SMĚRNICE ŘEDITELE ŠKOLY Č. 1

O řádném zacházení s osobními údaji a dodržování předpisů na ochranu osobních údajů

Datum vydání:	**23.5.2018**
Datum účinnosti:	24. 5. 2018
Určeno:	- všem zaměstnancům Správce, - osobám, které jsou vůči Správci v obdobném poměru jako zaměstnanci, - dalším osobám, které na pokyn Správce zachází s osobními údaji
Dozorový orgán:	Úřad pro ochranu osobních údajů - www.uoou.cz

---

Článek 1
Preambule

1. Vnitřní organizační směrnice O řádném zacházení s osobními údaji a dodržování předpisů na ochranu osobních údajů (dále jen „**Směrnice**“) je vydávána za účelem konkretizace povinností vyplývajících („**Správce**“) z předpisů na ochranu osobních údajů – zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), dále také jako jen „**GDPR**“ a navazující legislativy k GDPR.

Článek 2
Působnost směrnice

1. Tato směrnice upravuje postupy školy (jako správce osobních údajů), jejích zaměstnanců, případně dalších osob, při zpracování osobních údajů, a upravuje dále pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů. Směrnice rovněž upravuje některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji.

2. Doporučené postupy se vztahují na zpracování osobních údajů všech kategorií subjektů osobních údajů, které byly identifikování v rámci organizace Správce.

3. Směrnice je závazná pro všechny osoby v zaměstnaneckém či obdobném poměru vůči Správci, a to vč. osob, které nejsou zaměstnanci, avšak na základě pokynů správce zpracovávají osobní údaje (dále jen souhrnně jako „**zaměstnanci Správce**“).

Článek 3
Vymezení základních pojmů

1. Osobní údaj (čl. 4 odst. 1 GDPR)
    a. Jakákoli informace o **identifikované** nebo **identifikovatelné** fyzické osobě (dále jen „subjekt údajů“);
    b. Za identifikovatelnou fyzickou osobou se považuje 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.

2. Správce osobních údajů (čl. 4 odst. 7 GDPR)
    a. fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení

3. Subjekt osobních údajů
    a. Nositel práv plynoucích z koncepce ochrany osobních údajů (čl. 12 a násl. GDPR) – jedná se o fyzickou osobu, které se týkají konkrétní zpracovávané osobní údaje.
    b. Hlavní kategorie subjektů osobních údajů, které v rámci organizace Správce existují:
        i. děti/žáci/studenti,
        ii. zaměstnanci,
        iii. dodavatelé/odběratelé služeb.

4. Zvláštní kategorie osobních údajů - citlivé osobní údaje (čl. 9 GDPR)
    a. Zvláštní kategorii osobních údajů jsou takové informace, které mohou zapříčinit zhoršení postavení subjektu osobních údajů ve společnosti, či vést k jeho diskriminaci → při jejich zneužití je riziko vyššího zásahu do základní lidských práv a svobod.
    b. Jedná se o údaje, které vypovídají o:
        i. rasovém či etnickém původu,
        ii. politických názorech,
        iii. náboženském vyznání či filozofickém přesvědčení,
        iv. členství v odborech,
        v. zpracování genetických údajů či biometrických údajů za účelem jedinečné identifikace,
        vi. údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

5. Zpracování osobních údajů (čl. 4 odst. 2 GDPR)
    a. Jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů, a to pomocí či bez pomoci automatizovaných postupů
        i. automatizovanými postupy jsou procesy, při nichž dochází k využívání nástrojů výpočetní technologie.
    b. Za zpracování se tak považuje zejména:
        i. shromáždění,
        ii. zaznamenání,
        iii. uspořádání,
        iv. strukturování,
        v. uložení,
        vi. přizpůsobení nebo pozměnění,
        vii. vyhledání,
        viii. nahlédnutí,
        ix. použití,
        x. zpřístupnění přenosem,
        xi. šíření nebo jakékoliv jiné zpřístupnění,
        xii. seřazení či zkombinování,
        xiii. omezení,
        xiv. výmaz nebo zničení.

6. Pseudonymizace osobních údajů
    a. Zpracování osobních údajů takovým způsobem, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě,
    b. Příkladem pseudonymizace je zveřejňování výsledku z přijímacího řízení za použití kódu dítěte/žáka/studenta.

7. Anonymizace osobních údajů
    a. Zpracování osobních údajů takovým způsobem, kdy informace v původním tvaru, či po provedeném zpracování, již nelze vztáhnout k identifikovanému či identifikovatelnému subjektu.

Článek 4
Základní principy

1. Škola v postavení správce údajů zpracovává osobní údaje několika kategorií subjektů osobních údajů. Seznam činností, při nichž dochází ke zpracování osobní údajů je uveden v závěrečné zprávě auditu GDPR. Součástí této Směrnice je i legislativní rámec, který upravuje ochranu osobních údajů. Tento rámec předpisů bude průběžně kontrolován pověřencem pro ochranu osobních údajů.

