SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

Směrnice pro nakládání s osobními údaji

(školy)

SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

1. Jak směrnici použít

1.1. Tuto Směrnici mohou ředitelé škol, zejména základních a mateřských, a dalších školských zařízení, především v malých obcích, využít buď tak, jak je, anebo s přihlédnutím k potřebě jednoduchosti
a konkrétních instrukcí zaměstnancům a dalším osobám její pasáže včlenit do pracovního nebo organizačního řádu nebo přímo do některých smluv a pracovních náplní. Konkrétní provedení by měli konzultovat s Pověřencem pro ochranu osobních údajů.

1.2. Směrnici vydává ředitel. Zřizovatel[1] zajistí, aby Směrnicí byli vázáni rovněž členové školské rady nebo rady školy, kteří nepodléhají řediteli..

2. Předmět směrnice a základní ustanovení

2.1. Touto směrnicí Základní škola Praha 9 – Dolní Počernice (dále jen „škola“) stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecného nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů jakožto přímo účinného předpisu EU (dále jen „Obecné nařízení“) a podle zákona o zpracování osobních údajů (dále jen „zákon“), zejména při zpracování osobních údajů vykonávaných školou, jejími zaměstnanci, případně dalšími osobami.

2.2. Ustanovení této směrnice jsou závazná pro všechny osoby v rámci školy, zejména pro zaměstnance školy (dále „zaměstnanci“). Obdobně jako pro zaměstnance je tato směrnice závazná i pro členy školské rady resp. rady školy[2] (dále „školská rada“), dále osoby, které mají se školou jiný právní vztah (smlouva o dílo, nájemní smlouva) a které se zavázaly postupovat podle této směrnice, především pokud se při své činnosti seznamují, případně zpracovávají osobní údaje školy jako správce údajů.

2.3. Jakékoliv smlouvy, podle kterých osobní údaje zpracovávají či se při plnění smlouvy s osobními údaji seznamují další osoby, (dále jen "zpracovatelé a další smluvní osoby"), musejí být písemné (včetně elektronické formy) a obsahovat závazek k dodržování této směrnice, konkretizaci povinností podle směrnice a potvrzení, že smluvní strana se se směrnicí seznámila.

2.4. Pokud pro školu zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt (zpracovatel), pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle Obecného nařízení a podle této směrnice a musí být upravena odpovědnost za tyto činnosti vůči správci a vůči kontrolním orgánům. Náležitosti smlouvy o zpracování osobních údajů upravuje Obecné nařízení.

[1] Zřizovatel zřizuje školskou radu, jedině on tedy může směrnicí zavazovat její členy, kteří nejsou zaměstnanci školy (§ 167 odst. 2 školského zákona).
[2] V případě školské právnické osoby, § 130 školského zákona.

SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

3. Základní pojmy

Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je

3.1. **osobním údajem** jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osoby (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby,

3.2. **citlivým osobním údajem** osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Osobní údaje týkající se rozsudků v trestních věcech a trestných činů se pro účel této směrnice hodnotí obdobně jako citlivé osobní údaje.

3.3. **zpracováním osobních údajů** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděna pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení; za zpracování osobních údajů se nepovažuje:

3.3.1. pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (vzdělávací a výchovné, kulturní, společenské, sportovní akce, schůze), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje[3],

3.3.2. běžné nahodilé používání jednotlivých osobních údajů v rámci vzdělávání a výchovy, včetně nahodilého hodnocení žáků,

3.4. **subjektem údajů** fyzická osoba, k níž se osobní údaje vztahují,

3.5. **souhlasem subjektu údajů** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů,

3.6. likvidací osobních údajů fyzické zničení jejich nosiče nebo jejich fyzické vymazání. K fyzickému vymazání nepostačuje vymazat data ze souboru nebo soubor z adresáře[4].

[3] Stanovisko č. 12/2012 - K použití fotografie, obrazového a zvukového záznamu fyzické osoby

[4] Je nutné použít specifický postup a software (elektronické skartovačky) k přepsání uvolněného úložného prostoru, kde jinak data zůstávají i po běžném „vymazání".

SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

4. Osobní údaje a jejich zpracování

4.1. Způsob zpracování osobních údajů a pověřené osoby

4.1.1. Osobní údaje lze zpracovávat pouze za podmínek stanovených Obecným nařízením, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem.

4.1.2. Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou:

4.1.2.1. zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů,

4.1.2.2. člen školské rady, pokud je to nezbytné pro výkon jeho funkce,

4.1.2.3. osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.

4.2. Účel zpracování, zákonnost a nově zaváděné účely zpracování[5]

4.2.1. Veškerá zpracování osobních údajů probíhají v rámci jednotlivých agend, tzv. „účelech zpracování“. Ten, kdo rozhoduje o činnosti zpracování (dále jen „odpovědný zaměstnanec“), pro každé zpracování (agendu, evidenci) stanoví účel zpracování, tedy jeho výstižný

a konkrétně vymezující popis v rozsahu několika slov. O účelu drobných zpracování (tj. zpracování s nízkým rizikem[6], např. pomocné a dočasné evidence menšího počtu žáků, zaměstnanců, dodavatelů apod., bez citlivých osobních údajů) rozhoduje osoba, do jejíž kompetence spadá úkol, který zpracování osobních údajů vyžaduje. V případě, kdy lze předpokládat, že účel zpracování zasahuje subjekty osobních údajů ve velkém rozsahu, je povinna předložit stanovení účelu k rozhodnutí řediteli.

4.2.2. Právní titul či tituly[7] každého účelu zpracování určí odpovědný zaměstnanec. Právními tituly jsou zpravidla

- plnění právní povinnosti
- plnění úkolu ve veřejném zájmu
- plnění smlouvy
- oprávněný zájem správce
- výjimečně též souhlas subjektu údajů

V případě, kdy agenda obsahuje také citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje. K obojímu určí také právní základ[8], je-li potřebný. Pokud je právním titulem souhlas subjektu údajů, jeho znění se vždy konzultuje s pověřencem.

[5] Čl. 5 odst. 1 písm. a) a b) Obecného nařízení

[6] Čl. 33 odst. 1 ON, případy, kdy není pravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob

[7] Právním titulem je některé ustanovení čl. 6 odst. 1 písm. a) až f) , čl. 9/2 písm. a) až j) , čl. 10 Obecného nařízení.

[8] Právním základem je konkrétní ustanovení právního předpisu ČR, o které se v daném případě zpracování opírá. Právní základ je potřebný u právních titulů podle čl. 6/1 písm. c) a e) ON. Dále též u některých právních titulů pro citlivé osobní údaje podle čl. 9/2 ON.

4.2.3. Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu a navrhne nezbytný rozsahu údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektů údajů.
4.2.4. Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec vyžádá posouzení pověřencem.
4.2.5. O každém nově zamýšleném účelu zpracování, vyjma drobných zpracování, jak jsou uvedena v bodu 4.2.1, je ten, kdo navrhuje jeho účel, povinen informovat pověřence, a to před jakýmkoliv krokem. Zahájit novou činnost zpracování lze jen na základě doložitelného posouzení pověřencem.
4.2.6. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícím z jejich funkce nebo smlouvy, a na místech k tomu určených.
4.2.7. Ustanovení tohoto článku se při výkonu jeho funkce přiměřeně vztahuje i na člena školské rady, který spolupracuje s odpovědným zaměstnancem a pověřencem, a to za podmínky, že není zaměstnancem.

4.3. Zásady zpracování osobních údajů

Pověřené osoby jsou povinny dodržovat tyto základní zásady při zpracování osobních údajů:

4.3.1. zpracovávat osobní údaje korektním a transparentním způsobem,
4.3.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování,
4.3.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu, včetně archivace v případech stanovených skartačním plánem, poté je likvidovat,
4.3.4. zpracovávat přesné osobní údaje a podle potřeby je aktualizovat. Třídní učitel má povinnost na začátku školního roku zkontrolovat aktuálnost údajů o žácích a jejich zákonných zástupcích, zejména je vyzvat k ohlášení změn (např. změna bydliště během prázdnin, telefonního spojení apod.) v listinné i elektronické formě, jakož i při každé změně i v průběhu školního roku,
4.3.5. zajišťovat náležité zabezpečení osobních údajů (článek 8 směrnice).

