SMĚRNICE Č. 1/2018

OCHRANA OSOBNÍCH ÚDAJŮ A DAT A POKYNY PRO PRÁCI S IT V ORGANIZACI

1. Úvodní ustanovení a působnost

Na základě Nařízení Evropského parlamentu a Rady (EU) 2016/679 (dále jen „Nařízení GDPR"), v platném znění a zákona č. 101/2000 Sb. o ochraně osobních údajů, v platném znění, je vydána tato směrnice upravující povinnosti zaměstnanců organizace při ochraně dat a upravující pravidla pro ochranu osobních dat zaměstnanců, žáků a dalších osob, které jsou s organizací v pracovněprávním nebo v jiném právním vztahu a dalších osob, které poskytují své osobní údaje organizaci k jejich využití. Směrnice je v souladu se základními principy GDPR, kterými jsou: zákonnost, konkrétnost a transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost, zodpovědný přístup a prokázání souladu.

Ochrana osobních údajů a dat se týká všech zaměstnanců, žáků a jejich rodičů, resp. zákonných zástupců a všech osob, které uzavřou smluvní vztah s organizací, při kterém budou zpracovávány osobní údaje.

2. Základní pojmy

Organizace je pro účely této směrnice Střední průmyslová škola stavební, České Budějovice, Resslova 2.

Osobním údajem je jakýkoli údaj, z něhož lze přímo či nepřímo zjistit identitu určité fyzické osoby – „subjektu údajů", jakýkoli údaj týkající se této osoby.

Zvláštní kategorií údajů (dříve citlivé údaje) se rozumí osobní údaje takového charakteru, které mohou subjekt údajů sám o sobě poškodit ve společnosti, v zaměstnání či jinde, nebo mohou zapříčinit jeho diskriminaci. Jedná se o údaje zahrnující informace:

- o národnostním, rasovém nebo etnickém původu,
- o politických postojích, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích,
- o náboženském či filozofickém přesvědčení,
- o trestné činnosti,
- o zdravotním stavu,
- o sexuálním životě,
- o jedinečných biometrických a genetických údajích.

Zpracování osobní údajů – jakákoliv operace s osobními údaji, jako je shromáždění, zaznamenání, uložení, pozměnění, nahlédnutí, použití, šíření, omezení, výmaz apod.

Správce osobních údajů – právnická nebo fyzická osoba (v tomto případě škola – „organizace“), která určuje účely a prostředky zpracování osobních údajů, zpracování provádí a odpovídá za něj.

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci či jiný subjekt, který zpracovává osobní údaje pro správce (správce si jej najímá – např. účetní, lékař,…) na základě smlouvy. Zpracovatel plní stejné nároky na ochranu osobních údajů jako správce; může zpracovávat osobní údaje po technické stránce jen na základě přesných pokynů správce.

Pověřenec – osoba, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje je, radí, dává doporučení. Ředitel školy jmenuje pověřence pro ochranu osobních údajů podle čl. 37 Nařízení GDPR (fyzickou, nebo právnickou osobu), uzavře s ním pracovně právní vztah, nebo smluvní vztah podle občanského práva.

3. Organizační opatření

3.1. Všichni zaměstnanci a členové organizace jsou povinni dodržovat při shromažďování, evidenci a zpracování osobních údajů ustanovení výše uvedených zákonů a nařízení o ochraně osobních údajů, které mimo jiné stanoví, co se těmito údaji a manipulací s nimi rozumí.

3.2. Organizace zajišťuje:

- úvodní proškolení všech zaměstnanců při nabytí účinnosti směrnice GDPR;
- vstupní školení všech nových zaměstnanců při vzniku jejich pracovněprávního vztahu;
- periodická školení;
- opatření při výskytu případů porušení zabezpečení osobních údajů;
- opatření při změně pravidel pro zabezpečení osobních údajů daných touto směrnicí, nebo právními předpisy, na které se odkazuje;
- sleduje aktuální bezpečnostní situaci, potenciální hrozby a pravidelně provádí testy zranitelnosti ICT;
- evidenci všech osobních údajů shromažďovaných a zpracovávaných v organizaci, tak aby byly shromažďovány pouze údaje skutečně nezbytné pro zajištění příslušných činností. V evidenci osobních údajů má vypsané i typové osobní údaje, např. včetně stážistů, dobrovolníků či dárců, osobní údaje kontaktních osob či rodinných příslušníků, uchazečů o zaměstnání apod., tak aby byla evidence úplná;
- uložení dokumentace s osobními údaji tak, aby se k dokumentaci dostaly pouze oprávněné osoby a bylo respektováno rozdělení pravomocí a odpovědností jednotlivých rolí zaměstnanců;
- aktualizuje matici rolí, odpovědností a přístupů k osobním údajům.

