Základní škola a mateřská škola, Hlušice, příspěvková organizace se sídlem Hlušice 144	
71A. -SMĚRNICE NA OCHRANU OSOBNÍCH ÚDAJŮ	
Č.j.: Spisový / skartační znak	**ZS2505 /2018 A.1. A10**
Vypracoval:	Mgr. Miloslav Cajska, zástupce ředitele školy
Schválil:	PaedDr. Marcela Vaňková, ředitelka školy
Provozní porada projednala dne	24. 5. 2018
Pedagogická rada projednala dne	23. 5. 2018
Směrnice nabývá platnosti ode dne:	25. 5. 2018
Směrnice nabývá účinnosti ode dne:	25. 5. 2018
Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu.	

Obsah

1 Úvodní ustanovení 2
1.1 Účel dokumentu 2
1.2 Základní pojmy 3
2 Agendy obsahující osobní údaje a jejich atributy 5
3 Role, pravomoci a odpovědnosti 5
3.1 Povinnosti správce osobních údajů (spravující orgán) 5
3.2 Pověřenec pro ochranu osobních údajů (POOÚ) 5
3.3 Ředitelka 5
3.4 Zaměstnanec pověřený zpracováním OÚ 7
3.5 Obecné povinnosti zaměstnanců při zabezpečení osobních údajů 7
4 Zpracování a zabezpečení agend s osobními údaji 8
4.1 Pravidla pro způsob ukládání agend 8
4.2 Řízení přístupových práv 9
4.3 Zajištění mlčenlivosti 9
4.4 Pravidla pro zabezpečení prostor 9
5 Zvláštní pravidla pro nakládání s OÚ 9
5.1 Souhlas se zpracováním OÚ 9
5.2 Pořizování audiovizuálních záznamů 9
5.3 Nakládání s osobními údaji dle zákona o svobodném přístupu k informacím 10
6 Řešení incidentů 10
7 Informační povinnost - žádosti subjektů OÚ 10
7.1 Informační povinnost správce 10
7.2 Žádosti subjektů OÚ 11
8 Přenesení oprávnění a odpovědností na třetí strany 11
9 Kontrolní a auditní činnost, řízení rizik 12
9.1 Kontrolní činnost 12
9.2 Posouzení shody a řízení rizik 12
9.3 Interní audit 13
10 Související legislativa 13
11 Přílohy 13
11.1 Příloha č. 1 Doložka o mlčenlivosti zaměstnanců 13
11.2 Příloha č. 2 Odpověď na žádost subjektu OÚ 14
11.3 Příloha č. 3 Ohlášení porušení ochrany osobních údajů 15
11.4 Příloha č. 4 Doložka o mlčenlivosti třetích stran 16

1 Úvodní ustanovení

1.1 Účel dokumentu

1) Směrnice o ochraně osobních údajů upravuje postup zaměstnanců při nakládání s osobními údaji a při stanovení účelu, prostředků a způsobu zpracování těchto údajů ve smyslu zákona č. 101/2000 Sb., o

ochraně osobních údajů ve znění pozdějších předpisů a Nařízení EU 2016/679 General Data Protection Regulation (GDPR) ze dne 27. dubna 2016.

2) Organizace je správcem a zpracovatelem osobních údajů a určuje účel, prostředky a odpovědnost za zpracování osobních údajů, provádí jejich zpracování a odpovídá za ně. Další Správci, pro které Organizace zpracovává osobní údaje, jsou uvedeni v Registru agend.

3) K zajištění ochrany osobních údajů je přijat soubor technicko - organizačních opatření, která jsou obsažena v této směrnici a dalších organizačně řídících dokumentech, na něž se tento dokument odkazuje.

1.2 Základní pojmy

Pojmy používané touto směrnicí musí být vykládány v souladu s jejich významem uvedeným v tomto článku a v souladu se zákonem.

1) **Organizace** – pro účely tohoto dokumentu se organizací rozumí ZŠ a MŠ Hlušice, se sídlem 503 56 Hlušice 144

2) **Osobním údajem (dále také OÚ)** jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. 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) **Účel zpracování** - důvody kvůli nimž jsou osobní údaje zpracovávány.

4) **Zvláštní kategorie osobních údajů („citlivé údaje“)**, které vypovídají 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, je povoleno v čl. 9 Nařízení EU 2016/679, který uvádí výjimky kdy je možné tyto údaje zpracovávat.

5) **Subjektem údajů** se rozumí fyzická osoba, k níž se osobní údaje vztahují.

6) **Správce osobních údajů** určuje účely a prostředky zpracování osobních údajů.

7) **Zpracovatel** osobních údajů je osoba pověřená Správcem. Zpracovatel zpracovává osobní údaje pro správce na základě doložitelných pokynů. Zpracovatelé (interní/externí) musí správci poskytnout dostatečné záruky zavedení vhodných technických a organizačních opatření. Zpracovatel nesmí bez souhlasu Správce zapojit dalšího zpracovatele.

