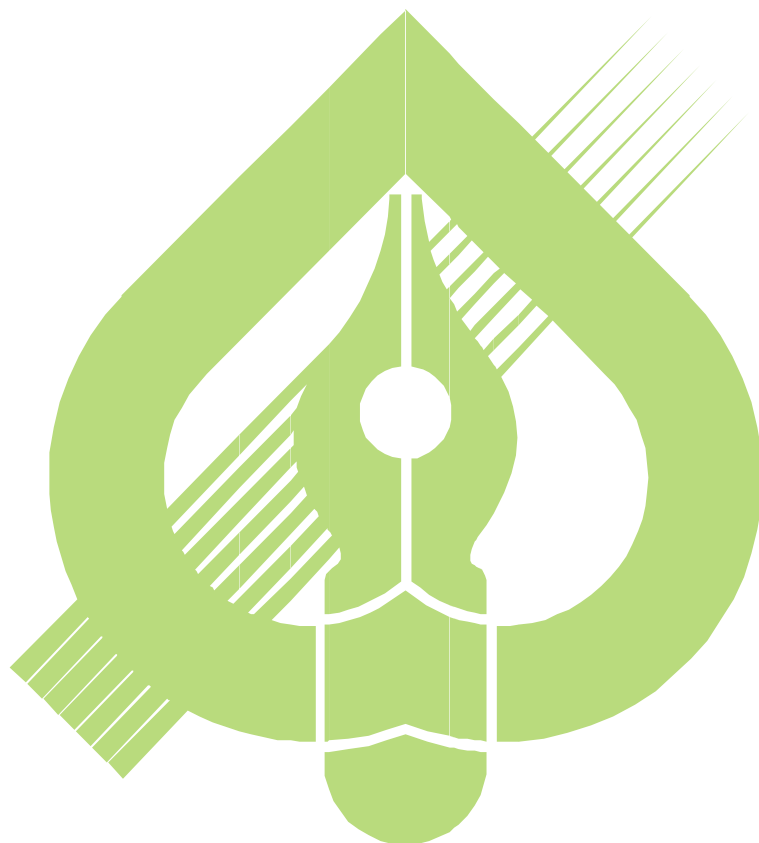


**Střední škola, Havířov-Prostřední Suchá, příspěvková organizace
Kapitána Jasioka 635/50, 735 64 Havířov-Prostřední Suchá, IČO: 13644271**



SMĚRNICE OCHRANA OSOBNÍCH ÚDAJŮ

1. OBECNÉ USTANOVENÍ

Směrnice upravuje způsob nakládání s osobními údaji, které škola zpracovává, tak aby byla zajištěna náležitá ochrana těchto osobních údajů. Škola zpracovává osobní údaje vždy za konkrétním účelem, který nesmí být v rozporu s platnými právními předpisy. Při zpracovávání osobních údajů může škola vystupovat jako:

- správce osobních údajů, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za ně,
- zpracovatel osobních údajů, který zpracovává osobní údaje na základě zvláštního zákona nebo pověření správce.

2. VYMEZENÍ ODPOVĚDNOSTI

Za zpracování osobních údajů, které škola provádí, vždy odpovídá ředitel, zejména v oblastech:

- plnění informační povinnosti k subjektům údajů,
 - uplatňování práv subjektů údajů,
 - zajištění technických a organizačních opatření na ochranu osobních údajů,
 - spolupráce se zřizovatelem a jeho pověřencem pro ochranu osobních údajů.
- Ředitel může pro oblast ochrany osobních údajů jmenovat odpovědnou osobu z řad pracovníků školy, kteří budou také zodpovídat za ochranu osobních údajů, v rozsahu, který určí ředitel, tím ale odpovědnost ředitele za zpracování osobních údajů není nijak dotčena. Odpovědnými osobami jsou zástupci ředitele podle svých úseků. Moravskoslezský kraj jako zřizovatel školy poskytuje metodickou pomoc v oblasti ochrany osobních údajů.