2. Při nakládání s osobními údaji se zaměstnanci Správce řídí následujícími zásadami:
    a. Dodržovat základní pravidla dobré správy – k subjektům osobních údajů a jejich zástupcům se chovat zdvořile a podle možností jim vycházet vstříc,
    b. Umožnit všem subjektům osobních údajů řádné uplatňování jejich práv - rovnocenně, a žádného z nich nediskriminovat,
    c. Postupovat při nakládání s osobními údaji v souladu s právními předpisy (zásada zákonnosti),
    d. S osobními údaji nakládat pouze v minimálně nezbytném rozsahu (zásada minimalizace),
    e. Souhlas se zpracováním osobních údajů nenadužívat a nevyžadovat ho pro případy, kdy Správci svědčí jiný právní titul ke zpracování (např. plnění právní povinnosti),
        i. Jakýkoli souhlas se zpracováváním osobních údajů musí být Správce schopen jednoznačně prokázat, a to po celou dobu zpracovávání.
    f. Zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu (zásada omezení účelu),
    g. Zajistit, aby zpracovávané osobní údaje byly vedeny v přesné a aktuální podobě (zásada přesnosti),
    h. Zpracovávat osobní údaje v souladu se zásadou zákonnosti – tj. pouze na základě povinností z právních předpisů, na základě plnění smlouvy, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména děti požívají vyšší ochrany), při ochraně oprávněných zájmů školy, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,
    i. Respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování, dále viz čl. 12 a násl. GDPR,
    j. Poskytovat při zpracování osobních údajů zvláštní ochranu dětem – osobám mladším 18 let,

k. Poskytovat veškerá vysvětlení a informace o zpracování osobních údajů srozumitelně, jasně, transparentním způsobem, komunikovat otevřeně a sdělovat veškeré informace pravdivě,
l. Při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,
m. Spolupracovat s pověřencem pro ochranu osobních údajů,
n. Spolupracovat s Úřadem pro ochranu osobních údajů.

3. Osobní údaje mohou být zpracovávány pouze po dobu nezbytně nutnou k plnění účelu jejich zpracovávání a/nebo po dobu nezbytné archivace. Pomine-li účel, pro který byly osobní údaje zpracovávány nebo uplynula zákonná doba pro jejich archivaci, zpracovávání takových osobních údajů musí být ukončeno. Zaměstnanci Správce jsou povinni průběžně kontrolovat dobu zpracování. Zjistí-li, že osobní údaje již nejsou potřebné k deklarovanému účelu nebo uplynula povinná doba jejich archivace, po konzultaci s pověřencem pro ochranu osobních údajů zajistí jejich řádnou likvidaci. Doba zpracování jednotlivé dokumentace je určena především spisovým a skartačním řádem Správce. Po uplynutí této doby mohou být osobní údaje zpracovávány pouze v anonymizované podobě – např. pro statistické či vědecké účely.

4. Správce uchovává osobní údaje následujících kategorií subjektů osobních údajů:
   a. O zaměstnanci či jiném smluvním pracovníkovi v jeho osobním spisu, jehož nedílnou součástí jsou podklady pro výpočet platu,
   b. O dítěti / žákovi / studentovi v evidenci žáků (školní matrika dle § 28 školského zákona) nebo v dokumentech vedených v souladu s ustanovením školského zákona, nebo v dokumentech, které plní obdobnou funkci za účely vedení pedagogické agendy,
   c. O zákonném zástupci dítěte/žák/studenta ve spisu založeném v rámci přijímání žáka ke vzdělání, v katalogovém listu žáka nebo v materiálu, který plní obdobnou funkci v mateřské škole, školní družině, jídelně a v matrice školy,
   d. O dodavatelích / odběratelích služeb v evidencích smluv vč. podkladů pro účetnictví.

5. Správce je oprávněn shromažďovat osobní údaje toliko za účelem, pro který jsou prokazatelně zpracovávány, a v takovém rozsahu, v jakém je to nezbytně nutné.

Článek 5
Obecné povinnosti zaměstnanců Správce

1. Každý zaměstnanec Správce při nakládání s osobními údaji respektuje povahu osobních údajů – že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí veškerá jednání s tím spojené.

2. Zaměstnanci Správce jsou při použití či jiném nakládání s osobními údaji, v rámci plnění svých pracovních úkolů, povinni chovat se tak, aby byla zajištěna ochrana lidské důstojnosti subjektů údajů. Dále jsou zaměstnanci povinni postupovat tak, aby údaje, s nimiž pracují, nemohly být odcizeny nebo zneužity k neoprávněným zásahům do soukromého či osobního života subjektů údajů. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokáží právo s nimi nakládat. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; jinak odkáže na ředitele školy nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů.

3. Zaměstnanci Správce jsou povinni se seznámit s informacemi, jakým způsobem a formou učinit nezbytná sdělení pro subjekty osobních údajů.

4. Každý zaměstnanec Správce, který s osobními údaji přichází do styku, je povinen zpracovávat pouze přesné osobní údaje, které byly získány v souladu s předpisy na ochranu osobních údajů. Pokud zaměstnanec Správce při nakládání s osobními údaji zjistí, že údaje nejsou s ohledem na stanovený účel řádně zpracovány, provede bez zbytečného odkladu nápravu a nezbytná opatření – např. omezení zpracování, doplnění údajů, pozastavení zpracování nepřesného osobního údaje. Nebude-li toto možné, po konzultaci s pověřencem pro ochranu osobních údajů provede likvidaci.

5. Zaměstnanci Správce jsou povinní pověřenci pro ochranu osobních údajů ihned oznámit každý bezpečnostní incident týkající se osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, především konkrétního žáka, studenta, zaměstnance, zákonného zástupce atd., bezodkladně tuto osobu informuje o nastalém incidentu vč. jeho popisu a sdělí, jaká opatření k nápravě byla přijata. O každém incidentu se sepíše záznam. O každém závažném incidentu Správce informuje Úřad pro ochranu osobních údajů (www.uoou.cz).

6. Zaměstnanci Správce všechny osobní údaje, které Správce zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Osobní údaje uchovávají v prostorách, na místech, v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený a v každý okamžik alespoň řediteli školy známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením ředitele školy nebo jím pověřené osoby.

