

**Súkromná stredná odborná škola ADVENTIM -  
Magán Szakközépiskola ADVENTIM,  
Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951**

---

# **Smernica**

**o technických, organizačných a bezpečnostných  
opatreniach spracovania osobných údajov**

**máj 2018**

## **OBSAH**

<b>1.</b>	<b>Predmet úpravy .....</b>	<b>3</b>
<b>2.</b>	<b>Definície základných pojmov .....</b>	<b>3</b>
<b>3.</b>	<b>Poučenie oprávnenej osoby .....</b>	<b>6</b>
<b>4.</b>	<b>Povinnosti oprávnených osôb .....</b>	<b>8</b>
4.1	Povinnosť dodržiavať opatrenia na spracovanie osobných údajov .....	8
4.2	Povinnosť zachovávať mlčanlivosť .....	8
4.3	Povinnosti pri získavaní osobných údajov .....	9
<b>5.</b>	<b>Povinnosti a opatrenia pri spracúvaní osobných údajov .....</b>	<b>10</b>
5.1	Povinnosti pri používaní informačných systémov .....	10
5.1.1	Aplikácia bezpečnostných záplat .....	10
5.1.2	Antivírusové opatrenia .....	11
5.1.3	Používanie a tvorba bezpečného hesla .....	11
5.1.4	Zálohovanie dát .....	11
5.2	Opatrenia sieťovej bezpečnosti .....	12
5.3	Opatrenia fyzickej bezpečnosti .....	13
5.4	Opatrenia pri prenose osobných údajov mimo priestorov prevádzkovateľa .....	14
<b>6.</b>	<b>Bezpečnostné incidenty .....</b>	<b>15</b>
6.1	Oznámenie porušenia ochrany osobných údajov .....	15
6.2	Opatrenia pri bezpečnostných incidentoch .....	16
<b>7.</b>	<b>Likvidácia osobných údajov .....</b>	<b>18</b>
<b>8.</b>	<b>Kontrolná činnosť .....</b>	<b>19</b>
	<b>príloha č. 1 .....</b>	<b>21</b>
	<b>príloha č. 2 .....</b>	<b>22</b>
	<b>príloha č. 3 .....</b>	<b>23</b>
	<b>príloha č. 4 .....</b>	<b>24</b>

## 1. Predmet úpravy

Táto smernica upravuje technické, organizačné a bezpečnostné postupy (ďalej len „opatrenia“) spracovania osobných údajov, povinnosti oprávnených osôb prevádzkovateľa s cieľom zabezpečiť ochranu osobných údajov pri manuálnom a automatizovanom spracúvaní osobných údajov v zmysle 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“) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „ZoOOÚ“)

Prevádzkovateľom na účely zákona je Súkromná stredná odborná škola ADVENTIM - Magán Szakközépiskola ADVENTIM, Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951, v mene ktorej spracováva osobné údaje aj sprostredkovateľ na účely zabezpečenia riadneho vedenia účtovníctva, daní a predpísanej evidencie prevádzkovateľa.

## 2. Definície základných pojmov

Na účely definície pojmov tejto smernice v súlade s GDPR a ZoOOÚ sa rozumie:

osobnými údajmi	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, 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,
oprávnenou osobou	fyzická osoba, ktorá spracováva osobné údaje podľa pokynov prevádzkovateľa, je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti a bola poučená prevádzkovateľom o zásadách ochrany osobných údajov a o povinnostiach vyplývajúcich z predpisov o ochrane osobných údajov,

súhlasom dotknutej osoby	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,
genetickými údajmi	osobné 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,
biometrickými údajmi	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,
údajmi týkajúcimi sa zdravia	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,
spracúvaním osobných údajov	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,
pseudonymizáciou	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,
profilovaním	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,
logom	záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
šifrovaním	transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,
informačným systémom	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,
porušením ochrany osobných údajov	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,
dotknutou osobou	každá fyzická osoba, ktorej osobné údaje sa spracúvajú,
prevádzkovateľom	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,
sprostredkovateľom	každý, kto spracúva osobné údaje v mene prevádzkovateľa,
príjemcom	každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu 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	každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,
zodpovednou osobou	osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní

	úlohy podľa tohto zákona,
zástupcom	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 ZoOOÚ,
podnikom	fyzická osoba – podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť,
medzinárodnou organizáciou	organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody,
členským štátom Dohody o Európskom hospodárskom priestore,	štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou,
treťou krajinou	krajina, ktorá nie je členským štátom,
integritou údajov	neporušenosť a celistvosť (úplnosť) údajov,
likvidáciou osobných údajov	postup zrušenia osobných údajov najmä ich vymazaním, fyzickým zničením hmotných nosičov, spoľahlivo zabezpečujúce neobnoviteľnosť, nereprodukovateľnosť osobných údajov.