3. POVINNOSTI ŠKOLY PŘI ZPRACOVÁNÍ ÚDAJŮ

Škola:

- řádně stanovit právní titul, rozsah a účel zpracování osobních údajů,
- průběžně monitorovat a upravit jednotlivá zpracování osobních údajů, v případě, že zpracování není v souladu s právními předpisy, spolupracovat s orgány veřejné moci při plnění jejich oprávnění v oblasti ochrany osobních údajů,
- v případě zpracovatele osobních údajů uzavřít smlouvu o zpracování osobních údajů, pokud nejsou při využití osobních údajů splněny jiné předpoklady ke zpracování,
- u nového zpracování osobních údajů si vyžádat konzultaci pověřence zřizovatele, a to ještě před zahájením zpracování osobních údajů.

Ředitel:

- zajistit, aby zpracování osobních údajů prováděné školou bylo v souladu se zákonem, tj. zásada zákonnosti, minimalizace, přiměřenosti, korektnosti a transparentnosti zpracování,
- zajistit plnění informační povinnosti, zejména prostřednictvím webových stránek školy, tiskopisů, které škola používá (např. přihlášky, formuláře apod.),
- zajistit vedení záznamů o zpracování osobních údajů a oznamování bezpečnostních incidentů dozorovému úřadu,
- zajistit náležitou ochranu osobních údajů, prostřednictvím opatření technického a organizačního charakteru,
- zajistit výkon práv subjektů údajů, tj. práva na informace o zpracování, provedení výmazu, opravy či omezení zpracování osobních údajů,
- vyžádat si stanovisko pověřence kraje při provádění rizikových operací s osobními údaji, např. předávání do ciziny, použití automatizovaného zpracování osobních údajů či použití prostředků pro zpracování osobních údajů, které mohou výrazně zasahovat do soukromí (čtečky otisků prstů, kamery, sledování polohy subjektů údajů prostřednictvím GPS).

Ředitel školy je při zpracování osobních údajů povinen zajistit, aby:

- osobní údaje byly zpracovávány v souladu se zákony i v případě, že jsou zpracovávány prostředky výpočetní techniky, v rámci informačních systémů, aplikací a jiných,

Střední škola, Havířov-Prostřední Suchá, příspěvková organizace
Kapitána Jasioka 635/50, 735 64 Havířov-Prostřední Suchá, IČO: 13644271

- všechny osoby, které se podílejí na zpracování osobních údajů, zachovávaly mlčenlivost,
- osobní údaje obsažené ve spisech a dokumentech byly zpracovávány pouze osobami, které jsou k tomu pověřené, jiné osoby nesmí mít k údajům přístup a nesmí je zpracovávat,
- byly stanoveny pracovníkům školy pravidla pro uchovávání dokumentů s osobními údaji v uzamykatelných prostorách,
- osobní údaje, které nelze zpracovávat na základě jiného právního titulu, než je souhlas se zpracováním osobních údajů, byly zpracovávány pouze s tímto souhlasem,
- vést evidenci souhlasů se zpracováním osobních údajů,
- při předávání osobních údajů uvnitř školy zajistit, aby byly předávány pouze osobám, které jsou ke zpracování osobních údajů pověřeny,
- k předávání osobních údajů mimo školu docházelo pouze, pokud tak stanoví právní předpis, uzavřená smlouva anebo je k předávání udělen souhlas dotčeného subjektu údajů,
- při komunikaci školy s veřejností (případně při vedení správního s účastníky řízení), a to v jakékoliv formě (ústně, písemně, elektronicky), při které dochází ke zpracování osobních údajů, bylo postupováno v souladu s právními předpisy,
- byly dokumenty v listinné podobě obsahující osobní údaje ukládány způsobem zamezujícím neoprávněnému či nahodilému přístupu neoprávněných osob k těmto dokumentům (uzamykatelné místnosti, skříně, šuplíky apod.),
- nebyly pořizovány kopie dokumentů obsahujících osobní údaje pro jiné využití,
- v případě zjištění porušení zabezpečení osobních údajů nebo podezření neprodleně, nejpozději do 24 hodin, od okamžiku, kdy se o něm dozvěděl informovat bezprostředně pověřence kraje. Bližší postup ohlášení a evidence porušení zabezpečení osobních údajů je uveden v Příloze č. 2 směrnice.