8) **Zpracováním osobních údajů** je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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).

9) **Oprávněné osoby** jsou zaměstnanci správce, externí zpracovatelé a příjemci OÚ, tj. další osoby, které mohou mít k osobním údajům přístup pro splnění účelu zpracování, nebo další osoby určené zákonem (subjekt údajů, kontrolní orgány, orgány veřejné moci atp.). Oprávněné osoby jsou uvedeny pro každou agendu v Registru agend.

10) **Souhlasem subjektu údajů** se rozumí prokazatelný, svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

11) **Zákonnost zpracování osobních údajů je možné**, pouze pokud je k tomu právní důvod, tzn. splněna nejméně jedna z uvedených podmínek:
    a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
    b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě;

Pro zpracování zvláštních kategorií OÚ nebo profilování platí zvláštní právní důvody.

12) **Profilování** je jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu atp. Může se jednat o výstupy/analýzy dat v tištěné i listinné podobě (GDPR čl. 22, R 24, 60, 63, 71).

13) **Porušením zabezpečení** osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

14) **Agendou** se rozumí souhrn informací (dokumentů, záznamů nebo elektronických dat), které jsou sdruženy podle společného účelu do jednoho administrativního celku.

15) **Pověřenec pro ochranu osobních údajů (POOÚ)** je osoba s pravomocemi a odpovědnostmi uvedenými v kap. 3.

16) **ÚOOÚ** – úřad pro ochranu osobních údajů – dozorový úřad.

17) **GDPR** - Nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů - General Data Protection Regulation.

18) **dbt** – databáze, kam software ukládá data.

19) **ICT** – informační a komunikační technologie.

20) **Systematičnost zpracování OÚ** - za systematické je považováno takové zpracování, které naplňuje jednu či více z následujících podmínek:
    a) dochází k němu na základě určitého systému,
    b) je dopředu připravené, organizované nebo metodické,
    c) dochází k němu na základě obecného plánu pro shromažďování osobních údajů nebo je prováděno na základě určité strategie.

21) **Rozsáhlost zpracování** - jedná se o případy, kdy dochází ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohlo mít dopad na velký počet subjektů údajů. Při posouzení rozsáhlosti se bere do úvahy počet zasažených subjektů údajů, buď absolutní počet, nebo poměr k celkovému počtu relevantní populace, množství osobních údajů nebo rozsah různých položek osobních údajů, dobu či stálost zpracování a geografický rozsah zpracování.

2 Agendy obsahující osobní údaje a jejich atributy

1) Ředitelka vede v aktuální podobě Registr agend obsahující osobní údaje a určuje, v souladu s touto směrnicí, které údaje/atributy (zejména odpovědnosti, oprávnění, účel, zákonnost, rozsah a způsob zpracování) jsou pro každou agendu v registru vedeny. Registr agend je pro zaměstnance (jen pro čtení) umístěn v ředitelně
2) Rozsah zpracování a nakládání s OÚ nesmí přesahovat rámec stanovený v Registru agend.
3) Správci ICT jsou pro každou agendu pověření zaměstnanci v rozsahu svých odpovědností, tj. správy provozu ICT.

3 Role, pravomoci a odpovědnosti

Kapitola definuje základní odpovědnosti při zabezpečení a zpracování osobních údajů. Další odpovědnosti jsou popsány v jednotlivých kapitolách tohoto dokumentu, ostatních vnitřních předpisech a dokumentech.

3.1 Povinnosti správce osobních údajů (spravující orgán)

Správce osobních údajů (Organizace):

1) určuje Pověřence pro ochranu osobních údajů, odpovídá za jeho zastupitelnost a odpovídá za oznámení kontaktních údajů na webu Organizace, resp. u ÚOOÚ,
2) zajišťuje schopnost Organizace doložit, že zpracování je prováděno v souladu se zákony a účelem zpracování,
3) zajišťuje prostředky zpracování a pravidla pro nakládání s osobními údaji,
4) v oblasti digitálního zpracování osobních údajů:
    a) zajišťuje, aby systémy používaly pouze oprávněné osoby a aby měly přístup na základě zvláštních uživatelských oprávnění,
    b) stanovuje pravidla k zabránění neoprávněného přístupu k OÚ,
5) určuje rozsah a způsob vedení záznamů o činnostech při zpracování OÚ,
6) zajišťuje dostatečné vzdělávání a zvyšování kvalifikace pracovníků v oblasti ochrany osobních údajů.

3.2 Pověřenec pro ochranu osobních údajů (POOÚ)

Pověřenec pro ochranu OÚ je osoba určená smlouvou. Jeho základní odpovědnosti (musí být obsahem smlouvy) jsou:

1) je kontaktní osobou pro ÚOOÚ,
2) poskytuje konzultace řediteli, zpracovatelům OÚ a dalším zaměstnancům Organizace, při praktické aplikaci ochrany OÚ v procesní a technologické rovině,
3) spolupracuje (předkládá posudek)při posuzování rizikovosti zpracování a hodnocení incidentů,
4) provádí kontrolní a auditní činnost.

