurovacie potrubie, kompenzačný člen vykurovania alebo je priestor umiestnený tak, že existuje riziko zatečenia, všetky aktívne prvky, rozvody napájania a dátové rozvody pre ochranu proti zatopeniu (zatečeniu) umiestniť minimálne 20 cm nad úrovňou podlahy, zabezpečiť prirodzený odtok vody z podlahy.
- Medzi aktívne prvky, rozvody napájania a dátové rozvody a potenciálny zdroj unikajúcej vody umiestniť zábrany chrániace pred striekajúcou vodou.
- Miestnosť servera vybaviť antistatickou podlahovou krytinou alebo podlahovou krytinou s antistatickou úpravou.
- Komponenty serverov IS, komponenty kritických častí komunikačnej infraštruktúry napájať samostatným elektrickým rozvodom.
- Elektrické rozvádzače umiestniť v priestoroch minimálne VZ a viac. Rozvádzač nesmie byť otvoriteľný bez použitia špecializovaného nástroja.

1.1.1.2 Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu:

ISOU (agendy) musia byť umiestnené v chránených priestoroch - oddelených miestnostiach s primeraným rozsahom technických opatrení, s vylúčením pohybu iných ako oprávnených osôb.

Všetky priestory u prevádzkovateľa musia byť rozdelené do fyzických okruhov. Pri vytváraní a definovaní okruhov prihliadať na dodržanie nasledovných požiadaviek:

- Každý bezpečnostný okruh riadne a jednoznačne definovať.
- Každý definovaný okruh musí byť fyzicky súvislý, ak to technické a organizačné podmienky prevádzkovateľa dovoľujú.
- Každému bezpečnostnému fyzickému okruhu jasne definovať spôsob prístupu a identifikácie vstupujúcich osôb.
- Pre zabezpečenie fyzického prístupu do jednotlivých oblastí použiť primerané technické prostriedky zodpovedajúce stupňu dôležitosti aktív nachádzajúcich sa v danej oblasti.
- V bezpečnostných okruhoch, v ktorých sa nachádzajú zvlášť citlivé aktíva zaviesť systémy na detekciu nepovolaných osôb.
- V každom objekte METAL TATRY, s.r.o. vytvoriť minimálne nasledovné bezpečnostné okruhy:

- Priestory určené pre styk s verejnosťou (PV), zásobovaním a odberateľmi. Zabezpečiť, aby nebolo možné z týchto priestorov prejsť do vyššej úrovne ochrany bez identifikácie a autorizácie vstupujúcej osoby.
- Priestory určené pre prácu zamestnancov (PZ). Do týchto priestorov umožniť vstup len zamestnancom po patričnej autorizácii. Návštevám a dodávateľom povoliť vstup len v sprievode zodpovedného zamestnanca.
- Špeciálne okruhy (ŠO) pre umiestnenie zvlášť citlivých aktív ako sú servery, prepínače, komunikačné prvky WAN sieťového rozhrania a podobne zariadenia. Sú to takzvané Serverovne. Vstup do týchto okruhov povoliť len pre vybraných zamestnancov. Kto má oprávnenie vstupovať do týchto priestorov, navrhuje riadiaci bezpečnostný orgán a schvaľuje manažment METAL TATRY, s.r.o.

O výnimkách z týchto požiadaviek rozhoduje manažment METAL TATRY, s.r.o. Výnimka musí byť riadne zdôvodnená a zdokumentovaná.

Opatrenia riadenia fyzického vstupu do zabezpečených oblastí

Jednotlivé definované okruhy fyzickej bezpečnosti musia byť vybavené na vstupoch primeranými technickými prostriedkami, tak aby sa zabránilo neautorizovanému vstupu.

Pri výbere opatrení sa musí prihliadať na nasledovné:

Požiadavky na zabezpečenie fyzického vstupu do jednotlivých zabezpečených oblastí:

PV:

Zaznamenávať dátum a čas príchodu a odchodu zamestnancov.
V prípade návštev, dodávateľov a odberateľov zaznamenávať do knihy návštev OÚ vstupujúcich FO v zmysle zákona o OOÚ a smernice o OOÚ.

PZ:

To isté ako PV plus nasledovné:
Vstup zamestnancov podlieha identifikácii vhodným autorizačným zariadením (čipová karta). Zo vstupov vykonávať záznam, ktorý uchovávať minimálne jeden rok.
Vlastných návštevníkov v PZ oblastiach sprevádzať zodpovedným zamestnancom.
Zamestnancov oboznámiť s tým, aby oznamovali bezpečnostnému personálu pohyb neoznačených osôb.

ŠO:

To isté ako PZ plus nasledovné:

- Prístup k týmto oblastiam riadiť a obmedziť len na autorizované osoby, pričom z každého vstupu vykonávať záznam, ktorý musí obsahovať informácie, kto vstupoval, kedy, za akým účelom a ako dlho v priestore zotrval.
- Priestory vybaviť mechanickými zámkami. Kľúče od priestorov musia mať len vybrani zamestnanci na základe kľúčového poriadku Názov prevádzkovateľa.
- Priestory vybaviť elektronickými uzamykacími mechanizmami. Identifikačné prostriedky poskytnúť len vybraným zamestnancom, na základe schválenia manažmentom.
- Na autorizáciu prístupov do zvlášť citlivých oblastí ŠO použiť technické prostriedky umožňujúce vytváranie auditných záznamov. Auditný záznam z týchto systémov udržiavať v bezpečí.
- Prístupové práva do ŠO zabezpečených oblastí pravidelne revidovať.

Je vhodné navrhnúť rozmiestnenie zabezpečených oblastí tak, aby boli navzájom vedené a to postupne od najnižšej úrovne až po najvyššiu.Za návrh vytvorenia a výber jednotlivých priestorov pre zabezpečené oblasti zodpovedajú poverení vedúci zamestnanci prevádzkovateľa. Schvaľuje ich štatutár prevádzkovateľa.

Požiadavky na priestory určené pre servery (ŠO)

Priestory určené pre serverovne vybaviť nasledovne:

- Klimatizáciou pre zabezpečenie klimatických podmienok vyžadovaných výrobcami inštalovaných technológií. Inštalácia klimatizácie musí byť vykonaná tak, aby neumožňovala zatečenie aktívnych prvkov IT unikajúcou chladiacou tekutinou.

- Elektronickým zabezpečovacím systémom (EZS) s nadefinovanou samostatnou bezpečnostnou zónou pre priestor miestnosti serverov. Funkčnosť EZS musí byť pravidelne kontrolovaná, zóna musí byť trvale aktívna. K deaktivácii môže dôjsť len pri odôvodnenom vstupe do priestoru serverovne.

- Snímačom teploty pracovného prostredia s akustickou signalizáciou prekročeného rozsahu a zabezpečením odoslania informácie zodpovednému zamestnancovi.

- Snímačom relatívnej vlhkosti prostredia s akustickým výstupom signalizácie prekročenia rozsahu a zabezpečením odoslania informácie zodpovednému zamestnancovi.

- Okná v miestnosti, kde je umiestnený server, v prípade prístupu z vonkajšej strany, chrániť proti vniknutiu nepovolanej osoby (bezpečnostnou mrežou) a v prípade ak to umiestnenie miestnosti servera vyžaduje (okno smerujúce do verejne prístupného priestoru, vzdialené menej ako 40 m od hranice verejne prístupného priestoru, resp. na 3. a nižšom nadzemnom podlaží) chrániť tiež proti vhodeniu zápalného predmetu (bezpečnostnou fóliou zabraňujúcou rozbitiu okennej tabule).

- Serverovňu chrániť proti zatopeniu z okolitých miestností, ale aj z podlaží nachádzajúcich sa nad serverovňou. Miestnosť nesmie byť umiestnená na miestach, ktoré sa nachádzajú v priestore pod sociálnymi zariadeniami budovy. Miestnosť musí byť vybavená havarijným odtokom tekutiny z podlahy.

- Dvere do serverovne vybaviť bezpečnostnou zámkou a bezpečnostným kovaním, s guľou namiesto kľučky na vonkajšej strane.

- Ak to konštrukcia budovy umožňuje, v miestnosti serverovne sa nesmú nachádzať žiadne prvky infraštruktúry budovy ako sú kanalizačné zvody, odkvapové zvody, vykurovacie telesa a pod...

- Ak je v miestnosti servera umiestnený radiátor, vodovodné alebo vykurovacie potrubie, kompenzačný člen vykurovania alebo je priestor umiestnený tak, že existuje riziko zatečenia, všetky aktívne prvky, rozvody napájania a dátové rozvody pre ochranu proti zatopeniu (zatečeniu) umiestniť minimálne 20 cm nad úrovňou podlahy, zabezpečiť prirodzený odtok vody z podlahy.

- Medzi aktívne prvky, rozvody napájania a dátové rozvody a potenciálny zdroj unikajúcej vody umiestniť zábrany chrániace pred striekajúcou vodou.

- Komponenty serverov IS, komponenty kritických častí komunikačnej infraštruktúry napájať samostatným elektrickým rozvodom.

- Elektrické rozvádzače umiestniť v priestoroch minimálne PZ a viac. Rozvádzač nesmie byť otvoriteľný bez použitia špecializovaného nástroja.

1.1.1.3 Umiestnenie IS v chránenom priestore

IS musia byť umiestnené v chránenom priestore, kde je zaručená ochrana pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.

1.1.1.4 Bezpečné uloženie fyzických nosičov OÚ

Na uchovávanie papierovej evidencie obsahujúcej osobné údaje z IS, v ktorých sa spracúvajú aj OÚ z kategórie zvlášť citlivých OÚ (RČ, zdravotný stav...), je nevyhnutné vyhradiť uzamykateľné skrine. Prístup ku skriniam musí byť riadený a manipulácia s kľúčmi zdokumentovaná v kľúčovom poriadku. Kľúče od skriniek musia mať len OO poverené spracúvaním OÚ príslušného IS.

1.1.1.5 Zamedzenie náhodného odpozerania OÚ zo zobrazovacích jednotiek IS

Zobrazovacie jednotky musia byť umiestnené tak, aby nebolo možné náhodné odpozeranie OÚ.
OÚ zo zobrazovacích jednotiek informačného systému je potrebné zabezpečiť, aby monitor (pracovnej stanice) informačného systému, na ktorom sú zobrazované osobné údaje, nebol zobrazovacou časťou orientovaný (otočený):

- smerom do kancelárskeho priestoru (resp. výrobnej časti) kde sa pohybujú aj neoprávnené osoby (návštevy, zamestnanci bez oprávnenia na spracúvanie danej agendy s osobnými údajmi)
- smerom ani k vchodovým dverám
- smerom k oknu (hlavne na prízemí)
- smerom k zrkadlu

Na pracovnej stanici je nutné aplikovať aby sa terminál (monitor) automaticky zablokoval po definovanej nečinnosti používateľa – oprávnenej osoby.

1.1.1.6 Zariadenie na ničenie fyzických nosičov OÚ

Pre potreby skartovania fyzických nosičov osobných údajov v papierovej forme (listiny), je potrebné využiť zariadenia na skartovanie listín (skartovačka). Zariadenia pre skartovanie listín je potrebné zabezpečiť na miestach, kde môže vzniknúť potreba skartovania dokumentov s osobnými údajmi, minimálne:

- v miestnosti personálneho odboru
- pri tlačiarňach kde sú tlačené dokumenty, ktoré obsahujú aj osobné údaje.

1.1.2 Ochrana pred neoprávneným prístupom

- Ochrana obsahu dátových nosičov – musí byť zabezpečená ochrana dátových nosičov ich bezpečnou manipuláciou a evidenciou.
- Pravidlá prístupu tretích strán k IS musia byť definované v zmluvách o poskytnutí externých služieb.
- Pri prenose údajov mimo organizáciu sa vyžaduje šifrovanie dát prostriedkami aplikácií alebo vhodným voľne šíriteľným šifrovacím programom.
- Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí Používanie šifrovacích technológií,
- Používanie elektronickej pošty a Internetu", Vzdialený prístup k aktívam".

Šifrová ochrana obsahu dátových nosičov:

- všetky dátové nosiče s OÚ, ktoré môžu opustiť chránené priestoryprevádzkovateľa musia mať dáta (s osobnými údajmi) pred prenosom zašifrované,
- šifrovanie je povinné aj pre prenosné dátové nosiče (vytvorené oprávnenými
- osobami),
- za šifrovanie dátových nosičov je zodpovedná tá oprávnená osoba, ktorá údaje na nosič uložila, prenesenie nezašifrovaných prenosných dátových nosičov mimo chránenýchpriestorov je potrebné klasifikovať ako bezpečnostný incident.

Šifrová ochrana údajov premiestňovaných v rámci služby e-mail prostredníctvom verejnej počítačovej siete:

- Pred prenosom osobných údajov prostredníctvom služby e-mail mimo chránenej
- Siete **spoločnosti** (komunikácia so sprostredkovateľmi) je nutné osobné údaje prenášať len v rámci zašifrovaných príloh.
- Šifrovanie súborov je nutné vykonať pred vložením prílohy do e-mail správy.
- Pre ochranu elektronickej pošty je nutné používať schválený typ šifrovania.
- Za šifrovanie obsahu e-mailov je zodpovedná tá oprávnená osoba, ktorá údaje
- odosiela.
- OÚ službou e-mail je možné zasielať iba tým sprostredkovateľom, s ktorými má prevádzkovateľ uzatvorenú zmluvu o sprostredkovaní

1.1.3 Riadenie prístupu OO

- Identifikácia, autentizácia a autorizácia OO v IS – musí byť zabezpečená jednoznačná identifikácia OO pomocou užívateľského profilu zriadeného správcom siete.
- Zaznamenávanie vstupov jednotlivých OO do IS – musí byť zabezpečené pomocou reportov v jednotlivých aplikáciách
- Je realizovaný pomocou PC a iných zariadení. Dáta sú umiestnené centrálne na databázových serveroch umiestnených v príslušných serverovniach.