4. ORGANIZAČNÍ A TECHNICKÁ OPATŘENÍ SOUVISEJÍCÍ S OCHRANOU OSOBNÍCH ÚDAJŮ

Škola je povinna přijmout technická a organizační opatření k zajištění náležité ochrany osobních údajů s ohledem ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům, rizikům pro práva svobody fyzických osob, k zamezení neoprávněného nebo nahodilého přístupu, změně, zničení či ztrátě, alespoň:

Přijmout a dodržovat organizační opatření:

- osoby provádějící zpracování osobních údajů mají stanoveny povinnosti ke zpracování osobních údajů, zejména prostřednictvím právních předpisů, pracovních smluv a jiných vnitřních předpisů organizace,
- dochází-li ke zveřejňování dokumentů, obsahujících osobní údaje je nutné provést anonymizaci osobních údajů, ledaže je jejich zveřejnění stanoveno zvláštním předpisem.

Přijmout a dodržovat personálně-organizační opatření:

- osoby provádějící ve škole zpracování osobních údajů mají v rámci své pracovní náplně (či jiným obdobným opatřeními) stanoven rozsah oprávnění k přístupu a zpracování osobních údajů zachycených ve fyzické podobě. Stejně tak je jim stanoven rozsah oprávnění přístupu do informačních systémů a aplikací, ve kterých jsou zpracovávány osobní údaje zachycené v elektronické podobě. O rozsahu takových přístupů je u každé osoby veden záznam.
- pracovníci školy jsou při zahájení pracovního poměru seznámeni s vnitřními předpisy organizace, zejména v oblasti ochrany osobních údajů. Pracovníci školy jsou informováni o aktuálním stavu právních předpisů, výkladové a rozhodovací praxi v oblasti ochrany osobních údajů.

Přijmout a dodržovat tato administrativně-organizační bezpečnostní opatření:

- dokumenty či spisy, které obsahují osobní údaje, mohou zpracovávat pouze oprávněné osoby, na základě pracovního zařazení či jiného oprávnění.

Střední škola, Havířov-Prostřední Suchá, příspěvková organizace
Kapitána Jasioka 635/50, 735 64 Havířov-Prostřední Suchá, IČO: 13644271

- při provádění kontrol, nahlížení účastníků řízení do spisu při vedení správního či jiné činnosti, při které by mohly osobní údaje zpřístupněny dalším osobám, je nutné zajistit ochranu osobním údajům, které nesouvisejí s prováděnou činností.
- dokumenty obsahující osobní údaje nesmí být vynášeny mimo prostory školy, pokud tak není činěno na základě právního předpisu; v ostatních případech je vynášení dokumentů obsahujících osobní údaje možné jen ve výjimečných případech a se souhlasem ředitele.
- dokumenty obsahující osobní údaje jsou ukládány tak, aby nedošlo ke zneužití osobních údajů, a to zejména uložením v uzamykatelných místnostech či skříních,
- škola při manipulaci s dokumenty postupuje dle spisového a skartačního řádu.

