Základní škola a Mateřská škola Frenštát pod Radhoštěm, Tyršova 913, okres Nový Jičín, Tyršova 913, 744 01 Frenštát pod Radhoštěm.

Směrnice č. 20

Směrnice pro ochranu osobních údajů

Číslo směrnice:	**20/2018**
Číslo jednací:	**ZSMSTYFR/114/2018**
Zodpovídá:	**RNDr. Zdeňka Murasová, ředitelka školy**
Schválil:	**RNDr. Zdeňka Murasová, ředitelka školy**
Verze dokumentu:	**1**
Poslední revize ze dne:	**25. 5. 2018**

Obsah:

ČL. 1. TABULKA ROLÍ ... 3

ČL. 2. PŮSOBNOST A VYMEZENÍ POJMŮ ... 3

ČL. 3. PŘEDMĚT A CÍL ÚPRAVY ... 5

ČL. 4. HLAVNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ... 6

ČL. 5. PLNĚNÍ INFORMAČNÍ POVINNOSTI SPRÁVCE ... 7

ČL. 6. ZÁKONNÉ DŮVODY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ... 7

ČL. 7. SOUHLAS ... 8

ČL. 8. REGISTR A ZÁZNAMY O ČINNOSTECH ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ ... 9

ČL. 9. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ ... 9

ČL. 10. REVIZE ORGANIZAČNÍCH A TECHNICKÝCH OPATŘENÍ ... 10

ČL. 11. HLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ – INCIDENT ... 10

ČL. 12. PŘIDĚLOVÁNÍ OPRÁVNĚNÍ PŘI ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ ... 11

ČL. 13. UPLATŇOVÁNÍ PRÁV SUBJEKTEM ÚDAJŮ ... 12

ČL. 14. POUŽITÍ TISKOPISŮ A FORMULÁŘŮ ... 12

ČL. 15. OCHRANA OSOBNÍCH ÚDAJŮ V ORGANIZACI ... 13

ČL. 16. ZPRACOVATELÉ ... 14

ČL. 17. ZÁVĚREČNÁ USTANOVENÍ ... 15

ČL. 18. SEZNAM PŘÍLOH ... 15

Čl. 1. Tabulka rolí

Role	Popis role	Pověřená osoba/role/organizace
Správce	Organizace zodpovědná za zpracovávání osobních údajů.	Ředitelka školy
Zaměstnanec	Výkon povinnosti a práv dle této směrnice	Všichni zaměstnanci správce a osoby přistupující k osobním údajům, za které zodpovídá správce.
Manažer osobních údajů	Osoba v organizaci zodpovědná za komplexní zpracovávání osobních údajů.	Ředitelka školy
Registrátor agend	Osoba zodpovědná za registr zpracovávání osobních údajů a evidenci jejich revizí.	Ředitelka školy (Zástupce ředitelky II, Hospodářka školy)
Pověřenec	Osoba jmenovaná Pověřencem dle legislativy na ochranu osobních údajů	JUDr. Tomáš Panáček
IT specialista	Osoba zodpovědná za IT	Koordinátor ICT (Technický pracovník)
Výbor pro řízení osobních údajů	Skupina pověřených rolí pro řízení ochrany osobních údajů správce.	Manažer osobních údajů, Registrátor agend, Pověřenec, IT specialista

Čl. 2. Působnost a vymezení pojmů

(1) **„Účelem směrnice“** je stanovit v podmínkách organizace dále jen **„správce**“ jednotný proces automatizovaného i neautomatizovaného zpracování osobních údajů jednotlivými zaměstnanci v souvislosti s výkonem jejich pracovní činnosti, a to jak prostřednictvím jednotlivých programových agend v informačních systémech správce, tak i v případě manuálního zpracování (např. kartotéka, pomocné evidence, příruční archivy) a vymezit práva a povinnosti na tomto procesu zúčastněných osob. Dále vymezit povinnosti každého externího zpracovatele, který zpracovává osobní údaje pro správce.

(2) Tato směrnice je závazná pro všechny zaměstnance správce.

(3) Tato směrnice se nevztahuje na zpracovávání osobních údajů pro vlastní potřebu zaměstnance, pokud je mu umožněno zpracovávat osobní údaje pro svou osobní potřebu na prostředcích správce.

