

SMĚRNICE

PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

Vydal/a: Základní škola, Dětský domov a Školní jídelna Litovel Palackého 938/30a 784 01 Litovel IČ: 61989771	Účinnost: 25. 5. 2018	Verze: 1	Podpis
---	---------------------------------	--------------------	---------------

Úvod

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 „**GDPR**“ upravuje ode dne 25. 5. 2018 problematiku ochrany osobních údajů.

Účelem a cílem vydání vnitřní Směrnice pro nakládání s osobními údaji (dále jen „Směrnice“) je aplikace pravidel GDPR na poskytování služeb **Základní škola, Dětský domov a Školní jídelna Litovel, se sídlem Palackého 938/30a, 784 01 Litovel, IČ: 61989771** (dále jen „Správce“), a to především při poskytování zajištění vzdělání (zápis k základnímu vzdělání, zajištění základního vzdělání, zájmové vzdělávání ve školní družině), zajištění služeb (zajištění péče o děti s nařízenou ústavní výchovou, poskytování poradenských služeb ve školách, zajištění školního stravování), zajištění interních procesů a provozu organizace (výběrová řízení na zaměstnance, pracovněprávní a mzdová agenda, evidence uchazečů o zaměstnání, evidence úrazů, poskytování informací dle zákona o svobodném přístupu k informacím, ochrana majetku a osob, prezentace příspěvkové organizace, organizování exkurzí, vedení účetnictví příspěvkové organizace, smlouvy a objednávky služeb) a s tím související další činnosti tak, aby bylo dosaženo požadované právní ochrany osobních údajů.

Článek 1 Preamble

1. Vnitřní organizační Směrnice je vydávána za účelem konkretizace povinností vyplývajících Správci 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 „GDPR“ a navazující legislativy k GDPR.

Článek 2 Působnost směrnice (věcná a personální)

1. Tato směrnice upravuje postupy Správce, jeho zaměstnanců, případně dalších osob, při zpracování osobních údajů, a upravuje dále pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů.
2. Směrnice rovněž upravuje některé povinnosti Správce, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji.
3. Doporučené postupy se vztahují na zpracování osobních údajů všech kategorií subjektů osobních údajů, které byly identifikovány v rámci organizace Správce.
4. 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 Základní pojmy

1. Osobním údajem (čl. 4 odst. 1 GDPR) se rozumí:
 - 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. fyzické osoby, kterým Správce poskytuje své služby (dále také jako „klient“),
 - ii. zaměstnanci,
 - iii. dodavatelé a odběratelé služeb nebo zboží.
4. Zvláštní kategorie osobních údajů - citlivé osobní údaje (čl. 9 GDPR)
 - a. Zvláštní kategorií 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 může být v situaci, kdy je riziko, že jméno a příjmení konkrétní osoby může být zveřejněno, použít namísto těchto údajů přiřazený číselný kód. Např. v e-mailové komunikaci s poskytovatelem účetních služeb nesdělovat jméno a příjmení zaměstnance, ale nahradit je přiřazeným personálním číslem.
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. 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 Správce, 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 případným pověřencem pro ochranu osobních údajů, (pokud byl jmenován),
 - n. Spolupracovat s Úřadem pro ochranu osobních údajů.
2. Osobní údaje mohou být zpracovávány pouze po dobu nezbytně nutnou k plnění účelu jejich zpracovávání a/nebo po dobu nezbytně archivace. Pomine-li účel, pro který byly osobní údaje zpracovávány (např. došlo k ukončení poskytování služeb) a uplynula zákonná doba pro jejich archivaci, zpracovávání takových osobních údajů musí být ukončeno.
3. Zaměstnanci Správce jsou povinni průběžně kontrolovat řádnou 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 (pokud byl jmenován), jinak s vedoucím zaměstnancem, zajistí jejich řádnou likvidaci. Doba zpracování jednotlivé dokumentace může být určena právními předpisy – např. zákonem č. 563/1991 Sb., o účetnictví, nebo může být také určena spisovým a skartačním řádem Správce. Po uplynutí takto stanovené 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 mzdy,
 - b. O klientech poskytovaných služeb v evidenci klientů,
 - c. O dodavatelích / odběratelích služeb nebo zboží 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 vedoucího zaměstnance nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů (pokud byl jmenován).
3. 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.
4. Správce je povinen dozorovému úřadu pro ochranu osobních údajů ihned oznámit bezpečnostní incident týkající se osobních údajů, a to v případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob a zároveň 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).
5. 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 vedoucímu zaměstnanci známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením Správce nebo jím pověřené osoby.
6. Za ochranu osobních údajů odpovídá Správce osobních údajů, který je povinen provádět ve spolupráci s pověřencem pro ochranu osobních údajů (pokud byl jmenován) 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.
2. K jednotlivým dokumentům obsahující osobní údaje mají přístup pouze zaměstnanci, kteří je nezbytně potřebují při výkonu své pracovní činnosti dle pracovního zařazení zaměstnance.
3. Veškeré dokument obsahující osobní údaje musí být zabezpečeny před odcizením, zneužitím či neoprávněným zpřístupněním. Doporučená zabezpečení jsou přílohou této směrnice.
4. 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.