Přijmout a dodržovat tato opatření v oblasti zabezpečení prostředků výpočetní techniky:

- osobní údaje, které jsou zpracovávány v rámci počítačové sítě, informačních systémů, aplikací a zařízení (tj. počítače, servery, tiskárny, kopírky, mobilní telefony, tablety), jsou chráněny tak, aby nedošlo k jejich zneužití. Zařízení jsou zabezpečena tak, aby k nim neměly přístup neoprávněné osoby.
- přístup k počítačové síti a zařízením je zabezpečen prostřednictvím autentizace a autorizace s využitím přihlašovacího jména a hesla či jiným obdobným bezpečnostním prvkem.
- významné součásti počítačové sítě, informačních systémů a aplikací provozovaných organizací (tj. servery a datová úložiště) jsou umístěny v prostorách, které jsou přístupné pouze osobám pověřeným.
- zařízení musí být chráněna antivirovým a antimalware softwarem, případně dalším bezpečnostním softwarem.
- data uložená v počítačové síti a zařízeních jsou pravidelně a plánovaně zálohována.
- aplikace a informační systémy, ve kterých jsou zpracovávány osobní údaje, vytvářejí auditní záznamy, ohledně přístupu k osobním údajům jednotlivými koncovými uživateli, tak aby bylo možné zjistit, jaká osoba měla k osobním údajům přístup. Auditní záznamy jsou zabezpečeny proti jejich modifikacím.
- přístup externích osob do počítačové sítě, informačního systému či aplikace je umožněn pouze osobám, na základě schválení ředitele či osoby pověřené.

Přijmout a dodržovat tato kontrolní opatření:

- ředitel školy kontroluje oblast ochrany osobních údajů, zejména:
 - ukládání spisů a dokumentů obsahujících osobní údaje,
 - oprávněnost prováděných zpracování osobních údajů z pozice platného právního titulu a účelu zpracování; přístup k prostředkům výpočetní techniky a jejich dostatečnému zabezpečení;
 - dodržování dalších povinností uložených právními předpisy v oblasti ochrany osobních údajů.
- Škola při realizaci kontrolních opatření spolupracuje s pověřencem kraje.

5. ZÁVĚREČNÁ USTANOVENÍ

Směrnice nabývá účinnosti dne 1. září 2025

V Havířově dne 29. 8. 2025

Mgr. Petr Szymeczek
ředitel školy

Příloha č. 1: Postup k vyřízení žádosti dle zákona o zpracování osobních údajů

Příloha č. 2: Postup nahlášení bezpečnostního incidentu dle zákona o zpracování osobních údajů

Příloha č. 1: Postup k vyřízení žádosti dle zákona o zpracování osobních údajů

- Tento postup je školou využit v případě, kdy subjekt údajů či jiná osoba vykonávající práva subjektu údajů, uplatní prostřednictvím žádosti právo vůči škole na informace. Za vyřízení žádosti odpovídá ředitel.
- Žádost může žadatel podat prostřednictvím písemného podání zaslaného běžnou poštou, elektronickou poštou, datovou schránkou nebo ústně do protokolu.
- Totožnost žadatele je ověřena v případě, že žádost je ve fyzické podobě opatřena jasnými identifikačními údaji žadatele a jeho podpisem. Totožnost je také ověřena, pokud je žádost v elektronické podobě opatřena zaručeným elektronickým podpisem a nepanují pochybnosti o totožnosti žadatele. Totožnost žadatele je rovněž ověřena v případě, kdy byla žádost podána ústně do protokolu, přičemž byla totožnost žadatele zjištěna z dokladu totožnosti či jiného dokladu. V případě, že je žádost podána elektronicky bez zaručeného elektronického podpisu a z okolností nevyplývá totožnost žadatele, je škola povinna vyzvat žadatele k objasnění své totožnosti.
- Pokud bude žadatel požadovat kopii osobních údajů je povinen žádost podat s úředně ověřeným podpisem, elektronicky se zaručeným elektronickým podpisem, datovou schránkou nebo osobně do protokolu po ověření totožnosti. Bez takového ověření nelze vydat kopie osobních údajů. Kopie osobních údajů budou vydávány do vlastních rukou žadatele.
- Žádost, kterou obdrží kterýkoliv pracovník školy, je povinen ji okamžitě postoupit řediteli.
- Po obdržení žádosti vyrozumí ředitel o této skutečnosti pověřence kraje, a to v následujícím rozsahu:
 - datum přijetí žádosti,
 - popis obsahu žádosti, tj. které právo subjektu údajů je uplatňováno,
 - předpokládaný termín vyřízení žádosti.
- Po vyřízení žádosti vyrozumí ředitel pověřence kraje o datu a způsobu vyřízení žádosti.
- V případě, kdy jsou podávány žádosti zjevně nedůvodné, nepřiměřené či opakované, je škola oprávněna žádost odmítnout s řádným odůvodněním.