3.3. Každý zaměstnanec je si vědom toho, že:

- nese odpovědnost za ochranu dat a zařízení organizace jak na svém pracovišti, tak i mimo něj;
- jsou přijata a musí být dodržována adekvátní opatření pro ochranu osobních údajů v rámci fyzické ochrany;
- veškeré osobní údaje a citlivá data mohou být uloženy jen na schválených úložištích a zařízeních organizace;
- musí chránit své bezpečnostní a osobní údaje (hesla, kódy PIN, přístupové kódy, apod.), nikomu je nesdělovat, hesla pravidelně měnit;

- na zařízení organizace smí být používán pouze podporovaný sw (včetně operačního systému a internetového prohlížeče), musí být vždy bezprostředně aplikovány bezpečnostní update/patche a používat aktuální antivirové a anti-spyware programy s nastavenou on-line ochranou;
- připojení přes Internet je možné pouze prostřednictvím firewallu a pouze přes prověřená datová spojení včetně wi-fi sítí;
- z internetu a ani z jiných zdrojů se nesmí stahovat neznámé soubory, příp. programy;
- je nutné věnovat pozornost nedůvěryhodným e-mailům (zprávy od neznámých odesílatelů, případně zprávy s podezřelým názvem či obsahem), takové neotvírat a bez otevření mazat.
- je nutné ověřovat platnost certifikátu stránky;
- při jakémkoliv podezření na možnost zneužití svých přístupových údajů do služeb a na stránky, které uživatel používá, musí uživatel službu buď ihned zablokovat či změnit přístupové údaje.

3.4. Všichni zaměstnanci a členové organizace jsou si vědomi toho, že při ukončení pracovněprávního vztahu zaměstnanců trvají jejich povinnosti při ochraně osobních údajů i po ukončení pracovněprávního vztahu k organizaci.

3.5. Obsahem školení je zvyšování povědomí zaměstnanců o povinnostech uvedených v předchozím odstavci.

4. Pořizování a zacházení s údaji a daty

4.1. Organizace shromažďuje a zpracovává pouze údaje, které:

- souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, a se sociálním a zdravotním pojištěním;
- související s poskytováním služeb organizace;
- souvisejí s identifikací pracovníků, žáků, dárců apod. v souladu se zákonem.

4.2. Nad rozsah daný právními předpisy je ke zpracování nutný souhlas osoby, jejíž osobní údaje jsou zpracovány. Před samotným zpracováním osobních dat organizace prokazatelně zajistí plnou informovanost těchto osob v rozsahu daném zákonem č. 101/2000 Sb., o ochraně osobních údajů a Nařízení GDPR. Poučení musí být zajištěno i v oblasti povinnosti zachování mlčenlivosti o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení zaměstnání nebo příslušných prací.

4.3. Lze shromažďovat a zpracovávat jen ty osobní údaje, které odpovídají stanovenému účelu a rozsahu zpracování. Ke zpracování se používají pouze pravdivé a přesné osobní údaje.

4.4. Každý subjekt údajů má právo na opravu osobních údajů, které se ho týkají. Může se jednat o změnu adresy, jména, bydliště, telefonního čísla a podobně.

4.5. Ke statistickým účelům je třeba osobní údaje anonymizovat.

5. Účelové omezení

5.1. Osobní údaje jsou organizací shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely.

5.2. Údaje pro různé účely nelze spojovat, musí být evidovány a zpracovány odděleně.

