

**INTERNÁ SMERNICA V OBLASTI OCHRANY  
OSOBNÝCH ÚDAJOV**

**účinná odo dňa 05.10.2020**

**vydaná zamestnávateľom:**

**Materská škola  
Bradáčova 773/30, 907 01 Myjava  
IČO: 42 378 508  
rozpočtová organizácia**

## I.

### Základné ustanovenia

1. Predmetom tejto Smernice je úprava ochrany a nakladania s osobnými údajmi pri činnostiach, ktoré vykonávajú oprávnené osoby zamestnávateľa, ktorým je Materská škola, Bradáčova 773/30, 907 01 Myjava, IČO: 42 378 508 (ďalej len ako „Prevádzkovateľ“).
2. Oprávnenou osobou sa na účely tejto Smernice rozumie zamestnanec Prevádzkovateľa, ktorý pri výkone svojej pracovnej činnosti nakladá s osobnými údajmi dotknutých osôb (ďalej len „Oprávnená osoba“).
3. Interná smernica je prístupná pre každého zamestnanca v sídle materskej školy.

## II.

### Všeobecné povinnosti

1. Osobné údaje musia byť adekvátne zabezpečené vo všetkých prípadoch, kedy sa s nimi v organizácii nakladá.
2. Oprávnená osoba môže nakladať s osobnými údajmi len za predpokladu, že je to na výkon jej pracovných činností nevyhnutné alebo na základe individuálneho písomného poverenia Prevádzkovateľa.
3. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými prichádza do styku pri výkone svojej pracovnej činnosti alebo činnosti vyplývajúcej z jej poverenia.
4. Povinnosť mlčanlivosti trvá aj po ukončení pracovného pomeru s oprávnenou osobou.
5. Oprávnená osoba môže nakladať len s takými osobnými údajmi, ktoré sú nevyhnutné na výkon jej pracovnej činnosti alebo činností vyplývajúcich z poverenia.
6. Oprávnená osoba môže vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na výkon jej pracovnej činnosti alebo činnosti vyplývajúcej z poverenia.
7. Oprávnená osoba nesmie získavať informácie týkajúce sa osobných údajov nad rámec jej pracovnej činnosti alebo poverenia.
8. Oprávnená osoba je povinná dbať o to, aby pri výkone jej pracovných činností alebo činností vyplývajúcich z poverenia nedošlo k úniku spracúvaných osobných údajov alebo k narušeniu bezpečnosti spracovateľských operácií.

## III.

### Získavanie osobných údajov

1. Osobné údaje prevádzkovateľa sú uložené a zálohované vo vlastnej databáze s externým úložiskom.
2. Do databázy sa oprávnená osoba dostane prostredníctvom individuálneho softvéru, ktorý je prístupný na každom firemnom počítači Prevádzkovateľa.
3. Každá oprávnená osoba má svoje prístupové meno a heslo potrebné na prístup do softvéru Prevádzkovateľa, pričom jej databáza poskytne len osobné údaje dotknutých osôb v rozsahu jej pracovnej činnosti alebo poverenia.
4. Pokiaľ by oprávnená osoba potrebovala prístup k osobným údajom vo väčšom rozsahu, ako má k dispozícii v databáze, je povinná žiadať od Prevádzkovateľa individuálny písomný súhlas na získanie týchto údajov na základe žiadosti.
5. Písomný súhlas udeľuje Prevádzkovateľ na žiadosť, a to len v rozsahu potrebnom na splnenie účelu oprávnenej osoby.
6. Oprávnená osoba následne predloží písomný súhlas vedúcemu IT oddelenia, ktorý jej poskytne osobné údaje len v rozsahu súhlasu, ktorý udelil Prevádzkovateľ.
7. Oprávnená osoba nesmie získané osobné údaje poskytovať iným osobám.
8. Oprávnená osoba nesmie poskytovať svoje prístupové údaje do softvéru Prevádzkovateľa iným osobám.
9. Oprávnená osoba nesmie používať softvér Prevádzkovateľa pre vlastné potreby.

