Směrnice NA OCHRANU dat zpracovaných výpočetní technikou

Obecná ustanovení

Na základě ustanovení § 248 zákona č. 262/2006 Sb., zákoníku práce, v platném znění, a zákona č. 101/2000 Sb. o ochraně osobních údajů, v platném znění, vydávám jako statutární orgán organizace tuto směrnici.

Působnost a zásady směrnice

Směrnice upravuje povinnosti zaměstnanců organizace při ochraně údajů zpracovávaných organizací.

Zásady směrnice:

a) tento předpis ukládá povinnosti všem zaměstnancům organizace,

b) je vydáván písemně,

c) nesmí být vydán v rozporu s právními předpisy,

d) nesmí být vydán se zpětnou účinností,

e) vzniká na dobu neurčitou,

f) ředitel školy seznamuje zaměstnance s vydáním, změnou nebo zrušením této směrnice prokazatelným způsobem, v organizaci obvyklým,

g) směrnice je přístupná všem zaměstnancům zveřejněním na místě obvyklém.

Pořizování, ukládání a zpracování dat

1) 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. 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.

2) 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 zpracovaní 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. Kontrolní orgány vždy vycházení ze skutečnosti, že odpovědným za řádné vedení dokumentace, ochranu dat, autorských práv a používání legálního software je vždy statutární orgán organizace, což je nejčastěji ředitel. V jeho zájmu je proto co nejpodrobněji určit povinnosti dalších pracovníků školy, a tím na ně přenést aspoň část svých povinností.

Ochrana dat

1) 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 organizace. Přijata opatřeni zamezí přístup k datům nepovolaným osobám.

2) 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.

3) Všichni zaměstnanci, kteří přicházejí do styku s výpočetní technikou, 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 ICT, požárem, živelní pohromou atp.

4) 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 v minimálně dvou od sebe oddělených kopiích.

5) 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 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 pořídit (aktualizovat) nejpozději před ukončením pracovní směny v den, kdy byla provozní data pořízena (změněna). Pokud jsou provozní data v průběhu pořízení (aktualizace) ukládána na disk

serveru (centrálního počítače), odpovídá za pořízení záložní kopie provozních dat správce. Záložní kopie provozních dat je pořizována automatizovaně.

6) 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. Neponechávání zapnuté techniky bez dozoru. Situování pracoviště tak, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami. Uložení tiskových výstupů mimo dosah nepovolaných osob. Ochrana přístupovým heslem, udržováni hesla v tajnosti, častá změna hesla. Heslo je tvořeno nejméně osmi znaky, vždy obsahuje kombinaci číslic, malých a velkých písmen, nejde o snadno odhalitelný text obsahující jména, příjmení, data narození. Důsledné odhlašování se z počítačové sítě při delší nepřítomnosti na pracovišti. Není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným zařízením.

7) Na počítačích mohou pracovat pouze zaměstnanci k tomu pověření. Počítače, na kterých je zpracováváno účetnictví, mzdová agenda a personalistika, chrání příslušní zaměstnanci před neoprávněným přístupem, zpravidla přístupovými hesly, uzamčením. Mimo běžnou pracovní dobu je místnost zabezpečena elektronickým zabezpečovacím systémem.

8) Jakoukoli závadu nebo i podezření na nestandardní fungování počítače zaměstnanec bez zbytečného odkladu hlásí svému nadřízenému nebo pověřenému zaměstnanci. Do odstranění závady nebo prověření nezávadného stavu nesmí zaměstnanci používat technické zařízení v síti (např. v systému elektronického bankovnictví).

9) Správce sítě je oprávněn v rámci své kompetence monitorovat vytížení sítě a oprávněnost využívání jednotlivými uživateli. Toto ustanovení může být využíváno pro identifikaci přestupků uživatelů v souladu s platnou právní úpravou.

Zásady pro práci s výpočetní technikou

1) 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, používat prostředky ICT pro jiné než schválené účely, instalovat a hrát počítačové hry.

2) Při zahájení práce s ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Ukončování činnosti programů se provádí předepsaným způsobem, včetně ukončení práce v síti. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobní počítače, tiskárny, modemy atd. vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své

určení trvale zapnuta.