5.3. Rozsah osobních údajů zpracovávaných o žácích, jejich rodičích a zákonných zástupcích je dán požadavky příslušných právních předpisů (zejména zákonem č. 561/2004 Sb., školský zákon); je stanoven tak, aby zpracovávané údaje spolehlivě a věrohodně prokazovaly záznamy vedené školní matrikou, evidenčními listy, záznamy týkajícími se bezpečnosti a ochrany zdraví, o průběhu přijímacího řízení, o průběhu vzdělávání, o ukončování vzdělávání; dále ke splnění povinností vůči třetím osobám (např. zdravotní pojišťovny, Česká správa sociálního zabezpečení, finanční úřad) a předpisů o archivaci.

5.4. Rozsah osobních údajů zpracovávaných o zaměstnancích organizace je dán požadavky právních předpisů, zejména zákoníku práce; je stanoven tak, aby zpracovávané údaje spolehlivě a věrohodně prokazovaly vznik, průběh a ukončení pracovně právního vztahu zaměstnance, včetně poskytování platu; dále splnění povinností vůči třetím osobám (např. zdravotní pojišťovny, Česká správa sociálního zabezpečení, finanční úřad) a předpisů o archivaci.

5.5. Rozsah osobních údajů zpracovaných o uchazečích o zaměstnání v organizaci:

- po uchazečích jsou vyžadovány pouze údaje nezbytné pro posouzení vhodnosti uchazečů v rámci výběrového řízení (kvalifikace, zdravotní způsobilost, bezúhonnost),
- další rozšiřující informace jsou požadovány až po případném rozhodnutí o uzavření pracovně právního vztahu,
- neúspěšným uchazečům jsou vráceny jimi zaslané dokumenty a jejich osobní údaje jsou vymazány ve lhůtě 3 měsíců od skončení výběrového řízení.

6. Přístup k osobním údajům

6.1. Všechny osoby musí vyvinout dostatečné a přiměřené úsilí k tomu, aby se zamezilo neoprávněnému přístupu ke shromažďovaným údajům.

6.2. K osobním údajům je povolen přístup pouze osobám k tomu zmocněným zákonem. Do osobního spisu zaměstnance mohou dále nahlížet vedoucí, jemu nadřízení pracovníci, orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Příslušní vedoucí zaměstnanci, v jejichž působnosti se nachází dokumentace s osobními údaji, určí v souladu s ustanovením Nařízení GDPR způsob s jejím nakládáním.

6.3. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele dle § 312 zákoníku práce.

7. Ochrana dat

7.1. 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.

7.2. Přijatá opatření zamezí přístupu k datům nepovolaným osobám.

7.3. Předmětem ochrany jsou veškeré osobní údaje v zpracovávané listinné i elektronické podobě a dále veškerá programová 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.

7.4. Všichni zaměstnanci, přicházející do styku s osobními a provozními daty v listinné podobě a výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí nenávratnou ztrátu a trvalé poškození osobních a provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, požárem, živelní pohromou, a podobně.

8. Zásady pro práci s výpočetní technikou

8.1. Je zakázáno:

- používat nelegální software;
- používat software, jehož použití nebylo schváleno správcem IT;
- používat neschválená externí datová úložiště pro ukládání osobních dat (flash disky, CD, DVD, apod.);
- instalovat bez svolení správce IT 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 ředitele školy;
- provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků IT;
- používat prostředky IT pro jiné, než schválené účely;
- instalovat a hrát počítačové hry.

8.2. Při zahájení práce s IT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. 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.

8.3. Při přerušení práce nebo vzdálení se od počítače je zaměstnanec povinen počítač uzamknout. Při ukončení práce je zaměstnanec povinen se od počítače odhlásit.

8.4. Při ukončení nebo změně pracovně právního vztahu správce sítě provede úpravu uživatelského účtu pracovníka, včetně přístupových práv dle pokynů nadřízeného pracovníka.