7. Za ochranu osobních údajů odpovídá Správce osobních údajů, který je povinen provádět ve spolupráci s pověřencem pro ochrnu osobních údajů kontrolní činnost, při které průběžně ověřuje, zda je s osobními údaji nakládáno v souladu s předpisy na ochranu osobních údajů, jakož i v souladu s touto Směrnicí. Za ochranu dat a osobních údajů odpovídá rovněž každý zaměstnanec Správce, který v rámci výkonu své pracovní náplně zachází s osobními údaji.

Článek 6
Organizační a technická opatření k ochraně osobních údajů

1. Dokumenty v listinné nebo digitální podobě podléhají režimu spisového a skartačního řádu. Při práci s takovými dokumenty postupuje zaměstnanec Správce se zvýšenou opatrností. K dokumentům mají přístup pouze zaměstnanci, kteří je nezbytně potřebují při výkonu své pracovní činnosti. Veškeré dokument obsahující osobní údaje musí být zabezpečeny před odcizením, zneužitím či neoprávněném zpřístupněním.

2. Každý zaměstnanec Správce má povinnost zachovávat mlčenlivost o všech skutečnostech, které se týkají osobních údajů, s nimiž v rámci výkonu své práce přichází do styku, jakož i o aplikovaných bezpečnostních opatřeních. Tato mlčenlivost se vztahuje i na dobu po ukončení pracovněprávního nebo jiného obdobného vztahu vůči Správci. Mlčenlivosti může být zbaven pouze v zákonem předvídaných situacích – např. na pokyn orgánu veřejné moci.

3. Každý zaměstnanec Správce má povinnost zachovávat co nejvyšší standard ochrany osobních údajů, s nimiž v rámci výkonu své práce přichází do styku.

4. Dokumenty obsahující evidence žáků (třídní výkazy, katalogové listy a další materiály ze školní matriky), musí být trvale uloženy v uzamykatelných boxech/skříních v kanceláři vedení školy - v kanceláři ředitele / zástupce ředitele. Třídním učitelům mohou být dokumenty toliko zapůjčeny, a to na nezbytně nutnou dobu k provedení potřebných zápisů. Vyučující jednotlivých předmětů zapisují pouze klasifikační údaje a zásadně v kanceláři ředitele nebo zástupce ředitele.
    a. Evidence žáků by měla obsahovat pouze nezbytné osobní údaje, které předvídá právní řád – viz § 28 školského zákona.

5. V propagačních materiálech školy (výroční zprávy, ročenka školy, internetové stránky, veřejně přístupné nástěnky apod.) lze se souhlasem ke zpracování uděleného žákem nebo jeho zákonným zástupcem uveřejňovat osobní údaje v rozsahu stanoveném v souhlasu. Při publikování v tisku se autor dotazuje na souhlas příslušného žáka nebo zákonného zástupce. Žák nebo zákonný zástupce má práva podle čl. 12 a násl. GDPR – zejm. požadovat omezení zpracování, odstranění informace či fotografie / video-záznamu týkající se jeho osoby, který nadále nechce zveřejňovat, přístup k osobním údajům apod. viz níže v textu Směrnice.

6. Zaměstnanci Správce jsou povinni zajistit, že třídní výkaz, katalogové listy a další materiály ze školní matriky či jejich části, nebudou vynášeny z budovy školy (určených kanceláří), neoprávněně předávány cizím osobám nebo kopírovány a kopie poskytovány neoprávněným osobám.

7. Zaměstnanci Správce nesmí poskytovat bez právního důvodu žádnou formou osobní údaje ostatních zaměstnanců Správce a dětí / žáků / studentů cizím osobám a institucím, tj. ani telefonicky ani mailem ani při osobním jednání.

8. Seznamy žáků se nezveřejňují, neposkytují bez vědomého souhlasu žáků či zákonných zástupců žáků jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného škole nebo nevyplývá-li to ze zákona.

9. V případě, že si některý orgán veřejné moci (např. soud, OSPOD, PČR apod.) vyžádá určité informace o zaměstnanci / dítěti / žákovi / studentovi, mohou být takového informace poskytnuty pouze v rozsahu nezbytně nutném pro splnění účelu a formou prokazatelné a zabezpečené komunikace – datovou schránkou. Je zakázáno poskytovat jakékoli informace o subjektech osobních údajů prostřednictvím telefonu, e-mailu, osobně.
    a. Písemná hodnocení a posudky, která se odesílají pro potřeby orgánů veřejné moci (soudního řízení), přijímacího řízení, zpracovávají zaměstnanci Správce výslovně pověření ředitelem školy. Tito zaměstnanci však nejsou oprávněni samostatně hodnocení podepisovat, poskytovat a odesílat jménem školy.