(4) **„Zpracováním osobních údajů“** se rozumí shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití,

zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení osobních údajů nebo jejich souborů.

(5) **„Agenda“** činnost správce při které dochází ke zpracovávání osobních údajů Subjektu údajů.

(6) **„Subjektem údajů“** se rozumí žijící fyzická osoba i podnikající fyzická osoba, a to jak osoba samostatně výdělečně činná, tak osoba vykonávající svobodné povolání, pokud se osobní údaje týkají její osoby, byť ve vztahu k její podnikatelské činnosti. Totéž platí i pro fyzické osoby zastupující právnickou osobu. (Subjektem údajů může být dítě, zaměstnanec, zákonný zástupce, rodič, občan, pacient, klient, zákazník, aj.)

(7) **„Osobním údajem“** se rozumí každá informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Jako identifikátor může sloužit zejména jméno a příjmení, adresa trvalého pobytu, rodné číslo subjektu osobních údajů, pracovní adresa, lokační údaje (GPS), síťový identifikátor (dynamická IP adresa, UDID u telefonu, IMEI u mobilu, sledovací cookies), genetické či biometrické údaje (fotografie, otisk prstů, hlas, rukopis) sledovací cookies (nástroj k monitorování aktivity uživatelů internetu za účelem předložení nabídky nebo reklamy).

(8) **„Citlivým údajem se rozumí zvláštní kategorie osobních údajů“,** 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 stravu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Pro účely této směrnice je jednotně používán pojem osobní údaj i pro kategorii citlivých údajů.

(9) „genetickými údaji“ zvláštní kategorie osobních údajů týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.

(10) **„biometrickými údaji“** zvláštní kategorie osobních údajů vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

(11) **„údaji o zdravotním stavu“** zvláštní kategorie osobních údajů týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.

(12) **„omezením zpracování“** označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu.

(13) **„profilováním“** 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.

(14) **„pseudonymizace“** zpracování osobních údajů tak, 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.

(15) **„anonymizace“** zpracování osobních údajů tak, že již nikdy nemohou být přiřazeny konkrétnímu subjektu údajů.

(16) **„evidencí“** jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska. Evidence může být analogová a digitální.

(17) **„správcem“** 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.

(18) **„zpracovatelem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje, za které je zodpovědný správce.

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

(20) **„příjemcem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

(21) **„třetí stranou“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, která je oprávněna ke zpracování osobních údajů.

(22) **„porušením zabezpečení osobních údajů“** porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů, které se hlásí se správci jako „**Incident“**.

(23) **„dozorovým úřadem“** nezávislý orgán veřejné moci zřízený členským státem. V ČR. www.uoou.cz.

(24) **„dotčeným dozorovým úřadem“** dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť: správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu; subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo u něj byla podána stížnost.

(25) **„službou informační společnosti“** služba ve smyslu čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535; Implementován do 127/2005 Sb., o elektronických komunikacích, a rovněž zákonem č. 480/2004 Sb. Patří sem Google, Facebook, LinkedIn, jakákoliv elektronická služba poskytovaná externím subjektem, při které dochází ke zpracovávání osobních údajů, za které správce zodpovídá.

Čl. 3. Předmět a cíl úpravy

(1) Předmětem úpravy v podmínkách správce je nastavení:

a) pravidel týkajících se ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů (dále jen „subjekt údajů“),
b) pravidel týkajících se volného pohybu osobních údajů subjektů údajů,
c) postupu při uplatňování práv subjekty údajů, kterými mohou vykonávat kontrolu nad zpracováním svých osobních údajů,
d) podmínek, za kterých je možné osobní údaje zpracovávat,
e) povinností zaměstnancům při zpracování osobních údajů subjektů údajů.

(2) Cílem úpravy je zejména ochrana základních práv a svobod subjektů údajů, zejména jejich práva na ochranu osobních údajů.

(3) Tímto příkazem nejsou dotčena práva a povinnosti stanovená obecně závaznými právními předpisy[1] nebo vnitřními předpisy správce.

(4) Manažer osobních údajů zodpovídá za aktuálnost této směrnice.