8.5. Počítačová (kybernetická) bezpečnost je zajišťována na všech počítačích organizace:

- instalací antivirových programů, firewallu;
- stanovením přístupových práv, hesel, zákazu sdílení hesel několika osobami;
- pravidelné zálohování dat, tak aby nedošlo k jejich ztrátě při případném odcizení či poruše počítače a byla zajištěna schopnost obnovy dat v případě fyzických či technických incidentů;
- zajištění automatických bezpečnostních aktualizací používaného software;
- pravidelné provádění testů zranitelnosti ICT;
- při jakékoli likvidaci hardwaru musí být znemožněna možnost získání uložených osobních údajů;

- používání pouze silných hesel (heslo o délce minimálně osmi znaků, vždy musí jít o kombinaci malých a velkých písmen a čísel, případně zvláštních znaků);
- mazání a neotvírání nevyžádané pošty, odmazávání SPAM v emailové schránce i v počítačích;
- pravidelný servis výpočetní techniky je zaměřen i na kontrolu oblasti bezpečnosti dat, je prováděno pravidelné testování přijatých technických a organizačních opatření;
- pravidelným školením zaměstnanců v této oblasti.

9. Archivace a likvidace

9.1. Osobní údaje jsou uchovávány pouze po dobu nezbytně nutnou pro účel jejich zpracování a po dobu nezbytné archivace. Tato doba vychází zejména ze školského zákona, zákona o archivnictví, zákona o účetnictví a ze souvisejících předpisů.

9.2. Pro archivaci dat se v organizaci používá vyměnitelné zálohovací zařízení. Technické nosiče jsou uschovávány pouze na pracovištích organizace. Jsou ukládány vždy v jiné místnosti než originální údaje. Zálohována jsou pouze všechna provozní data, nikoli software. Účetní informace se zálohují na pracovišti organizace.

9.3. Na konci úložní doby jsou elektronická i listinná data přezkoumána a odstraněna, pokud neexistuje oprávněný důvod pro jejich další uchování.

9.4. Listinné dokumenty jsou ničeny pomocí skartovacích kancelářských zařízení, při větším rozsahu externí firmou na základě smlouvy.

9.5. Dokumenty uložené v elektronické podobě jsou ničeny:

- fyzickou destrukcí, jde-li o CD, DVD;
- použitím software zabezpečující vymazání, v tomto případě nesmí jít o pouhé smazání dokumentu, protože i poté by byla možná obnova smazaných souborů, musí jít o opakované přepsání původních souborů novými údaji.

10. Krizový plán

10.1. V případě poškození nebo ztráty vyměnitelného zálohovacího zařízení je zaměstnanec povinen informovat vedoucího zaměstnance, který neprodleně informuje správce sítě nebo technického pracovníka. Ty dále informují pověřence, který splní oznamovací povinnost o možném úniku osobních údajů. Správce sítě nebo technický pracovník provede blokaci zařízení (např. mobilní telefon) a provede obnovu dat ze zálohy.

10.2. V případě zavirování zařízení – zaměstnanec neprodleně informuje vedoucího pracovníka a správce sítě. Správce sítě provede odpojení napadeného zařízení od sítě a následně odviruje zařízení. Napadená data obnoví správce sítě ze zálohy.

10.3. V případě napadení počítačové sítě zvenčí – správce sítě odpojí server od sítě. Informuje pověřence pro možný únik osobních údajů. Správce sítě prověří následky útoku a způsob útoku. Dále provede virovou kontrolu a přeheslování napadeného zařízení.

11. Závěrečná ustanovení

11.1. Ustanovení této směrnice jsou závazná pro všechny zaměstnance organizace a osoby, které přicházejí s osobními daty správce do styku, aby byla zajištěna ochrana osobních dat zaměstnanců, žáků a dalších osob, které jsou s organizací v pracovněprávním nebo v jiném právním vztahu a dalších osob, které poskytují své osobní údaje organizaci k jejich využití.

11.2. Ustanovení této směrnice jsou závazná pro všechny uživatele počítačového vybavení v rámci sítě organizace a zaměstnance zajišťující činnosti správce osobních údajů.

11.3. Kontrolou dodržování této směrnice je pověřen správce sítě, který je zároveň kontaktní osobou externího správce sítě ve věci zajištění bezproblémového chodu a využívání počítačového vybavení v organizaci.

Směrnice nabývá platnosti dnem: 25. května 2018
Směrnice nabývá účinnosti dnem: 25. května 2018

V Českých Budějovicích 24. května 2018

RNDr. Vladimír Kostka
ředitel školy