10. Správce vede školní matriku dětí / žáků / studentů také v elektronické školní matrice. Povinností Správce je zabezpečit informační systém elektronické matriky.
    a. Do elektronického systému mají přístup pedagogičtí pracovníci. Jiné osoby pouze s výslovným a písemným pověřením ředitele školy, a to jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením.
    b. Každý, kdo má přístup do elektronické evidence může pracovat pouze s daty a takovým způsobem, jaký odpovídá jeho funkčního zařazení a pracovní náplně – aplikace řízeného přístupu k osobním údajům.
    c. Při práci s elektronickou evidencí musí být dodržovány základní pravidla práce s ICT prostředky:
        i. Zaměstnanci Správce nesmí opouštět počítač bez odhlášení se,
        ii. Není přípustné nechat nahlížet do evidence jinou osobu
        iii. Zaměstnanci Správce musí zabezpečit důvěrnost (utajení) přihlašovacích údajů do elektronické evidence; a v případě nebezpečí jeho vyzrazení jej ihned (ve spolupráci se správcem sítě) změnit.
        iv. Přihlašovací heslo musí být dostatečně silné – alespoň 8 znaků, obsahovat kombinaci velkých a malých písmen a speciální znaky (např. 1AzaK5KL#).
        v. Je nezbytné měnit heslo cca 90 až 120 dnech.
        vi. Přístupy do systémů nastavuje pověřený zaměstnanec, který nastavuje potřebné zabezpečení dat a školní počítačové sítě. Zákonní zástupci žáků a žáci mají zajištěn zabezpečený dálkový přístup výhradně k vlastním údajům o klasifikaci na základě přihlašovacího kódu a hesla.

vii. V případě, že je využíván externí dodavatel dalších služeb, je zakázáno takové osobě sdělovat přihlašovací údaje k evidenci, ledaže je její přístup nezbytný pro vykonávání poskytovaných služeb.

11. Personální spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři ředitele školy / pověřené osoby. Přístup k nim má toliko ředitel školy nebo zástupce ředitele, případně, je-li to potřebné k výkonu práce též sekretářka školy nebo mzdová účetní.

12. Každý zaměstnanec má právo uplatnit přístup k osobním údajům a seznámit se tak s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni v prohlášení o ochraně osobních údajů.

13. Kamerové systémy
    a. Nezáznamové kamerové systémy v souladu se stanoviskem Úřadu pro ochranu osobních údajů nejsou regulovány předpisy na ochranu osobních údajů. Přesto je nezbytné dodržovat základní pravidla ochran soukromí a osobnosti sledovaných osob.
    b. V případě, že se Správce rozhodne užívat záznamový kamerové systém, je nezbytné dodržovat následující zásady:
        i. kamerový systém musí být až posledním prostředkem (*ultima ratio*), jak zajistit daný účel (např. střežené prostory nelze monitorovat přímým dohledem prováděným namátkově zaměstnancem)
        ii. je nutné vyhotovit tzv. záznamy o činnostech zpracování podle čl. 30 GDPR
        iii. záznam by měl být ukládán pouze po nezbytně nutnou dobu, nejdéle několik dní (1 až 3 dny)
        iv. bezpečnostní kamery musí směřovat pouze na místa, kde není nepřiměřeným způsobem zasahováno do soukromí osob (nelze nahrávat WC vč. vstupů, prostory kde dochází k převlékání, osobní kanceláře zaměstnanců apod.)
        v. měla by být dodržována vnitřní směrnice pro zacházení s bezpečnostními kamerami
        vi. právním důvodem pro využívání bezpečnostních kamer může být pouze i) článek 6 odst. 1 písm. f) GDPR – oprávněné zájmy (zaměstnanci, jiné osoby navštěvující budovu) v kombinaci s ii) článkem 6 odst. 1 písm. f) GDPR – souhlas se zpracováním osobních údajů (pro žáky)

14. Uzavírá-li Správce jakoukoli smlouvu (o poskytování služeb, o zajištění likvidace dokumentů, smlouvu o dílo, jinou nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, Správce vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:
    a. dodržovat příslušná pravidla této Směrnice,
    b. ve smlouvě, která je základem závazkového vztahu začlenit text této Směrnice do přílohy,
    c. zpracovávat předávané osobní údaje pouze pro účely plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím),
    d. přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení či zneužití předávaných osobních údajů,
    e. bez předchozího písemného souhlasu Správce nezapojit do zpracování žádné další osoby,
    f. zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele (zaměstnanci) byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
    g. zajistit, že smluvní strana bude Správci bez zbytečného odkladu nápomocna při plnění povinností Správce, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 GDPR, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 GDPR a povinnosti provádět předchozí konzultace dle čl. 36 GDPR, a že za tímto

účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých informuje Správce,

h. po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je bezpečně předá v kompletní podobě zpět Správci, příp. vymaže existující kopie apod.,
i. poskytnout Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené předpisy na ochranu osobních údajů,
j. umožnit kontrolu, audit či inspekci prováděné Správcem nebo příslušným orgánem dle právních předpisů, a to za účelem kontroly dodržování povinností plynoucích ze smlouvy a předpisů na ochranu osobních údajů,
k. poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou určí Správce, součinnost potřebnou pro plnění zákonných povinností spojených s ochranou osobních údajů,
l. osobním údajům zajistit odpovídající standard ochrany – zejm. důvěrnost a nedotknutelnost.

15. Doporučená technicko-organizační opatření jsou Přílohou č. 1 této Směrnice

16. K osobním údajům mají v rámci organizace Správce přístup jen osoby k tomu oprávněné zákonem nebo na základě zákona. Do jednotlivých dokumentů Správce, které obsahují osobní údaje, mohou nahlížet:
    a. do osobního spisu zaměstnance - vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni, nebo zaměstnanci výslovně pověření z důvodu výkonu jejich pracovní činnosti. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. 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,
    b. do údajů žáka ve školní matrice pedagogičtí pracovníci školy (v rozsahu daném pedagogickou funkcí), sekretářka,
    c. do údajů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv - výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel,
    d. do spisu, vedeném ve správním řízení účastníci správního řízení, sekretářka, vedoucí pedagogičtí pracovníci (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