Čl. 4. Hlavní zásady zpracování osobních údajů

(1) Hlavními zásadami při zpracování osobních údajů jsou:
a) **zákonnost, korektnost, transparentnost** – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,
b) **omezení účelu** – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
c) **minimalizace údajů – osobní** údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
d) **přesnost** – osobní údaje musí být přesné,
e) **omezení uložení** – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
f) **integrita a důvěrnost** – technické a organizační zabezpečení osobních údajů, které zajistí, že nebude porušena integrita a důvěrnost osobních údajů.

(2) Každý zaměstnanec je odpovědný za obsahovou správnost, úplnost a ochranu jím zpracovávaných osobních údajů a za tím účelem je povinen:
a) zachovávat mlčenlivost o osobních údajích, s nimiž se při výkonu své práce seznámí i o bezpečnostních opatřeních k jejich ochraně,
b) bezpečně ukládat analogové dokumenty, které zpracovává a které obsahují osobní údaje, aby nemohla být narušena jich důvěrnost pomocí listinných úložišť (uzamykatelné šuplíky, kontejnery a skříně, trezory, příruční archívy),
c) při používání ostatních informačních kanálů (elektronická pošta, telefon) a při ukládání digitálních dokumentů, které zpracovává a které obsahují osobní údaje, postupovat tak, aby nemohla být narušen jich důvěrnost – elektronická úložiště (strukturovaná – sdílené disky, informační systémy i nestrukturovaná – vlastní, přenosná uložiště).

[1] např.: zákon č. 89/2012 Sb., občanský zákoník, v platném znění, zákon č. 40/2009 Sb., trestní zákoník v platném znění, zákon č. 262/2006 Sb., zákoník práce v platném znění, školní řád.

d) důsledně dodržovat všechna bezpečnostní opatření (technického, administrativního i personálního charakteru) zavedená ostatními vnitřními předpisy správce a pravidelně se v jejich dodržování proškolovat dle pokynu správce.
e) hlásit nadřízenému/pověřenci pro ochranu osobních údajů všechna podezření na narušení ochrany zpracovávaných osobních údajů.
f) V maximální míře, pokud to situace vyžaduje a umožňuje provádět pseudonymizace a anonymizaci osobních údajů v dokumentech.

Čl. 5. Plnění informační povinnosti správce

(1) Za účelem splnění informační povinnosti správce[2] je pod odkazem http://www.zstyrfren.cz/ochrana-osobnich-udaju způsobem umožňujícím dálkový přístup zveřejněn povinný dokument **„Ochrana osobních údajů – Informace poskytované správcem**“. (příloha č. 1 směrnice). V případě jakéhokoliv získávání osobních údajů je zodpovědný zaměstnanec povinen subjekt údajů s dokumentem seznámit, resp. předat jeho listinné vyhotovení nebo odkázat na jeho elektronickou verzi uveřejněnou na webových stránkách města, pokud je subjektem údajů k tomu vyzván.

(2) Zaměstnanec je povinen znát místo – odkaz, kde je dokument **„Ochrana osobních údajů – Informace poskytované správcem“** uložen a na vyžádání jej vždy subjektu údajů poskytnout.

(3) Manažer osobních údajů je zodpovědný za aktuálnost a umístění dokumentu **„Ochrana osobních údajů – Informace poskytované správcem“**

Čl. 6. Zákonné důvody zpracování osobních údajů

(1) Zákonné důvody zpracování osobních údajů znamenají oprávnění zaměstnance osobní údaje zpracovávat.

(2) Osobní údaje lze zpracovávat, pokud lze identifikovat alespoň jeden z těchto zákonných důvodů:
a) subjekt údajů udělil **souhlas** pro jeden či více konkrétních účelů zpracování,
b) zpracování je nezbytné pro **plnění 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 správce pověřen,
f) zpracování je nezbytné pro účely **oprávněných zájmů správce** či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

[2] Čl. 13 resp. 14 obecného nařízení

(3) Pokud zpracovávání osobních údajů v rámci činnosti správce není založeno na jednom z výše uvedených zákonných důvodů, zaměstnanec nesmí osobní údaje zpracovávat.