3.3 Ředitelka

Ředitelka:

1) odpovídá za rozsah a účel, k němuž mají být OÚ zpracovány, kde platí zásada, že jsou zpracovávány OÚ pouze zákonným způsobem a údaje nezbytně nutné k dosažení účelu zpracování, tzn., rozsah zpracování musí být omezen na nezbytné minimum a správce musí být schopen prokázat, že určený rozsah je nezbytný pro plnění účelu,
2) odpovídá, že účel zpracování OÚ není v rozporu se zákonností zpracování (popř. rozsahem uděleného souhlasu) a rozsah a způsob zpracování OÚ není v rozporu s účelem zpracování,
3) určuje a pověřuje zpracováním zaměstnance a externí zpracovatele a specifikuje další oprávněné osoby/příjemce OÚ,

4) definuje veškeré údaje/atributy agendy ve struktuře a rozsahu podle Registru agend a odpovídá za jejich správnost,

5) posuzuje slučitelnost zpracování OÚ s původními podmínkami, pokud má být provedena změna již stanoveného účelu a pokud je tato změna u OÚ zpracovávaných na základě souhlasu (chce využít již OÚ získané za jiným účelem, např. zavedení jiné služby) informuje v dostatečném předstihu subjekty OÚ o tomto záměru a zabezpečí získání jejich opětovného souhlasu,

6) umožní zpracování zvláštních kategorií OÚ tzv. citlivé údaje pouze v souladu s čl. 9 Nařízení EU 2016/679 a to pokud:
    a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;
    b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
    c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
    d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto OÚ nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
    e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
    f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí;
    g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;
    h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem;
    i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;
    j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 Nařízení EU 2016/679 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,

7) umožní rozhodnutí založená výhradně na automatizovaném zpracování, včetně profilování, které má právní účinky nebo se ho obdobným způsobem významně dotýká subjektu údajů, pouze pokud to je:
    a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;
    b) povoleno obecně závazným právním předpisem;
    c) založeno na výslovném souhlasu subjektu údajů.

3.4 Zaměstnanec pověřený zpracováním OÚ

Zaměstnanci pověření zpracováním OÚ jsou pro každou agendu určeni ředitelem v Registru agend. Tito zaměstnanci musí mít dostatečné kompetence a poskytovat záruky použití vhodných/předepsaných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto dokumentu, a nesmí zapojit do zpracování žádnou další osobu, která není uvedena v Registru agend. Zaměstnanci pověření zpracováním musí:

1) shromažďovat pouze OÚ uvedené v Registru agend, tzn. v rozsahu nezbytném pro naplnění tohoto účelu a zpracovávat OÚ pouze v souladu s účelem, k němuž byly shromážděny,
2) zpracovávat pouze přesné OÚ, zjistí-li že jím zpracované OÚ nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, tzn., že OÚ opraví nebo doplní, jinak to oznámí řediteli, pokud se jedná o opravu na základě požadavku subjektu údajů, oznámí mu neprodleně, prostřednictvím Pověřence pro ochranu osobních údajů, jak byly tyto údaje upraveny, či podá vysvětlení,
3) vždy zabezpečit OÚ proti neoprávněnému přístupu, tzn. dodržovat zásadu čistého stolu a prázdné obrazovky, při nepřítomnosti ukládat OÚ v uzamčeném prostoru/skříni kam nemá přístup neoprávněná osoba, „zamknout“ počítač atp.
4) prokazatelně a neprodleně upozornit ředitele zjistí-li, porušení účelu, zákonnosti nebo zabezpečení osobních údajů, nebo že Organizace porušuje povinnosti stanovené touto směrnicí nebo zákonem,
5) zabezpečit, že nebudou sdružovány OÚ, které byly získány k rozdílným účelům,
6) bez souhlasu ředitele nesmí OÚ předat jiné osobě pokud to neumožňuje Registr agend.
7) vyhledávat nepřesné OÚ, pokud to je možné.