5. Každý zaměstnanec Správce má povinnost zachovávat co nejvyšší standard ochrany osobních údajů, s nimiž v rámci výkonu své práce přichází do styku.
6. Dokumenty obsahující osobní údaje klientů a zaměstnanců musí být uloženy v uzamykatelných prostorech. Je dále vhodné dokumenty v uzamykatelných prostorech ukládat do uzamykatelných registratur, a to s ohledem na kategorie osobních údajů a jejich množství.
7. Zaměstnanci Správce jsou povinni zajistit, že zdravotnická dokumentace a personální spisy zaměstnanců, nebudou vynášeny z budovy Správce, kde je jeho sídlo a/nebo provozovna a nebudou neoprávněně předávány cizím osobám nebo kopírovány a kopie poskytovány neoprávněným osobám.
8. Zaměstnanci Správce nesmí poskytovat bez právního důvodu žádnou formou osobní údaje cizím osobám a institucím.
9. V případě, že si některý orgán veřejné moci (např. soud, OSPOD, PČR apod.) vyžádá určité informace subjektu osobních údajů, mohou být takové 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, není-li náležité a prokazatelně ověřena identita žadatele a oprávněnost jeho požadavku.
10. Pokud Správce vede evidenci osobních údajů také v elektronickém systému, je jeho povinností zabezpečit informační systém proti neoprávněnému zpřístupnění a zneužití osobních údajů.
 - a. do elektronického systému mají přístup pouze pověřeni pracovníci, a to v rozsahu, který odpovídá jejich pracovnímu zařazení. Jiné osoby pouze s výslovným a písemným pověřením Správce, a to jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením (např. IT správce).
 - b. Elektronická evidence vč. samotného PC nosiče musí být zabezpečena heslem proti neoprávněnému přístupu.
 - c. Zpracování osobních údajů v elektronické evidenci by mělo být podrobena tzv. logování přístupů vč. uvedení důvodu zpracování.
 - d. 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.
 - e. Při práci s elektronickou evidencí musí být dodržovány základní pravidla práce s IT prostředky:
 - i. Zaměstnanci Správce nesmí opouštět počítač bez odhlášení se,
 - ii. Není přípustné nechat nahlížet do evidence jinou (neoprávněnou) osobu,
 - iii. Zaměstnanci Správce musí zabezpečit důvěrnost (utajení) přihlašovacích údajů do elektronické evidence; a v případě nebezpečí jeho vyžrazení 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 přístupové heslo cca po 120 dnech,
 - vi. Přístupy do systémů nastavuje pověřená osoba, která nastavuje potřebné zabezpečení dat a počítačové sítě,
 - 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 prostorech. Přístup k nim má toliko statutární orgán Správce nebo osoba jím pověřená – např. 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. Každý zaměstnanec je povinen pro pracovněprávní účely hlásit změnu evidovaných osobních údajů.

13. 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:
- dodržovat příslušná pravidla této Směrnice,
 - ve smlouvě, která je základem závazkového vztahu začlenit text této Směrnice do přílohy,
 - zpracovávat předávané osobní údaje pouze pro účely plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím),
 - 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,
 - bez předchozího písemného souhlasu Správce nezapojit do zpracování žádné další osoby,
 - zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele (zaměstnanci) byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,
 - 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,
 - 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.,
 - poskytnout Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené předpisy na ochranu osobních údajů,
 - umožnit kontrolu, audit či inspekci prováděné Správce nebo příslušným orgánem dle právních předpisů, a to za účelem kontroly dodržování povinností plynoucích ze smlouvy a předpisů na ochranu osobních údajů,
 - poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou určí Správce, součinnost potřebnou pro plnění zákonných povinností spojených s ochranou osobních údajů,
 - osobním údajům zajistit odpovídající standard ochrany – zejm. důvěrnost a nedotknutelnost.
14. Doporučená technicko-organizační opatření jsou Přílohou č. 1 této Směrnice
15. 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:
- do osobního spisu zaměstnance - vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni, nebo zaměstnanci výslovně pověřeni 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,
 - do evidence osob, kterým Správce poskytuje své služby, pouze zaměstnanci, kteří jsou oprávněni dle svého pracovního zařazení nakládat s osobními údaji takových osob.