Čl. 7. Souhlas

(1) Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

(2) Je žádoucí, aby byl souhlas subjektu údajů využíván pouze v případech, kdy není možné zpracování osobních údajů subjektu údajů podřadit pod jiný právní důvod (viz čl. 6 odst. 2 písm. b) až f).

(3) Souhlas se vždy poskytuje k určitému účelu zpracování, který musí být subjektu údajů zřetelně předem sdělen.

(4) Zaměstnanec je povinen jakoukoliv změnu souhlasu nebo před jeho prvním použitím konzultovat s manažerem osobních údajů a případně s pověřencem.

(5) Souhlas stejně jako jeho odvolání se stává úředním dokumentem a nakládání s ním podléhá platnému spisovému a skartačnímu řádu[3].

(6) Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.

(7) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

(8) Souhlas musí být pro konkrétní účel, nikoliv paušální pro jakékoliv zpracování osobních údajů! Pro každý údaj musí být jednoznačně definovatelné, byl-li k jeho zpracování poskytnut souhlas, či nikoli.

(9) Pokud je více účelů nebo souhlas pro jiné záležitosti musí být od sebe souhlasy odděleny.

(10) Souhlas musí být udělen na určitou dobu. Doba souhlasu musí být jednoznačná a nezaměnitelná. Doba souhlasu nesmí být nekonečná.

(11) Na souhlase musí být jasně uvedeny kontaktní údaje správce.

(12) Zaměstnanec je povinen souhlasy evidovat a uchovávat v rámci vedených spisů nebo samostatně.

(13) Souhlas obsahuje osobní údaje a musí být tímto i dostatečně chráněn a bezpečně uložen.

(14) Pokud souhlas uděluje dítě, je zpracování osobních údajů dítěte zákonné, je-li dítě ve věku nejméně 15 let. Je-li dítě mladší, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.

[3] Spisový a skartační řád Správce

(15) Zaměstnanec vyvine přiměřené úsilí a kontrolu s ohledem na dostupnou technologii a situaci, aby v takovýchto případech ověřil, že byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.

Čl. 8. Registr a záznamy o činnostech zpracovávání osobních údajů

(1) Správce vede **„registr a záznamy o činnostech zpracovávání osobních údajů“,** (příloha 2 této směrnice) ve kterém má zpracovány veškeré činnosti (agendy) při kterých dochází ke zpracovávání osobních údajů.

(2) Tento registr obsahuje všechny tyto informace: Kontaktní údaje správce. Kontaktní údaje pověřence. **„registrátora agend“.** Odbor nebo útvar, kde je agenda zpracovávána; Název Agendy; Účel zpracování; Kategorie subjektů údajů; Kategorie osobních údajů; Zvláštní kategorie osobních údajů; Kategorie příjemců údajů; Zákonný způsob zpracovávání; Zákony, vyhlášky, předpisy; Doba Uchovávání; Technicko – organizační zabezpečení; Organizační zodpovědnost; Technická zodpovědnost.

(3) Zaměstnanec má povinnost zpracovávat osobní údaje jen v souladu s tímto registrem. Pokud zpracovávání osobních údajů neodpovídá záznamům v registru nebo zaměstnanec má pochybnosti nebo dochází ke změně agendy informuje o tom bezodkladně svého nadřízeného nebo pracovníka uvedeného v registru zpracovávání osobních údajů mající organizační zodpovědnost za příslušnou agendu.

(4) Vedoucí pracovník nebo pracovník mající organizační zodpovědnost za agendu konzultují s manažerem osobních údajů nebo s pověřencem, úpravu, ukončení nebo vznik nové agendy. Pokud úpravu nebo vznik nové agendy schválí manažer osobních údajů, předají tuto změnu „**registrátorovi agend**“

(5) Povinností registrátora agend, je provést změnu v registru a formou verzování dokumentu zaznamenávat veškeré změny v registru po dobu 3 let zpětně. Verze registrů zpracovávání osobních údajů vzniklé změnami se považují za základ pro povinné **„záznamy o činnostech zpracování“.**

Čl. 9. Pověřenec pro ochranu osobních údajů

(1) Pověřenec pro ochranu osobních údajů poskytuje komplexní poradenství při zpracování osobních údajů v podmínkách Správce zejména s ohledem na plnění povinností při dodržování ochrany osobních údajů subjektu údajů ze strany správce a zaměstnanců. Současně přispívá k rozvoji a udržování zásad, postupů a procesů ochrany osobních údajů, zajišťuje jejich aktualizaci a průběžnou kontrolu ve spolupráci s vedením správce.