### 3. Poučenie oprávnenej osoby

Prevádzkovateľ spracováva osobné údaje vo vlastnom mene oprávnenými osobami najmä zamestnancami prevádzkovateľa. Fyzické osoby, ktoré budú spracovávať osobné údaje musia byť pred spracovaním osobných údajov poučené o:

- politike ochrany osobných údajov,
- rozsahu spracovávaní osobných údajov prevádzkovateľom (sprostredkovateľom),
- účele spracovávaní osobných údajov,
- právnom základe spracovávaní osobných údajov,
- spracovateľských operáciách prevádzkovateľa,

- technických organizačných a bezpečnostných opatreniach a povinnostiach uvedených v tejto smernici, najmä o povinnosti zachovávať mlčanlivosť o osobných údajoch o ktorých sa dozvedeli,
- ďalších povinnostiach vyplývajúcich zo ZoOOÚ a GDPR a o
- zodpovednosti za ich porušenie.

Poučenie vykonáva prevádzkovateľom poverená osoba. O poučení osôb spracovávajúcich osobné údaje sa vyhotoví písomný záznam, ktorý obsahuje:

- a) identifikačné údaje prevádzkovateľa,
- b) vymedzenie rozsahu poučenia,
- c) titul, meno, priezvisko, pracovné zaradenie a podpis poučenej osoby,
- d) miesto a dátum poučenia,
- e) titul, meno, priezvisko, pracovné zaradenie podpis toho, kto vykonal poučenie a
- f) dátum, odkedy fyzická osoba prestala byť oprávnenou osobou; tento údaj doplní prevádzkovateľ po ukončení jej činnosti ako oprávnenej osoby.

Záznam o poučení oprávnenej osoby je uvedený v prílohe.

Poučená osoba sa považuje za oprávnenú osobu, ktorá je oprávnená spracovávať osobné údaje prevádzkovateľa podľa pokynov prevádzkovateľa.

Prevádzkovateľ opätovne poučí oprávnenú osobu, ak:

- a) došlo k podstatnej zmene v politike ochrany osobných údajov, zmene pracovného, služobného alebo funkčného zaradenia oprávnenej osoby, ak sa tým významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného zaradenia,
- b) v pravidelných intervaloch, spravidla pred začatím školského roku.

Po ukončení spracúvania osobných údajov, najmä z dôvodu skončenia pracovnoprávneho vzťahu oprávnenej osoby, prevádzkovateľ zabezpečí vykonanie opatrení, najmä zrušenie prístupových práv k informačnému systému a prístupu do priestorov a poučí zodpovednú osobu o povinnosti zachovávať mlčanlivosť aj po skončení spracúvania osobných údajov a o následkoch porušenia zákonných povinností.

## **4. Povinnosti oprávnených osôb**

### **4.1 Povinnosť dodržiavať opatrenia na spracovanie osobných údajov**

Oprávnené osoby sú povinné:

- osobne sa zúčastniť na poučení oprávnených osôb o povinnostiach podľa smernica o technických, organizačných a bezpečnostných opatreniach spracovania osobných údajov,
- oboznámiť sa s politikou ochrany osobných údajov školy,
- dodržiavať povinnosti a opatrenia pri spracúvaní osobných údajov,
- oznámiť zachovávať primeranú ostražitosť a každé čo i len podozrenie alebo porušenie ochrany osobných údajov oznámiť štatutárovi prevádzkovateľa alebo zodpovednému zástupcovi.

### **4.2 Povinnosť zachovávať mlčanlivosť**

Oprávnené osoby sú povinné chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, odcudzením, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmkoľvek inými neprípustnými spôsobmi spracúvania; v takomto prípade sú povinné bez zbytočného dokladu informovať prevádzkovateľa, ak majú za to, že sa porušuje ZoOOÚ a GDPR, alebo ustanovenia tejto smernice.

Oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prichádzajú do styku a nesmú ich využiť ani pre osobnú potrebu.

Je zakázané akékoľvek zverejňovanie, poskytovanie alebo sprístupňovanie osobných údajov prostredníctvom elektronických komunikačných prostriedkov alebo prostredníctvom sociálnych sietí vrátane telefonátov (cez telefón).

Osobné údaje je možné poskytnúť len oprávneným príjemcom. Pri komunikácii s klientmi je nevyhnutné dodržiavať mlčanlivosť o iných klientoch.

Povinnosť zachovávať mlčanlivosti trvá aj po ukončení spracúvania osobných údajov alebo po ukončení pracovnoprávneho vzťahu oprávnenej osoby.

Povinnosť mlčanlivosti platí aj pre iné osoby, ktoré v rámci svojej činnosti (údržba, oprava, servis IT, počítačov,..) prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti trvá aj po zániku funkcie alebo po skončení servisnej činnosti.