Autorizácia užívateľov je trojstupňová:

- Autorizácia operačným systémom zariadenia, z ktorého sa pristupuje k aplikácii. (jej vykonávanie sa zabezpečuje menom a heslom,
- Overovanie identity sa vykonáva nastavením príslušnej domény v danej LAN, do ktorej sa pristupuje. Pre heslo je nastavená príslušná politika zahŕňajúca požiadavku na dĺžku hesla, zloženie hesla, pravidelnú zmenu hesla, a pamätanie si určitého počtu predchádzajúcich hesiel).
- Autorizácia samotnou aplikáciou. (Vykonáva sa menom a heslom užívateľa. Ak to aplikácia umožňuje, je potrebné nastaviť politiku pre heslá, ako v bode a.).

1.1.4 Ochrana proti škodlivému kódu

Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov – musí byť zabezpečená pomocou nainštalovaného, správne konfigurovaného, aktualizovaného a pravidelne monitorovaného antivírového programu.

Ochrana pred nevyžiadanou elektronickou poštou – musí byť zabezpečená v nastaveniach prichádzajúcej pošty.

Používanie legálneho a prevádzkovateľom schváleného softvéru – prevádzkovateľ môže používať len legálny softvér, ktorý je inštalovaný správcom IS.

Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete – Oprávnená osoba využíva služby Internetu (povolené je využívanie iba verejných služieb WWW - worldwide web a FTP - file transfer protocol) za účelom plnenia pracovných úloh, pričom dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov, nepoužíva verejné komunikačné systémy na rýchly prenos správ (ICQ, AOL, IRC a pod.),

Systém riadenia ochrany proti škodlivému softvéru musí byť zdokumentovaný v IT dokumentácii; v dokumentácii systému ochrany proti škodlivému softvéru musia byť pridelené zodpovednosti za kontrolu funkčnosti a nastavení ochrany. Systém musí podliehať pravidelnej revízii a monitorovaniu stavu používanej ochrany z hľadiska jej dostatočnosti.

Ochrana musí zabezpečovať minimálne tieto činnosti:

- rezidentná ochrana všetkých zariadení.
- pravidelné skenovanie vybraných zariadení na prítomnosť nežiaduceho softvéru.

- pravidelná automatická aktualizácia vírusovej databázy.
- pravidelná automatická aktualizácia antivírovej aplikácie.
- automatická reakcia aplikácie na rôzne druhy incidentov.
- blokovanie zmeny nastavení aplikácie užívateľmi.
- vykonávanie log záznamov o incidentoch.
- automatické hlásenie incidentu zamestnancovi zodpovednému za ochranu proti škodlivému softvéru.

1.1.5 Sieťová bezpečnosť

- Kontrola, obmedzenie alebo zamedzenie prepojenia IS, v ktorom sú spracúvané OÚ s verejne prístupnou počítačovou sieťou – musí byť zabezpečené konfiguráciou siete a nastavením bezpečnostnej politiky.
- Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete – musí byť vedená v dokumentácii IT.
- Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti je zabezpečená pomocou firewall.
- Sieťovú bezpečnosť zabezpečiť tak, aby sa minimalizovala možnosť neoprávneného prístupu. Systém ochrany pred útokom z internetu je potrebné zdokumentovať v dokumentácii IT. Táto časť dokumentácie podlieha určitému stupňu utajenia. Dokumentácia musí obsahovať pridelenie zodpovednosti za správu, udržiavanie a kontrolu funkčnosti nastavených bezpečnostných prvkov.

Systém ochrany musí zabezpečiť minimálne nasledovné:

- šifrovanie komunikácie v prípade, ak sa prenos dát realizuje aj prostredím verejnej dátovej siete (napr. Internet).
- oddelenie lokálnej siete od Internetu prostredníctvom firewallu.
- blokovanie nepotrebných komunikačných portov.
- autorizáciu externých HW zariadení pristupujúcich do lokálnej siete.

Servery a aktívne prvky siete: musia byť umiestnené tak, aby sa zabránilo príležitosti na neautorizovaný fyzický prístup. Znamená to, že sú umiestňované v zónach s najvyšším stupňom autorizácie, podľa platnej bezpečnostnej politiky Názov prevádzkovateľa.

Kabeláž sieťovej infraštruktúry: musí byť zabezpečená proti neoprávnenému prístupu vhodnými ochrannými prvkami. Primárne musí byť kabeláž vedená v priestoroch, ktoré nie sú prístupné verejnosti.

1.1.6 Zálohovanie

- Test funkcionality dátového nosiča zálohy – sa vykonáva po jeho vytvorení

- Vytváranie záloh s vopred zvolenou periodicitou – zálohy sa musia vytvárať denne na zálohovací server. Musí sa vytvoriť aj duplicitný systém zálohovania na externý DVD disk, ktorý musí byť ukladaný v protipožiarnej skrini v archíve.
- Test obnovy IS zo zálohy vykonávať podľa potreby.
- Bezpečné ukladanie záloh – zálohy sa musia ukladať v uzamykateľnej skrini.
- Servery prevádzkovateľa musia byť vybavené zálohovaním a archiváciou dát. Systém zálohovania jednotlivých IS obsahujúcich OÚ musí byť zdokumentovaný v IT dokumentácii. Dokumentácia musí obsahovať pridelenie zodpovednosti za vytváranie záloh, popis technológie zálohovania, spôsob uloženia záložných médií.

Systém zálohovania musí zabezpečovať minimálne nasledovné požiadavky:

- pravidelné zálohovanie údajov z IS.
- pravidelné zálohovanie systémových nastavení.
- primeranú úroveň ochrany záložných médií (média musia byť uložené v inom priestore ako ostré dáta; prístup k záložným médiám musí byť riadený).
- pravidelnú kontrolu funkčnosti vytváraných záloh formou obnovy dát na testovacom zariadení.

Zálohovanie dodávky elektrickej energie: Servery a dôležité zariadenia prevádzkovateľa (routery, komunikačné prvky...) sú vybavené záložnými zdrojmi napájania. Zariadenia zabezpečujúce zálohovanie dodávky elektrickej energie musia zabezpečiť nasledovné:

a. dodávku energie minimálne na 30 min. prevádzky.
b. komunikáciu so zálohovanými zariadeniami, tak aby sa zálohované zariadenia včas dozvedeli o výpadku hlavného zdroja energie a mohli na ňu bezpečne reagovať.
c. komunikáciu s personálom zabezpečujúcim správu technických prostriedkov.

1.1.7 Likvidácia OÚ a dátových nosičov

Bezpečné vymazanie OÚ z dátových nosičov, fyzicky zničiť CD, DVD ich prelomením.
Zariadenie zlikvidovať na likvidáciu dátových nosičov OÚ – vždy použiť skartovačku alebo listinné dokumenty spálením.

Bezpečné vymazanie OÚ z dátových nosičov OÚ z dátových nosičov je nutné vymazať v nasledovných prípadoch:

- Po poruche dátového nosiča (pri riziku, že na pamäťovom médiu môžu zostaťzostatky OÚ),
- Pred použitím dátového nosiča, na ktorom boli OÚ, na iné účely (resp.pred ich použitím mimo chránených priestorov bez dohľadu oprávnenej osoby),

- V prípadoch, keď prenosné dátové nosiče majú pre plnenie pracovných úlohopustiť chránené priestory a uložené osobné údaje na nich nie sú šifrované.
- Pre vymazanie OÚ z dátových nosičov je nutné aplikovať patričné opatrenia.

1.1.8 Aktualizácia operačného systému a programového aplikačného vybavenia

Operačné systémy a aplikačný softvér sa aktualizujú vždy pri uvoľnení novej verzie externým správcom IT technológií. Dbať na dodržiavanie zmluvných podmienok s externým dodávateľom.

Operačný systém musí zabezpečovať nasledovné:

- Nesmie dovoliť užívateľovi meniť nastavenia operačného systému.
- Nesmie dovoliť užívateľovi použiť možnosť zapamätania hesla.
- Nesmie dovoliť užívateľovi ukladanie dát na lokálne zariadenia (pevné disky, USB...), len na tie, ktoré schváli prevádzkovateľ.
- Nesmie umožniť užívateľovi výber tlače na tlačiarne, ktoré by sa nenachádzali v miestnosti, z ktorej sa realizuje pripojenie.
- Musí zabezpečiť automatické odpájanie užívateľov pri nečinnosti užívateľov trvajúcej dlhšie ako 30minút.
- Musí zabezpečiť automatické spustenie šetriaceho režimu pri reaktivite užívateľa trvajúcej dlhšie ako 5min. Prechod zo šetriaceho do aktívneho režimu musí vyžadovať zadanie hesla užívateľa.

1.1.9 Pseudonymizácia OÚ

Zabezpečiť pseudonymizáciu spracúvaných osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia 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 fyzickej osobe alebo identifikovateľnej fyzickej osobe.

1.2 Organizačné opatrenia

1.2.1 Personálne opatrenie

1.2.1.1 Všeobecné personálne opatrenia

Poverenie osoby zodpovednej za výkon ochrany OÚ u prevádzkovateľa: Štatutárny orgán prevádzkovateľa písomne poverí výkonom dohľadu nad OOÚ vybraného zamestnanca. Toto poverenie je poverením zodpovednej osoby v zmysle zákona č. 18/2018 Z. z. Takto poverená Zodpovedná osoba vystupuje voči Úradu na ochranu osobných údajov ako zodpovedná osoba.

Nahlásenie poverenej zodpovednej osoby na úrad: Poverený zamestnanec bude nahlásený na úrad na ochranu osobných údajov.

Zmena zodpovednej osoby: Poverená zodpovedná osoba môže byť nahradená inou osobou v prípade, ak si neplní riadne svoje povinnosti ustanovené touto smernicou alebo z organizačných a personálnych dôvodov.

Zodpovednosť za ochranu OÚ: Zodpovednosť za ochranu OÚ musí byť zahrnutá do pracovných náplní zamestnancov. Za realizáciu zodpovedá personálny odbor.

Dohody o uchovávaní dôvernosti: Zamestnanci prichádzajúci do styku s OÚ, musia podpisovať dohody o uchovávaní dôvernosti, ako súčasť pracovných zmlúv. Dohoda musí byť podpísaná pred prvým spracúvaním OÚ. Za uzatváranie dohôd zodpovedá personálny odbor.

Školenia a vzdelávanie: Všetci zamestnanci, a kde je to relevantné aj užívatelia z tretích strán musia prechádzať pravidelnými školeniami o prostriedkoch, procesoch a procedúrach používaných u prevádzkovateľa. Školenia musia byť realizované pred prvým začatím práce a taktiež musia byť vykonávané preškolenia z príslušných postupov v pravidelných intervaloch. Za zabezpečenie školení zodpovedá personálny odbor.

Poučenie oprávnených osôb: Podľa § 21 zákona o OOÚ vyplýva povinnosť poučiť všetky osoby, ktoré majú alebo môžu mať prístup k IS tak, aby nedochádzalo k chybám pri spracúvaní OÚ. Poučenie vykonáva osoba poverená dohľadom nad OOÚ tzv. „zodpovedná osoba". O poučení sa vykonáva písomný záznam, ktorý je treba uchovať, ako doklad o vykonaní poučenia. Záznam musí podpísať osoba, ktorá poučenie vykonala aj osoba, ktorá bola poučená. Vzor záznamu je prílohou tejto smernice.

Vzdelávanie administrátorov a užívateľov: Administrátori systémov a užívatelia prevádzkovateľa absolvujú minimálne raz ročne vhodné školenia (v súvislosti s používaním a bezpečnosťou AIS). Školenia musia slúžiť aj na budovanie povedomia o informačnej bezpečnosti a ochrane OÚ. Za vypracovanie návrhu plánu vzdelávania pre príslušný rok zodpovedá oddelenie informatiky.

1.2.1.2 Rozsah zodpovednosti osoby poverenej dohľadom nad OOÚ

Osoba zodpovedná za dohľad nad OOÚ je povinná:

1. Neustále sledovať a posudzovať zákonnosť spracúvania OÚ v IS prevádzkovateľa, sledovať a posudzovať, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd DO.

2. V prípade zistenia narušenia práv a slobôd DO pred začiatkom spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania, písomne bezodkladne oznámiť toto zistenie prevádzkovateľovi.

3. Poučiť v mene prevádzkovateľa všetky OO v rozsahu ich oprávnení, ako aj ďalšie právnické alebo FO, ktoré majú alebo môžu mať prístup k OÚ spracúvaným v IS prevádzkovateľa o právach a povinnostiach vyplývajúcich z ustanovení zákona č. 18/2018 Z. z..

4. Zabezpečiť realizáciu organizačných, technických a personálnych opatrení na zabezpečenie ochrany OÚ pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním, ktoré sa spracúvajú v IS prevádzkovateľa. Na plnenie týchto úloh môže vyžadovať súčinnosť príslušných organizačných zložiek prevádzkovateľa, ktoré sú povinné poskytnúť mu pomoc pri plnení týchto úloh (zákona č. 18/2018 Z. z.).

5. Zachovávať mlčanlivosť o OÚ, s ktorými príde do styku. Informácie o OÚ nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa IS ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po zániku tejto funkcie alebo po skončení štátnozamestnaneckého pomeru, alebo obdobného pracovného vzťahu (zákona č. 18/2018 Z. z.). Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov pri plnení jeho úloh (zákona č. 18/2018 Z. z.).