3.5 Obecné povinnosti zaměstnanců při zabezpečení osobních údajů

3.5.1 Zasílání, předávání, přenos a přeprava agend

Povolené komunikační kanály a prostředky, které je pro předávání osobních údajů možné použít jsou definovány v Registru agend. Při použití těchto prostředků se musí dodržovat tato pravidla:

1) při přenášení a posílání souborů, které obsahují citlivé OÚ, pomocí přenosných paměťových médií a zařízení nebo elektronickou poštou musí být tyto soubory šifrovány. Pokud není zaměstnanci obsah přenášených elektronických dat (souborů) znám, musí s nimi nakládat, jako by obsahovaly takové údaje,
2) při používání elektronické pošty (e-mail) používat pouze účet zs.hlusice@tiscali.cz,
3) při osobním styku, telefonickém rozhovoru nebo reprodukci osobních údajů musejí zaměstnanci postupovat tak, aby nedošlo k úniku osobních údajů neoprávněné osobě (ověření totožnosti, zavření dveří pracoven, vyloučení přítomnosti dalších osob, atp.).
4) při přepravě osobní údajů v listinné i elektronické podobě (na datových nosičích) musí být takové informace chráněny proti neoprávněnému přístupu a zneužití (např. nesmí být bez dozoru ponechány v obchodu, autě atp.),
5) při zasílání osobních údajů licencovanou přepravní společností (např. Česká pošta a.s., kurýr atp.) musí být dokumenty zaslány v zalepené obálce

3.5.2 Práce s výpočetní technikou

Zaměstnanec musí:

1) při opuštění pracoviště (i krátkodobém) uzamknout počítač (ctr+alt+del) a při návratu k relaci se opět autorizovat pomocí zadáním hesla,
2) udržovat hesla v tajnosti a ihned změnit heslo v případě možného náznaku prozrazení/prolomení,
3) používat silné heslo k účtům a aplikacím (pokud to aplikace umožňuje), tj. délka min. 8 znaků obsahující kombinaci písmen, číslic a speciálních znaků, které není založeno na informacích snadno zjistitelných (např. jméno, telefonní číslo, datum narození apod.) a hesla obměnit alespoň jednou za rok.

Zaměstnanec nesmí:

1) pracovat pod cizí identitou (cizím uživatelským účtem),
2) v SW nastavovat volby „Pamatovat si heslo“,
3) měnit systémový čas na počítačích,
4) instalovat jakýkoli software bez souhlasu ředitelky,
5) používat pro ukládání informací jiná média a zařízení, než která jsou předepsána v Registru agend,
6) spouštět neznámé odkazy a soubory, např. v elektronických zprávách.

3.5.3 Další povinnosti zaměstnanců

1) dodržovat stanovené kodexy chování[1],
2) pokud zjistí, že jsou zpracovávány jiné OÚ, než jsou uvedené v Registru agend, nebo je zpracování v rozporu se stanoveným účelem a zákonností, musí to neprodleně nahlásit ředitelce
3) dodržovat ustanovení zákonů, interní předpisy, pokyny vedoucích zaměstnanců a všechna další opatření, která byla přijata z důvodu zajištění ochrany osobních údajů,
4) při nahodilém nálezu osobních údajů není zaměstnanec oprávněn se s nimi seznamovat, nález odevzdá (upozorní) neprodleně svému vedoucímu, který ho předá ředitelce,
5) zaměstnanec nesmí umožnit neoprávněným osobám, přístup k osobním údajům, tzn. přístup k dokumentům, nahlédnutí na zobrazovací zařízení - monitor, na výstup z tiskárny, vyfocení OÚ atd.),
6) nakládat s osobními údaji, k nimž mají z důvodu své pracovní činnosti přístup, takovým způsobem, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu jiných osob k těmto údajům, k jejich zneužití, zničení či ztrátě, neoprávněnému zpracování, poskytnutí jiným osobám nebo použití k jinému účelu než k jakému jsou oprávněni je používat v souvislosti s výkonem své pracovní činnosti, bez ohledu na formu jejich zpracování,
7) neprodleně upozornit ředitele na incidenty nebo případná rizika možného zneužití osobních údajů.

4 Zpracování a zabezpečení agend s osobními údaji

4.1 Pravidla pro způsob ukládání agend

4.1.1 Omezení doby uložení a likvidace/mazání OÚ

Ředitel stanovuje v Registru agend minimální a maximální dobu pro uložení agendy v souladu se Spisovým a skartačním řádem, obecně závaznými právními předpisy a účelem zpracování agendy.

Uchovávat OÚ lze pouze po dobu určenou Registrem agend a skartovat/vymazávat je pouze způsobem stanoveným Spisovým a skartačním řádem.

Likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich vymazání nebo jejich trvalé vyloučení z dalších zpracování. Likvidace/mazání osobních údajů probíhá:

a) bezpečnou likvidací paměťového média, na kterém jsou data uložena - odpovídá ředitelka
b) vymazáním digitálních dat (a to včetně všech záloh) obsahující OÚ v souladu se Spisovým a skartačním řádem
c) skartací listinné podoby osobních údajů v souladu se Spisovým a skartačním řádem.

4.1.2 Zálohování agend ukládaných v digitální podobě

Zálohování dat probíhá podle Plánu záloh, který schvaluje ředitelka

4.1.3 Dostupnost agend

Organizace nastavila systémy tak, aby v případě havárie, porušení integrity nebo zničení dat byla obnovena jejich dostupnost v čase určeném viz IT.