### 4.3 Povinnosti pri získavaní osobných údajov

Pri získavaní a spracúvaní osobných údajov sú oprávnené osoby povinné dodržiavať nasledovné pravidlá:

- pred získavaním osobných údajov od dotknutej osoby ju treba oboznámiť s účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a o tretích krajinách, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov,
- pri získavaní osobných údajov vyžadovať od dotknutej osoby len nevyhnutný rozsah osobných údajov potrebný pre účel ich spracúvania,
- pri osobnom získavaní a spracúvaní osobných údajov zabezpečiť diskretnosť, aby prítomné tretie osoby nemohli nahliadať do písomností obsahujúcich osobné údaje alebo sa inak oboznamovať so získavanými osobnými údajmi,
- oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov pri ich získaní,
- zakazuje sa, aby sa získavali osobné údaje fyzických osôb pod zámienkou iného účelu, než na účel, na ktorý sú spracovávané; ak osoba uviedla iniciatívne nepožadované osobné údaje, tieto budú ihneď diskretné zlikvidované,
- vykonávať spracovateľské operácie podľa pokynov prevádzkovateľa,
- nesprávne alebo neúplné osobné údaje je potrebné opraviť alebo doplniť; ak to nie je možné, prevádzkovateľ je povinný ich blokovat' do času ich likvidácie,
- zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v informačnom systéme, ak sa osobné údaje spracúvajú na základe súhlasu dotknutej osoby. Súhlas musí byť poskytnutý slobodne, vyjadrený jasne prostredníctvom aktívnej účasti dotknutej osoby (vopred označené políčko alebo nečinnosť a mlčanie sa nepokladajú za súhlas). Súhlas musí byť poskytnutý pred začatím spracúvania osobných údajov, na konkrétny účel, o ktorej je dotknutá osoba vopred informovaná v zrozumiteľnej forme. Udelenie súhlasu musí byť urobený vo forme, aby prevádzkovateľ súhlas vedel kedykoľvek preukázať (napr. písomne) a v prípade prenosu osobných údajov do tretích krajín, ktoré nezaručujú primeranú úroveň ochrany osobných údajov alebo ak ide o automatizované individuálne rozhodovanie vrátane profilovania, musí byť súhlas výslovný.

- v prípade osôb (študentov) mladších ako 16 rokov, musí byť súhlas poskytnutý alebo schválený zákonným zástupcom dotknutej osoby (študenta) a prevádzkovateľ overuje túto skutočnosť primeraným spôsobom (kontrola vzhľadu podpisu, ktorá je očakávané vzhľadu podpisu zákonného zástupcu).

## **5. Povinnosti a opatrenia pri spracúvaní osobných údajov**

### **5.1 Povinnosti pri používaní informačných systémov**

Automatizovaný informačný systém prevádzkovateľa vrátane jeho súčastí (počítače, software, sieťová infraštruktúra) nesmú byť používané na súkromné, alebo iné účely, ktoré nesúvisia s činnosťou prevádzkovateľa.

Každý používateľ sa prihlasuje do informačného systému prevádzkovateľa svojím používateľským menom a heslom.

Používateľ je povinný utajiť svoje heslo.

Všetky zmeny v konfigurácii počítača a ostatného technického vybavenia môžu byť vykonávané len administrátorom informačného systému.

Používateľ sa nesmie žiadnymi prostriedkami pokúšať sa získať prístupové práva administrátora, alebo privilegovaný stav, ktorý mu nebol nastavený administrátorom informačného systému. Pokiaľ používateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené a nastavené, je povinný túto skutočnosť bezprostredne oznámiť štatutárovi prevádzkovateľa.

Používateľ nesmie vykonávať takú činnosť, ktorá by ostatným používateľom bránila v riadnom používaní informačného systému.

Je zakázané:

- sťahovať a inštalovať software, používať a šíriť nelegálne software, kopírovať a distribuovať nainštalované software ani súvisiacu dokumentáciu a príručky,
- otváranie príloh elektronickej pošty pochybného pôvodu, ktoré môžu ohroziť bezpečnosť spracovania osobných údajov,
- meniť nastavenia, konfigurácie, robiť zásahy do technických zariadení infraštruktúry a
- pripájať alebo odpájať technické zariadenia.

#### **5.1.1 Aplikácia bezpečnostných záplat**

Prevádzkovateľ zabezpečuje pravidelnú a včasnú aktualizáciu inštalovaného software. Aktualizácia operačného systému a programového aplikačného vybavenia sa zabezpečuje nastavením automatickej inštalácie bezpečnostných záplat poskytovaných dodávateľom

operačného systému. Nastavenie automatickej inštalácie bezpečnostných záplat operačného systému s minimálnou periódou jeden deň.