6. Zodpovedná osoba ďalej zabezpečuje:

- potrebnú súčinnosť s úradom pri plnení úloh patriacich do jeho pôsobnosti; na požiadanie je zodpovedná osoba povinná úradu kedykoľvek predložiť svoje písomné poverenie, písomné oznámenia vystavené pre prevádzkovateľa podľa odseku 2, preukázať rozsah získaných vedomostí odborným školením;
- dohľad nad plnením základných povinností prevádzkovateľa podľa zákona č. 18/2018 Z. z. ;
- vybavovanie žiadostí DO podľa zákona č. 18/2018 Z. z. ;
- realizáciu technických, organizačných a personálnych opatrení a dohliada na ich aplikáciu v praxi; ak je prevádzkovateľ povinný vypracovať bezpečnostný projekt v súlade so zákonom č. 18/2018 Z. z. , zabezpečuje ich vypracovanie;
- dohľad pri výbere sprostredkovateľa podľa zákona č.18/2018 Z. z., prípravu písomnej zmluvy alebo písomného poverenia pre sprostredkovateľa v súlade so zákonom č. 18/2018 Z. z. a zodpovedá za jeho obsah; počas trvania zmluvného vzťahu alebo poverenia preveruje dodržiavanie dohodnutých podmienok;
- dohľad nad cezhraničným tokom OÚ;

7. Porušenie povinností ustanovených v odsekoch 1 až 6 sa považuje za porušenie pracovnej disciplíny.

1.2.1.3 Rozsah zodpovednosti OO

1. OO je každý zamestnanec, ktorý prichádza do styku s OÚ v rámci svojho pracovného zaradenia, a ktorý môže OÚ spracúvať len na základe pokynu prevádzkovateľa. Zoznam OO pre jednotlivé IS je uvedený v prílohe BS. OO majú nasledovné zodpovednosti, oprávnenia a povinnosti, platné pre všetky OO (špeciálne oprávnenia sú uvedené pre každú osobu samostatne v prílohe BS):

a) uplatňovať a dodržiavať organizačné a technické opatrenia popisované touto smernicou na zabezpečenie OOÚ spracúvaných v IS prevádzkovateľa pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním;
b) zachovávať mlčanlivosť o OÚ, s ktorými príde do styku. Informácie o OÚ nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa IS ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti trvá aj po zániku tejto funkcie alebo po skončení štátnozamestnaneckého pomeru, alebo obdobného pracovného vzťahu. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu na ochranu osobných údajov pri plnení jeho úloh;
c) spracúvať OÚ len v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve alebo v písomnom poverení;
d) od DO vyžadovať len také OÚ, ktoré sú nevyhnutné na dosiahnutie účelu spracúvania. K takýmto OÚ môže priradiť ďalšie OÚ DO, ktoré bezprostredne súvisia s daným účelom spracúvania, len ak na ne DO upozorní a táto s tým písomne súhlasí;
e) od DO získať písomný súhlas so spracúvaním OÚ, ak sa jedná o spracúvanie OÚ na základe súhlasu a tento súhlas archivovať v súlade s registratúrnym poriadkom a plánom. Súhlas obsahuje najmä údaj o tom, kto súhlas poskytol, komu sa tento súhlas dáva, na aký účel, zoznam OÚ, dobu platnosti súhlasu a podmienky jeho odvolania;
f) v priestoroch prístupných verejnosti zabezpečiť diskrétnosť spracúvania OÚ, teda nepripustiť, aby sa k OÚ DO dostali nepovolané osoby;
g) získavať OÚ nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak s tým DO písomne súhlasí alebo ak to umožňuje osobitný zákon;
h) zabezpečovať správnosť a aktuálnosť OÚ;
i) informovať prevádzkovateľa o nutnosti likvidácie OÚ, pokiaľ takáto povinnosť vyplynie z registratúrneho poriadku a plánu, alebo z ustanovení zákona č. 18/2018 Z. z. ;

j) na likvidáciu papierových dokumentov s OÚ použiť vhodné skratkovacie zariadenie;
k) príslušné OO sú v mene prevádzkovateľa oprávnené získavať potrebné OÚ od okruhu DO vymedzených v evidenčnom liste jednotlivých IS;
l) OO sú oprávnené vstupovať do IS obsahujúcich OÚ, ktoré sú spracúvané v písomnej alebo elektronickej podobe a spracúvať ich výlučne v rámci plnenia si svojich pracovných povinností.

2. Porušenie povinností popísaných v odseku 1 sa považuje za porušenie pracovnej disciplíny.

1.2.2 Vedenie zoznamu aktív a jeho aktualizácia

Je potrebné vypracovať podrobnú dokumentáciu o sieťovej infraštruktúre. Dokumentácia musí obsahovať nasledovné informácie o každom technickom zariadení používanom u prevádzkovateľa:

- označenie zariadenia
- presne fyzické umiestnenie zariadenia
- funkcia zariadenia
- fyzické prepojenia zariadení
- popis nastavenia parametrov zariadenia
- informáciu o vlastníkovi zodpovednom za správu zariadenia.

Všetky aktíva s OÚ musia byť inventarizované tak, aby im mohla byť poskytnutá technická starostlivosť a zodpovedajúca úroveň bezpečnosti.

Inventarizácia aktív.
Za vedenie zoznamu aktív a jeho aktualizáciu je zodpovedný vlastník aktív (oprávnená osoba).

Pozn.: Aktíva informačného systému, ktoré sú v správe sprostredkovateľa **spoločnosti** aktualizuje daný sprostredkovateľ.
Riadenie prístupu oprávnených osôb k osobným údajom
Kontrola vstupu do objektu a chránených priestorov prevádzkovateľa
Identifikácia a autentizácia pri vstupe do objektu alebo priestorov
- Zamestnanci **spoločnosti** sú identifikovaní pri vstupe do objektu na základe platného OP /preukazu zamestnanca /elektronická identifikačná karta zamestnanca/.

1.2.3 Riadenie prístupu OO k OÚ

1.Heslá sú bežným prostriedkom overenia užívateľskej identity pre prístup do IS alebo službe. Užívatelia sú preto povinní používať heslo pri prihlasovaní sa do operačného systému, siete a aplikácie spracúvajúcej OÚ.
2. Heslá nesmú byť uložené na počítačovom systéme v nechránenej podobe. Heslá je treba udržovať v dôvernosti.

3. Všetci užívatelia sa musia vyvarovať držania záznamu hesiel na papieri, ak takýto záznam nemôže byť bezpečne uložený.
4. Administrátorské heslá najvyššej úrovne uložiť na zabezpečenom mieste pre prípad núdze (napríklad bezpečnostná schránka v banke, trezor, ...) V žiadnom prípade nesmú byť heslá ukladané v elektronickej forme v nechránenom dokumente.
5. Užívatelia sú povinní zmeniť heslá vždy, keď existuje akákoľvek indícia ohrozenia systému alebo hesla.
6. Užívatelia sú povinní vyberať alebo vytvárať len také kvalitné heslá ktoré majú minimálnu dĺžku 6 znakov (okrem administrátorských hesiel,ktoré musia mať minimálne 8 znakov), ktoré sú:

- nie sú ľahko zapamätateľné;
- nie sú založené na ničom, čo by mohol niekto iný ľahko uhádnuť alebo získať použijúc informácie týkajúce sa danej osoby (napr. mená, priezviská, telefónne čísla, dátumy narodení atď.;
- obsahujú okrem malých písmen aj ďalšie znaky, t.j. číslice, špeciálne znaky, veľké písmená
- neobsahujú po sebe idúce identické znaky alebo čisto číselné, alebo abecedné skupiny

7. Správca IT zabezpečí nastavenie príslušnej politiky pre akceptáciu užívateľských hesiel.
8. Užívateľom sa odporúča používať jedno kvalitné heslo aj pri prístupe k viacerým službám a tiež platformám.

1.2.4 Organizácia spracúvania OÚ

1.2.4.1 Pravidlá spracúvania OÚ v chránenom priestore

1. OO sa povoľuje používať výlučne softvér, ku ktorému má prevádzkovateľ platnú licenciu. Používať neautorizovaný softvér sa zakazuje.
2. Na jednotlivých pracoviskách dodržiavať politiku tzv. čistého stola a obrazovky – papierové a počítačové médiá s OÚ nie je povolené nechávať bez dozoru voľne položené na pracovisku. PC nesmú zostať bez dozoru prihlásené do systému; pri opustení pracoviska je potrebné systém uzamknúť, aby sa zabránilo neautorizovanému prístupu do počítačov. Papierové a počítačové médiá s OÚ sa musia ukladať do vhodných uzamykateľných skríň, a to najmä v mimopracovnom čase.
3. Je dovolené kopírovanie a tlač len takých dokumentov, ktoré sú potrebné k výkonu pracovnej činnosti. Tlačiť alebo kopírovať iné písomnosti sa zakazuje.
4. K zabráneniu odcudzenia a šírenia OÚ je zakázané ponechávať kopírované alebo vytlačené dokumenty obsahujúce OÚ bez dozoru v kopírke, alebo tlačiarňach. Po skopírovaní alebo vytlačení dokumentu obsahujúceho OÚ je

zamestnanec, ktorý kopírovanie, alebo tlač vykonal, povinný skopírované, alebo vytlačené dokumenty ihneď z kopírky, alebo tlačiarne odobrať.

5. Vytlačené dokumenty, ktoré obsahujú OÚ a nie sú už potrebné, alebo boli vytlačené omylom je osoba, ktorá ich vytlačila, povinná okamžite skartovať. V žiadnom prípade sa nesmú použiť na ďalšiu tlač alebo ako pracovný papier, ani ako papier určený do zberu. Do zberu môžu ísť len skartované dokumenty.
6. Zakazuje sa poskytovanie OÚ o inej osobe prostredníctvom telefónu, okrem poskytovania údajov orgánom činným v trestnom konaní (túto problematiku rieši samostatný dokument), faxu a nechránenej emailovej komunikácie.
7. Heslá sú bežným prostriedkom overenia užívateľskej identity pre prístup do IS alebo službe. Užívatelia sú preto povinní používať heslo pri prihlasovaní sa do operačného systému, siete a aplikácie spracúvajúcej OÚ.

1.2.4.2 Riadenie komunikácie a prevádzky

1. **Akceptácia nových prostriedkov spracúvania OÚ:** Musia byť stanovené akceptačné kritéria pre nové IS, aktualizácie existujúcich systémov prípadne pre nové verzie a pred samotnou akceptáciou musia byť vykonané vhodné testy a zálohovanie systému (za predpokladu, že to dané systémy umožňujú). Za realizáciu zodpovedá odbor IT.

2. **Likvidácia zariadení:** Likvidácia nefunkčných, poškodených alebo vyraďovaných zariadení, na ktorých sa nachádzajú spracúvané OÚ sa musí vykonávať bezpečným spôsobom tak, aby nemohlo dôjsť k strate dôvernosti OÚ nachádzajúcich sa na príslušnom zariadení. Pri likvidácii zariadení sa musí brať na zreteľ najmä: likvidácia pevných diskov, USB, Flash, CD, DVD, magnetických pások, diskiet.... Za bezpečnú likvidáciu zariadení zodpovedá odbor IT.

1.2.4.3 Zásady jednotného poskytovania informácií DO:

Poskytovanie informácií DO:

Na základe zákona č. 18/2018 Z. z. je METAL TATRY, s.r.o. povinná poskytovať DO informácie o stave spracúvania jej OÚ . Právo na poskytnutie informácie DO vzniká na základe písomnej žiadosti. METAL TATRY, s.r.o. ako prevádzkovateľ IS v zmysle zákona č. 18/2018 Z. z. má podľa tohto zákona povinnosť zabezpečiť primeranú úroveň ochrany OÚ prijatím vhodných technických, personálnych a organizačných opatrení. Z tejto požiadavky vyplývajú určité obmedzenia v použití informačných kanálov, ktorými sa vykonáva komunikácia medzi

DO a METAL TATRY, s.r.o. Na druhej strane je potrebné snažiť sa maximálne vyjsť vstretý DO pri poskytovaní informácií., za dodržania všetkých požadovaných bezpečnostných opatrení.

Existujúce komunikačné kanály pre poskytovanie informácií DO:

- telefonická komunikácia.
- elektronická komunikácia emailom.
- komunikácia prostredníctvom faxu.
- písomná komunikácia slovenskou poštou.
- osobná komunikácia.

Pri použití ktoréhokoľvek z vyššie uvedených komunikačných kanálov, je potrebné zabezpečiť nasledovné:

- presnú identifikáciu žiadateľa. Jeho autenticitu. Preukázateľné zabezpečenie skutočnosti, že žiadosť o poskytnutie informácií je skutočne od DO alebo osoby, ktorá je oprávnená žiadať v mene DO o poskytnutie informácií.
- nepopierateľnosť odoslania žiadosti, preukázateľné zabezpečenie nemožnosti poprieť skutočnosť, že žiadosť o poskytnutie informácií bola odoslaná DO.
- zabezpečenie dôvernosti a integrity odosielaných informácií počas ich prenosu k DO.
- preukázateľné zabezpečenie toho, že informácie boli DO komunikačným kanálom doručené.

Žiadosť o poskytnutie informácií DO:

Na základe zákona č.18/2018 Z. z. má DO právo vyžadovať poskytnutie informácií len na základe písomnej žiadosti. Žiadosť musí obsahovať presnú identifikáciu DO a autorizáciu žiadosti vlastnoručným podpisom.

METAL TATRY, s.r.o. umožňuje aj iné formy žiadosti o poskytnutie informácií než je písomná forma. Postup pre akceptáciu žiadosti poskytnutej v inej forme ako písomnej a zabezpečenie požiadaviek na bezpečnosť podľa článku 4 tejto BS, je popísaný v nasledujúcich článkoch pri jednotlivých druhoch komunikácie.

Využívanie telefonickej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti

Pri telefonickej komunikácii je veľmi ťažké zabezpečiť autenticitu DO, ktorá telefonicky žiada o poskytnutie informácie. A to aj napriek tomu, ak osoba na druhej strane linky môže poznať všetky dôležité identifikátory DO.

Z tohto dôvodu nemôže byť na odpoveď použitý telefonicky komunikačný kanál, ale len písomná forma odpovede.

Zamestnanec prijímajúci žiadosť zaeviduje a upozorní DO , že odpoveď dostane iným komunikačným kanálom (slovenská pošta, elektronická pošta) na adresu, ktorú má daná DO zadanú ako komunikačnú. Bezpečnostné opatrenia , ktoré je potrebné dodržať, sú popísané v nasledujúcich článkoch príkazu.

Odosielanie informácií

DO, ktorej OÚ METAL TATRY, s.r.o. spracúva je možné poskytovať telefonicky len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke METAL TATRY, s.r.o. Telefonicky je možné poskytovať rady DO. Na tieto úkony nie je potrebná identifikácia klienta (DO).

Využívanie elektronickej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti

Pri elektronicky zaslanej žiadosti o poskytnutie informácií DO sa riadi pravidlami uvedenými pre telefonickú komunikáciu. Žiadosť možno akceptovať, no odpoveď musí byť zaslaná buď emailom so zabezpečením bezpečnostných požiadaviek alebo v písomnej forme slovenskou poštou na komunikačné adresy DO.