Příloha č. 2: Postup nahlášení bezpečnostního incidentu dle zákona o zpracování osobních údajů

- Tento postup je školou využit v případě, kdy je nutné dozorovému úřadu nahlásit porušení zabezpečení osobních údajů, tj. bezpečnostní incident.
- Za oznámení bezpečnostního incidentu dozorovému úřadu odpovídá ředitel.
- Za bezpečnostní incident je považováno takové narušení zabezpečení osobních údajů, které by mohlo způsobit náhodné či protiprávní zničení, ztrátu, změnu, zpřístupnění či přenesení osobních údajů zpracovávaných organizací. Příkladem bezpečnostního incidentu může být např. odcizení dokumentů obsahujících osobní údaje, vážná porucha serveru.
- Ihned po zjištění, nejpozději do 48 hodin, možného bezpečnostního incidentu ředitel kontaktuje pověřence Moravskoslezského kraje, se kterým zkonultuje další postup.
- Při kontaktu s pověřencem kraje je povinností školy, co nejpřesněji bezpečnostní incident popsat, tj. alespoň:
 - popis povahy bezpečnostního incidentu (popis co a kde se stalo),
 - uvedení data a hodiny vzniku či zjištění bezpečnostního incidentu,
 - popis kategorií osobních údajů, které jsou bezpečnostním incidentem ohroženy (citlivé osobní údaje, osobní údaje nezletilých apod.),
 - alespoň přibližný počet subjektů údajů, které mohou být bezpečnostním incidentem ohroženy (nelze-li určit přesně aspoň přibližný počet),
 - popis případného rizika, které v souvislosti s bezpečnostním incidentem může vzniknout subjektům údajů.
- Pověřenec kraje provede vyhodnocení bezpečnostního incidentu v rozsahu rizika nízkého, středního či vysokého. V případě vyhodnocení bezpečnostního incidentu jako vysoce rizikového, je nutné provést oznámení dozorovému úřadu vždy. V případě vyhodnocení bezpečnostního incidentu jako středně rizikového záleží na okolnostech případu a vyjádření pověřence kraje, zda je nutné dozorovému úřadu incident ohlásit.
- Ředitel školy je povinen zajistit evidenci bezpečnostních incidentů v tomto rozsahu:
 - datum a čas zjištění incidentu,
 - datum a čas kontaktování pověřence kraje,
 - popis bezpečnostního incidentu,
 - popis důsledků bezpečnostního incidentu,
 - informace o posouzení rizika posouzení rizika pověřencem kraje,
 - popis případných přijatých opatření v souvislosti s řešením bezpečnostního incidentu,
 - datum, čas a způsob případného ohlášení bezpečnostního incidentu dozorovému úřadu, případně subjektům osobních údajů.
- V případě, že je nezbytné ohlásit dozorovému úřadu bezpečnostní incident, bude toto ohlášení obsahovat následující:
 - popis povahy bezpečnostního incidentu (co kdy a kde se stalo),
 - popis pravděpodobných důsledků bezpečnostního incidentu,
 - popis opatření, která již byla organizací přijata nebo jsou navržena k přijetí s cílem vyřešit daný bezpečnostní incident.