Článek 7
Práva subjektů osobních údajů

1. Právo na informace
    a. Subjekty osobních údajů musí být informování o skutečnostech, které se týkají procesů zpracování osobních údajů, a to v rozsahu stanoveném čl. 13 a násl. GDPR. Za tímto účelem byl Správcem vydán souhrnný dokument „Prohlášení o ochraně osobních údajů“, který je v elektronické podobě dostupný na internetových stránkách Správce a v tištěné podobě v budově sídle Správce.
    b. Každý zaměstnanec Správce je povinen na žádost subjektu osobních údajů zajistit, že tento bude s Prohlášením o ochraně osobních údajů patřičně seznámen.
    c. Správce zajistí, že jeho zaměstnanci, v postavení subjektů osobních údajů, budou s Prohlášením taktéž seznámeni.
    d. Informace o zpracování osobních údajů vždy obsahuje údaje o:
        i. Osobních údajích, které Správce zpracovává, včetně informací o zdroji údajů,
        ii. Kopii osobních údajů,
        iii. Účelu zpracovávání,
        iv. Plánovaná doba zpracování,

v. Existence práva požadovat opravu nebo výmaz,
vi. Poučení o právu podat stížnost k dozorovému úřadu,
vii. Zda dochází k automatizovanému zpracovávání, příp. profilování,
viii. Příjemci, případně kategorie příjemců osobních údajů.

2. Právo odvolat souhlas
    a. Subjekt osobních údajů má právo kdykoli svobodně svůj souhlas se zpracováním údajů odvolat, a to min. stejným způsobem, jakým jej učinil.

3. Právo na přístup k osobním údajům
    a. Pokud subjekt osobních údajů uplatní své právo na přístup k údajům, ověří zaměstnanec Správce totožnost žadatele a je-li to možné, vyřídí žádost obratem (např. sdělí lokaci údajů, jaké údaje jsou o dotyčném shromažďovány apod.). V případě, že žádost nelze vyřídit zaměstnancem Správce, předá bezodkladně žádost k vyřízení pověřenci pro ochranu osobních údajů a o tomto subjekt osobních údajů obratem informuje.
    b. Žádost musí být vyřízena bezodkladně, jinak nejdéle do 30 dnů. O tomto musí být subjekt údajů zaměstnancem Správce poučen.

4. Právo na opravu a doplnění
    a. Zaměstnanci Správce jsou povinni dbát na pravdivost, aktuálnost a správnost shromažďovaných osobních údajů.
    b. Subjekt osobních údajů má právo žádat opravu nebo doplnění osobních údajů, které se ho týkají. Žádost může být vyřízena obratem u zaměstnance Správce po ověření totožnosti subjektu osobních údajů příp. jeho zákonného zástupce.
    c. Zjistí-li Zaměstnance Správce, že v evidenci osobních údajů došlo ke zjevnému překlepu, zajistí bezodkladnou opravu.

5. Právo na výmaz
    a. V případě, že nastane právním řádem předvídaná situace:
        i. Údaje již nejsou potřebné vzhledem k deklarovanému účelu (ledaže je zde zákonný požadavek archivace),
        ii. Subjekt osobních údajů odvolal souhlas se zpracováním údajů,
        iii. Byly vzneseny oprávněné námitky proti zpracování,

        Má subjekt osobních údajů právo na výmaz údajů v rozsahu, který požaduje.

Článek 8
Zpracování pomocí zpracovatele

1. Pokud není možné, aby zpracování osobních údajů bylo zajišťováno a prováděno přímo Správcem, nebo rozhodne-li se tak Správce, může být za účelem zpracování údajů uzavřena smlouva s externím dodavatelem služeb. Tato smlouva musí odpovídat požadavkům čl. 28 odst. 3 GDPR – tzv. zpracovatelská smlouva (viz článek 6 odst. 13 Směrnice). Součástí tohoto smluvního ujednání musí být odpovídající ustanovení o ochraně osobních údajů.

Článek 9
Zabezpečení IS školy

1. Přístup k osobním údajům mají pouze zaměstnanci Správce, kteří disponují příslušným pověřením / oprávněním. Taková činnost musí spadat do pracovní náplně daného zaměstnance. Nastavení přístupových práv, včetně jejich úrovně, provádí osoba odpovědná za správu IT.

2. U aplikací, které obsahují osobní údaje a neumožňují nastavení takových práv, je zabezpečení proti neoprávněnému přístupu na serverech zajištěno pomocí nastavení uživatelských práv na úrovni souborového systému serveru či stanice. Za splnění takové podmínky odpovídá správce IT.

3. Uchovávání datových nosičů obsahující osobní údaje definuje provozní řád IS Správce. Výjimku tvoří datové nosiče, které jsou součástí spisového archivu. Takové nosiče podléhají režimu spisového a skartačního řádu.

4. Datové soubory je nutné umisťovat pouze na jednotlivá PC uživatelů, kteří jsou oprávněny k nakládání s těmito soubory. Výjimku tvoří aplikace, jejichž instalace není možná jiným způsobem.

5. Není dovoleno uchovávání datových nosičů obsahující osobní údaje, které již nebudou využívány. O likvidaci takových nosičů se postará správce IT. Informatik je oprávněn vytvářet kopie datových nosičů obsahující osobní údaje pouze na základě konzultace s pověřencem pro ochranu osobních údajů.

6. Úroveň a hodnoty přístupových oprávnění každého zaměstnance jsou uvedeny na kartě zaměstnance. Ta obsahuje seznam aplikací obsahující osobní údaje a hodnoty uživatelských oprávnění, kterými zaměstnanec disponuje. Karta zaměstnance je vyplněna na základě obsahu pracovní náplně, které odpovídá funkčnímu zařazení každého zaměstnance Správce.