Odosielanie informácií

DO, ktorej OÚ spracúva METAL TATRY, s.r.o. je možné poskytovať nezabezpečenou elektronickou poštou len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke METAL TATRY, s.r.o.

Odoslať informácie obsahujúce OÚ DO elektronickou poštou je možné len v prípade, ak využíva ZEP a prevádzkovateľ vlastní jeho verejný kľúč, ktorým môže zašifrovať odosielané informácie, alebo sa použije s DO dohodnutá bezpečná forma šifrovania odosielaných informácií . Informácie sa odosielajú na emailovú adresu, ktorú má DO uvedenú ako komunikačnú. Je zakázané odosielať odpoveď na adresu, z ktorej prišla žiadosť, v prípade že sa nezhoduje s adresou uvedenou ako komunikačná adresa. Heslo alebo dešifrovací kľúč musí byť DO doručený inou cestou , než akou išli odosielané informácie.

Využívanie komunikácie prostredníctvom faxu na poskytovanie informácií DO:

Prijatie žiadosti

Pri faxom zaslanej žiadosti o poskytnutie informácií DO sa riadi pravidlami uvedenými pre telefonickú komunikáciu. Žiadosť možno akceptovať, no odpoveď musí byť zaslaná buď emailom so zabezpečením bezpečnostných požiadaviek, alebo v písomnej forme slovenskou poštou na komunikačné adresy jednotlivých DO.

Odosielanie informácií

DO, ktorej OÚ spracúva METAL TATRY, s.r.o. je možné poskytovať nezabezpečenou faxovou komunikáciou len všeobecné informácie, napr. také, ktoré sú verejne publikované na webovej stránke METAL TATRY, s.r.o.

Odoslať informácie faxom, ktoré obsahujú OÚ DO je zakázané.

Využívanie písomnej komunikácie (Slovenská pošta) na poskytovanie informácií DO:

Prijatie žiadosti

Písomnú žiadosť, pokiaľ spĺňa požadované náležitosti na identifikáciu, je možné akceptovať v plnom rozsahu. Informácie je možné odoslať len na komunikačnú adresu DO.

Odosielanie informácií

Odoslať informácie obsahujúce OÚ DO slovenskou poštou je možné len v prípade, ak je pošta odoslaná do vlastných rúk. Adresa, na ktorú sa informácie odosielajú, musí byť zhodná s adresou uvedenou ako komunikačná adresa.

Využívanie osobnej komunikácie na poskytovanie informácií DO:

Prijatie žiadosti

Pri osobnej návšteve DO a požadovaní poskytnutia informácií, OO vykoná identifikáciu DO vyžadovaním predloženia preukazu totožnosti a porovnaním identifikátorov ako je meno, priezvisko, dátum narodenia a RČ so záznamom v evidencii DO (Napríklad mzdová a personálna agenda, ...). Ak sa identifikátory zhodujú , OO žiadosť akceptuje a poskytne DO požadované informácie.

Odosielanie informácií

Informácia požadovaná DO pri osobnej návšteve môže byť poskytnutá ústnou formou, alebo na požiadanie DO aj písomnou formou.

Vytváranie záznamov súvisiacich s poskytovaním informácií DO:

OO, ktoré prijímajú a vybavujú žiadosti DO sú povinné vykonávať záznam o prijatí žiadosti a poskytnutí informácií DO. Záznamy sa vedú v elektronickej forme. Záznam obsahuje informáciu o dátume prijatia žiadosti, dátume poskytnutia informácií, komunikačnom kanále, ktorým bola prijatá žiadosť, komunikačnom kanále, ktorým boli OÚ odoslané DO, identifikácia OO, ktorá žiadosť prijala, identifikácia OO, ktorá žiadosť splnila.

Komunikácia s treťou stranou:

V prípade, ak OO zasiela OÚ DO tretej strane (napríklad jedná sa o poskytovanie OÚ) je OO povinná zabezpečiť primeranú úroveň dôvernosti

zasielaných OÚ. Musí zabezpečiť ochranu OÚ počas prenosu vhodnou formou šifrovania a musí zabezpečiť dôvernosť OÚ doručením OÚ len OO tretej strany. Za výber vhodnej formy šifrovania zodpovedá odbor IT.

Riadenie prístupu:

1. Od užívateľov sa musí vyžadovať, aby zabezpečili primeranú ochranu nestrážených prostriedkov.
2. Užívatelia musia mať prístup len k prostriedkom, na ktorých používanie boli autorizovaní.
3. K zabráneniu neautorizovaného spustenia PC, na ktorých sa spracúvajú OÚ, musí byť operačný systém nastavený tak, aby jeho spustenie nebolo možné bez zadania prístupového mena a hesla užívateľa (vytvoriť užívateľské konto, prípadne kontá, ak má byť viac užívateľov).
4. K zabráneniu neautorizovaného spustenia aplikácie spracúvajúcej OÚ je treba systém tejto aplikácie nastaviť tak, aby jej spustenie nebolo možné bez zadania prístupového mena a hesla užívateľa (vytvoriť užívateľské konto, prípadne kontá, ak má byť viac užívateľov).
5. V systéme aplikácii spracúvajúcich OÚ je potrebné (ak to aplikácia umožňuje) nastaviť pravidlá pre blokovanie užívateľského konta (po niekoľkonásobnom zadaní chybného hesla); nastaviť možnosť informovania užívateľa pri jeho prihlásení o pokusoch o neoprávnené vniknutie do aplikácie.
6. K zamedzeniu neoprávneného prístupu k aplikáciám musia byť stanovené záväzné pravidlá pre tvorbu silných hesiel, v každom prípade identifikácie a autentizácie užívateľov.
7. Registrácia a deregistrácia užívateľov IS sa u prevádzkovateľa riadi samostatným pracovným postupom. Postup musí zabezpečiť jednoznačnú identifikáciu každého užívateľa (každý užívateľ má jednoznačný a jedinečný identifikátor). Postup musí ďalej zabezpečiť dôvernosť užívateľských hesiel tak , aby si užívatelia nepoznali navzájom heslá. Heslá užívateľov nesmie poznať ani administrátor systému).
8. Zodpovednosť za prezradenie hesla nesú užívatelia.

1.2.4.4 Všeobecné opatrenia

K zabezpečeniu dodržiavania požiarnych predpisov a predpisov BOZP neustále aktualizovať dokumentáciu dodržiavania predpisov PO a BOZP.

Pre minimalizovanie možností neoprávneného šírenia dát, neautorizovaného používania softvéru, prípadne inej neoprávnenej manipulácie s dátami treba odstrániť, prípadne softvérovo zablokovať používanie zapisovacích médií (disketové mechaniky, CD RW mechaniky, USB kľúče), ktoré nie sú nutné pre výkon práce .

V zmysle zákona č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov musí byť vypracovaný registratúrny poriadok a plán. Z neho vyplývajúce úlohy a opatrenia je potrebné zaviesť neodkladne do praxe - najmä zabezpečenie, aby sa IS s OÚ v písomnej podobe zabezpečil proti požiaru a iným

degradačným vplyvom (v zmysle vyhlášky č. 628/2002 Z. z.), a aby sa zabránilo neoprávnenému prístupu k IS v podobe dokumentov s OÚ.

K zabráneniu neautorizovaného prístupu k zasielaným správam používať šifrovanie komunikácie v prípadoch, keď predmetom komunikácie sú OÚ.

Všetky citlivé aplikácie musia vyžadovať autentizáciu užívateľa pri spúšťaní aplikácie.

U prevádzkovateľa je zakázané používať fax na prenos OÚ.

K odstráneniu, alebo minimalizovaniu rizika odpočúvania, alebo neoprávneného prístupu k dátam, je zakázané poskytovanie a sprístupňovanie OÚ o inej osobe cez telefón.

Zoznam IS: Poverená zodpovedná osoba vedie zoznam jednotlivých IS, v ktorých prevádzkovateľ spracúva OÚ..

Zmluvy so sprostredkovateľmi: V prípade zmlúv, na základe ktorých sú externe dodávané služby, pričom zamestnanci dodávateľa majú, alebo môžu mať prístup k OÚ spracúvaných prevádzkovateľom, alebo tretia strana je priamo poverená spracúvaním OÚ, je potrebné spracúvať dodatky týchto zmlúv s cieľom upraviť práva a povinnosti v súvislosti s OOÚ. Zmluva musí spĺňať zákonom stanovené náležitosti a musí obsahovať články, v ktorých sa dodávateľ zaväzuje plniť ustanovenia zákona č.18/2018 Z. z., berie na seba povinnosť vykonať poučenie osôb, ktoré môžu prísť pri výkone svojej činnosti do styku s OÚ prevádzkovateľa a berie na seba prípadnú zodpovednosť za porušenie zákona svojimi zamestnancami pri výkone činnosti vyplývajúcich zo zmluvného vzťahu.

Údržba HW a SW: Musí byť zabezpečené vykonávanie preventívnej údržby hardvéru a softvéru v plánovaných intervaloch, podľa vopred určeného harmonogramu. Plán preventívnej údržby musí byť súčasťou IT dokumentácie a musí obsahovať presné termíny a popis jednotlivých činností a zodpovedností za ich vykonanie (napr. kontrola funkčnosti záložných zdrojov napájania a stavu ich akumulátorov....). Za implementáciu opatrenia zodpovedá sekcia informatiky.

Servis HW a SW: Na správu a servis hardvéru a softvéru musí byť vybratá vhodná organizácia, s ktorou sa uzavrie písomná zmluva o spolupráci tak, aby bola zabezpečená technická podpora pre všetky systémy prevádzkovateľa v prípade výskytu problémov technického rázu alebo potreby rozšírenia systémov. Pri servise (opravách zariadení) je potrebné zabezpečiť, aby pri výkone servisných činností nemohlo dôjsť k strate informácií z IS obsahujúcich OÚ. Zariadenia, na ktorých sa nachádzajú citlivé OÚ nesmú opustiť priestor prevádzkovateľa. Za dodržiavanie zodpovedá sekcia informatiky.

Získavanie OÚ: Spôsob a forma získavania OÚ Musí byť zdokumentovaná a popísaná v pracovných manuáloch. Za vypracovanie manuálov zodpovedajú správcovia jednotlivých IS, uvedení v bezpečnostnom projekte, časti popisujúcej IS.

Všeobecné pravidlá pri získavaní OÚ: Pri získavaní OÚ od DO je zakázané získavať OÚ kopírovaním osobných dokladov bez súhlasu DO. Toto je dovolené len s písomným súhlasom DO, alebo ak to dovoľuje, alebo prikazuje osobitný zákon. Ďalej je zakázané získavať od DO OÚ, ktoré nie sú nevyhnutne potrebné k dosiahnutiu účelu spracúvania a teda nie sú vymedzené v dokumentácii príslušného IS(agendy) podľa definovaného účelu spracúvania..
Pred samotným získaním OÚ OO oznámi DO nasledovné náležitosti:

a. názov a sídlo prevádzkovateľa IS;
b. názov a sídlo sprostredkovateľa (ak bol poverený spracúvaním OÚ);
c. zodpovednú osobu;
d. účel spracúvania OÚ;
e. zákon, ktorý poskytnutie OÚ vyžaduje, ak nie sú získavané na základe súhlasu DO. Ak sú OÚ spracúvané na základe súhlasu DO treba túto skutočnosť oznámiť DO a požiadať ju o písomný súhlas;
f. vykoná poučenie DO o jej právach, ktoré sú nasledovné;

DO má právo od prevádzkovateľa požadovať:

- informácie o stave spracúvania jej OÚ v IS,
- presné informácie o zdroji, z ktorého získal jej OÚ na spracúvanie,
- odpis jej OÚ, ktoré spracúva v IS,
- opravu nesprávnych, neúplných alebo neaktuálnych OÚ, ktoré sú predmetom spracúvania,
- likvidáciu jej OÚ, ak bol splnený účel spracúvania; ak sú predmetom spracúvania úradné doklady obsahujúce OÚ, môžete požiadať o ich vrátenie,
- likvidáciu jej OÚ, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona č. 18/2018 Z. z. o OOÚ, zo strany prevádzkovateľa.

Súhlas DO: Pre IS, v ktorých sú OÚ spracúvané na základe súhlasu DO, príslušná OO zabezpečí získanie súhlasu od DO. Súhlas DO musí obsahovať nasledovné náležitosti:

- kto súhlas dáva;
- komu sa súhlas dáva;
- na aký účel spracúvania OÚ alebo dokladu je súhlas daný;
- na aké OÚ sa súhlas dáva;
- na akú dobu je súhlas vydaný;
- podmienky odvolania súhlasu;
- súhlas musí byť v písomnej forme a osobne podpísaný DO;
- v prípade emailu musí byť súhlas podpísaný elektronickým podpisom.

Vzor súhlasu je obsahom bezpečnostnej dokumentácie

Poskytnutie OÚ je dobrovoľné, súhlas si nemožno vynucovať odmietnutím poskytnutia nejakej služby, iba v prípade, kedy poskytnutie údajov vyžaduje zákon.

V prípade, že do organizácie príde email obsahujúci OÚ a na ich spracúvanie sa vyžaduje súhlas DO, musí byť z počítača spoľahlivým spôsobom zlikvidovaný a odosielateľ musí byť o tom informovaný. Pod spoľahlivým spôsobom sa rozumie taká likvidácia, aby OÚ obsiahnuté v emailoch už nebolo možné zrekonštruovať.

V prípade, že príde do organizácie listová zásielka obsahujúca OÚ, na ktorých spracúvanie sa vyžaduje súhlas DO a zásielka nebude obsahovať požadovaný súhlas DO, musí byť obratom od odosielateľa vyžiadaný príslušný súhlas na spracúvanie OÚ obsiahnutých v listovej zásielke. Ak DO v stanovenom termíne príslušný súhlas neposkytne, nebudú jej OÚ spracúvané.

Kopírka a fax musia byť v mimopracovnom čase uzamknuté alebo iným vhodným spôsobom chránené pred neautorizovaným prístupom.

