



Nařízení ředitele č. :	13/2018
Platnost od:	1.zář 2018
Obsah:	Směrnice GDPR – Ochrana dat / pravidla pro práci se zařízením ICT
Určeno pro:	Zaměstnance a externí spolupracovníky

Obecná ustanovení

V souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“), vydává Soukromá střední odborná škola a Střední odborné učiliště s.r.o., zapsaná ve VR vedeném KS v Brně, oddíl C, vložka 25705, IČ: 25 32 55 31, se sídlem Znojemska 1027, 674 01 Třebíč (dále jen „škola“) tuto směrnici. Tato směrnice upravuje pravidla pro ochranu, pořizování, zpracování a ukládání dat, informací a údajů, jakož i pravidla pro práci se zařízeními ICT školy. Porušení jakékoli povinnosti zaměstnance dle této směrnice se považuje za porušení povinnosti zaměstnance vztahující se k výkonu jeho pracovní činnosti.

1. Základní pojmy

Správce ICT – zástupce ředitelky školy Mgr. Leszek Cieslak.

Správce sítě – Zdeněk Neumann, externí spolupracovník školy.

Zařízení ICT – informační a komunikační technologie (např. počítače, notebooky, tablety, tiskárny, mobilní telefony atd.)

Web školy – webové stránky školy na adrese <http://www.ssos-sou.cz/dokumenty>, kde jsou průběžně zveřejňovány aktualizovaná znění platných směrnic vydaných školou. Škola informuje zaměstnance o aktualizacích jednotlivých směrnic prostřednictvím e-mailové zprávy.

2. Pořizování, ukládání a zpracování dat

- Zpracováním dat se rozumí jakákoliv operace nebo soustava operací, které jsou systematicky prováděny s osobními údaji, bez ohledu na to, zda automatizovaně nebo jinými prostředky či zařízeními ICT. Zejména se jedná o shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a likvidaci takových údajů.
- Za obsahovou správnost, kompletnost a následné uložení dat v počítačové evidenci v okamžiku pořízení či změny zodpovídá vždy ten, kdo data pořídil či změnil bez ohledu na to, odkud byla data získána a v čí pracovní náplni je sběr a zpracování těchto dat. Zaměstnanec, zadávající údaje do počítačové evidence, je povinen vždy si řádně ověřit věrohodnost a správnost těchto údajů. Zaměstnanec, který zjistí nesrovnalost mezi aktuálně zjištěným údajem a údajem v počítačové evidenci, je povinen tuto skutečnost neprodleně ohlásit příslušnému správci daného údaje a spolupodílet se na zajištění nápravy.

3. Ochrana dat

- Smyslem ochrany dat je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat, minimalizují negativní dopady způsobené poškozením nebo ztrátou dat na další činnost školy. Přijata opatření zamezí přístup k datům nepovolaným osobám.

- Předmětem ochrany je veškeré programové vybavení včetně doprovodné dokumentace, všechna provozní data uložená na nosičích informací, v operační paměti počítačů, tiskáren a dalších zařízení výpočetní techniky, záložní a archivní kopie dat uložené na nosičích informací, údaje zobrazené nebo vytištěné na výstupních zařízeních; přístupová hesla, technické informace o informačním systému a návody.
- Všichni zaměstnanci, kteří přicházejí do styku s jakýmkoli zařízením ICT školy, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí možnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou zařízení ICT, požárem, živelní pohromou atp.
- Provozní data, která jsou uložena na pevných discích počítačů, musí být zálohována v počítačové síti, popřípadě na dalších nosičích informací. V případě zálohování dat uložených na lokálním disku osobního počítače musí být data zálohována na externím disku či školním serveru v předem určené složce.
- Vytvoření záložní kopie je nutno zajistit při jakémkoli pořízení či změně provozních dat v počítačové evidenci. Pokud nejsou provozní data v průběhu pořízení (aktualizace) ukládána na disk školního serveru (centrálního počítače), ale pouze lokálně na disk osobního počítače, odpovídá za pořízení záložní kopie provozních dat vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána a v čí pracovní náplni je sběr a zpracování těchto dat. Záložní kopie dat je v těchto případech nutno pořídít (aktualizovat) bez zbytečného odkladu.
- Mezi způsoby ochrany patří zejména znemožnění jakéhokoli přístupu nepovolaných osob k výpočetní technice a datům, a to jak v pracovní, tak i v mimopracovní době. Zaměstnanec je povinen při vzdálení se od zařízení ICT (nepřítomnosti na pracovišti) jej zabezpečit vypnutím či uzamčením. Zaměstnanec je rovněž vždy povinen zamknout místnost, opouští-li ji jako poslední, a to i v průběhu pracovní doby. Zaměstnanec je povinen si při práci se zařízením ICT počínat tak, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami a musí zabezpečit tisk a/nebo uložení tiskových výstupů mimo dosah nepovolaných osob. Zaměstnanec nikomu nesděluje přístupová hesla do zařízení ICT, aplikací a databází. Rovněž nesmí heslo a ani jeho část ponechat zaznamenané na nezabezpečeném místě. Heslo je tvořeno nejméně osmi znaky, vždy obsahuje kombinaci číslic, malých a velkých písmen, nejde o snadno odhalitelný text obsahující jména, příjmení, data narození. Není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným zařízením ICT.
- Na zařízeních ICT mohou pracovat pouze zaměstnanci k tomu oprávnění.
- Zaměstnanec nesmí ukládat osobní údaje (či dokumenty obsahující osobní údaje) do cloudového úložiště, ani je nesmí vkládat do internetových úložišť.
- Jakoukoli závadu nebo i podezření na nestandardní fungování zařízení ICT zaměstnanec bez zbytečného odkladu hlásí svému nadřízenému nebo pověřenému zaměstnanci. Do odstranění závady nebo prověření nezávadného stavu nesmí zaměstnanci používat dané zařízení ICT v počítačové síti školy.
- Správce sítě je oprávněn v rámci své kompetence monitorovat vytížení sítě a oprávněnost využívání zařízení ICT jednotlivými zaměstnanci. Toto ustanovení může být využíváno pro identifikaci porušení pracovně právních předpisů vztahujících se na pracovní činnost zaměstnanců v souladu s platnou právní úpravou.
- Zaměstnanec nesmí zasílat osobní údaje žáků nebo zaměstnanců školy v elektronické podobě prostřednictvím soukromého e-mailu.