### **5.1.2 Antivírusové opatrenia**

Prevádzkovateľ zabezpečuje odolnosť počítačových systémov proti škodlivým kódom antivírusovým softwarom, ktorý kontroluje prítomnosť škodlivého kódu v počítačoch, v prílohách a prichádzajúcej elektronickej pošte a na dátových nosičov.

Antivírusový software musí byť automaticky aktualizovaný. V prípade varovania o hrozbe infikácie, že sa v elektronickej pošte, na disku alebo prenosnom médiu nachádza škodlivý kód, je oprávnená osoba povinná hlásiť túto skutočnosť štatutárovi prevádzkovateľa alebo zodpovednej osobe je povinná zdržať sa manipulácie s týmto súborom alebo prílohou (nepreposielať elektronicnú poštu inému adresátovi).

### **5.1.3 Používanie a tvorba bezpečného hesla**

Pre prístup do informačného systému sa pre oprávnených používateľov zriaďuje prístupový kód (používateľské meno), pokiaľ sa nepoužíva iný bezpečnejší typ autorizácie (ID karta s PKI certifikátom, atď..).

Používateľ si zvolí heslo pre prístup do informačného systému minimálnej dĺžky 8 znakov, ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak (napr. (!, #, \$, %, & \*, -, +, :, ;, ... atď.).

Pre prístup k zašifrovaným archívom sa volí heslo minimálnej dĺžky 12 znakov, ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak.

Používateľ je povinný chrániť heslá pred vyzradením iným osobám a nesmie uchovávať heslo na miestach dostupných iným osobám (napr. na papieri v kancelárii alebo uchovávať svoje prístupové heslo vo webových prehliadačoch.

Bezpečné heslo nesmie byť ako celok všeobecne známe (tzv. slovníkové slovo).

Používateľ je povinný zmeniť si heslo aspoň raz štvrťročne alebo okamžite v prípade, ak má podozrenie o prístupe k heslu inou osobou.

Nové heslo má byť odlišné od hesla, ktoré už v minulosti použil.

Používateľ nesmie v informačných systémoch prevádzkovateľa používať rovnaké heslo aké používa v iných systémoch.

### **5.1.4 Zálohovanie dát**

Pre zabezpečenie minimalizácie rizika náhodnej straty, výmazu, alebo poškodenia osobných údajov sa pravidelne realizuje zálohovanie dát.

Zálohovanie sa vykonáva najmenej raz týždenne alebo aj skôr, ak dôjde k spracovaniu väčšieho objemu údajov.

Pred vykonaním zálohovania sa vykoná test záložného média zápisom a čítaním zapísaných údajov.

Záložné kópie osobných údajov, prípadne súvisiace metadáta a konfiguračné údaje potrebné pre obnovu, musia byť uložené v dátových kontajneroch umožňujúce ich zašifrovanie technologickými prostriedkami s heslom minimálnej dĺžky 12 znakov (napr. Bitlocker, TrueCrypt, atď.), ktoré obsahuje aspoň jedno veľké písmeno, aspoň jednu číslicu alebo špeciálny znak.

Záložné nosiče dát (USB disk, CD, DVD nosiče) musia byť uskladnené v inom priestore, kde sa nachádza HW vybavenie zálohovaného informačného systému.

Zálohované údaje musia byť uchovávané minimálne po dobu trojnásobnej periódy zálohovania.

Údaje uchované po dobu dlhšiu, ako je doba životnosti média, na ktorom sú uložené, musia byť zálohované aj na inom nosiči. Tieto údaje musia byť periodicky ukladané na nové nosiče ešte pred uplynutím životnosti pôvodného nosiča, tak aby sa tak predišlo strate spôsobenej nečitateľnosťou média.

## 5.2 Opatrenia sieťovej bezpečnosti

Opatrenia sieťovej bezpečnosti sú určené na prevenciu a monitorovanie pred neoprávneným prístupom, zneužitím, narušením sieťovej infraštruktúry prevádzkovateľa. Pracovné počítače, notebooky sa pripájajú k sieti Internet prostredníctvom lokálnej počítačovej siete cez firewall. Nie je prípustné zapájať iné sieťové prvky umožňujúce prepojenie lokálnej počítačovej siete so sieťou Internet.