1.2.5 Likvidácia OÚ

1. V prípade ukončenia účelu spracúvania OÚ musí byť zabezpečená ich bezodkladná likvidácia bezpečným spôsobom (za predpokladu, že iný zákon neustanovuje iné podmienky). Likvidácia musí byť prevedená na písomných dokumentoch ale aj na všetkých počítačových médiách (pevné disky, DVD, CD, USB kľúče, diskety....). Za účelom dodržiavania likvidácie OÚ musí byť zdokumentovaný proces monitorovania IS za účelom identifikovania OÚ, ktoré treba zlikvidovať. Za bezpečnú likvidáciu zodpovedá „Zodpovedná osoba" a jednotlivé OO.

2. **Oznámenie o likvidácii OÚ:** DO musia byť vhodnou formou oboznámené o likvidácii ich OÚ. Napríklad elektronickou poštou.

3. **Likvidácia dokumentov:** Likvidácia dokumentov obsahujúcich OÚ musí byť prevádzaná výlučne skartovaním. Zakazuje sa odkladať nepotrebné dokumenty obsahujúce OÚ akýmkoľvek spôsobom (zberné suroviny, kôš, opätovné použitie čistej strany na tlač...).

4. **Likvidácia pamäťových médií:** Likvidácia pamäťových médií, na ktorých sa nachádzajú OÚ, musí byť prevádzaná fyzickým zničením nosičov dát.

1.2.6. Bezpečnostné incidenty

1.2.6.1 Nahlasovanie BI:

Všetci zamestnanci prevádzkovateľa aj tretích strán, majú povinnosť nahlasovať BI, ktoré sa vyskytnú počas ich práce. BI sa nahlasujú „Zodpovednej osobe". Zodpovedná osoba je povinná viesť databázu incidentov a zabezpečuje realizáciu mechanizmu poučenia sa z BI. „Zodpovedná osoba" musí zabezpečiť nasledovné:

a. zadefinovať dovolené spôsoby nahlasovania BI,

b. oboznámenie zamestnancov s definíciou, čo to BI je,
c. stanoviť klasifikačnú stupnicu BI a zabezpečiť ich klasifikáciu podľa stanovenej stupnice,
d. vedenie databázy incidentov s informáciami o tom, kto incident nahlásil, popis incidentu, jeho klasifikácia, dátum a čas nahlásenia, kto bude incident riešiť, kedy boli vykonané aké úkony, ako a kedy bol incident vyriešený.
e. spätnú odozvu pre zamestnancov, ktorí BI nahlásili, ako sa problém rieši a prehľadný prístup k jednotlivým informáciám.
f. **Nahlásenie BI Úradu a všetkým DO, ktorých sa BI týka do 72 hodín od zistenia BI**

1.2.6.2 Poučenie sa z BI:

„Zodpovedná osoba" zabezpečí aplikovanie mechanizmu z poučenia sa z incidentov. Mechanizmus musí zabezpečiť nasledovné :

a. vyhodnotenie BI zaevidovaného v databáze incidentov z hľadiska jeho závažnosti,
b. vykonanie analýzy prečo sa BI stal,
c. vyhodnotenie, aký mal BI dopad,
d. návrh ochranných opatrení, ktoré majú zabrániť opakovaniu sa daného BI,
e. schválenie navrhnutých ochranných opatrení manažmentom,
f. implementáciu schválených ochranných opatrení.

Porušenie BS: Porušenie BS zo strany zamestnancov musí byť riešené disciplinárnym procesom. Za realizáciu zodpovedá personálny odbor.

1.2.6.3 Postupy po vzniku mimoriadnych situácií a plány obnovy

Haváriou, poruchou alebo mimoriadnou situáciou sa pre účely tejto smernice rozumejú incidenty, ktoré sú schopné spôsobiť škodu na IS, zlyhanie IS, stratu poskytovania služieb, odopretie služieb, chyby následkom nekompletných, alebo nepresných dát, narušenie dôvernosti – napr. požiar, odcudzenie, strata dát, zlyhanie aplikácii, neoprávnené šírenie dát a pod..

K predchádzaniu haváriám, poruchám a iným mimoriadnym udalostiam sú prijaté viaceré opatrenia, ako opatrenia na dodržiavanie protipožiarnych predpisov, ktoré sú dokumentované v protipožiarnej dokumentácii, opatrenia na dodržiavanie predpisov bezpečnosti a zdravia pri práci, ktoré sú popisované v dokumentácii BOZP. K zabráneniu incidentov v súvislosti s výpadkom dodávky elektrickej energie sú inštalované záložné zdroje elektrickej energie.

Všetci užívatelia IS sú povinní ihneď po zistení ohlásiť priamemu nadriadenému alebo správcovi IT udalosť týkajúcu sa neštandardného správania výpočtového prostriedku alebo počítačovej siete.
K neštandardnému správaniu výpočtového prostriedku patrí najmä:

- nemožnosť jeho zapnutia
- problémy so zavedením operačného systému
- nemožnosť prihlásiť sa do lokálneho operačného systému

- neodôvodnené hlásenie o inštalovaní nových hardvérových zariadení
- nemožnosť spustiť pridelené programy a aplikácie
- nemožnosť prihlásiť sa do aplikácie
- pozorovateľné zníženie výkonnosti počítača (pomalé odozvy na zadané príkazy)
- hlásenie o zlyhaní hardvérových zariadení
- zobrazovanie neznámych a nezmyselných hlásení.

Ďalej je každý užívateľ systému povinný okamžite po zistení hlásiť v súlade s príslušnými dokumentmi udalosť, ktorou je:

- prítomnosť dymu
- vznik požiaru
- prienik vody

Pre technické prostriedky, ktoré slúžia na spracúvanie OÚ, je potrebné dodržiavať postupy pri haváriách a poruchách celého IS alebo jeho častí. Ich zmysel spočíva jednak v garancii zachovania funkčnosti IS prostredníctvom technických prostriedkov, ako aj zachovania bezpečnosti OÚ, ktoré sa na týchto technických prostriedkoch spracúvajú.

Postupy riešenia havarijných situácií sú výsledkom procesu plánovania kontinuity činností, ktorý pozostáva z nasledujúcich etáp:

a) **analýza problémov a funkčných dopadov** – identifikácia problémov, ich vážnosti a dopadu pôsobenia na IS s ohľadom na OÚ

b) **stanovenie stratégie obnovy** – stanovenie spôsobu, akým sa musí pristupovať k obnove prvkov IS (servery, klientsky počítač, príslušná časť siete LAN)

c) **realizácia technických a organizačných opatrení na vytvorenie východiskového stavu** – pre zabezpečenie obnovy v zmysle definovanej stratégie, je potrebné zabezpečiť technické a organizačné predpoklady pre obnovu (napr. je potrebné zabezpečiť zálohovanie)

d) **testovanie, nácvik a aktualizácia postupov** – overenie toho, či plány zodpovedajú skutočnosti a či realizácia činností podľa plánov vedie k obnove.

Plán obnovenia činnosti nadväzuje na dokumenty Požiarne a poplachové smernice a Evakuačný plán. Plán uvedené dokumenty nenahrádza, ale ich rozširuje o postupy po vzniku poruchy, havárie alebo inej mimoriadnej udalosti, ktoré je potrebné vykonať za účelom zotavenia IS spracúvajúcich OÚ ako celkov alebo len niektorého z ich prvkov.

Pri riešení úloh Plánu je nevyhnutné najprv lokalizovať a identifikovať problémovú udalosť a jej pôsobenie a následne vykonať stanovené aktivity na zmiernenie alebo eliminovanie jej účinkov.

Plán zahŕňa obnovu technických a programových prostriedkov serverov a klientskych počítačov prevádzkovateľa.

Ak v dôsledku havárie, poruchy alebo mimoriadnej situácie dôjde k znefunkčneniu pracovných priestorov, obnova stavu pred haváriou sa vykoná v náhradných pracovných priestoroch.

Za obnovu funkčnosti IS zodpovedá odbor IT.

1.2.7 Kontrolná činnosť

1. Zodpovedná osoba, prípadne iná poverená osoba je povinná vykonať kontrolu bezpečnosti IS pravidelne v polročných intervaloch.
2. Zodpovedná osoba, prípadne iná poverená osoba, vykonáva kontrolu bezpečnosti IS fyzickou previerkou účinnosti prijatých bezpečnostných opatrení.
3. Z kontrolnej činnosti je zodpovedná osoba, prípadne iná poverená osoba povinná vyhotoviť záznam, ktorý obsahuje nasledovné skutočnosti:
    - dátum a miesto vykonania kontroly;
    - oblasť zamerania kontroly;
    - identifikáciu osoby vykonávajúcej kontrolu;
    - zistené skutočnosti v priebehu kontroly;
    - záverečné zhodnotenie, či bezpečnostné opatrenia plnia svoju úlohu, a že zodpovedajú požiadavkám dokumentovaným v bezpečnostnom projekte;
    - iné skutočnosti hodné osobitného zreteľa týkajúce sa bezpečnosti IS zistené vykonanou kontrolou;
    - návrh opatrení potrebných k vykonaniu nápravy nedostatkov zistených v priebehu kontroly;
    - vyjadrenia kompetentných vedúcich zamestnancov k záverom kontroly;
    - vlastnoručný podpis osoby, ktorá vykonala kontrolu.
4. Porušenie povinností stanovených v odsekoch 1 až 3 sa považuje za porušenie pracovnej disciplíny.

SPRACOVANIE OÚ V RÁMCI WEBOVÝCH STRÁNOK A E-SHOP

Spracúvanie osobných údajov je neoddeliteľnou súčasťou prevádzky našich **webových stránok**. Je pre nás dôležité, aby osobné údaje zákazníkov boli spracúvané spôsobom, ktorý neodporuje zásadám a požiadavkám NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „GDPR") ani zákonu č. 18/2018 Z. z. o ochrane osobných údajov. Z tohto dôvodu, ale aj v záujme transparentnosti nakladania s osobnými údajmi pripravil prevádzkovateľ webových stránok túto informáciu o ochrane osobných údajov.

V prípadoch, keď sa od zákazníka ako od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytuje prevádzkovateľ pri získavaní osobných údajov nasledovné informácie:

Účelom spracúvania osobných údajov je realizácia prevádzky webovej stránky ako aj rezervácie či objednávky tovarov a služieb na základe požiadavky zákazníka a tiež marketingové aktivity prevádzkovateľa na základe oprávneného záujmu. **Právnym základom** spracúvania osobných údajov je tak článok **6 odsek 2 písm. b) a f) GDPR**, a na jeho plnenie je nevyhnutné získať a spracúvať osobné údaje v minimálnom potrebnom a tiež možnom rozsahu.

Pri prevádzke webových stránok dbáme o **dôvernosť osobných údajov našich zákazníkov** a ich osobné údaje **neposkytujeme žiadnym iným subjektom**, okrem tých, ktorých zapojenie do procesu dodania je nevyhnutné, ako sú prepravné spoločnosti, ktoré zabezpečujú doručenie tovaru alebo služieb, poskytovateľ platobných služieb alebo iné subjekty s oprávnením v zmysle osobitného zákona. v takom prípade sú tieto subjekty tretími stranami.

Osobné údaje zákazníkov súvisiace s dodaním tovarov a služieb **uchovávame po dobu nevyhnutnú na splnenie archivačných povinností vyplývajúcich z osobitných predpisov** (napr. príslušné právne predpisy upravujúce povinnosti pri vedení účtovníctva a pod.).

Zákazník ako dotknutá osoba má právo na informácie a prístup ku svojim osobným údajom, právo na ich opravu, právo na portabilitu a tiež právo na vymazanie, právo na namietanie či obmedzenie spracúvania a právo obrátiť sa kedykoľvek na dozorný orgán ochrany osobných údajov. Právom každej dotknutej osoby je tiež právo podať sťažnosť dozornému orgánu, ktorým je Úrad na ochranu osobných údajov Slovenskej republiky.

Je našim cieľom získavať a **spracúvať osobné údaje zákazníkov v najmenšom možnom rozsahu**. **Zabezpečenie dodania tovarov a služieb však bez spracúvania osobných údajov nie je možné.** Poskytnutie minimálneho rozsahu údajov je teda požiadavkou, ktorá je potrebná na uzavretie zmluvného vzťahu.

Je našim oprávneným záujmom vedieť akým spôsobom naši návštevníci používajú naše webstránky s cieľom zlepšiť možnosti a pohodlie ich návštevy a používania ako aj možnosť realizácie marketingovej komunikácie. S týmto zámerom využívame v minimálnom možnom rozsahu aj nástroje tretích strán, ktoré nám to umožňujú. Ide najmä o Google, Doubleclick, Facebook. IP adresy a cookies nám v tomto pomáhajú. Cookies si kedykoľvek môžete vymazať v nastaveniach svojho prehliadača.

Ak zákazník pri vytváraní objednávky v e-shope súhlasil so spracúvaním osobných údajov na marketingové účely, vykonávame ho zasielaním e-mailových správ (napr. newsletter, alebo ponuka obdobných tovarov a služieb) na kontaktnú e-mailovú adresu.

Svoj súhlas môže zákazník kedykoľvek odvolať zaslaním Odvolania so spracúvaním osobných údajov, pričom tieto okamžite blokujeme alebo likvidujeme a z našej strany Vami poskytnuté osobné údaje už nebudeme používať na marketingové účely

Kamerový systém podľa GDPR

Doteraz každý kto inštaloval kamerový systém v skutočnosti nepremýšľal o dôsledkoch svojho konania. Akonáhle využívate rozpoznateľné obrazy z vášho Kamerový systém systému, potom spravujete „osobné údaje". Takže skutočnosťou je, že teraz pracujete ako riadiaci pracovník a s tým prichádza zodpovednosť. Prevádzkovateľ musí byť schopný zdôvodniť získanie a používanie osobných údajov prostredníctvom systému Kamerový systém

Ak inštalujete kamery ako perimetrickú ochranu vášho objektu, aby ste odhalili narušiteľov, mali by ste ich použitie odôvodniť jednoducho. V prípade ak používate kamery na monitorovanie zamestnancov, potom oprávnenie nie je až tak jednoduché. Považuje sa to za narušenie súkromia. Je potrebné dokázať napr. z minulosti, že kamery sú používané z dôvodov ochrany zdravia a bezpečnosti zamestnancov. V takomto prípade to môže byť prijateľné

Pri snímaní priestoru považovaného za súkromie je potrebné ospravedlniť potrebu týchto záberov. Napríklad v oddychových priestoroch alebo verejných priestoroch, ak sa vyskytla zjavná úroveň bezpečnostných incidentov. Je nutné preukázať, že tieto kamery sú opodstatnené. Je nutné vykonať analýzu rizík s uvedením každej kamery a snímanej oblasti pre konkrétnu kameru.