4.4. Záznamy o zpracování a kontrolní seznam

4.4.1. Každý odpovědný zaměstnanec vede ve formuláři, jímž byla provedena implementace Obecného nařízení (dále jen „Kontrolní seznam“):
4.4.1.1. záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování“)[9]
4.4.1.2. záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením jako je likvidace či výmaz dat, lhůty pro likvidaci, forma a lhůty zálohování, šifrování přenosných médií,
4.4.1.3. záznamy o bezpečnostních incidentech jako je únik, ztráta, neoprávněný přenos či zveřejnění,
4.4.1.4. další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů.

[9] Čl. 30 Obecného nařízení

4.4.2. Ke kontrolnímu seznamu mají přístup odpovědní zaměstnanci a pověřenec. O změnách v kontrolním seznamu musejí odpovědní zaměstnanci vždy informovat pověřence, např. sdílením aktualizované verze.

4.4.3. Ředitel nebo jím určená osoba zajistí pravidelné zálohování kontrolního seznamu a případných souvisejících dokladů.

4.5. Zveřejňování informací o subjektech údajů

4.5.1. Ve veřejně šířených informačních materiálech a prostředcích školy, například v ročence, na webu, ve školním zpravodaji se používají především takové ilustrativní fotografie/videa a související informace, které žáka/žákyni neidentifikují jednoznačně i pro cizí osoby[10], například celkové fotografie a záběry ze třídy, z akce, kde nejsou žáci/žákyně zobrazeni s podrobným portrétem a/nebo se neuvádí více, než křestní jméno. Takové zobrazení nevyžaduje svolení.

4.5.2. V případech, kdy je to pro prezentaci žáka/žákyně vhodné, lze použít uvedené fotografie/videa tak, že lze určit totožnost, zejména uvedením jména a příjmení a/nebo podrobného portrétu, jde o zachycení podoby a její rozšiřování ve smyslu § 84 a 85 občanského zákoníku; takové použití vyžaduje svolení, které nemusí být písemné a může vyplývat ze situace. Od žáků mladších 15 let[11] je však nutné vyžádat od zákonného zástupce toto svolení anebo sdělení, že žákovi k němu udělil souhlas ve smyslu § 32 občanského zákoníku, a to na určené období až 5 školních roků (první stupeň, druhý stupeň), a to písemně anebo doloženým prohlášením, například na třídní schůzce na základě prezenční listiny[12].

4.5.3. V případech zvláštních akcí pořádaných školou, kdy je to pro prezentaci žáka/žákyně vhodné, lze k takto zachycené podobě žáka/žákyně připojit ke jménu a příjmení další údaje, například o třídě, věku, účasti na akci konkrétního data, úspěchů ve vzdělání, vítězství v soutěžích včetně sportovních apod. V takovém případě jde o zpracování osobních údajů podle Obecného nařízení a pořízení a zveřejnění údajů vyžaduje souhlas ve smyslu čl. 4 bod 2 a 11 Obecného nařízení EU č. 2016/679. Pro získání souhlasu platí totéž jako pro získání svolení podle předchozího bodu, souhlas musí být písemný, včetně elektronické formy.

4.5.4. Seznamy žáků se nezveřejňují, pokud nejde o zvláštní případ zpracování, pro který žáci nebo jejich zákonní zástupci dali souhlas.

[10] Rozsudek NS 30 Cdo 936/2005: I. Podmínkou poskytnutí ochrany práva na podobu je, aby osoba zobrazeného byla na základě zobrazení obecně identifikovatelná.