Nastavenie firewallu:

- prednastavené heslo administrátora firewallu sa zmení pri prvom prístupe k modemu podľa pravidiel tvorby hesiel uvedenej v kapitole 5.1.3 Používanie a tvorba bezpečného hesla,
- pre typ modemu TP LINK sa heslo pre prístup k sieti zmení v záložke Maintenance v záložke Údržba -> Interface Setup -> Wireless v časti WPA2-PSK pole "Pre-Shared Key", podľa pravidiel tvorby hesiel uvedenej v kapitole 5.1.3 Používanie a tvorba bezpečného hesla,
- pre vyššiu úroveň bezpečnosti sa na Wifi routri aktivuje filtrácia MAC adries pripájaných zariadení prevádzkovateľa, ktorým sa umožňuje pripojenie sa do lokálnej siete. Administrácia vybraných počítačov / zariadení s MAC adresami, ktoré sú povolené sa zadajú v menu, v záložke Interface Setup -> Wireless v tabuľke s názvom Wireless MAC Address Filter. V nej sa zapíše fyzická adresa/MAC adresu zariadení (notebookov, mobilov, tabletov), ktorým sa povolí pripojiť sa do siete,
- pre ochranu proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok) sa aktivujú v ponuke firewallu ochrany proti rôznym druhom DDoS útokov a hlavne správne nastavenia politiky firewallu,

- blokujú sa vstupné porty so zamedzením prístupu k sieťovým komponentom z vonkajšej siete (zakázaný vzdialený prístup).

Je zakázané používať nešifrované služby ako je napr. telnet, ftp, http, a verejné komunikačné systémy (Viber, WahtsUp,..atď.) na prenos osobných alebo dôverných údajov.

### 5.3 Opatrenia fyzickej bezpečnosti

Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska a zverených pracovných prostriedkov.

Miestnosti, v ktorých sa skladujú listiny s osobnými údajmi musia byť v neprítomnosti oprávnenej osoby uzamknuté, vrátane okien.

Pri osobnej návšteve tretej osoby v priestoroch, kde sa spracúvajú osobné údaje prevádzkovateľa sa tretia osoba vždy sprevádza oprávnenou osobou od vstupu až do jeho odchodu.

V rokovacej miestnosti, na recepcii za prítomnosti tretej osoby sa nesmú na pracovných stoloch nachádzať otvorené spisy s osobnými údajmi, rozložené dokumenty, listiny, do ktorých by mohla tretia osoba hoci aj náhodne nahliadnuť.

Pri dočasnom opustení informačného systému sú oprávnené osoby povinné zabrániť prístupu tretej osoby k osobným údajom, odhlasovať sa z programov na spracovanie osobných údajov, zamknúť počítač alebo aktivovať šetrič obrazovky s povinne nastaveným heslom, odložiť do uzamykateľných skríň listiny s osobnými údajmi alebo uzamknúť miestnosť.

Pri odchode z pracoviska je oprávnená osoba povinná uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu a aktivovať elektrický zabezpečovací systém objektu. Ak zamestnanec nemôže túto povinnosť splniť, oznámi to ihneď štatutárovi prevádzkovateľa.

Listiny, pamäťové médiá (USB disky, CD, DVD nosiče) s osobnými údajmi musia byť ukladané v uzamykateľnej kovovej skrini s bezpečnostným zámkom, ktorá je umiestnená v uzamykateľnej miestnosti. O vydaných kľúčoch vedie prevádzkovateľ evidenciu.

Strata kľúčov sa nahlasuje u štatutára prevádzkovateľa, ktorý zabezpečí výmenu zámkov.

V čase upratovania v priestoroch, kde sa spracúvajú osobné údaje sa zabezpečuje nepretržitá prítomnosť oprávnenej osoby.

Zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarnach alebo faxoch bez dozoru.

## 5.4 Opatrenia pri prenose osobných údajov mimo priestorov prevádzkovateľa

Osobné údaje okrem prevádzkovateľa a oprávnených subjektov na základe zákona (napr. Sociálna poisťovňa, zdravotné poisťovne, Finančná správa SR, atď.) môže spracovávať len sprostredkovateľ, s ktorým prevádzkovateľ uzatvoril zmluvu o spracovaní osobných údajov, rozsah a účel spracovania osobných údajov, práva a povinnosti strán pri ochrane spracovávaní osobných údajov (napr. spracovanie účtovníctva). Prenos osobných údajov iným subjektom je prísne zakázaný.

Listiny a nosiče s osobnými údajmi môžu byť fyzicky prenášané mimo priestory prevádzkovateľa len z oprávnených dôvodov a to zabezpečeným spôsobom.

Prenášanie listín s osobnými údajmi je povolený len v uzatvorených obaloch alebo uzatvorených balíkoch.

Prenášanie osobných údajov na dátových nosičoch mimo priestory prevádzkovateľa je povolené len v zašifrovaných dátových kontajneroch, do ktorých sa uložia osobné údaje. Na prenášaných dátových nosičoch môžu byť uložené len tieto zašifrované dátové kontajnery a nesmú sa na nich nachádzať nezašifrované osobné údaje.