(2) Monitoruje soulad činností správce s platnou legislativou v oblasti ochrany osobních údajů a s koncepcemi správce v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů a kontrol.

(3) Vystupuje jako kontaktní osoba správce a spolupracuje s orgánem dohledu.

(4) V případě Incidentu doporučuje manažeru osobních údajů, zda je třeba hlásit dozorovému úřadu.

(5) Manažer osobních údajů zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.

(6) Manažer osobních údajů zajistí, aby kontaktní údaje pověřence byly včas nahlášeny dozorovému úřadu www.uoou.cz .

(7) Správce podporuje pověřence pro ochranu osobních údajů při plnění úkolů tím, že mu poskytuje zdroje nezbytné k plnění těchto úkolů, přístupy k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí.

(8) Správce zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů, které by mohly ovlivnit objektivitu nebo monitoring jeho činnosti. V souvislosti s plněním svých úkolů není správcem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen manažeru osobních údajů.

(9) Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv u správce.

(10) Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností.

Čl. 10. Revize organizačních a technických opatření

(1) Za účelem aktualizace a pravidelného prověřování fungování zavedených technických, organizačních a bezpečnostních opatření při zpracování osobních údajů je minimálně jednou ročně prováděno **„vyhodnocení zpracovávání osobních údajů“** v podobě zprávy pro správce a s návrhem změn technických a organizačních opatření. K naplnění těchto povinností se touto směrnicí zřizuje pracovní skupina „**výbor pro řízení ochrany osobních údajů“**, dále jen výbor.

(2) Výbor řídí a svolává „**manažer ochrany osobních údajů**“, Výbor provede:

a. Analýzu všech záznamů o incidentech.
b. Analýzu všech změn v legislativě.
c. Reviduje aktuálnost dokumentu „Ochrana osobních údajů – Informace poskytované správcem“
d. Revidují přístupová oprávnění k jednotlivým analogovým, SW aplikacím formou jejich výpisu a jeho odsouhlasením osobou odpovědnou za příslušné agendy a manažerem osobních údajů.
e. Navrhne změnu této směrnice, případně jiných směrnic, nařízení a pracovních postupů nebo školního řádu.

(3) Výbor ze své schůzky provádí zápis, který je v evidenci „**manažera ochrany osobních údajů**“.

Čl. 11. Hlášení porušení zabezpečení osobních údajů – Incident

(1) Každý zaměstnanec je povinen bezodkladně nahlásit jakékoliv porušení (incident) zabezpečení osobních údajů svému nadřízenému, a ukončit nezákonné zpracování osobních údajů, jinak odpovídá za škodu, která subjektu osobních údajů vznikne.

(2) K nahlášení incidentu použije zaměstnanec email reditel@zstyrfren.cz nebo telefonní číslo 556 835 038 na kontaktní osobu správce pro řízení incidentů (manažer osobních

údajů). Manažer osobních údajů rozhodne o tom, zda zaměstnanec vyplní formulář **„hlášení incidentu“** (Příloha č. 3 směrnice).

(3) Po nahlášení incidentu manažer osobních údajů ve spolupráci s pověřencem a IT specialistou rozhodnou o technických a organizačních opatřeních, která je třeba učinit a rozhodnou o tom, zda hlášení incidentu musí být nahlášeno dozorovému úřadu www.uoou.cz a subjektům údajů.

(4) V případě, že bude rozhodnuto o nahlášení incidentu i dozorovému úřadu a subjektům údajů provede manažer osobních údajů toto nahlášení do 72 hodin od nahlášení incidentu.

(5) Za nastavení postupu a evidenci incidentů je zodpovědný manažer osobních údajů.

(6) Pro naplnění zásady integrity a důvěrnosti je zaměstnanec povinen vycházet ze zásad ochrany majetku, dat a informací stanovených platnými vnitřními předpisy[4] správce.