3) Při ukončení nebo změně pracovněprávního vztahu správce sítě provede úpravu uživatelského účtu pracovníka, včetně přístupových práv.

4) Tiskové výstupy obsahující data podléhající ochraně osobních údajů musí příslušný pracovník zabezpečit před neoprávněným přístupem. Časté problémy se vyskytují při používání centrální tiskárny umístěné v jiné místnosti. Než si pracovník vyzvedne vytištěné materiály, mají k nim přístup i další osoby.

Archivace, skartace dat

1) Pro archivaci dat se v organizaci používají (*příklad*) CD-ROM a DVD. Technické nosiče jsou uschovávány pouze na pracovištích organizace, u pracovníka _____ v uzamykatelných skříních. Jsou ukládány vždy v jiné místnosti než originální údaje. Není-li uvedeno jinak, ukládají se zálohy vybraných aplikací na dvou místech: na serverech WWWLNX a WIN2K. Pro přenos dat se v organizaci používá síť, USB flash disky, pro archivaci CD-ROM (DVD). Archivní média se označí údajem o počítači, zálohované aplikaci, datem vytvoření zálohy. Při volbě archivních médií je nezbytné počítat i s občasným ověřováním, zda jsou záznamy na nich stále funkční. Životnost médií jako CD a DVD je zatím omezená a nelze spoléhat na to, že uchovají informace po celou předepsanou úložnou dobu, která je v některých případech i několik desítek let.

2) Každý zaměstnanec je povinen provádět zálohování dat podle rozpisu zálohování. Denně jsou zálohována data v účetnictví. Týdně jsou zálohována data, ze kterých jsou vytvářeny tiskové výstupy. Zaměstnanci uchovávají data na počítači v určené složce, aby je bylo možné snadno zálohovat (nebo aby byly zálohovány automaticky).

3) Zálohována jsou všechna data, nikoli programy nebo operační systém. Zálohy jsou ukládány mimo místnost, kde je počítač umístěn (aby zálohy nemohly být odcizeny nebo poškozeny spolu s počítačem, který je zálohován).

4) Je prováděna vždy plná záloha, kompletní kopie všech zálohovaných dat, nikoli jen tzv. přírůstková záloha (data, která se změnila od poslední plné zálohy).

5) Měsíčně jsou zálohována data na CD-ROM (DVD) u mzdové účetní, účetní a ředitele školy a data e-mailové pošty.

6) Zálohování dat se provádí vždy při ukončení pracovněprávního vztahu pracovníka.

7) 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 z účetní organizace 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.

8) Správce ICT vede přehled o instalaci software na jednotlivé pracovní stanice a jeho kontrolách. Jakékoli porušení této směrnice hlásí svému vedoucímu pracovníkovi.

9) Na všech počítačích organizace je používán jeden typ antivirového programu, je nastaven tak, aby jeho aktualizace byly prováděny automaticky prostřednictvím internetu.

10) Na počítačích organizace je dovoleno používat pouze legálně pořízený software. Instalaci a aktualizace programů provádí pouze pověřený zaměstnanec. Pro ostatní zaměstnance platí zákaz manipulace s instalovanými programy, změny konfigurace, nelegální pořizování kopií programů.

11) Kromě statistických sledování a hlášení nadřízeným orgánům je zakázáno poskytovat přes internet údaje o škole a zaměstnancích.

12) Externí pracovníci nebo dodavatelé služeb, zejména účetní a mzdová účetní, odevzdávají výstupy své práce vždy i v elektronické podobě. Občas dochází k problémům při ztrátě dat zpracovávaných externím pracovníkem či firmou – účetní či mzdovou účetní, při zániku firmy, neshodách. Vhodné je zajistit s každou výplatou či účetní uzávěrkou předání dokumentů nejen v listinné podobě. Optimální

je instalace účetního programu na obou počítačích – organizace i externího pracovníka. Externí účetní zpracovává účetnictví doma, ale příslušné datové soubory přenáší v pravidelných intervalech do školního počítače.

V Praze 1. 9. 2024

Mgr. Petr Procházka

ředitel školy