Tvorba dátových kontajnerov umožňujúce zašifrovanie ich obsahu technologickými prostriedkami s heslom minimálnej dĺžky 12 znakov sa riadi postupom podľa kapitoly 5.1.3 o zálohovaní dát.

Oprávnená osoba je povinná skontrolovať obsah dátového nosiča pred prenosom či neobsahuje nezašifrované osobné údaje.

Prenášanie osobných údajov prostredníctvom elektronických komunikačných sietí (napr. email) je povolené len oprávnenému príjemcovi (napr. na spracovanie účtovníctva) len v zašifrovanej forme napr. uložením dátových súborov do zašifrovaného kontajnera a zaslanie tohto kontajnera ako prílohy emailu. Zasielanie osobných údajov týkajúce sa konkrétneho zamestnanca emailom je povolené zasielať:

- a) len na emailovú adresu tohto zamestnanca, ktorú tento zamestnanec poskytol,
- b) len ako prílohu elektronickej pošty vo forme zašifrovaného súboru s heslom (napr. zip súbor výplatnej pásky chránený heslom).
- c) heslo k prílohe nesmie byť zasielané súčasne e-mailom, ale napr. môže byť vopred dohodnuté, alebo zaslané iným kanálom (napr. sms-kou na mobil dotknutej osoby).

Prenos osobných údajov cez portály napr. medzi prevádzkovateľom alebo sprostredkovateľom a oprávneným subjektom (napr. Sociálna poisťovňa, zdravotné poisťovne, Finančná správa SR, atď.), je povolený vyplnením údajových formulárov na zabezpečenej stránke oprávneného subjektu. Pred prihlásením sa na portál je používateľ povinný overiť dôveryhodnosť stránky prostredníctvom platnosti certifikátu stránky (kliknutím na zelený zámok pred „https://...“ ->

pripojenie -> informácie o certifikáte -> porovnanie názvu subjektu komu bol certifikát vydaný s názvom stránky/s názvom inštitúcie kam sa prihlasujeme).

## 5.5 Vybavovanie žiadostí dotknutých osôb

Prevádzkovateľ je povinný vybaviť a odpovedať na uplatnené právo dotknutej osoby bez zbytočného odkladu, najneskôr však do jedného mesiaca, odkedy si dotknutá osoby právo uplatnila.

V prípade požiadavky dotknutej osoby odovzdať jej osobné údaje, prevádzkovateľ zabezpečí vhodným opatrením, aby s odovzdanými údajmi neboli prístupné, odovzdané osobné údaje iných osôb.

V prípade namietania dotknutej osoby voči spracúvaniu osobných údajov, prevádzkovateľ posúdi rozsah, účel, právny základ spracúvania osobných údajov a v prípadoch, ak ide o vyhodnotenie našich legitímnych oprávnených záujmov, tak prevádzkovateľ vykoná test proporcionality. V prípade, ak sa nepreukáže presvedčivý legitímny oprávnený dôvod na spracúvanie, prevádzkovateľ nebudeme osobné údaje namietajúcej osoby ďalej spracúvať.

## 6. Bezpečnostné incidenty

### 6.1 Oznámenie porušenia ochrany osobných údajov

Všetci zamestnanci, oprávnené osoby sú povinné zachovávať primeranú ostražitosť a každé čo i len podozrenie alebo porušenie ochrany osobných údajov oznámiť štatutárovi prevádzkovateľa.

Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

O incidente sa vyhotoví záznam, ktorý obsahuje:

- miesto, dátum a čas zistenia incidentu,
- opis spôsobu, ako bol incident zistený – uvedie sa najmä meno osoby, ktorá incident ohlásila,
- opis priebehu incidentu, jeho začiatku a skončenia, hrozby, ktoré incident vyvolal,
- opis prijatých opatrení,
- návrh na prijatie opatrení pre zabránenie opakovania incidentu,
- opis porušených opatrení, ktoré zapríčinili, že incident nastal,
- meno a priezvisko, podpis, kto záznam zapísal.

Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.

Oznámenie o porušení ochrany osobných údajov bude obsahovať aspoň:

- opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
- kontaktné údaje zodpovednej osoby v našej spoločnosti, kde možno získať viac informácií o porušení ochrany osobných údajov;
- opis pravdepodobných následkov porušenia ochrany osobných údajov;
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