[1] Pokud jsou takové kodexy pro organizaci závazně stanoveny, viz článek 40, Nařízení EU 2016/679.

4.2 Řízení přístupových práv

Přístupová práva uživatelů ICT přiděluje:

1) ředitelka na základě Plánu přístupových práv uživatelů, který schvaluje
2) ředitelka je oprávněna rozhodnout o jednorázové změně v rozsahu práv, pokyn dá prokazatelnou formou a musí být vždy na dobu určitou.

Ředitelka 1x/rok přezkoumává správnost přidělených práv.

4.3 Zajištění mlčenlivosti

1) Doložka mlčenlivosti pro zaměstnance, viz příloha č. 1, musí být obsahem pracovních smluv a dohod se zaměstnanci, stážisty, brigádníky atp., mlčenlivost jiných subjektů (třetích stran) je definována v příloze č. 4.
2) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů a předávání informací oprávněným osobám uvedených v Registru agend.

4.4 Pravidla pro zabezpečení prostor

Za klíčový režim a další zabezpečovací systémy (EZS atp.) odpovídá ředitelka. Vede všechny související záznamy o přidělování, vracení klíčů popř. kódů.

Zaměstnanec je povinen:

1) při opuštění prostor s OÚ uzamknout dveře a zavřít okna,
2) nezanechat neoprávněnou osobu v prostorách s OÚ bez dozoru,
3) neumožnit neoprávněné osobě (úklid, údržba atp.) bez dozoru přístup do prostor kde jsou nezabezpečené OÚ,
4) nosit odděleně služební klíče od osobních klíčů,
5) uzamknout vchod do budovy při odchodu ze zaměstnání 30 min. po skončení obvyklé pracovní doby,
6) okamžitě nahlásit vedoucímu ztrátu klíčů,
7) zaměstnancům je zakázáno pořizovat duplikáty klíčů (k této činnosti je oprávněn pouze ředitelka)
8) vstupovat do prostor, které nesouvisí s výkonem jeho práce dle pracovní náplně.

5 Zvláštní pravidla pro nakládání s OÚ

5.1 Souhlas se zpracováním OÚ

1. Souhlas subjektu OÚ se zpracováním OÚ musí být odlišitelný od jiných skutečností a musí obsahovat informace o tom, kdo souhlas dává, jaký je účel zpracování, ke zpracování kterých osobních údajů je souhlas dáván (např. jméno, bydliště, kontaktní údaje atp.), jakému správci (komu je souhlas dáván – název a kontaktní údaje organizace) a na jaké období (např. na 1 rok, po dobu trvání účelu zpracování atp.).
2. Souhlas subjektu OÚ eviduje odpovědná osoba. Poskytnutí souhlasu musí být Organizace schopna prokázat po celou dobu zpracování osobních údajů.
3. Organizace musí přiměřeným způsobem ověřit identitu toho, kdo souhlas dává a odvolává.
4. Subjekt údajů může souhlas kdykoliv odvolat, v tom případě musí být zpracování OÚ ukončeno.
5. Odvolání souhlasu musí být pro subjekt údajů stejně snadné jako jeho poskytnutí. Záznam o odvolání souhlasu eviduje odpovědná osoba.
6. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Odvolání souhlasu tedy nemá účinky zpětně, a netýká se zpracování, které bylo na základě platného souhlasu učiněno až do momentu jeho odvolání.

5.2 Pořizování audiovizuálních záznamů

1. Zveřejňování obrazových materiálů z akcí je bez písemného souhlasu subjektů OÚ možné za podmínek, kdy:

a. nejde o systematické zpracování, tzn. k zobrazeným či zaznamenaným osobám nejsou systematicky přiřazovány další osobní údaje a nejsou na základě toho vytvářeny další evidence,
b. nejedná se o momentky, znevažující záznamy a je časově omezené,
c. nemá jiný účel než informační a nepoukazuje např. na nějaké citlivé údaje jako je rasa, národnost atd.,
d. subjekty OÚ o fotografování vědí, nebo mohou vědět, aby měly možnost ho vyloučit.
e. není určeno pro marketingové využití (např. náborový leták k přilákání nových uchazečů atp.) a slouží tedy výhradně k dokumentaci a informaci o akci (nikoliv o jednotlivém člověku),
f. zveřejňování obrazových je pouze na vlastních informačních médiích (např. web, Facebook, informační leták atp.) nebo podle tiskového zákona.

2. Podle občanského zákoníku je pořizování a zveřejňování fotek z akcí možné bez souhlasu osob podle § 89 – tzn., jedná se o „obdobné zpravodajství“.

5.3 Nakládání s osobními údaji dle zákona o svobodném přístupu k informacím

1. Osobní údaje poskytne ředitel žadateli o informace výhradně se souhlasem fyzické osoby, které se týkají.
2. Není-li takový souhlas k dispozici, musí být osobní údaje u poskytnutých informací vhodnou formou anonymizovány. Toto ustanovení platí také pro žádost o informace zveřejněné na webových stránkách.