7. Nový zaměstnanec získá přístup k IS na základě vyplněné a podepsané karty zaměstnance. Podle této karty provede správce IT nastavení přístupových práv.

8. Při ukončení pracovního poměru zaměstnance je přístup k aplikacím obsahující osobní údaje zrušen a jsou deaktivovány všechny uživatelské účty tohoto zaměstnance. To provede bezodkladně správce IT. Ohledně těchto úkonů se provede zápis do karty zaměstnance, která je následně uložena.

9. Dojde-li při změně pracovní činnosti zaměstnance k změně pracovní náplně, která vyžaduje změnu úrovně oprávnění k aplikacím obsahující osobní údaje, musí být změněna též karta zaměstnance. Následně informatik školy provede úpravu přístupů zaměstnance k aplikacím obsahujícím osobní údaje tak, aby odpovídaly novým skutečnostem.

Článek 10
Mlčenlivost

1. Zaměstnanci Správce, kteří zpracovávají osobní údaje, jinak nakládají, či k nim mají přístup, jsou povinni zachovávat mlčenlivost o všech skutečnostech, které se v souvislosti se zpracováním osobních údajů dozvědí. Mlčenlivost se vztahuje též na všechna technicko-organizační opatření, která slouží k zachování důvěrnosti osobních údajů a pro jejich ochranu. Mlčenlivost trvá i po skončení pracovního poměru.

Článek 11
Porušení zabezpečení

1. Zjistí-li kterýkoli zaměstnanec Správce, že došlo k porušení zabezpečení osobních údajů, případně úniku osobních údajů, neprodleně o tom odešle zprávu odpovědnému zaměstnanci nebo pověřenci pro ochranu osobních údajů.

2. Pověřený zaměstnanec nebo pověřenec pro ochranu osobních údajů vyhodnotí riziko pro práva a svobody subjektů osobních údajů (nebo jiných fyzických osob), a vyhodnotí-li, že riziko existuje,

ohlásí tuto skutečnost nejpozději do 72 hodin od porušení zabezpečení Úřadu pro ochranu osobních údajů.

3. Pokud je riziko pro práva a svobody vysoké, zejm. pokud došlo k úniku hesel do dokumentů obsahující základní evidenci osobních údajů, zaměstnanci Správce vhodným způsobem informují subjekty osobních údajů.

Článek 12
Likvidace osobních údajů

1. Pomine-li účel, pro který byly osobní údaje získány a následně zpracovávány, je nutné jejich zpracovávání ukončit a následně provést jejich likvidaci, ledaže delší doba uchování je určena jiným právním předpisem nebo se jedná o výjimky dle čl. 17 odst. 3 GDPR.

2. Data, která jsou uchovávána na datových nosičích, jsou po uplynutí archivační doby řádně likvidována.

3. Data z přepisovatelných datových nosičů vymazána, nosiče, u kterých tento postup nelze provést, jsou likvidovány fyzicky takovým způsobem, aby je nebylo možné rekonstruovat.

4. Likvidaci osobních údajů provádí správce nebo na základě jeho pokynů zpracovatel. O každé likvidaci osobních údajů se provádí zápis, který je podepsán příslušným zaměstnancem Správce. Zápisy o provedené likvidaci jsou ukládány.

Článek 13
Závěrečná ustanovení

1. Tato směrnice je nedílnou součástí vnitřních norem Správce.

Směrnice nabývá účinnost dne: 24.5.2018

V Kunčině dne 25.5.2018

Mgr. Miloslava Hutirová
Ředitelka

Příloha č. 1: technicko-organizační opatření k zajištění bezpečného zpracování osobních údajů

Technická opatření

Osobní údaje zpracovávané v nedigitální podobě:

1. systematizované evidence osobních údajů (např. personální spisy, mzdové podklady, katalogové listy) fyzicky zabezpečit proti zneužití či úniku
    a. místnost, ve které jsou údaje ukládány, zabezpečit zámkem proti neoprávněnému vniknutí,
    b. klíče od dané místnosti poskytnout pouze osobám, které jsou oprávněny do místnosti vstupovat, či nakládat s osobními údaji,
    c. vytvořit seznam osob, které mají přístupové klíče,

2. v případě, že do místnosti, do které jsou osobní údaje ukládány, mají přístup i jiné osoby (např. nepedagogičtí pracovníci), než které jsou oprávněny do dokumentů s údaji nahlížet a pracovat s nimi, ukládat samotné evidence údajů ukládat do uzamykatelné skříně na dokumenty;

3. zavést systém řízeného přístupu do evidence údajů
    a. každý zaměstnanec by měl mít přístup pouze k takovým osobním údajům, které nezbytně potřebuje pro vykonávání svých povinností;
    b. neměl by tak mít zároveň umožněný přístup k osobním údajům, s nimiž nezbytně nepotřebuje zacházet (např. řadový učitel by neměl mít klíč od skříně s dokumenty, v nichž jsou personální spisy ostatních zaměstnanců);

4. evidovat osoby, které mají oprávnění přistupovat do evidencí osobních údajů vč. zaznamenávání samotného způsobu nakládání;

5. Omezit/zakázat přenášení jakékoliv části evidence mimo stanovenou místnost;

6. údaje o osobách (zejm. dětí) nezveřejňovat bez souhlasu se zpracováním osobních údajů na internetu;

7. evidence s osobními údaji vést na jednom místě (centrálně) → vyvarovat se dělení evidence a zároveň i odpovědnosti;