Účel zozbieraných údajov by mal byť jasný. Je to obzvlášť dôležité, ak účel nie je zrejmý. Ak napr. ide o monitorovanie zamestnancov pre ochranu zdravia a bezpečnosti, je potrebné to zdôrazniť osobám zachyteným kamerami.

Zákonnosť spracovávania osobných údajov je bežne ošetrená udelením súhlasu s ich spracovávaním. Avšak tento titul by sa ťažko dodržiaval pri spracovaní údajov kamerovými systémami. Preto môže spracovanie prebiehať bez súhlasu, ak je to potrebné na oprávnené účely prevádzkovateľa alebo tretej strany. Je ale potrebné predovšetkým zrozumiteľne informovať dotknuté osoby o spracovávaní takýchto údajov.

V tomto prípade je dôležité, aby informácie o monitorovanom objekte (značka zvýrazňujúca používanie Kamerový systém **a kontaktné číslo) boli uvedené na viditeľných miestach,** t.j. pri všetkých vstupoch/vjazdoch a následne pre prehľadnosť na nástenke. Pre názornosť je možné doplniť písomné informácie jednoduchými a názornými obrázkami. Rovnako tak môže správca informovať subjekty elektronickou formou.

Vo všeobecnosti (v SR) platí 15 dňové uchovávanie záznamov. Ak máte pocit, že musíte vaše záznamy Kamerový systém uchovávať dlhšie, vaše hodnotenie rizika by

malo uvádzať, ako dlho a prečo. Moderný kamerový systémvám umožňuje nastaviť konkrétne obmedzenia pre každú kameru

GDPR uvádza: **„Každá osoba, ktorej obraz je zaznamenaný na kamerovom systéme, má právo požadovať a mať k dispozícii kópiu vlastných osobných údajov zo záznamu."**
Takže každý, kto je zachytený vašimi kamerami, má právo požadovať túto nahrávku, považuje sa to za osobné údaje. Musia postupovať podľa stanoveného postupu, ale majú na to právo. Ak sú v záznamoch viditeľné nejaké iné osoby, je potrebné upraviť záznam, t.j. rozostrenie tvárí iných osôb.
Polícia môže od vás požiadať videozáznam a môžete im ho poskytnúť, ale vždy sa uistite, že je **priložená písomná žiadosť na hlavičkovom papieri.** Polícii často stačí len prezrieť videozáznamy v priestoroch Vášho dátového centra, táto akcia nevzbudzuje obavy o ochranu údajov.
Súkromné bezpečnostné spoločnosti (SBS) pôsobia ako spracovatelia údajov v rámci GDPR. **„Klienti SBS by mali mať uzavretú zmluvu, ktorá podrobne opisuje, čo môže táto spoločnosť s údajmi robiť, aké bezpečnostné normy by mali byť zavedené a aké postupy overovania by sa mali uplatňovať."**
Zabezpečte, aby subdodávatelia pracujúci vo vašom mene, napr. SBS alebo integrátori kamerových systémov, postupovali podľa tohto postupu. Buďte na pozore pri porušovaní pravidiel, ak tretia strana môže distribuovať alebo odstraňovať osobné údaje vo forme obrazových záznamov kamerového systému bez toho, aby dodržiavali vyššie uvedené postupy.
Skutočný poskytovateľ bezpečnostných služieb bude automaticky dodržiavať všetky predpisy GDPR. Požiadajte poskytovateľa systému o svoje pravidlá v súvislosti s GDPR. Berúc do úvahy uvedené skutočnosti, mnohé spoločnosti potrebujú audit svojich bezpečnostných opatrení a zabezpečiť, aby nedošlo k porušeniu predpisov. Nie je prijateľné **„nepochopenie"** alebo **„nevedomosť"** zákonov súvisiacich s kamerovými systémami. Zatiaľ čo je rýchlejšie, lacnejšie a jednoduchšie zakúpiť a inštalovať svoj vlastný kamerový systém, bez vstupu profesionálnych poskytovateľov bezpečnostných systémov sa môže stať, že budete trestne stíhaní alebo dostanete vysokú pokutu. V takomto prípade sa odporúča uzatvoriť „Zmluvu na poskytovanie technickej služby" s vašim správcom príp. dodávateľom kamerového systému. Takýto dokument vám zároveň môže poslúžiť aj v prípade auditu alebo poistnej udalosti.

GDPR sa dotkne rozsahu poskytovaných informácií. Bude potrebné uvádzať kontakt na prevádzkovateľa systému, účely spracovania, kategórie dotknutých osobných údajov a ich príjemcu. Ak to bude nevyhnutné pre transparentnosť využívania spracovaných údajov, mala by byť uvedená doba uloženia osobných údajov, oprávnené záujmy správcu alebo tretej strany. Dôležité je, aby bol prevádzkovateľ schopný reagovať na tieto otázky v primeranej lehote po získaní osobných údajov. Rovnako ako dnes ponesie zodpovednosť prevádzkovateľ, ktorý

rozhodol o prevádzkovaní kamerového systému. Vždy bude musieť zaviesť primerané technické a organizačné opatrenia, aby mohol doložiť súlad s GDPR. Dôležité je, aby boli spracovávané dáta nevyhnutné pre daný účel. Týka sa to predovšetkým množstva zhromažďovaných osobných údajov, rozsahu spracovania, doby uloženia a v neposlednom rade ich dostupnosti.

Povinnosťou prevádzkovateľa bude vedenie záznamov o činnostiach spracovania údajov. Nemali by chýbať meno a kontaktné údaje prevádzkovateľa, účely spracovania údajov, opis kategórie údajov, príjemcu, ktorým sú údaje sprístupnené, lehoty na vymazanie, ale aj technické a organizačné bezpečnostné opatrenia. Záznamy musia byť vyhotovované písomne a prevádzkovateľ bude povinný ich na požiadanie poskytnúť dozornému úradu.

Novou povinnosťou bude od mája 2018 tiež ohlásenie porušenia zabezpečenia či úniku dát dozornému úradu do 72 hodín od zistenia nedostatkov.

EVIDENCIA DRUHOV AGENDY VEDENÝCH PREVÁDZKOVATEĽOM

Názov IS	Mzdová a personálna agenda
Označenie agendy	1
Umiestnenie IS	Externá firma Ing. Mária Langová – Partizánska 687/88, Poprad
Účel spracúvania OÚ v IS	Plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom, obdobným vzťahom (napr. na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane predzmluvných vzťahov.
Právny základ	- Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, - Zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, - Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov, - Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení v znení neskorších predpisov, - Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - Zákon o povinnom zmluvnom poistení zodpovednosti za škodu spôsobenú prevádzkou motorového vozidla, - Zákon o cestnej premávke
Okruh DO	- zamestnanci firmy , - rodinní príslušníci zamestnanca v rozsahu manžel/manželka, deti, - bývalí zamestnanci firmy
Oprávnené osoby	Michal Baran Ing. Mária Langová
Kategória OÚ	- meno, priezvisko, rodné priezvisko a titul, - rodné číslo, dátum a miesto narodenia, - podpis, - rodinný stav - štátna príslušnosť, štátne občianstvo - trvalé bydlisko, prechodné bydlisko, - pohlavie, - údaje o vzdelaní, - spôsobilosť na právne úkony, - poberanie prídavkov na deti,

	- mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, - údaje o odpracovanom čase - údaje o bankovom účte fyzickej osoby, - sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, - peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, - neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, - ročný úhrn vyplateného dôchodku, - údaje o pracovnej neschopnosti, - údaje o dôležitých osobných prekážkach v práci, údaje o zamestnávateľoch, - pracovné zaradenie a deň začiatku výkonu pracovnej činnosti, - údaje o rodinných príslušníkoch v rozsahu meno, priezvisko, adresa, dátum narodenia, - údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa - údaje z potvrdenia o zamestnaní, - údaje o čerpaní materskej dovolenky a rodičovskej dovolenky, - údaje z dokladu o bezúhonnosti, - údaje o priznaní dôchodku, o druhu dôchodku, - údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne, - údaje o členstve v odborovej organizácii a platbe členského príspevku odborovej organizácii, - osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, - fotografia na účely identifikácie na služobnom preukaze, údaje uvedené v životopise,
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na výmaz OÚ	70 rokov (vo verejnom záujme), 50 rokov (v štátnej službe)
Prenos údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania	Osobné údaje sa nezverejňujú

OÚ	
Poskytovanie osobných údajov	
Tretie strany	Právny základ
Sociálna poisťovňa	zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zdravotné poisťovne	zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č.95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
daňový úrad	zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov
doplnkové dôchodkové sporiteľne	zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)	zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov zákon č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých v znení neskorších predpisov zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práce a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Ústredie práce, sociálnych vecí a rodiny	zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov zákon č. 53/2003 Z. z. o orgánoch štátnej správy v oblasti sociálnych vecí, rodiny a služieb zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
súd, orgány činné v trestnom konaní	zákon č. 99/1963 Zb. Občiansky súdny poriadok v znení neskorších predpisov zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
exekútor	zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Pracovná zdravotná služba	Zákon č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, v ktorej vystupuje dotknutá osoba ako jedna zo zmluvných strán, alebo v predzmluvných vzťahoch s dotknutou osobou alebo pri rokovaní o zmene zmluvy, ktoré sa uskutočňujú na žiadosť dotknutej osoby

Názov IS	Kamerový informačný systém
Označenie agendy	3

Umiestnenie IS	Hôrka 1024 – sídlo prevádzky Hôrka 8 - sídlo firmy
Účel spracúvania OÚ v IS	- Osobné údaje slúžia pre potreby ochrany majetku spoločnosti a odhaľovanie kriminality. Účel je stanovený zákonom č.18/2018 Z. z. o ochrane osobných údajov - zákon 18/2018 o ochrane osobných údajov - Monitorovanie pre zvýšenie bezpečnosti, ochrana zdravia, majetku a osôb pred krádežami, vandalizmom, prevencia pred páchaním trestných činov, porušovaním verejného poriadku, bezpečnosť a odhaľovania kriminality
Právny základ	- Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov - Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Okruh DO	- zamestnanci prevádzkovateľa, - návštevníci, - zamestnanci externých organizácií vstupujúci do areálu firmy - Občania SR
Oprávnené osoby	Michal Baran
Kategória OÚ	Videozáznam, fotografia, fyzické črty osoby
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	Max 15 dní starý záznam
Poskytovanie osobných údajov	
Tretie strany	Právny základ
Orgán činný v trestnom konaní	Zákon č. 301/2005 z.z. Trestný poriadok
Inšpektori Úradu na ochranu osobných údajov	Zákon č. 18/2018 o ochrane osobných údajov
Priestupkový orgán	Zákon č. 372/1990 o priestupkoch
Prenos údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania OÚ	Osobné údaje sa nezverejňujú

Názov IS	Agenda BOZP a PO
Označenie agendy	4
Umiestnenie IS	TATRAHASIL, s.r.o. Lidická 1623/39 059 51 Poprad

Účel spracúvania OÚ v IS	Plnenie povinností zamestnávateľa pri vzniku pracovných úrazov, pri vytváraní rizikových pracovísk pre pracovníkov vo svojej spoločnosti.
Právny základ	- Zákon č. 124/2006 Z. z. o BOZP, - Zákon č. 125/2006 o inšpekcii práce, - Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov
Okruh DO	- zamestnanci prevádzkovateľa, - bývalí zamestnanci prevádzkovateľa
Oprávnené osoby	Technik PO
Kategória OÚ	Bežné osobné údaje meno, priezvisko, adresa, podpis, kontakt
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	10 rokov
Prenos údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania OÚ	Osobné údaje sa nezverejňujú

Názov IS	Účtovnícka agenda
Označenie agendy	5
Umiestnenie IS	Externá firma Ing. Mária Langová – Partizánska 687/88 Poprad
Účel spracúvania OÚ v IS	Vedenie agendy účtovníctva, fakturácie a účtovanie pokladnice. Vedenie agendy pracovných jázd služobným alebo súkromným autom, spotreba pohonných hmôt, náklady spojené s prevádzkou automobilov. Tvorba a vyúčtovanie cestovných príkazov, vedenie agendy služobných mobilných telefónov a ostatných mobilných aplikácií.
Právny základ	- Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, - Zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, - Zákon o dani z príjmov č. 595/2003 Z. z. v znení neskorších predpisov, - Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, - Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, - Zákon č. 152/1994 Z. z. o sociálnom fonde a o

	zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov, - Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, - Zákon č. 283/2002 Z. z. Zákon o cestovných náhradách – zákon 18/2018 o ochrane osobných údajov
Okruh DO	- zamestnanci firmy, - rodinní príslušníci zamestnanca – manžel, manželka, deti FO súvisiace s podnikateľskou činnosťou firmy
Oprávnené osoby	Ing. Mária Langová Michal Baran
Kategória OÚ	meno, priezvisko, titul, adresa trvalého pobytu, adresa prechodného pobytu, telefónne číslo, e-mailová adresa, dátum narodenia, druh a číslo dokladu totožnosti, podpis, číslo bankového účtu fyzickej osoby
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	10 rokov
Prenos údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Zverejňovanie OÚ	Osobné údaje sa nezverejňujú
Poskytovanie osobných údajov	
Tretie strany	Právny základ
Sociálna poisťovňa	zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov; zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zdravotné poisťovne	zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Daňový úrad	zákon č. 595/2003 Z. z. o dani z príjmov znení neskorších predpisov

Názov IS	Agenda zmlúv
Označenie agendy	6
Umiestnenie IS	Externá firma Ing. Mária Langová – Partizánska 687/88 Poprad