## 6.2 Opatrenia pri bezpečnostných incidentoch

bezpečnostný incident	ohrozenie	opatrenia
vyzradenie alebo zverejnenie hesla pre vstup do informačného systému	narušenie integrity, strata, alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• zmeniť všetky prihlasovacie heslá do informačného systému,</li> <li>• vykonať poučenie osôb o ochrane a utajení hesiel,</li> <li>• vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice</li> </ul>
prístup neoprávnenej osoby	narušenie integrity, strata, alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• zmeniť všetky prihlasovacie heslá do informačného systému,</li> <li>• vykonať poučenie osôb o ochrane a utajení hesiel,</li> <li>• vykonať disciplinárne opatrenie pri preukázanom porušení ustanovení tejto smernice</li> </ul>



narušenie priestorov prevádzkovateľa	narušenie integrity, strata alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• zabezpečenie priestorov</li> </ul>
krádež, strata kľúčov	neoprávnený vstup do priestorov prevádzkovateľa, narušenie integrity, strata alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• výmena zámkov</li> </ul>
strata záložných médií	strata alebo zneužitie osobných údajov, ak neboli dostatočne chránené šifrovaním s bezpečným heslom,	<ul style="list-style-type: none"> <li>• zabezpečiť vytvorenie novej zálohy osobných údajov v zašifrovanom kontajneri s bezpečným heslom</li> </ul>
odcudzenie záložných médií	zneužitie osobných údajov, ak neboli dostatočne chránené šifrovaním s bezpečným heslom	<ul style="list-style-type: none"> <li>• zabezpečiť úložné miesto záložných nosičov proti odcudzeniu,</li> <li>• zabezpečenie osobných údajov na záložnom médiu uložením v zašifrovanom kontajneri</li> </ul>
napadnutie vírusom	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• aktualizovať antivírusovú ochranu,</li> <li>• nová inštalácia operačného systému tzv. „čistý disk“,</li> <li>• obnova údajov zo záložných médií,</li> <li>• neinštalovať software z neoverených zdrojov,</li> <li>• nepripájať neoverené zariadenia (USB disky, DVD/CD nosiče),</li> <li>• neotvárať nevyžiadané e-mailové prílohy,</li> <li>• sledovanie sieťovej aktivity na lokálnej sieti</li> </ul>

neautorizovaný vstup z vonkajšej siete	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• analyzovať logy o prevádzke firewallu, routerov,</li> <li>• aktualizácia antivírusového programu,</li> <li>• obnova údajov zo záložných médií,</li> <li>• skontrolovať a prehodnotiť nastavenia firewallu,</li> <li>• zmena hesla administrátorského prístupu k routrom a firewallom</li> </ul>
neautorizovaný prístup cez Wifi do vnútornej siete	narušenie integrity, strata, odcudzenie alebo zneužitie osobných údajov	<ul style="list-style-type: none"> <li>• zmena hesla pre prístup cez Wifi,</li> <li>• nastavenie filtrácie prístupu podľa MAC adres, <ul style="list-style-type: none"> <li>• obnovenie konfigurácie Wifi routra,</li> </ul> </li> <li>• kontrola záznamov prístupu na Wifi routri</li> </ul>

## 7. Likvidácia osobných údajov

Likvidácia osobných údajov je postup zrušenia osobných údajov najmä ich vymazaním, fyzickým zničením hmotných nosičov, spoľahlivo zabezpečujúce neobnoviteľnosť, nereprodukovateľnosť osobných údajov.

Likvidáciu osobných údajov, ktoré sú zachytené na nepotrebných listinách (bez archivačnej hodnoty), vykoná oprávnená osoba fyzickým zničením listiny, najmä skartáciou.

Osobné údaje z pamäťových médií (USB disky, CD, DVD nosiče, pamäťové karty a pod.) sa likvidujú bezpečným vymazaním, naformátovaním nosiča a následným úplným zaplnením kapacity nosiča napr. náhodnými údajmi alebo verejne publikovanými súborami neobsahujúce osobné údaje, tak aby sa z nich zmazané súbory s osobnými údajmi nedali reprodukovať.

Bezpečné vymazanie osobných údajov z dátových nosičov sa vykoná týmto postupom:

1. otvorí sa súbor elektronického dokumentu (napr. editorom),
2. prepíše sa obsah dokumentu náhodným textom,
3. dokument sa uloží pod rovnakým menom pod akým bol otvorený,
4. vymaže sa dokument z adresára.

Pre fyzickú likvidáciu dátových nosičov osobných údajov (CD a DVD médiá a pod.) sa použije skartovacie zariadenie.

Za dodržiavanie postupu likvidácie osobných údajov zodpovedá oprávnená osoba, kontrolu dodržiavania postupu likvidácie osobných údajov zabezpečuje štatutár prevádzkovateľa v rámci pravidelnej a náhodnej kontroly.

## **8. Kontrolná činnosť**

Kontrolnú činnosť vykonáva štatutár prevádzkovateľa, ktorá je zameraná na dodržiavanie zásad spracúvania osobných údajov, dodržiavania technických, organizačných a bezpečnostných opatrení spracúvania osobných údajov.