8. v případě zveřejňování osobních údajů (např. při vyvěšování výsledků z přijímacího řízení) zavést prvky pseudonymizace
    a. tj. identifikační údaje subjektů osobních údajů (typicky jméno a příjmení žáka) skrýt pod anonymní identifikátor – např. číslo přihlášky a pod tímto pseudonymizovaným identifikátorem je možné zveřejnit informace → např. „*č. P102 – dosaženo 15 bodů = přijat ke studiu*“
    b. výsledkem je tak zveřejnění informací, avšak v takové podobě, že nelze připojit jednotlivé informace (např. zda (ne)byla dotyčná osoba přijata ke studiu) přímo k identifikované fyzické osobě;

9. nastavit pravidla pro uchování aktuálního stavu osobních údajů - v případě evidence žáků na začátku roku vždy vyzvat zákonného zástupce, zda nedošlo ke změně osobních údajů, které škola eviduje o žácích a v případě, že ke změně došlo, aby byla bezodkladně nahlášena;

10. Fyzicky zabezpečit počítače před krádeží

11. Prevence ztráty mobilu / notebooku obsahující osobní údaje – blokace složek souborů obsahující osobní údaje pomocí hesla či šifrování

12. Zjistit a zlikvidovat nerelevantní osobní údaje (zásada minimalizace)
    a. V případě, že správce osobních údajů nemá souhlas se zpracováním, pak odstranit (případně anonymizovat) následující osobní údaje, které jsou Správcem zpracovávány:
        i. Zaměstnanci:
            1. národnost
            2. životopisy zaměstnanců a nepřijatých uchazečů,
            3. číslo občanského průkazu (dále „OP“),
            4. číslo průkazu pojištěnce vč. data uplynutí lhůty platnosti průkazu

13. Zaznamenat dobu platnosti zpracování (časovou délku) na dokumentu – řádným přiřazením spisových a skartačních znaků

14. Provádět náhodné kontroly administrativních úkonů zaměstnanců a dodržování výše uvedených pravidel.

Osobní údaje zpracovávané v digitální podobě:

1. Zajistit fyzické zabezpečení místnosti, ve které je uložen páteřní server („serverovna“), a to před neoprávněným vniknutím – vstupním zámkem na dveřích
    a. páteřní server tak umístit v místnosti, která je zabezpečena proti neoprávněnému vniknutí
    b. klíče od dané místnosti poskytnout pouze osobám, které jsou oprávněny do místnosti vstupovat, či nakládat s osobními údaji
2. Samotný server fyzicky ukládat do uzamykatelného nástěnného rozvaděče („rack“)
    a. rozvaděč následně instalovat do vyšší polohy
    b. klíče od rozvaděče poskytnout výlučně osobám, které jsou oprávněny se serverem zacházet (IT správce)
3. Zabezpečit PC stanice před neoprávněným použitím – při zapnutí PC vyžadovat heslo
    a. Nastavit odpovídající politiku hesel (min. 8 znaků, kombinace velká a malá písmena a číslice, speciální znaky vč. nastavení obměny hesla po uplynutí 90 dnů);
4. Přístupová hesla nesdělovat osobám, které nejsou oprávněny zacházet s PC (např. návštěvy, rodinní příslušníci zaměstnance), ani je neuchovávat na viditelných místech (lepení papírků s hesly na monitor či na podložku myši apod.);
5. Nesdílet administrátorská hesla s dodavateli služeb;
6. Řádně zálohovat data v přiměřené době;
    a. Elektronická evidence žáků by měla být zálohována každý den
7. Vyvarovat se nadměrnému připojování externích zařízení (USB flash, apod.) *a* pokud nelze zakázat připojování externích médií, pak pomocí bezpečnostních politik vynutit co nejbezpečnější použití externích médií – heslování externího flash zařízení např. pomocí nástroje BitLocker;
8. Používat PC stanice s aktualizovaným operačním systémem;
9. Na PC stanicích využívat aktualizovaný antivirový software
    a. nedoporučujeme používat základní vestavené antivirové programy či jejich základní bezplatné verze;
10. Provádět pravidelné kontroly PC a externích médií pomocí antivirového softwaru;
11. Nepoužívat již nepodporované operační systémy (aktuálně OS do MS Windows Vista);
12. Pravidelně aktualizovat operační systém;
13. Poučit zaměstnance, aby „uzamykali“ či ukončovali session při opuštění PC automaticky → při odcházení od počítače přepnout PC do režimu uzamčení (zk.: windows key + L);
14. Databáze osobních údajů zajistit při internetovém přístupu šifrovacím protokolem
    a. Poskytovatel takovéto internetové služby je zpracovatelem osobních údajů → je tak nezbytné uzavřít tzv. zpracovatelskou smlouvu podle čl. 28 odst. 3 GDPR
15. Vyžadovat po poskytovateli výpočetních služeb funkci logování přístupů do databáze údajů vedené v digitální podobě;

16. V případě přístupu zpracovatelů a jiných dodavatelů k osobním údajům prověřit a zkontrolovat přístupová oprávnění, monitorovat přístup těchto stran a zabezpečit spojení (viz šifrování);

17. Kontrolovat zacházení s osobními údaji a vyhodnocovat zjištěná data vzhledem k dodržování uvedených pravidel.

Organizační opatření

1. Organizační opatření pro zabezpečení důvěrnosti osobních údajů se týkají především procesů zacházení s osobními údaji zaměstnanci, a to v rámci organizace Správce. **Smyslem je prevence úniku / zneužití osobních údajů způsobeného lidským faktorem.** Organizační opatření tak mají za cíl zabezpečit náležité zpracování.