## IV.

### Využívanie internetu

1. Využívanie služieb internetu oprávnenými osobami je určené pre plnenie pracovných úloh.



2. Používanie internetu musí brať do úvahy dôvernosť prenášaných informácií.
3. Oprávnená osoba pri prístupe do siete internet je povinná dodržiavať nasledujúce zásady:
  - a. prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou/funkciou,
  - b. riadiť sa hláseniami antivírusového programu,
  - c. nepripájať sa na neznáme internetové stránky s neprevereným obsahom, ak to nie je potrebné na výkon pracovných úloh/funkcie,
  - d. nepoužívať heslá, ktoré sa používajú pre prístup k vnútorným informačným systémom, na prístup k verejným internetovým službám.

## V.

### Elektronická pošta

1. Elektronická pošta sa používa pre účely internej a externej komunikácie.
2. V prípade skončenia pracovnoprávneho alebo iného vzťahu s oprávnenou osobou ukončí prevádzkovateľ používanie emailovej adresy danej oprávnenej osoby v lehote do 30 dní od skončenia daného vzťahu.

## VI.

### Personálna bezpečnosť

1. Pri skončení pracovnoprávneho vzťahu alebo iného vzťahu (napr. skončenie funkcie konateľa) je oprávnená osoba (zamestnanec, konateľ...) povinná odovzdať pracovnú agendu vrátane spisov, všetky pridelené inventárne predmety, zapožičané knihy a kľúče.
2. Všetky oprávnené osoby musia byť poučené o základných bezpečnostných zásadách predtým, ako získajú prístup k informačnému systému prevádzkovateľa a k účelom spracúvania. Poučenie vykoná zodpovedná osoba. Doklad o poučení sa zakladá v osobnom spise zamestnanca
3. Oprávnenej osobe môže byť pridelený technický prostriedok (napr. služobný mobil, notebook), ktorého prevzatie oprávnená osoba potvrdí na potvrdení o prevzatí prostriedku. Pri vrátení prostriedku má oprávnená osoba právo žiadať potvrdenie o odovzdaní.

## VII.

### Fyzická bezpečnosť

1. Informačná technika (počítače, notebooky a pod.) musí byť umiestnená v uzamykateľných priestoroch. Miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode oprávnenej osoby uzamknutá. Po skončení práce je oprávnená osoba povinná:
  - a. vypnúť osobný počítač alebo sa z neho odhlásiť,
  - b. uzamknúť skrine s materiálmi obsahujúcimi osobné údaje (ak sú skrine uzamykateľné).

## VIII.

### Správa kľúčov a vstupných kariet

1. Oprávnenej osobe je pri nástupe do zamestnania/funkcie pridelený jeden kľúč od dverí do miestnosti, v ktorej bude vykonávať pracovnú činnosť/funkciu.
2. Každú stratu kľúča od kancelárie je oprávnená osoba povinná bezodkladne e-mailom nahlásiť svojmu nadriadenému a zodpovednej osobe.
3. Za kľúče zodpovedá osoba, ktorej boli pridelené. Tieto kľúče je oprávnená osoba povinná odovzdať nadriadenému v prípade skončenia jej pracovnoprávneho alebo iného vzťahu.

## IX.

### Ostatné opatrenia

1. Oprávnená osoba (zamestnanec, konateľ) je povinná pri každom opustení miestnosti v prípade, že v miestnosti už nie je iná oprávnená osoba, miestnosť uzamknúť a kľúč vziať so sebou.
2. Pred odchodom z miestnosti je oprávnená osoba povinná skontrolovať uzatvorenie okien vo svojej miestnosti.
3. Oprávnená osoba nesmie meniť nastavenia antivírusového programu ani vypínať rezidentný