Kontrolnú činnosť prevádzkovateľ vykonáva:

- pravidelne, minimálne raz ročne,
- náhodne, kedykoľvek,
- následnú kontrolu po zistení porušenia zásad alebo porušenia technických, organizačných a bezpečnostných opatrení spracúvania osobných údajov.

Kontrolná činnosť prevádzkovateľa sa zameriava najmä na dodržiavanie:

- účelu a rozsahu spracovávaných osobných údajov, zákonnosť spracúvania osobných údajov,
- spôsobu vykonávaných spracovateľských operácií,
- spôsob a lehotu vybavenia o žiadosti dotknutých osôb,
- dodržiavania opatrení tejto smernice.

O priebehu a výsledku vykonanej kontroly spíše prevádzkovateľ protokol, ktorý obsahuje najmä:

- miesto, dátum a čas kontroly,
- rozsah kontroly,
- opis zistených nedostatkov,
- opis prijatých opatrení,
- zoznam osôb zodpovedných za vykonanie opatrení a určenie termínu vykonania opatrení,
- dátum kontroly splnenia opatrení,
- meno a priezvisko, podpis kontrolujúcej osoby.



príloha č. 1

## Záznam o poučení oprávnenej osoby

### Prevádzkovateľ:

Súkromná stredná odborná škola ADVENTIM - Magán Szakközépiskola ADVENTIM,  
Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951

### Rozsah poučenia:

- politika ochrany osobných údajov (mlčanlivosť, zásady ochrany osobných údajov),
- rozsah spracovávania osobných údajov prevádzkovateľom (sprostredkovateľom),
- účel spracovávania osobných údajov,
- právny základ spracovávania osobných údajov,
- spracovateľské operácie prevádzkovateľa,
- technické, organizačné a bezpečnostné opatreniach spracovania osobných údajov,
- povinnosť zachovávať mlčanlivosť o osobných údajoch, o ktorých sa dozvedela,
- povinnosti vyplývajúce zo ZoOOÚ a GDPR a o zodpovednosti za ich porušenie.

### Poučené osoby:

p.č.	titul, meno a priezvisko	pracovné zaradenie	podpis poučenej osoby	dátum ukončenia činnosti

Poučenie vykonal v Dunajskej Strede, dňa:.....

.....  
PhDr. Andrea Olejníková  
riaditeľka školy

príloha č. 2

## **Záznam o bezpečnostnom incidente**

### **Prevádzkovateľ:**

Súkromná stredná odborná škola ADVENTIM - Magán Szakközépiskola ADVENTIM,  
Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951

**Miesto, dátum a čas zistenia incidentu:** .....

**Opis spôsobu, ako bol incident zistený:** (uvedie sa najmä meno osoby, ktorá incident ohlásila):

.....

**Opis priebehu incidentu, jeho začiatku a skončenia, hrozby, ktoré incident vyvolal:**

.....

**Opis prijatých opatrení:**

.....

**Návrh na prijatie opatrení pre zabránenie opakovania incidentu:**

.....

**Opis porušených opatrení, ktoré zapríčinili, že incident nastal:**

.....

**Meno priezvisko a podpis:** .....

príloha č. 3

## **Záznam o kontrole**

dodržiavania zásad a technických, organizačných a bezpečnostných opatrení  
spracúvania osobných údajov

**Prevádzkovateľ:**

Súkromná stredná odborná škola ADVENTIM - Magán Szakközépiskola ADVENTIM,  
Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951

**Miesto, dátum a čas kontroly:** .....

**Rozsah kontroly:**

.....  
.....

**Opis zistených nedostatkov:**

.....  
.....

**Opis prijatých opatrení:**

.....  
.....

**Osoby zodpovedné za vykonanie opatrení a termín vykonania opatrení:**

.....  
.....

**Dátum kontroly splnenia opatrení:** .....

**Meno priezvisko a podpis kontrolujúcej osoby:** .....

príloha č. 4

## Záznam o poučení servisného technika

### Prevádzkovateľ:

Súkromná stredná odborná škola ADVENTIM - Magán Szakközépiskola ADVENTIM,  
Komenského ulica 1219/1 , 929 01 Dunajská Streda, IČO 51895951

### Rozsah poučenia o:

- povinnosti zachovávať mlčanlivosť o osobných údajoch o ktorých sa dozvedel pri výkone servisnej činnosti,
- zákaze oboznamovať sa s osobnými údajmi, s ktorými príde do styku,
- právnej zodpovednosti za porušenie zásad ochrany osobných údajov,
- ďalších povinnostiach vyplývajúcich zo ZoOOÚ a GDPR.

### Poučené osoby:

p.č.	titul, meno a priezvisko	vykonávaný servis	podpis poučenej osoby

Poučenie vykonal v Dunajskej Strede, dňa:.....

.....

PhDr. Andrea Olejníková  
riaditeľka školy