Článek 7

Práva subjektů osobních údajů

- Právo na informace
 - Subjekty osobních údajů musí být informovány a skutečnostech, které se týkají procesů zpracování osobních údajů, a to v rozsahu stanoveném čl. 13 a násl. GDPR. Za tímto účelem byl Správce 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.
 - Každý zaměstnanec Správce je povinen na žádost subjektu osobních údajů zajistit, že tento bude s Prohlášením o ochraně osobních údajů patřičně seznámen.
 - 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 (pokud byl dán)
 - 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 Zaměstnanec 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.
6. Uplatnění práva musí být ihned zaznamenáno v Záznamu o uplatnění žádosti subjektem osobních údajů.

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 informačních systémů

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. Informační systémy obsahující osobní údaje musí být instalovány pouze na PC stanicích, které pro přístup vyžadují unikátní přístupové jméno zaměstnance a heslo. Stejně zabezpečení je vhodné aplikovat pro jednotlivý software, ve kterém dochází ke zpracovávání osobních údajů – např. elektronický systém pro správu personalistiky a mezd.
3. 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 se Správcem. Úroveň a hodnoty přístupových oprávnění každého zaměstnance odpovídají jeho funkčnímu zařazení a pracovní náplni. Správce vypracuje seznam aplikací obsahující osobní údaje a hodnoty uživatelských oprávnění, kterými jednotlivý zaměstnanec disponuje.
4. 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.
5. Dojde-li při změně pracovní činnosti zaměstnance k změně pracovní náplně, která vyžaduje změnu úrovně oprávnění k aplikacím obsahující osobní údaje. Následně správce IT 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 (pokud byl jmenován).
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.

V Litovli_ dne 25. května 2018 _____

Správce

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, evidence klientů) jsou fyzicky zabezpečené proti zneužití či úniku
 - a. místnost, ve které jsou údaje ukládány, je zabezpečena zámkem proti neoprávněnému vniknutí;
 - b. klíče od dané místnosti jsou poskytnuty pouze osobám, které jsou oprávněny do místnosti vstupovat, či nakládat s osobními údaji;
 - c. seznam osob, které mají přístupové klíče k místnosti v budově školy: ředitelka, zástupkyně ředitelky, uklízečka;
 - d. seznam osob, které mají přístupové klíče k místnostem v budově DD: ředitelka, zástupkyně ředitelky, sociální pracovnice, vedoucí vychovatel, hospodářka, ekonomka;
 - e. jelikož do místností má vstup osoba, která není oprávněná do dokumentů s údaji nahlížet a pracovat s nimi, jsou systematizované evidence osobních údajů ukládány v uzamykatelné skříni na dokumenty.
2. Systém řízeného přístupu do evidence údajů
 - a. každý zaměstnanec má přístup pouze k takovým osobním údajům, které nezbytně potřebuje pro vykonávání svých povinností;
 - b. zaměstnanec nemá umožněný přístup k osobním údajům, s nimiž nezbytně nepotřebuje zacházet.
3. Do evidence osobních údajů zaměstnanců má oprávnění přistupovat ředitelka, zástupkyně ředitelky. Do evidence osobních údajů žáků (osobní spisy, třídní kniha, třídní výkaz) má oprávnění přistupovat ředitelka, zástupkyně ředitelky, třídní učitelé a učitelé vyučující dané předměty. Všechny tyto osoby, vyjma učitelů daných předmětů, mají oprávnění nakládat s těmito osobními údaji. Do evidence osobních údajů klientů DD má oprávnění přistupovat ředitelka, zástupkyně ředitelky, sociální pracovnice, vedoucí vychovatel a vychovatelé jednotlivých rodinných skupin. Všechny tyto osoby mají oprávnění nakládat s těmito osobními údaji.
4. Je zakázáno přenášení jakékoliv části evidence mimo prostory provozovny Správce.
5. Všichni zaměstnanci mají povinnost neodkladně hlásit změny související s osobními údaji pro uchování aktuálního stavu osobních údajů.
6. Všechny místnosti, kde jsou umístěny počítače, musí být uzamčeny, abychom fyzicky zabezpečili počítače před krádeží (ředitelna, kancelář zástupkyně, učebna č. 7, kancelář soc. pracovnice, kancelář hospodářky a ekonomky, kancelář vedoucího vychovatele, vychovatelna). Klíče nesmí být volně dostupné, budou s nimi disponovat pouze pověřeni pracovníci.
7. Budou zlikvidovány nerelevantní osobní údaje (zásada minimalizace)
 - a. V případě, že správce osobních údajů nemá souhlas se zpracováním, pak budou odstraněny následující osobní údaje, které jsou Správcem zpracovávány:
 1. národnost zaměstnance / klienta,
 2. životopisy zaměstnanců a nepřijatých uchazečů,
 3. kopie občanského průkazu zaměstnance / klienta (dále „OP“),
 4. kopie průkazu pojištěnce vč. data uplynutí lhůty platnosti průkazu u zaměstnance / klienta.
8. Na všech dokumentech bude zaznamenána doba platnosti zpracování přiřazením spisových a skartačních znaků.