(7) Za účelem zajištění trvalé a plnohodnotné ochrany osobních údajů při jejich zpracování je správce povinen každoročně provádět školení zaměstnanců v této oblasti. Zaměstnanec je povinen se těchto školení účastnit. Manažer osobních údajů je povinen 1x ročně toto školení zaměstnanců zorganizovat.

(8) Za účelem zajištění trvalé a plnohodnotné ochrany osobních údajů při jejich zpracování je správce povinen každoročně provádět poučení žáků o ochraně osobních údajů a implementovat zásady ochrany osobních údajů do školního řádu. Za implementaci tohoto bodu do školního řádu je zodpovědný manažer osobních údajů.

Čl. 12. Přidělování oprávnění při zpracovávání osobních údajů

(1) Za účelem zpracování osobních údajů v různých informačních systémech správce, jsou jednotlivým zaměstnancům přidělovány přístupová oprávnění, a to na základě písemných požadavků jejich nadřízených (emailem).

(2) Přístupová oprávnění schvaluje manažer osobních údajů nebo jim pověření pracovníci a přístupová oprávnění technicky nastavuje na pokyn manažera osobních údajů vedoucí IT nebo jím pověřený zaměstnanec.

(3) Zaměstnanci jsou povinni bezodkladně ohlásit jakékoliv požadavky na změnu přístupových oprávnění svému přímému nadřízenému, který je povinen je bezodkladně sdělit manažeru osobních údajů. Skutečnostmi, které mohou vyvolat požadavek změny přístupových oprávnění, jsou zejména vznik nebo ukončení pracovního poměru, vznik nebo zánik práva zpracovávání osobních údajů z titulu změny pracovního zařazení, zánik oprávnění ke zpracování osobních údajů ze zákona nebo jiná projektová činnost.

(4) Písemný požadavek musí obsahovat jméno a příjmení zaměstnance, jeho pracovní pozici dle organizačního řádu, určení agend v **„registru zpracovávání osobních údajů“,** a tím sw aplikací a datových uložišť a analogových evidencí, do kterých má být umožněn přístup a požadovaný rozsah přístupových oprávnění.

(5) V případě ohrožení ochrany osobních údajů v důsledku porušení povinnosti uvedené v odst. 3 nese zaměstnanec odpovědnost spolu s vedoucím odboru nebo útvaru. V případě ohrožení ochrany osobních údajů v důsledku neoprávněného nebo

[4] Organizační řád. Směrnice Informační bezpečnosti. Pracovní řád. Školní řád.

nedostatečného technického postupu zabezpečení nese odpovědnost vedoucí IT nebo pověřený specialista IT pro danou agendu.

Čl. 13. Uplatňování práv subjektem údajů

(1) Zaměstnanec je povinen usnadňovat výkon práv subjektu údajů a znát postup uplatňování těchto práv, který je dán **„Žádost – Uplatňování práv subjektem údajů“.** (Příloha č. 4 směrnice).

(2) Veškeré postupy uplatňování práv subjektem údajů se řídí interně organizačním postupem „**Uplatňování práv subjektem údajů“**

(3) Zaměstnanec je povinen přijímat žádosti jen takovým způsobem, který zaručuje maximální možné ověření žadatele, zda se skutečně jedná o subjekt údajů, který o práva žádá.

a) Při osobním kontaktu stačí ověření žadatele pověřeným pracovníkem správce.
b) V případě plné moci poskytnuté jiné fyzické osobě stačí podepsání plné moci před pověřeným pracovníkem správce nebo předložení plné moci s úředně ověřeným podpisem žadatele.
c) Přípustné je zaslání žádosti elektronickou poštou podepsanou uznávaným kvalifikovaným podpisem žadatele na elektronickou podatelnu správce.
d) Přípustné je zasláním z datové schránky žadatele do datové schránky správce
e) Přípustné je předání žádosti v elektronickém dokumentu podepsaném uznávaným kvalifikovaným elektronickým podpisem žadatele na elektronickou podatelnu správce.

Čl. 14. Použití tiskopisů a formulářů

(1) Pokud při získávání, zpracovávání osobních údajů je použito tiskopisu, formuláře nebo jiného dokumentu (dále jen formulář), jehož tvorba je v plném řízení správce (dále jen vlastní formulář), je povinností zaměstnance použít jen takový vlastní formulář, který je v souladu s povinnostmi správce transparentně informovat subjekt údajů o zpracovávání osobních údajů.