[11] Ve skutečnosti mohou žáci v zásadě podle § 31 OZ tato svolení a souhlasy udělovat sami podle rozumové a volní vyspělosti, tedy podle situace asi od 13 let. Pro tuto směrnici se však pro jistotu stanoví napevno 15 let. (*§ 31 OZ: „Má se za to, že každý nezletilý, který nenabyl plné svéprávnosti, je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jeho věku.“)*

[12] Například pokud se učitel na třídní schůzce dotáže rodičů, zda svolují s takovýmto používáním fotografií a videí, a nikdo neprojeví nesouhlas, pak je třeba to poznamenat k prezenční listině a tuto uchovat jako doklad. Toto svolení nelze zaměnit se souhlasem podle následujícího bodu č. 4.5.3.

SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

5. Doklady o souladu s Obecným nařízením

5.1. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou

5.1.1. smlouvy, pro jejichž plnění se zpracovávají osobní údaje,

5.1.2. doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu,

5.1.3. doklady o vyřízení žádostí subjektů údajů,

5.1.4. souhlasy se zpracováním osobních údajů,

5.1.5. balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby,

5.1.6. evidence klíčů, je-li potřebná,

5.1.7. evidence přístupů do počítačů a přístupových práv v informačním systému, je-li potřebná,

5.1.8. údaje o zpřístupnění záznamu kamerového, docházkového systému, či dalších specifických záznamů osobních údajů,

5.1.9. další obdobné doklady.

5.2. Tyto doklady vede odpovědný zaměstnanec v kontrolním seznamu, pokud to jejich povaha umožňuje, jinak se v kontrolním seznamu pouze uvede, kde jsou uloženy.

6. Práva subjektů údajů

6.1. Informování subjektů údajů[13]

6.1.1. Odpovědný zaměstnanec zajistí informování subjektů údajů, jejichž údaje škola zpracovává, zejména na webu školy, případně při uzavření smlouvy nebo získání souhlasu se zpracováním. Zajistí též stručný, transparentní, srozumitelný a snadno přístupný způsob těchto sdělení[14].

6.1.2. Odpovědný zaměstnanec zajistí také doložitelnost uvedeného informování. V rámci své kompetence může tento úkol uložit jinému zaměstnanci.

6.2. Přístup k osobním údajům[15]

6.2.1. Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec, který může v rámci své kompetence tento úkol uložit jinému zaměstnanci. Pro vyřízení se přiměřeně postupuje podle obecného předpisu pro přístup k informacím (zákon č. 106/1999 Sb.), neuplatní se správní řád. Podrobnosti upravuje také manuál Postupy správce při splnění požadavků, plynoucích z práv subjektů údajů - Manuál pro školy, školky a školská zařízení, vydaný SMS služby s.r.o.

[13] Čl. 13 a 14 Obecného nařízení
[14] Čl. 12 Obecného nařízení
[15] Čl. 15 Obecného nařízení

6.2.2. Požádá-li subjekt údajů o sdělení svých osobních údajů, ověří se totožnost žadatele a potvrdí na žádosti, případně se ověření totožnosti k žádosti přiloží, např. číslo průkazu, podle kterého byla ověřena, ověření uznávaného elektronického podpisu, datové schránky (dále jen „ověření totožnosti“).

6.2.3. Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí zaměstnanec podle okolností co nejdříve.

6.2.4. K vyřízení ostatních žádostí o přístup k osobním údajům (zejm. export údajů) je příslušný odpovědný zaměstnanec. Žádost se vyřídí do 30 dnů.

6.2.5. V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec prodloužit lhůtu vyřízení žádosti o další dva měsíce, přičemž o tom informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

6.2.6. Jestliže subjekt údajů podává žádost v elektronické formě a je-li to možné, poskytnou se informace v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob.

6.3. Právo na výmaz, opravu, doplnění, omezení zpracování a námitku

6.3.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů. Při vyřízená žádostí postupují v podrobnostech podle manuálu Postupy správce při splnění požadavků, plynoucích z práv subjektů údajů - Manuál pro školy, školky a školská zařízení, vydaný SMS služby s.r.o.