6 Řešení incidentů

1) Každý zaměstnanec včetně Správce ICT je povinen ohlásit ředitelce jakoukoliv událost, která má nebo by mohla mít vliv na bezpečnost OÚ.
2) Ředitelka dokumentuje tato oznámení v Knize incidentů včetně skutečností týkajících se daného porušení a příčin, jejich odstranění a přijetí nápravných/preventivních opatření.
3) Ředitelka provádí ve spolupráci s POOÚ kategorizaci všech incidentů takto:
    a) Incident - je jedna nebo více nechtěných nebo neočekávaných událostí, u kterých existuje pravděpodobnost kompromitace činnosti a možného ohrožení bezpečnosti OÚ bez zjevného dopadu na subjekty OÚ,
    b) závažný incident - je incident s velkou pravděpodobností následku, nebo následkem pro práva a svobody subjektů dotčených OÚ.
4) POOÚ je povinen bezodkladně a vhodným způsobem ohlásit každý závažný incident v oblasti zabezpečení osobních údajů dozorovému úřadu (ÚOOÚ) nejpozději do 72 hod. od zjištění incidentu. Ohlášení porušení ochrany osobních údajů se podá na formuláři, viz příloha č. 3 nebo pomocí webového formuláře ÚOOÚ.
5) Ředitelka je povinna bezodkladně a vhodným způsobem ohlásit každý závažný incident v oblasti zabezpečení OÚ postiženým subjektům údajů. Oznámení není nutné při splnění podmínek čl. 34, odst. 3 GDPR.

7 Informační povinnost - žádosti subjektů OÚ

7.1 Informační povinnost správce

1) Ředitelka odpovídá za zveřejnění údajů o rozsahu a způsobu zpracování na webu organizace (v souladu s čl. 12 – 14 GDPR). Tyto informace jsou poskytovány v případě, že jsou získány od subjektu OÚ nebo z jiných zdrojů a musí být poskytnuté před zpracováním OÚ.

2) Informace podle odst. 1 musí obsahovat:
    a) kontaktní údaje správce a kontaktní údaje pověřence pro ochranu osobních údajů,

b) účel zpracování, pro které jsou osobní údaje určeny, a právní základ (zákonnost) pro zpracování,
c) případné příjemce nebo kategorie příjemců osobních údajů,
d) právo subjektu OÚ odvolat kdykoli souhlas, který pro zpracování OÚ dal, podat stížnost u dozorového úřadu a právo požadovat od správce přístup k osobním údajům, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování a právo na přenositelnost údajů,
e) případný úmysl správce předat osobní údaje do třetí země.

3) Další informace, nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů správce nemusí poskytovat.

7.2 Žádosti subjektů OÚ

1) Subjekt údajů má právo (v souladu s čl. 16 – 20 GDPR) získat od Správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:
   a) účely zpracování;
   b) kategorie dotčených osobních údajů;
   c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;
   d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
   e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
   f) právo podat stížnost u dozorového úřadu;
   g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
   h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a informace týkající se použitého postupu;

2) Správce poskytne na žádost subjektu OÚ kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může účtovat přiměřený poplatek na základě administrativních nákladů. Právem získat kopii uvedenou nesmějí být nepříznivě dotčena práva a svobody jiných osob.

3) Na žádosti subjektů OÚ odpoví ředitel viz formulář uvedený v příloze č. 2. Žádost musí být vyřízena bez zbytečného odkladu, nejdéle do 30 dnů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

4) Žádosti a záznamy s ní související vede ředitelka v Knize žádostí,

8 Přenesení oprávnění a odpovědností na třetí strany

1. Pokud je pro Správce nezbytné určit Zpracovatelem nebo jinou Oprávněnou osobou třetí stranu (např. dodavatele ICT služeb, úklid atp.), musí zvážit související rizika a zabezpečit přenesení relevantních povinností, kompetencí a odpovědností vyplývajících z této směrnice a do písemného smluvního ujednání, které mj. obsahuje:
   a. technické a organizační podmínky zpracovávání OÚ u dodavatele včetně:
      1) způsobu a rozsahu zpracování OÚ,
      2) rozsahu a formy (typy) přístupu k informacím a způsobu validace přístupu,
      3) stanovení minimálních bezpečnostních požadavků na zabezpečení informací,
      4) způsobu zajištění integrity informací poskytovaných nebo procesovaných dodavatelem,
      5) způsobu řešení incidentů,
      6) způsobu a rozsahu vedení záznamů souvisejících se zpracováním OÚ,
      7) možnosti auditu/kontroly u dodavatele,

8) nouzových plánů pro zajištění dostupnosti informací nebo služeb poskytovaných dodavatelem,
9) způsobu a rozsahu přenesení sjednaných odpovědností na zaměstnance dodavatele, další subdodavatele atp.

b. doložku (ustanovení) o mlčenlivosti třetích stran viz příloha č. 4.,
c. odkaz na kodexy a pravidla chování, které musí být dodavatel povinen dodržovat[2].