4. Zásady pro práci se zařízením ICT

- Je zakázáno používat nelegální software; používat software, jehož použití nebylo schváleno správcem ICT, instalovat bez svolení správce ICT na disky počítačů jakýkoliv software či data s tímto programovým vybavením související, odstraňovat instalovaný software, provádět změny v nastavení a umístění software a souvisejících dat, pořizovat kopie software a dat pro jinou než služební potřebu, předávat data jiným subjektům bez předchozího souhlasu příslušného vedoucího pracovníka, provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků ICT.

- Zaměstnanec nesmí používat prostředky ICT či Wi-Fi školy pro jiné než schválené účely, nesmí instalovat či hrát počítačové hry, navštěvovat a/nebo prohlížet nevhodné webové stránky (např. webové stránky obsahující pornografii, extremistickou tematiku, sdílená videa a/nebo sociální sítě, hazardní hry atd.).
- Při zahájení práce se zařízením ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených zařízení ICT. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěžené zařízení ICT vypnuty, s výjimkou těch zařízení ICT, která musí zůstat s ohledem na své určení trvale zapnuta.
- Při ukončení nebo změně pracovněprávního vztahu zaměstnance provede správce sítě úpravu (zrušení či blokaci) uživatelského účtu daného zaměstnance, včetně změny či blokace přístupových práv.
- Tiskové výstupy obsahující data podléhající ochraně osobních údajů musí každý zaměstnanec neprodleně zabezpečit před neoprávněným přístupem ze strany jiných osob.
- Zaměstnanec nesmí používat soukromé e-maily na zařízeních školy nebo prostřednictvím W-IFI sítě školy.
- Zaměstnanec nesmí otevírat prostřednictvím Wi-Fi sítě školy a/nebo na zařízení ICT školy nevyžádanou či zavírovanou elektronickou poštu (zejména pak její přílohy).

5. Archivace, skartace dat

- Zálohována jsou data, nikoli programy nebo operační systém.
- Na základě ustanovení § 32 zákona č. 563/1991 Sb., o účetnictví, v platném znění, se doklady osvědčující legální nabytí software uchovávají po celou dobu užívání licence, není možné je skartovat spolu s ostatními doklady v účetnictví. Z tohoto důvodu správce ICT vede v součinnosti s účetní školy evidenci všech typů licencí s odkazy na účetní doklady a evidenci umístění instalačních médií a souvisejících tiskovin – manuálů. Doklad o nabytí software musí obsahovat jasnou identifikaci dodavatele a odběratele, datum nabytí, specifikaci produktu včetně čísla verze a jazykové mutace, počet licencí.
- Správce ICT vede přehled o instalaci software na jednotlivá zařízení ICT a jeho kontrolách. Jakékoli porušení této směrnice hlásí ředitelce školy.
- Na všech počítačích školy je používán jeden typ antivirového programu, je nastaven tak, aby jeho aktualizace byly prováděny automaticky prostřednictvím internetu.

V Třebíči 27. srpna 2018

JUDr. Michal Vostrý, MBA, LL.M.
jedenatel školy

Ing. Renata Hrušková
ředitelka školy