6.3.2. Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají[16]. Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17 odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů; článek 6.2.5. Směrnice se použije obdobně. Pokud má ověření oprávněnosti požadavku trvat delší dobu, zejména by se osobní údaje dotčené žádostí měly zpracovávat ke stanovenému účelu zpracování (např. zaslat pravidelné vyúčtování s chybným údajem), zajistí jejich vyřazení ze zpracování [17] a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.

6.3.3. Oznámí-li subjekt údajů (např. telefonicky nebo e-mailem), že osobní údaje, které se ho týkají, se změnily, a nelze dostatečně ověřit jeho totožnost s ohledem na závažnost požadované změny (např. na základě osobní znalosti hlasu, znalosti e-mailové adresy), vyzve ho odpovědný zaměstnanec k postupu, umožňujícímu totožnost ověřit.

6.3.4. Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní (např. překlepu), informuje odpovědného zaměstnance a údaj opraví.

6.3.5. Požádá-li subjekt údajů o omezení zpracování svých osobních údajů anebo podá námitku proti jejich zpracování, vyřídí odpovědný zaměstnanec žádost obdobně jako podle bodu 6.3.2, přičemž vždy si vždy vyžádá posouzení pověřencem.

[16] Čl. 16, 17 Obecného nařízení
[17] „omezení zpracování“

7. Pověřenec pro ochranu osobních údajů

7.1. Pro školu vykonává úkoly pověřence pro ochranu osobních údajů Jakub Iran, e-mailová adresa:jakub.iran@sms-sluzby.cz, telefon: 732 633 384.

7.2. Ředitel zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.

7.3. Všechny pověřené osoby jsou povinny[18]:

7.3.1. konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením,

7.3.2. poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování,

7.3.3. zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem,

7.3.4. neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů.

7.4. Zaměstnanci, žáci/žákyně, jejich zákonní zástupci a další osoby, jejichž osobní údaje škola zpracovává, se mohou kdykoliv obrátit na pověřence s žádostí o radu, týkající se jejich osobních údajů.

7.5. Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.

8. Bezpečnost informací

8.1. Obecné postupy při zabezpečení osobních údajů

8.1.1. Přiměřeně zabezpečeny musejí být zpracovávané osobní údaje, jakož i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.

8.1.2. Úroveň zabezpečení lze přiměřeně snížit u osobních údajů, u nichž je riziko pro subjekty údajů nepatrné nebo jsou běžně dostupné veřejnosti:

8.1.2.1. na základě zákona o svobodném přístupu k informacím,

8.1.2.2. na základě oprávněného zveřejnění (například ve veřejně přístupných registrech),

8.1.2.3. nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.

8.1.3. V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.

8.1.4. Osobní údaje musí být zabezpečeny před neoprávněným nebo nahodilým přístupem k nim, proti jejich změně, zničení či ztrátě (zejména dostatečné zálohování), neoprávněným a nezabezpečeným přenosům, proti jejich jinému neoprávněnému zpracování, jakož i proti jinému zneužití osobních údajů. Zabezpečení spočívá při nepřítomnosti pověřených osob zejména v uchovávání záznamových médií (listinných i elektronických), obsahujících osobní údaje, v uzamčených skříních, v uzamykání kanceláří a jiných míst.

8.1.5. Pověřené osoby jsou povinny dodržovat pravidla informační bezpečnosti, zejména nesmějí bez souhlasu správce informačního systému instalovat nedůvěryhodné programy (zejm.

[18] Čl. 38 Obecného nařízení

„zdarma“). Je zakázáno otevírat podezřelé odkazy nebo přílohy e-mailů. V případě nejasnosti je pověřená osoba povinna kontaktovat nadřízeného anebo správce informačního systému.