2. Smlouvy musí jednoznačně stanovit, zda má dodavatel právo využít při plnění zakázky další subdodavatele, v jakém rozsahu a za jakých podmínek, opačném případě musí smlouva dodavateli zakázat využití subdodavatelů[3].
3. Smlouvy s „jednorázovými" dodavateli (např. revizní technici, opraváři, poradci, úklid atp.), kteří by na základě jejich obsahu mohli získat přístup k osobním údajům, nebo k informačním majetkům Organizace, musí obsahovat Doložku (ustanovení) o mlčenlivosti třetích stran viz příloha č. 4.

9 Kontrolní a auditní činnost, řízení rizik

9.1 Kontrolní činnost

Kontrolní činnost:

1. Vedoucí zaměstnanci průběžně kontrolují vedení záznamů podle kap. 7, způsob zpracování OÚ a dodržování pravidel.
2. Kontrola a monitoring ICT činností provádí v rozsahu a způsobem podle Plánu monitoringu a kontrol.

9.2 Posouzení shody a řízení rizik

Ředitel provádí posouzení shody účelu zpracování s rozsahem a způsobem zpracování u každé agendy. Výsledek posouzení zaznamená v Registru agend. Posouzení umožňuje zejména přijímání dostatečných opatření ke zmírnění rizika zpracování.

1. <u>Prvotní posouzení</u>

V rámci posouzení úrovně rizika je nutné přihlížet k povaze, rozsahu, kontextu a účelům zpracování a zhodnotit, jestli zpracování představuje vysokou pravděpodobnost rizika pro práva a svobody fyzických osob. Je prováděno pro všechny agendy a je posuzováno, zda jde o:

a. systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
b. rozsáhlé zpracování zvláštních kategorií údajů,
c. rozsáhlé systematické monitorování veřejně přístupných prostorů,
d. zpracování, které ÚOOÚ označil, jako rizikové a
e. zpracování, u kterého existuje pravděpodobnost, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob (např. rizika uvedená ve strategii ICT).

Škála posouzení vlivu:

Hodnota rizika zpracování	Popis hodnocení
Nízké	Pokud není splněna žádná z výše uvedených podmínek (písm. a – e)
Vysoké	Pokud je splněna alespoň jedna z výše uvedených podmínek (písm. a – e)

Výsledky posouzení

[2] Pokud jsou takové kodexy stanoveny, viz článek 40, Nařízení EU 2016/679.
[3] Zákon 101/2000 Sb. §4, písm. j) a k), resp. Nařízení EU 2016/679 článek 4), bod 8).

Pokud jsou zaznamenaná vysoká rizika, musí být přijímána účinná opatření pro snížení rizikovosti při zpracování OÚ podle následující kapitoly „Analýza bezpečnostních rizik“.

2. Následné posouzení

Následné posouzení se provádí vždy při významných změnách ve způsobu zpracování a rozsahu zpracování OÚ, nejméně však 1x/3roky.

9.2.1 Analýza bezpečnostních rizik

Analýza rizik posuzuje bezpečnost při zpracování OÚ u všech oblastí, které jsou uvedeny ve Strategii rozvoje ICT. Za analýzu bezpečnostních rizik odpovídá ředitel. Provádí ji vždy, pokud je při posouzení vlivů na zpracování OÚ (viz předchozí kapitola) zjištěné vysoké riziko nebo alespoň 1x/rok.

1. Analýza rizik musí zohlednit hrozby působící na bezpečnost informací a posoudit slabá místa (úroveň zranitelnosti) v technickém a organizačním zabezpečení.
2. Pokud nejsou u jednotlivých oblastí zjištěna slabá místa v zabezpečení, je riziko hodnocené jako „Nízké“, které lze akceptovat, v opačném případě jako „Vysoké“. Na vysoká rizika jsou realizována opatření pro jejich snížení. Přijímaná opatření musí být přiměřená možnostem organizace a souměřitelná s cenou dopadů.
3. Pokud je i po přijetí možných opatření (technická, organizační) riziko hodnocené jako vysoké, musí být takové zpracování konzultováno s dozorovým orgánem (ÚOOÚ). Konzultace s dozorovým úřadem předchází (pokud je to možné) zpracování OÚ, tzv. předchozí konzultace.

9.3 Interní audit

Interní audit provádí Pověřenec pro ochranu osobních údajů nebo ředitelem pověřená osoba. IA má za účel prověření procesů a plnění pokynů pro zpracování osobních údajů a ověření dodržování přijatých technicko-organizačních opatření. O provedeném auditu musí být vyhotoven zápis s vyznačením návrhů pro zlepšení.