Účel spracúvania OÚ v IS	Osobné údaje slúžia pre potreby vybavenia škodovej udalosti spôsobenej zamestnancom
Právny základ	- Zákon o poisťovníctve č. 8/2008 Z. z. - zákon 18/2018 o ochrane osobných údajov
Okruh DO	- zamestnanci firmy
Oprávnené osoby	Ing. Mária Langová Michal Baran
Kategória OÚ	Bežné osobné údaje zákazníkov prevádzkovateľa
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	10 rokov
Prenos osobných údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania OÚ	Osobné údaje sa nezverejňujú

Názov IS	Zákaznícka agenda
Označenie agendy	7
Umiestnenie IS	Externá firma Ing. Mária Langová – Partizánska 687/88 Poprad
Účel spracúvania OÚ v IS	Vypĺňanie reklamačných lístkov a vybavovanie reklamácií v zmysle Občianskeho zákonníka a Zákona o ochrane spotrebiteľov.
Právny základ	- Zákon č. 250/2007 Z. z. O ochrane spotrebiteľa v znení neskorších predpisov, - Zákon č. 40/1964 Z. z. Občiansky zákonník - Zákon č. 18/2018 o ochrane osobných údajov
Okruh DO	- zákazníci prevádzkovateľa
Oprávnené osoby	Ing. Mária Langová Michal Baran
Kategória OÚ	Bežné osobné údaje zákazníkov prevádzkovateľa
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	10 rokov
Prenos osobných údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania osobných údajov	Osobné údaje sa nezverejňujú

Názov IS	Evidencia prijatej a odoslanej pošty
Označenie agendy	12
Umiestnenie IS	Hôrka 8, 059 12
Účel spracúvania OÚ v IS	Evidencia došlej a odchádzajúcej pošty
Právny základ	- zákon č.18/2018 o ochrane osobných údajov - Zákon č. 395/2002 Z. z. o archívoch a registratúrach
Okruh DO	- zamestnanci firmy fyzické osoby – odosielatelia a prijímatelia korešpondencie
Oprávnené osoby	
Kategória OÚ	titul, meno, priezvisko, podpis, adresa, e-mailová adresa, telefónne číslo
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici
Lehoty na zmazanie OÚ	10 rokov
Prenos osobných údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania OÚ	Osobné údaje sa nezverejňujú
Poskytovanie osobných údajov	
Ministerstvo vnútra SR	zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
Iný oprávnený subjekt	Zákon č.18/2018 o ochrane osobných údajov

Názov IS	Agenda marketingu
Označenie agendy	13
Umiestnenie IS	Hôrka 8, 059 12
Účel spracúvania OÚ v IS	Osobné údaje slúžia pre marketingové potreby spoločnosti.
Právny základ	- zákon č.18/2018 o ochrane osobných údajov - súhlas dotknutej osoby
Okruh DO	- zamestnanci firmy
Oprávnené osoby	Michal Baran
Kategória OÚ	Bežné osobné údaje uverejnené na internetovej stránke www.tatrametal.sk
Bezpečnostné opatrenia	Bezpečnostný projekt informačného systému osobných údajov Podľa bezpečnostných opatrení popísaných v smernici

Lehoty na zmazanie OÚ	10 rokov
Prenos osobných údajov do tretích krajín	Prenos osobných údajov sa neuskutočňuje
Spôsob zverejňovania OÚ	Osobné údaje sa nezverejňujú

<u>Odporučenie</u> k zlepšeniu procesov spracovávania OÚ

- Šifrovanie mailov a komunikácie smerom von i dnu do prevádzky v prípade zasielania OÚ –FO napr. sprostredkovateľovi, či externému prevádzkovateľovi
- Uzatvoriť zmluvné vzťahy Prevádzkovateľ - sprostredkovateľ

- Pravidelne a aj opakovane školiť nových aj stálych zamestnancov o spôsobe a manipulácii s OÚ –FO a ich povinnostiach z toho vyplývajúcich.

- Informovanie doterajších i budúcich klientov , spolupracujúcich spoločností o tom že spracovávame ich OÚ pre potreby firmy v súlade s GDPR a zák. 18\2018 len v nevyhnutnom rozsahu a dĺžke a len osobou oprávnenou.

- Informovať DO o dĺžke uchovávania jej OÚ .
- Lekárske záznamy \psychotesty\ uchovávať v uzamknutých trezoroch a miestnostiach, pracovať s nimi môže len preškolená zodpovedná osoba aby neprišlo k úniku OÚ.
- Používať a spracovávať len OÚ nevyhnutné pre výkon povolania a súvisiacu pracovnú činnosti a len Oprávnenou osobou.

Evidencia odovzdaných kľúčov:

Kľúče odovzdal:

Meno	Priezvisko	Funkcia

Prehlásenie

Preberám uvedené kľúče. Som si vedomý/a zodpovednosti a v prípade straty alebo odcudzenia túto skutočnosť bezodkladne nahlásim vedúcemu zamestnancovi.

Číslo kľúča	**Kľúč od miestnosti, budovy**	**Prebral Podpis/ dňa**	**Odovzdal Podpis/ dňa**

Evidencia Zodpovedných osôb:

Firma	**Zodpovedná osoba**	**od**	**do**

Evidencia incidenty úniku OÚ- nahlásiť ÚOOÚ do 72 h. po zistení
Krádež PC, Krádež záloh IS, Strata USB, Požiar , atď...

Por. číslo	Zoznam incidentov	Názov	Dátum	Druh	Prijaté opatrenia

Prílohy – Vzory

Príloha č.1

Súhlas so spracúvaním osobných údajov

Dotknutá osoba: (uviesť identifikačné údaje dotknutej osoby)
Meno a priezvisko:
Adresa:
Telefónne číslo/email:
(ďalej len dotknutá osoba)

Prevádzkovateľ: (uviesť identifikačné údaje prevádzkovateľa)
Obchodné meno a právna forma:
Sídlo:
IČO:
Kontaktné údaje: (tel. číslo/email/fax)
Identifikačné a kontaktné údaje zástupcu: (ak bol poverený)
Kontaktné údaje zodpovednej osoby: (ak bola určená)
(ďalej len „prevádzkovateľ")

Ako dotknutá osoba týmto udeľujem súhlas prevádzkovateľovi so spracúvaním svojich osobných údajov v rozsahu osobných údajov uvedených v životopise a motivačnom liste (uviesť zoznam osobných údajov, ktoré bude prevádzkovateľ spracúvať na vymedzený účel, vrátane osobných údajov slúžiacich na identifikáciu dotknutej osoby v informačnom systéme osobných údajov; napr. meno, priezvisko, adresa, tel. kontakt, e-mail, dátum narodenia, fotografia, a pod.) na účel evidencie vhodných uchádzačov o zamestnanie vo vlastnej databáze prevádzkovateľa (uviesť konkrétny účel, napr. na účel poskytnutia benefitu vo forme zamestnaneckej zľavy na nákup tovaru v podnikovej predajni; na účel zverejnenia fotografie zamestnanca na webovom sídle zamestnávateľa s cieľom propagácie spoločnosti a/alebo informovania klientov o úspechoch spoločnosti).

Dané osobné údaje budú uchované po dobu piatich (uviesť dobru spracúvania primeranú sledovanému účelu spracúvania) mesiacov. Po uplynutí tejto doby budú zlikvidované. Získané osobné údaje nepodliehajú profilovaniu ani automatizovanému rozhodovaniu. Prevádzkovateľ informuje dotknutú osobu o tom, že jeho osobné údaje budú poskytnuté materskej spoločnosti prevádzkovateľa so sídlom v Bratislave (identifikovať príjemcov alebo kategórie príjemcov: t. j. či sa osobné údaje budú poskytovať sprostredkovateľom, tretím stranám – ak príjemcovia neexistujú, informácia sa vynechá; príjemcom nie sú orgány verejnej moci).

Prevádzkovateľ nezamýšľa prenos osobných údajov do tretej krajiny ani medzinárodnej organizácii (ak sa zamýšľa, vyžaduje sa identifikácia tretej krajiny/medzinárodnej organizácie a identifikácia tzv. primeraných záruk). Poskytnutie osobných údajov, ako aj udelenie Vášho súhlasu s ich spracúvaním je dobrovoľné. Súhlas môžete kedykoľvek odvolať zaslaním písomného odvolania súhlasu na adresu prevádzkovateľa. Odvolanie súhlasu je účinné dňom jeho doručenia.

Udelením súhlasu nie sú dotknuté Vaše práva dotknutej osoby. Na základe písomnej žiadosti alebo osobne u prevádzkovateľa máte právo:

- žiadať o prístup k svojim osobným údajom a o opravu, vymazanie alebo obmedzenie spracúvania svojich osobných údajov;
- namietať spracúvanie svojich osobných údajov;
- na prenosnosť osobných údajov;
- podať návrh na začatie konania na Úrade na ochranu osobných údajov SR.

Dotknutá osoba vyhlasuje, že poskytnuté osobné údaje sú pravdivé, aktuálne a boli poskytnuté slobodne.

V..... dňa.....

.....
podpis dotknutej osoby

Príloha č.2

Sprostredkovateľská zmluva

mluva o spracúvaní osobných údajov
zatvorená v súlade s čl. 28 ods. 3 nariadenia Európskeho parlamentu a Rady EÚ č. 016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom ohybe takýchto údajov, ktorým sa zrušuje smernica č. 95/46/ES (všeobecné ariadenie o ochrane údajov, ďalej len GDPR) a § 34 ods. 3 zákona č. 3../2017 Z. z. ochrane osobných údajov (ďalej len „zmluva") medzi:

revádzkovateľ (názov, právna forma):
dresa sídla:
ČO:
IČ:
Č DPH:
apísaný: v Obchodnom registri Okresného súdu...., oddiel: ....., vložka č. ....
astúpený:
ontaktné údaje: (ďalej len „prevádzkovateľ")

prostredkovateľ (názov, právna forma):
dresa sídla:
CO:
IČ:
Č DPH:
apísaný: v Obchodnom registri Okresného súdu...., oddiel: ....., vložka č. ....
astúpený: Kontaktné údaje: (ďalej len „sprostredkovateľ")

evádzkovateľ a sprostredkovateľ ďalej spolu len ako „zmluvné strany" uzatvárajú to zmluvu o sprostredkovaní spracúvania osobných údajov

I. I Úvodné ustanovenia a predmet zmluvy

Sprostredkovateľ poskytuje pre prevádzkovateľa činnosť/služby.....(napr. xterné spracovanie personálnej a mzdovej agendy, monitoring osôb vstupujúcich do eálu prevádzkovateľa, archivácia a likvidácia podnikovej agendy a pod.) na základe nluvy/dohody..... zo dňa..... .

Predmetom tejto zmluvy je úprava vzájomných práv a povinností zmluvných strán i spracúvaní osobných údajov dotknutých osôb sprostredkovateľom v mene

prevádzkovateľa a poverenie sprostredkovateľa prevádzkovateľom spracúvaním osobných údajov, ktoré prevádzkovateľ spracúva vo svojich informačných systémoch, a to za podmienok dohodnutých v tejto zmluve.

Čl. II Poverenie na spracúvanie osobných údajov

1. Prevádzkovateľ touto zmluvou poveruje sprostredkovateľa spracúvaním osobných údajov v mene prevádzkovateľa:

1.1. predmet spracúvania: sprostredkovateľ vykonáva spracúvanie osobných údajov prostredníctvom automatizovaných/neautomatizovaných prostriedkov (vybrať) spracúvania z databázy personalistika a mzdy/kniha návštev/účtovníctvo (uviesť informačný systém, z ktorého prevádzkovateľ poskytuje osobné údaje sprostredkovateľovi);

1.2. **doba spracúvania**: odo dňa nadobudnutia účinnosti tejto zmluvy (alebo odo dňa podpisu zmluvy/dohody podľa čl. 1 bodu 1) až po skončenie zmluvného vzťahu medzi zmluvnými stranami podľa čl. VII tejto zmluvy;

1.3. **povaha spracúvania**: na spracúvanie osobných údajov sa vyžaduje/nevyžaduje súhlas dotknutej osoby, (resp. uviesť na akom právnom základe sa osobné údaje spracúvajú),

1.4. **na účel**: vedenia personálnej a mzdovej agendy/identifikácie fyzickej osoby pri jednorazovom vstupe do priestorov spoločnosti/archivácie a likvidácie personálnej agendy a pod.

1.5. **typy a zoznam osobných údajov, ktoré sú predmetom spracúvania**: (vypísať, ktoré všeobecné osobné údaje a ktoré citlivé osobné údaje bude sprostredkovateľ spracúvať na základe tejto zmluvy), napríklad: • na účel vedenia personálnej a mzdovej agendy sprostredkovateľ bude spracúvať všeobecné osobné údaje ako titul, meno, priezvisko, rodné priezvisko, trvalé bydlisko, prechodné bydlisko, dátum narodenia, rodné číslo, miesto narodenia, vek, rodinný stav, štátna príslušnosť, štátne občianstvo, všetky údaje a iné záznamy uvedené v úradnom doklade o vzdelaní, podpis, kontaktné údaje (najmä telefónne číslo a e-mail), pracovné zaradenie, základná mzda, osobné ohodnotenie, výkonová zložka mzdy a iné zložky súvisiace s pracovným zaradením, údaje o odpracovanom čase, údaje o bankovom účte fyzickej osoby, sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom, peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov, neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych

dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpisu, údaje z potvrdenia o zamestnaní, údaje o vedení zamestnanca v evidencii uchádzačov o zamestnanie, údaje o čerpaní materskej dovolenky, rodičovskej dovolenky, údaje o priznaní dôchodku, o druhu dôchodku, názov zdravotnej poisťovne, v ktorej je zamestnanec poistený, názov doplnkovej dôchodkovej poisťovne, osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách, údaje uvedené v životopise, jazykové znalosti a citlivé údaje týkajúce sa zdravotného stavu zamestnanca ako údaje o pracovnej neschopnosti, údaje o dôležitých osobných prekážkach v práci, údaje o zdravotnom postihnutí a pod. • na účel vstupu do objektu prevádzkovateľa sprostredkovateľ spracúva všeobecné osobné údaje, a to: meno a priezvisko, tituly, číslo občianskeho preukazu alebo číslo služobného preukazu alebo číslo cestovného dokladu, ak ide o cudzinca;

1.6. **kategórie dotknutých osôb**: zamestnanci, bývalí zamestnanci, osoby blízke zamestnancom, uchádzači o zamestnanie, zamestnanci dodávateľov, klienti, školitelia a iné návštevy.