8.1.6. Dále jsou pověřené osoby povinny vyvarovat se jakéhokoliv jednání, které by mohlo být chápáno jako neoprávněné zveřejňování osobních údajů nebo vést k neoprávněnému přístupu třetích osob k osobním údajům. Zejména, ale nikoliv pouze:

8.1.6.1. sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem. Tím není dotčena možnost používat osobní údaje při běžné činnosti školy ve smyslu článku 3.3.1 (pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (vzdělávací a výchovné, kulturní, společenské, sportovní akce, schůze), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje,) a 3.3.2 (běžné nahodilé používání jednotlivých osobních údajů v rámci vzdělávání a výchovy, včetně nahodilého hodnocení žáků,

8.1.6.2. hlasitě sdělovat podrobné osobní údaje ve veřejně přístupných prostorách (např. šatny, chodby, jídelna apod.),

8.1.6.3. umožnit nepovolaným osobám nahlížet do dokumentů s osobními údaji nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny, nechávat třetí osoby samotné v kabinetech nebo nechávat ve třídách dokumenty obsahující osobní údaje bez dozoru,

8.1.6.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením, v případě jeho vyzrazení ihned zajistit jeho změnu.

8.1.7. Pověřené osoby nesmějí zpracovat osobní údaje mimo konkrétně uložené pracovní úkoly či své pověření, zejména bezdůvodně pořizovat si jejich kopie. Před skončením smluvního vztahu či pověření jsou povinny všechny přidělené nosiče osobních údajů odevzdat. Dále jsou povinni zkontrolovat, zda na jejich soukromém nosiči či zařízení nezůstaly osobní údaje, s nimiž přišli do styku v rámci svého pověření, a pokud ano, bezpečně fyzicky je vymazat podle článku 3.6.

8.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje

8.2.1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních, popř. na jiných místech, zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.

8.2.2. Třídní knihy, výkazy, katalogové listy, individuální vzdělávací plány a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou trvale uloženy v uzamykatelných skříních v kanceláři školy, ředitele nebo zástupce ředitele (dále jen „kancelář“). Pokud je to nutné, mohou je v nezbytném rozsahu ukládat také třídní učitelky/učitelé v zamykatelných skříňkách ve třídě nebo kabinetu. Tyto materiály či jejich části nelze ponechávat bez dozoru, vynášet ze školy, předávat nebo jejich kopie poskytovat neoprávněným osobám.

8.2.3. Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři, přístup k nim má ředitel školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to nutné, též

sekretářka školy nebo mzdová účetní. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu[19].

8.2.4. Likvidace osobních údajů se provádí podle spisového a skartačního řádu školy. Pokud skartace určitého typu osobních údajů není skartačním řádem upravena, likvidují se po uplynutí doby nezbytné k danému účelu. Osobní údaje se likvidují zároveň v listinné i elektronické formě, pokud jejich účely zpracování nejsou odlišné.

8.2.5. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

8.3. Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích

8.3.1. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů. To platí i pro služební telefony, pokud obsahují osobní údaje zpracovávané v agendách školy podle článku 4.2.1. nebo k nim mají dálkový přístup.

8.3.2. Počítače s přístupem k osobním údajům musejí mít alespoň zabezpečený přístup do počítače (přihlášení pod heslem) a nastaveno uzamčení obrazovky po době nečinnosti nejvýše
5 minut. Při odchodu z pracoviště (např. pauza na oběd) se oprávněná osoba odhlásí (např. klávesová zkratka Win+L).

8.3.3. Významné evidence osobních údajů (například mzdová, personální agenda, rozsáhlá evidence žáků s dalšími, zejména kontaktními údaji, záznamy z výchovných komisí, individuální vzdělávací plány) musejí být zabezpečeny také zvláštním přístupem do programového vybavení anebo být jako soubor šifrované.

8.3.4. Elektronická školní matrika se vede v zabezpečeném informačním systému, do kterého mají přístup jednotliví pedagogové písemně pověření ředitelem, a to jen na základě jedinečného přihlášení a pouze v rozsahu oprávnění daného funkčním zařazením. Při práci s elektronickou evidencí nesmějí pověřené osoby opouštět počítač bez odhlášení. Přístupy nastavuje správce informačního systému podle pokynů ředitele a zástupce ředitele. Žáci a jejich zákonní zástupci mohou mít zabezpečený dálkový přístup na základě jedinečného přihlášení výhradně k vlastním údajům o klasifikaci.