10 Související legislativa

- Zákon č. 101/2000 Sb. o ochraně osobních údajů;
- Nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (účinnost 25. květen 2018);
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě;
- Zákon č. 340/2015 Sb., o uveřejňování smluv a o registru smluv;
- Zákon č. 106/1999 Sb. o svobodném přístupu k informacím;
- Zákon č. 40/2009 Sb. Trestní zákoník (§180);
- Zákon č. 418/2011 Sb. o trestní odpovědnosti právnických osob;
- Zákon č. č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce

Další související legislativa (na základě které jsou OÚ zpracovávány) je uvedena v Registru agend.

11 Přílohy

11.1 Příloha č. 1 Doložka o mlčenlivosti zaměstnanců

Zaměstnanec/brigádník/stážista „je povinen/a zachovávat mlčenlivost o osobních údajích, se kterými se seznámil/a při výkonu své pracovní činnosti a rovněž o všech bezpečnostních opatřeních, jejichž zveřejnění by zabezpečení osobních údajů mohlo ohrozit. Zachovávat mlčenlivost je povinen/a i po skončení pracovního poměru/smluvené činnosti“.

11.2 Příloha č. 2 Odpověď na žádost subjektu OÚ

Odpověď na žádost subjektu OÚ			
Adresát - subjekt OÚ			
Žádost podána dne			
Popis žádosti / požadavku subjektu OÚ			
Odpověď – sdělení správce osobních údajů			
Zdůvodnění sdělení			
Seznam příloh			
Zpracoval		Dne	

11.3 Příloha č. 3 Ohlášení porušení ochrany osobních údajů

Ohlášení porušení ochrany osobních údajů			
Správce osobních údajů			
Jméno a kontaktní údaje pověřence			
Popis incidentu/jeho povahy			
Popis pravděpodobných důsledků			
Popis příčin			
Důvod odkladu zaslání oznámení (déle než 72 hod)			
Popis přijatých opatření			
Kategorie OÚ		Přibližný počet dotčených subjektů	
Datum a čas vzniku		Přibližný počet dotčených záznamů	
Zpracoval		Dne	

11.4 Příloha č. 4 Doložka o mlčenlivosti třetích stran

Pro účely této doložky se rozumí Objednatelem Správce OÚ a Poskytovatelem Zpracovatel OÚ.

„Zpracovatel OÚ se zavazuje, že její zaměstnanci, a pokud to tato smlouva výslovně umožňuje, další subdodavatelé a jejich zaměstnanci, nebudou neoprávněně a mimo smluvní ujednání nakládat s osobními údaji, se kterými přijdou v rámci plnění předmětu smlouvy do styku. Nebudou zcizovat a zpřístupňovat informace o činnosti, systému řízení a kontroly, které se vztahují ke Správci OÚ. Stejně tak zachovají mlčenlivost o všech skutečnostech a bezpečnostních opatřeních na ochranu informací, se kterými se seznámí při své činnosti v rámci plnění předmětu této smlouvy a nebudou vyvíjet žádnou činnost, která nesouvisí s předmětem této smlouvy.

Zpracovatel OÚ je odpovědný i za zcizení nebo zpřístupnění informací třetí straně nebo osobám, které nejsou zainteresovány na výkonu předmětu činnosti této smlouvy z nedbalosti.

Zpracovatel OÚ, ani její zaměstnanci nesmí bez vědomí a prokazatelného souhlasu Správce OÚ, pořizovat žádné kopie dat včetně testovacích dat a informací, k nimž získají přístup na základě plnění předmětu smlouvy.

Zpracovatel OÚ je povinen dodržovat ustanovení smlouvy, zákon č. 101/2000 Sb. a Nařízení EU 2016/679 a v případě jejich porušení nese plnou odpovědnost s tím, že je povinna uhradit Správci OÚ smluvní pokutu ve výši 500,- Kč za každé takové porušení.

Zpracovatel OÚ seznámí s podmínkami smlouvy všechny své zaměstnance, kteří získají nebo mohou získat přístup k informacím Správce OÚ.

Správce OÚ má právo provést kontrolu u Zpracovatele OÚ a rovněž má právo odmítnout přístup k informacím a informačním zařízením zaměstnancům Zpracovatele OÚ, kteří neprokáží potřebné znalosti nebo jejichž chování bude v rozporu s předmětem této smlouvy nebo obecně závazných právních předpisů, aniž by to Zpracovatelem OÚ bylo považováno za porušení potřebné součinnosti ze strany Správce OÚ.

Tímto ustanovením není dotčeno právo Správce OÚ požadovat náhradu vzniklé škody, která může zaviněním Zpracovatelem OÚ nebo jeho zaměstnance vzniknout Správci OÚ“.

V Hlušicích dne 17. 5. 2018

(běžné razítko)

(podpis)
PaedDr. Marcela Vaňková, ředitel školy