Čl. III Oprávnenia a povinnosti sprostredkovateľa

1. Sprostredkovateľ je oprávnený: (vymenovať spracovateľské operácie, na ktoré je sprostredkovateľ oprávnený a ktoré zodpovedajú účelu spracúvania)

a. získavať, zhromažďovať, šíriť, zaznamenávať, usporadúvať, preskupovať, kombinovať, prehliadať, premiestňovať, uchovávať, kopírovať, sprístupňovať a likvidovať osobné údaje;

b. kontrolovať preukázanie pravdivosti poskytnutých osobných údajov predloženým dokladom;

c. uchovávať osobné údaje, a to výhradne na technických prostriedkoch prevádzkovateľa pod dobu ..... mesiacov;

d. spracúvať osobné údaje za účelom vytvárania štatistických zostáv po dohode s prevádzkovateľom;

2. Sprostredkovateľ je povinný:

a. postupovať pri spracúvaní osobných údajov podľa všeobecne záväzných právnych predpisov a podľa ďalších písomných pokynov prevádzkovateľa;

b. informovať bez zbytočného odkladu prevádzkovateľa, ak má za to, že sa pokynom prevádzkovateľa porušujú všeobecne záväzné právne predpisy týkajúce sa ochrany osobných údajov;

c. zachovávať mlčanlivosť o osobných údajoch získaných od prevádzkovateľa/ s ktorými príde do styku, a to aj po skočení poverenia;

d. spracúvať osobné údaje len na určený účel podľa čl. II. bodu 1.4. tejto zmluvy;

e. spracúvať len také osobné údaje, ktoré rozsahom a obsahom zodpovedajú určenému účelu a sú nevyhnutné pre jeho dosiahnutie;

f. spracúvať iba správne, kompletné a aktuálne osobné údaje vo vzťahu k účelu ich spracúvania a naložiť s nesprávnymi a nekompletnými údajmi v súlade so zákonom;

g. udržiavať osobné údaje získané na rozdielne účely oddelene a zabezpečiť osobné údaje pred odcudzením, stratou, poškodením, zničením, neoprávneným prístupom, zmenou a rozširovaním, na tento účel prijme primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania osobných údajov;

h. neposkytovať a nesprístupňovať osobné údaje bez predchádzajúceho písomného súhlasu prevádzkovateľa, okrem prípadov, ak poskytnutie a/alebo sprístupnenie je nevyhnutné na zabezpečenie spracúvania osobných údajov podľa tejto zmluvy alebo povinnosť poskytnutia a/alebo sprístupnenia osobných údajov vyplýva z osobitných právnych predpisov alebo na základe rozhodnutia orgánu verejnej moci;

i. poskytnúť súčinnosť prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti prijímať opatrenia na základe žiadosti dotknutej osoby pri uplatňovaní jej práv; j. zlikvidovať osobné údaje dotknutých osôb bezodkladne pod dosiahnutí účelu spracúvania osobných údajov; prevádzkovateľ je oprávnený žiadať od sprostredkovateľa potvrdenie o zlikvidovaní osobných údajov, a sprostredkovateľ je povinný takejto požiadavke bezodkladne vyhovieť; týmto nie sú dotknuté ustanovenia všeobecne záväzných právnych predpisov ukladajúcich sprostredkovateľovi povinnosti uchovávania týchto osobných údajov;

k. zabezpečiť, že všetky ním určené oprávnené osoby budú pred spracúvaním osobných údajov poučené a zaviazané povinnosťou mlčanlivosti o týchto údajoch, a to aj po zániku ich právneho vzťahu k sprostredkovateľovi;

l. nahradiť prevádzkovateľovi škodu, ktorá mu vznikne v dôsledku porušenia tejto zmluvy zo strany sprostredkovateľa;

m. vrátiť bezodkladne po zániku tejto zmluvy prevádzkovateľovi všetky dokumenty obsahujúce osobné údaje, ktoré prevádzkovateľ poskytol a vymazať všetky ich kópie/alternatíva: vymazať bezodkladne po zániku tejto zmluvy prevádzkovateľovi všetky dokumenty obsahujúce osobné údaje, ktoré

prevádzkovateľ poskytol a vymazať všetky ich kópie; týmto nie sú dotknuté ustanovenia všeobecne záväzných právnych predpisov ukladajúcich sprostredkovateľovi povinnosti uchovávania týchto osobných údajov.

Čl. IV Vyhlásenie a oprávnenia prevádzkovateľa

1. Prevádzkovateľ vyhlasuje, že pri výbere sprostredkovateľa postupoval v súlade s čl. 28 ods. 1 GDPR a § 34 ods. 1 zákona o ochrane osobných údajov, t. j. dbal na odbornú, technickú, organizačnú a personálnu spôsobilosť sprostredkovateľa a jeho schopnosť poskytnúť dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo zákonné požiadavky a aby sa zabezpečila ochrana práv dotknutej osoby.

2. Prevádzkovateľ je oprávnený požadovať od sprostredkovateľa preukázanie splnenia všetkých povinností vrátane vykonania všetkých predpísaných bezpečnostných opatrení na ochranu osobných údajov.

3. Prevádzkovateľ je oprávnený vykonať u sprostredkovateľa audit ochrany osobných údajov a sprostredkovateľ je povinný poskytnúť súčinnosť v rámci auditu ochrany osobných údajov a kontroly zo strany prevádzkovateľa alebo audítora, ktorého poveril prevádzkovateľ.

Čl. V Podmienky zapojenia subdodávateľa
Alternatíva, ak prevádzkovateľ nesúhlasí

1. Prevádzkovateľ nesúhlasí, aby sprostredkovateľ spracúval osobné údaje prostredníctvom inej osoby, t. j. prostredníctvom subdodávateľa.
2. Sprostredkovateľ priebežne písomne predkladá prevádzkovateľovi aktuálny zoznam svojich zamestnancov, ktorí sú oprávnení spracúvať osobné údaje v rozsahu tejto zmluvy (ďalej tiež „oprávnené osoby"), spolu s prehlásením, že títo zamestnanci boli poučení. Sprostredkovateľ je povinný predložiť prevádzkovateľovi uvedený zoznam zamestnancov kedykoľvek, keď ho o to prevádzkovateľ požiada, najneskôr však do troch pracovných dní od vyžiadania predmetného zoznamu zamestnancov.

Alternatíva, ak prevádzkovateľ súhlasí

1. Prevádzkovateľ súhlasí, aby sprostredkovateľ spracúval osobné údaje prostredníctvom inej osoby (ďalej tiež „subdodávateľ") za splnenia nasledujúcich podmienok:

a) sprostredkovateľ písomne oznámi prevádzkovateľovi obchodné meno každého subdodávateľa pred tým, ako sprostredkovateľ uzatvorí s konkrétnym subdodávateľom zmluvu o spracúvaní osobných údajov;

b) sprostredkovateľ je povinný v zmluve so subdodávateľom uložiť mu rovnaké povinnosti týkajúce sa ochrany osobných údajov ako sú ustanovené v tejto zmluve alebo v inom právnom úkone medzi prevádzkovateľom a sprostredkovateľom, najmä podľa čl. 3 bod 2 tejto zmluvy;
c) sprostredkovateľ nesie zodpovednosť za subdodávateľa, že spracúvanie a ochrana osobných údajov budú zabezpečené v súlade s touto zmluvou a všeobecne záväznými právnymi predpismi; tým nie je dotknutý nárok sprostredkovateľa na náhradu škody voči subdodávateľovi;
d) sprostredkovateľ priebežne písomne predkladá prevádzkovateľovi aktuálny zoznam svojich zamestnancov, ak aj zamestnancov subdodávateľa, ktorí sú oprávnení spracúvať osobné údaje v rozsahu tejto zmluvy (ďalej tiež „oprávnené osoby") spolu s prehlásením, že títo zamestnanci boli poučení. Sprostredkovateľ je povinný predložiť prevádzkovateľovi uvedený zoznam zamestnancov kedykoľvek, keď ho o to prevádzkovateľ požiada, najneskôr však do troch pracovných dní od vyžiadania predmetného zoznamu zamestnancov.

Čl. VI Ostatné dohodnuté podmienky

1. Zmluvné strany si do siedmich dní od nadobudnutia účinnosti tejto zmluvy písomnou formou oznámia mená a kontaktné údaj zamestnancov, ktorí sú oprávnení konať za zmluvnú stranu pri plnení úloh vyplývajúcich z tejto zmluvy. Prípadnú zmenu uvedených údajov si zmluvné strany bezodkladne oznámia ústne, e – mailom alebo telefonicky a následne aj doručením zmeny predmetných údajov v písomnej forme na adresu druhej zmluvnej strany uvedenú v zmluve.

2. Sprostredkovateľ nesmie prenášať osobné údaje do tretích krajín alebo do medzinárodnej organizácie bez predchádzajúceho písomného súhlasu prevádzkovateľa, okrem prenosu na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná; sprostredkovateľ je pri takom prenose povinný oznámiť prevádzkovateľovi túto požiadavku pred spracúvaním osobných údajov, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, takéto oznámenie nezakazuje z dôvodov verejného záujmu.

Čl. VII Doba trvania a zánik zmluvy Alternatíva 1

1. Zmluva sa uzatvára na dobu určitú, do doby trvania zmluvného vzťahu medzi prevádzkovateľom a sprostredkovateľom podľa čl. 1 bodu 1.

Alternatíva 2

1. Táto zmluva sa uzatvára na dobu neurčitú.
2. Zmluvu je možné ukončiť:

2.1. Písomnou výpoveďou doručenou druhej zmluvnej strane na adresu uvedenú v zmluve z akéhokoľvek dôvodu alebo bez udania dôvodu. Výpovedná

lehota je tri mesiace a začína plynúť prvý deň mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená druhej zmluvnej strane.

2.2. Písomnou dohodou zmluvných strán.

2.3. Písomným odstúpením od zmluvy. Od zmluvy môže odstúpiť ktorákoľvek zo zmluvných strán v prípade podstatného porušenia zmluvy druhou zmluvnou stranou. Odstúpenie od zmluvy je účinné jeho doručením na adresu druhej zmluvnej strany uvedenú v zmluve.

ČI. VIII Záverečné ustanovenia

1. Práva a povinnosti touto zmluvou neupravené sa riadia príslušnými ustanoveniami všeobecne záväzných právnych predpisov.
2. Ukončenie zmluvného vzťahu a upozornenie na nedodržiavanie ustanovení tejto zmluvy sa vždy doručí druhej zmluvnej strane v písomnej forme na adresu uvedenú v záhlaví tejto zmluvy, dokiaľ nie je zmena adresy písomne oznámená zmluvnej strane, ktorá písomnosť doručuje. Ak sa písomnosť vráti nedoručená, platí, že účinky doručenia nastávajú tretím dňom po vrátení zásielky zmluvnej strane, ktorá zásielku doručuje.
3. Táto zmluva nadobúda platnosť a účinnosť dňom jej podpisu obidvoma zmluvnými stranami.
4. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, inak prostredníctvom vecne a miestne príslušného súdu v SR.
5. Zmeny a doplnenia tejto zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k zmluve.
6. Zmluvné strany vyhlasujú, že si túto zmluvu pred jej podpísaním prečítali, že bola uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok. Zmluvné strany s obsahom tejto zmluvy súhlasia a na znak súhlasu ju vlastnoručne podpisujú.
7. Táto zmluva bola vyhotovená v dvoch originálnych rovnopisoch, po jednom rovnopise pre každú zmluvnú stranu.

V..... dňa.....

.....	.....
za prevádzkovateľa	za sprostredkovateľa

Príloha č.3

Oznámenie prevádzkovateľa o poverení zodpovednej osoby výkonom dohľadu nad ochranou osobných údajov

podľa § 44 ods. 8 zákona č. 18/2018 Z. z.
o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

IDENTIFIKAČNÉ ÚDAJE PREVÁDZKOVATEĽA

Identifikačné číslo organizácie (IČO)

Názov prevádzkovateľa (obchodné meno)

PSČ **Obec**

Ulica **číslo**

Právna forma

ZODPOVEDNÁ OSOBA

Priezvisko **Meno**

Titul **Dátum narodenia**

Deň, kedy sa fyzická osoba stala zodpovednou osobou

Číslo potvrdenia o absolvovaní skúšky **Dátum vydania potvrdenia**

Prevádzkovateľ vyhlasuje, že zodpovedná osoba spĺňa predpoklady podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

....

Odtlačok pečiatky prevádzkovateľa Dátum, meno a podpis štatutárneho orgánu

Preškolenie oprávnených osôb OO

Vstupné školenie dátum:
Firma: METAL TATRY, s.r.o.
Miesto výkonu činnosti sprac. OÚ
Objednávateľ : Michal Baran
Záznam o školení zamestnancov pre dodržiavanie zásad ochrany Osobných údajov /GDPR
Pracovisko : Hôrka 8, 059 12
O prevencii správania sa zamestnancov pri spracovávaní OÚ, ich zabezpečení pred ďalším zneužitím
a povinnosti predchádzať incidentom zneužitia a straty OÚ pri výkone pracovných povinností.
O potrebe riadneho zabezpečenia priestorov kde sa OÚ spracovávajú či už mechanickými ale aj technologickými /softvér /prostriedkami.
Zamestnancom ktorý prichádzajú na pracovisku do kontaktu s OÚ boli poskytnuté potrebné informácie a pokyny na zaistenie bezpečnosti a ochrany pred zneužitím pri práci s nimi.

Číslo	Titul meno priezvisko	Pracovné zaradenie	Identifikačné údaje	podpis	Poučenie vykonal
1	Michal Baran	Konateľ			
2	Ing. Mária Langová	Účtovníčka			
3					
4					
5					
6					