- antivírusový program bez súhlasu vedúceho IT oddelenia.
4. Každé podozrivé, netradičné správanie sa počítača, resp. poruchu je oprávnená osoba povinná nahlásiť ihneď vedúcemu IT oddelenia.
  5. Oprávnená osoba nesmie svojvoľne inštalovať počítačové programy, či už z pamäťových médií alebo z internetu. Inštalovať programy môže len so súhlasom nadriadeného po predchádzajúcej konzultácii s vedúcim IT oddelenia.
  6. Každá oprávnená osoba musí mať pridelené heslo, ktorým sa autentifikuje a toto uchováva v tajnosti. Oprávnená osoba nesmie prezradiť svoje heslo, ktorým sa autentifikuje. Heslo nesmie byť zapísané a uložené na viditeľnom alebo ľahko dostupnom mieste. Oprávnená osoba je zodpovedná za neoprávnené sprístupnenie svojho hesla inej osobe, následne i za jeho zneužitie a spôsobené škody.
  7. Oprávnená osoba nesmie dovoliť pracovať s počítačom osobe, ktorá nie je oprávnená.
  8. Ak na jednom počítači pracuje viac osôb, musí sa oprávnená osoba prihlásiť svojim prihlasovacím menom a heslom po predchádzajúcom odhlásení sa oprávnenej osoby, ktorá predtým pracovala s daným počítačom.

## **X.**

### **Porušenie bezpečnosti**

1. V prípade, že dôjde k porušeniu bezpečnosti osobných údajov, je oprávnená osoba bezodkladne povinná informovať o tejto skutočnosti svojho nadriadeného a vedúceho IT oddelenia.
2. Oprávnená osoba je povinná prerušiť svoju činnosť, pričom nesmie vykonať akékoľvek úkony, ktoré by mohli viesť k zvýšeniu rizika bezpečnosti osobných údajov.
3. Oprávnená osoba je povinná spísať zápisnicu, v ktorej uvedie všetky podrobnosti v rozsahu:
  - a. o aké osobné údaje ide,
  - b. kedy sa o narušení bezpečnosti dozvedela,
  - c. k akému porušeniu bezpečnosti došlo,
  - d. ako sa o tomto porušení dozvedela,
  - e. aké kroky podnikla.
4. Oprávnená osoba odovzdá zápisnicu vedúcemu IT oddelenia.
5. Vedúci IT oddelenia oznámi povahu a rozsah narušenia bezpečnosti Prevádzkovateľovi bezodkladne po tom, čo sa o tejto informácii dozvedel.
6. Vedúci IT oddelenia je povinný vyvinúť čo najväčšiu snahu o to, aby k ďalšiemu porušovaniu bezpečnosti pri spracúvaní osobných údajov nedošlo, pričom je povinný v čo najkratšom čase odstrániť vzniknuté problémy.
7. Oprávnená osoba smie vykonávať svoje pracovné činnosti až po súhlase vedúceho IT oddelenia, ktorý potvrdí, že výkon pracovných činností nepredstavuje riziko pre bezpečnosť osobných údajov.
8. Vedúci IT oddelenia je povinný vypracovať zápisnicu, ktorá bude obsahovať:
  - a. druh osobných údajov, ktorých ochrana bola narušená,
  - b. pôvod a formu narušenia,
  - c. rozsah narušenia a predpokladanú mieru rizika,
  - d. opatrenia, ktoré boli vykonané s cieľom odstránenia vzniknutého stavu,
  - e. opatrenia, ktoré boli vykonané s cieľom zabezpečenia bezpečnosti osobných údajov.
9. Vedúci IT oddelenia odovzdá svoju zápisnicu a zápisnicu oprávnenej osoby Prevádzkovateľovi.

## **XI.**

### **Spracúvanie podaní dotknutých osôb**

1. Žiadosti a námietky dotknutých osôb spracúva osoba, ktorej to vyplýva z poverenia (ďalej len „zodpovedná osoba“).
2. Zodpovedná osoba po prijatí žiadosti, námietky alebo sťažnosti dotknutej osoby (ďalej len „podanie“) informuje dotknutú osobu o jej prijatí a ďalšom postupe.
3. Zodpovedná osoba je povinná vyhodnotiť podanie dotknutej osoby najneskôr v lehote 30 dní odo dňa jej doručenia.
4. Pokiaľ by si vyhodnotenie podania vyžadovalo viac času, je zodpovedná osoba povinná kontaktovať Prevádzkovateľa a primerane o tom informovať aj dotknuté osoby.
5. Po vyhodnotení podania je zodpovedná osoba povinná náležite informovať dotknuté osoby vo vyššie stanovenej lehote.