8.3.5. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, úložiště souborů mobilního telefonu a podobně, musejí být, i když se nepředpokládá jejich vynášení z objektu alespoň:

8.3.5.1. zajištěna šifrováním disku či jiného úložiště pomocí šifrovacího programu,

8.3.5.2. zajištěna zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně,

8.3.5.3. být jako soubor šifrované, nebo

8.3.5.4. je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizována.

8.3.6. Pokud přenosné médium sloužilo jen k přenosu, musejí být data s osobními údaji bezodkladně po přenosu bezpečně fyzicky vymazána podle článku 3.6.

[19] § 312 zákoníku práce

SMS služby s.r.o.
IČO: 067 84 771
V Rovinách 934/40, 140 00 Praha 4
Tel: +420 723 644 867
E-mail: gdpr@sms-sluzby.cz

8.3.7. Před vyřazením jakéhokoliv elektronického nosiče dat (likvidace, prodej, výpůjčka, darování) musí být nosič zkontrolován a všechny osobní údaje bezpečně fyzicky vymazány podle článku 3.6.

8.3.8. Pověřené osoby pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika pro subjekty osobních údajů a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily.[20]

8.3.9. Pověřené osoby zejména dbají na dostatečnou kvalitu hesel (nejméně 8 znaků, obsahuje minimálně 3 ze 4 položek: Velká písmena, malá písmena, čísla, symboly jako pomlčka či lomítko), pravidelné obměny hesel a je-li to možné vzhledem k nutné zastupitelnosti, důvěrnosti pouze pro jednoho uživatele. V případě potřeby ukládají hesla zabezpečeně a zcela odděleně od počítačů a médií, na nichž jsou použita.

8.3.10. Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol http:/) a jejich uložení na nezabezpečených uložištích (běžné e-mailové schránky, přechodná úložiště jako Úschovna.cz) je přípustný jen se zašifrováním souboru a předáním hesla příjemci jinou cestou, například SMS zprávou na ověřené číslo telefonu či pomocí jiné bezpečné aplikace.

8.3.11. Umožňuje-li to programové vybavení, pověřené osoby vždy využijí možnosti záznamu přístupů a činnosti (auditního záznamu, logu) na počítačích nebo v informačním systému. Záznamy pravidelně kontrolují. Tímto úkolem může být pověřen určený zaměstnanec.

8.3.12. Za plnění povinností stanovených v tomto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

9. Porušení zabezpečení a míra jeho rizika

9.1. Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, například úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů (dále jen „incident“), neprodleně o tom informuje ředitele, pověřence a odpovědného zaměstnance.

9.2. Odpovědný zaměstnanec, je-li to možné, bezodkladně zabrání dalšímu neoprávněnému nakládání, zejména zajistí znepřístupnění, dále vyhodnotí riziko pro práva a svobody fyzických osob, a konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob (dále jen „nízké riziko“), provede o incidentu záznam k příslušnému účelu zpracování v kontrolním seznamu. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl některý odpovědný zaměstnanec[21].

9.3. Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec vhodným způsobem navíc informuje subjekty údajů[22]. Pokud v konzultaci s pověřencem však vyhodnotí, že již existuje či lze přijmout opatření, díky němuž se vysoké riziko pro subjekty údajů neprojeví,

[20] Čl. 32 Nařízení
[21] Čl. 33 Nařízení
[22] Čl. 34 Nařízení

anebo by informování vyžadovalo nepřiměřené úsilí, pouze zveřejní informaci o incidentu na webu školy na výrazném místě.

10. Závěrečná ustanovení

10.1. Kontrola dodržování směrnice

10.1.1. Ředitel, případně jeho zástupce zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji.

10.1.2. Ředitel, případně jeho zástupce zajistí, aby byly se Směrnicí pro nakládání s osobními údaji seznámeny všechny pověřené osoby.

10.2. Revize směrnice

10.2.1. Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.

10.2.2. Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá ředitel, případně jeho zástupce.

10.2.3. Revize směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů.

10.3. Účinnost směrnice

Směrnice pro nakládání s osobními údaji nabývá platnosti a účinnosti dnem vydání.

V Praze dne 25.5.2018