Příloha č. 2: vzorový dokument pro určení doby archivace

Skupina	Spis. Znak	číselná řada	skupina, typ dokumentace	Skart. Znak	Skart. Lhůta	poznámka
A	Povinná dokumentace a pedagogická dokumentace					
	A0	001-100	Třídní katalogy, katalogové listy	A	50	
	A1	101-200	Třídní knihy, záznamy o práci v nepovinném předmětu	S	10	
	A2	201-300	Písemné maturitní práce	V	10	
	A3	301-400	Maturitní protokoly	A	50	
	A4	401-500	Rejstřík škol (zařazení, vyřazení, změny)	A	10	
	A5	501-600	Přijímací řízení - protokoly, kritéria, odvolací řízení	S	10	
	A6	601-700	Osobní spisy žáků	S	10	
	A7	701-800	Přihlášky k ubytování na DM, záznamy o ubytovaných	S	5	
	A8	801-900	Deník výchovné skupiny	S	5	
	A9	901-1000	Základní pedagogické dokumenty (účeb. plány, osnovy)	V	5	
	A10	1001-1100	Kniha úrazů, záznamy o úraze - těžké a smrtelné	A	10	
	A11	1101-1200	Záznamy o úraze - ostatní	S	10	
	A12	1201-1300	Protokoly o závěrečné zkoušce	A	50	
	A13	1301-1400	Deník evidence odborného výcviku	S	10	
	A14	1401-1500	Školní řád	A	5	
	A15	1501-1600	Rozvrh hodin	S	1	
B	Organizace řízení					
	B0	001-100	Zřizovací listiny	A	10*	*po ztrátě platnosti
	B1	101-200	Směrnice a pokyny zřizovatele, vnitřní org. směrnice	A	5*	*po ztrátě platnosti
	B2	201-300	Výkazy o škole - roční	A	10	
	B3	301-400	Výkazy o škole - s kratší než roční periodicitou, hlášení	S	5	
	B4	401-500	Výroční zprávy, vlastní hodnocení školy	A	10	
	B5	501-600	Kontroly nadřízených orgánů	V	10	
	B6	601-700	Zprávy z technických kontrol a revizí	S	10	
	B7	701-800	Pojištění organizace, pojištění žáků	S	5*	*po ztrátě platnosti
	B8	801-900	Korespondence běžná - došlá i odeslaná	V	5	
	B9	901-1000	Porady, pedagogické rady	V	10	

	B10	1001-1100	Školská rada	V	10	
	B11	1101-1200	Hospitace	S	5	
C	Hospodářské záležitosti					
	C0	001-100	Inventarizace - zápisy, sumáře	A	10	
	C1	101-200	Inventarizace - ostatní (seznamy apod.)	A	10	
	C2	201-300	Rozpočty	A	10	
	C3	301-400	Objednávky	S	5	
	C4	401-500	Archivní knihy	A	20*	*po uzavření
	C5	501-600	Podací deníky, výpůjčky ze spisovny, evidence razítek	A	5*	*po uzavření
	C6	601-700	Skartační řízení - návrhy, protokoly	A	10	
	C7	701-800	Stavební dokumentace budov	A		dlouhodobě
	C8	801-900	Evidence majetku - pozemky, budovy	A		dlouhodobě
	C9	901-1000	Veřejné zakázky	S	5	
	C10	1001-1100	Projekty ESF	S	20	
D	Mzdové a personální záležitosti					
	D0	001-100	Osobní spisy zaměstnanců	A	50	
	D1	101-200	Mzdové listy zaměstnanců	S	50	
	D2	201-300	Mzdové listy žáků	S	50	
	D3	301-400	Mzdová rekapitulace, daň z příjmu, nemocenské a sociální pojištění, zdravotní pojištění	S	10	
	D4	401-500	Doklady o pracovní neschopnosti zaměstnanců	S	10	
	D5	501-600	Podklady pro výpočet mezd zaměstnanců	S	5	
	D6	601-700	Podklady pro výpočet mezd žáků	S	5	
E	Účetní doklady					
	E0	001-100	Knihy došlých a vydaných faktur	S	10	
	E1	101-200	Vydané faktury - hlavní činnost	S	10	
	E2	201-300	Vydané faktury - doplňková činnost	S	10	
	E3	301-400	Pokladní kniha, peněžní deník	S	10	
	E4	401-500	Příjmové a výdajové pokladní doklady	S	10	
	E5	501-600	Výpisy z bankovních účtů	S	10	
	E6	601-900	Účetní knihy - hlavní, účetní doklady, doklady o stravování, účetní výkazy	S	10	
	E7	901-1200	Přijaté faktury	S	10	
	E8	1201-1300	DPH, daň z příjmu, ostatní daně	S	10	
	E9	1301-1400	Podklady k evidenci nedokončené výroby	S	10	
	E10	1401-1500	Účetní evidence skladu materiálu, příjemky, výdejky	S	10	

Příloha č. 3: základní legislativa ochrany osobních údajů

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) – tzv. GDPR
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Adaptační zákon k Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 – zákon o zpracování osobních údajů, který bude nahrazovat zákon č. 101/2000 Sb. (pozn. není schválen, aktuálně teprve připravován a projednáván)
- Zákon č. 262/2006 Sb., zákoník práce
- Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)
- Vyhláška č. 364/2005 Sb., o dokumentaci škol a školských zařízení
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 500/2004 Sb., správní řád
- Zákon š. 563/1991 Sb., o účetnictví