9. Správce bude provádět náhodné kontroly administrativních úkonů zaměstnanců a dodržování výše uvedených pravidel.

Osobní údaje zpracovávány v digitální podobě:

1. Naše školské zařízení nemá vlastní server;
2. PC stanice je před neoprávněným použitím zabezpečena – při zapnutí PC je požadováno heslo;
 - a. Nastavit odpovídající politiku hesel (min. 8 znaků, kombinace velká a malá písmena a číslice, speciální znaky);
 - b. hesla se budou obměňovat každých 90 dnů.
2. Je zakázáno sdělovat přístupová hesla osobám, které nejsou oprávněny zacházet s PC (např. návštěvy, rodinní příslušníci zaměstnance). Hesla nesmí být zapsána na viditelných místech;
3. Není dovoleno sdílet administrátorská hesla s dodavatelem služeb.
4. Všechna data týkající se osobních údajů se musí řádně zálohovat 1x měsíčně.
5. Smí se používat PC stanice s aktualizovaným operačním systémem.
6. Na PC stanicích se využívá aktualizovaný antivirový software.
7. Správce bude provádět pravidelné kontroly PC a externích médií pomocí antivirového softwaru.
8. Přísný zákaz používání již nepodporovaných operačních systémů (aktuálně OS do MS Windows Vista).
9. Pravidelně aktualizovat operační systém.
10. Všichni zaměstnanci musí „uzamykat“ či ukončovat session při opuštění PC automaticky → při odcházení od počítače přepnout PC do režimu uzamčení (zk.: windows key + L).
11. Osobní údaje se budou zpracovávat a ukládat na přenosných zařízeních (např. notebooky, flash a externí disky atd.) pouze za podmínky, že je zajištěna jejich ochrana šifrováním disku tohoto zařízení.
12. Vyžadovat po výrobci software, ve kterém jsou zpracovávány osobní údaje, funkci logování přístupů do databáze údajů vč. uvedení důvodu zpracování.
13. V případě přístupu zpracovatelů a jiných dodavatelů k osobním údajům musí být prověřena a zkontrolována přístupová oprávnění, monitorován přístup těchto stran a náležitě zabezpečeno spojení (viz šifrování).
14. Správce bude kontrolovat zacházení s osobními údaji a vyhodnocovat zjištěná data vzhledem k dodržování uvedených pravidel.

Organizační opatření

Organizační opatření pro zabezpečení důvěrnosti osobních údajů se týkají především procesů zacházení s osobními údaji zaměstnanců, a to v rámci organizace Správce.

Smyslem je prevence úniku / zneužití osobních údajů způsobeného lidským faktorem.

1. Připravit zvláštní dokumentaci popisující zpracování osobních údajů a jejich ochranu (analýza zpracovatelských procesů - audit).
2. Funkci pověřence pro ochranu osobních údajů vykonává společnost Schola Servis GDPR, s.r.o., se sídlem Palackého 150/8, Prostějov, IČ: 04223748.
3. Všichni zaměstnanci byli seznámeni se Směrnicí pro nakládání s osobními údaji v souladu s předpisy pro nakládání s osobními údaji.

4. Všichni zaměstnanci byli proškoleni v oblasti ochrany osobních údajů.
5. Všichni zaměstnanci byli proškoleni, jak bezpečně zacházet s výpočetní technikou.
6. Všichni pedagogičtí pracovníci, kterým byla přidělena služební e-mailová adresa, musí používat ke služební komunikaci pouze tuto adresu. Není dovoleno svévolně měnit zadaná hesla.
7. V případě zjištění incidentu (např. porušení zabezpečení osobních údajů) musí zaměstnanec tuto informaci neprodleně oznámit Správci.
8. Správce zdokumentuje:
 - a. jaký incident nastal,
 - b. co bylo příčinou (proč k němu došlo),
 - c. zda bylo možné se incidentu vyvarovat,
 - d. přijatá opatření, aby se v budoucnu incident neopakoval.
9. V případě, že se zaměstnanec dozví o neplatnosti či neaktuálnosti osobních údajů, musí tuto informaci předat osobě (Správci), která je oprávněna zjištěný stav zavést do evidence osobních údajů.
10. Subjekty osobních údajů mají právo – na přístup k osobním údajům, opravu, výmaz, přenositelnost, omezení zpracování, podání stížnosti. V případě žádosti o výmaz osobních údajů musí subjekt podat písemnou žádost.
11. Správce musí řádně dodržovat transparentnost a informační povinnost vůči subjektům osobních údajů.