(2) Pokud jsou formuláře součástí právní povinnosti, použijí se v takovém stavu, jak vyplývá ze zákona nebo vyhlášky.

(3) Tvorba vlastního formuláře se řídí těmito zásadami:

a. Na formuláři musí být uvedeny totožnost a kontaktní údaje správce a jeho případného zástupce.
b. Webový odkaz na dokument „Ochrana osobních údajů – Informace poskytované správcem“
c. Účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování.
d. Pokud jsou osobní údaje získávány na základě zákona je třeba uvést, které zákony to umožňují včetně správního zákona, pokud ho lze využít.
e. Je třeba rozlišit, které osobní údaje jsou získávány na základě právní povinnosti nebo ve veřejném zájmu či z důvodu výkonu veřejné moci a které jsou na základě souhlasu.

f. Jsou-li na formuláři získávány osobní údaje z důvodu právní povinnosti a zároveň na základě souhlasu. Musí být tyto odděleny a podepsány samostatným podpisem.
g. Dobrovolné osobní údaje mohou být získány pouze na základě souhlasu a měly by být na formuláři jasně odděleny.
h. Každý vlastní formulář musí být předem odsouhlasen manažerem ochrany osobních údajů a pověřencem.

Čl. 15. Ochrana osobních údajů v organizaci

(1) Zaměstnanec je povinen přistupovat a získávat oprávnění k osobním údajům v analogové a digitální evidenci jen dle oprávnění schváleného vedením správce podle článku 12. **„Přidělování oprávnění při zpracovávání osobních údajů“.**

(2) Jakákoliv pomocná dokumentace (tabulky, seznamy, výpisy), obsahující osobní údaje sloužící k provoznímu zabezpečení pracovního výkonu zaměstnance musí být dostatečně chráněna tak, aby nedocházelo k neoprávněnému přečtení, kopírování nebo skenovaní dokumentace a po skončení účelu musí být neprodleně skartovány, pokud nejsou součástí zákonné evidence, která vyplývá z právní povinnosti správce.

(3) Manažer osobních údajů zajistí, aby kritická pracoviště, kde dochází ke zpracovávání osobních údajů, byla uspořádána vhodným uspořádáním stolů a nábytku tak, aby nedocházelo k narušení důvěrnosti zpracovávaných osobních údajů.

(4) Zaměstnanec dodržuje zásadu prázdného stolu a čisté obrazovky. Pravidelně při odchodu z pracoviště delším než 15 minut uzamyká obrazovku (svůj účet) tak, aby nedocházelo k neoprávněnému přístupu na zpracovávané osobní údaje.

(5) Jakékoliv přenášení osobních údajů na přenositelných médiích nebo přeposílání z vnitřní sítě musí být prováděno jen se souhlasem manažera osobních údajů a nadřízeného, a to organizačním a technickým postupem definovaným ve směrnici na ochranu informačních aktiv správce.

(6) Jakékoliv tisky obsahující osobní údaje musí být tištěny na sdílených tiskárnách jen pro potřebu zpracovávání osobních údajů v rámci definovaných agend v „**registru činnosti zpracovávání osobních údajů“**. Musí být včas vyzvednuty a nezapomenuty v tiskových frontách tiskových zařízeních.

(7) Zaměstnanec si je vědom, že jakékoliv neoprávněné zpracovávání osobních údajů může být ze strany správce monitorováno a kontrolováno a může být porušením povinností vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci.

(8) Zaměstnanec ukládá osobní údaje na prostředcích správce pomocí sw aplikací, které jsou k tomu určeny a zajišťují dostatečné řízení přístupových práv a evidenci změn na úrovni osobního údaje. V případě, že taková sw aplikace pro danou agendu neexistuje, nebo je nedostatečná, tak zaměstnanec ukládá osobní údaje do samostatných souborů, u kterých lze zajistit řízení přístupových práv a evidenci změn jen na úrovni souboru, jen se souhlasem manažera osobních údajů.

(9) Zaměstnanec ukládá a poskytuje osobní údaje na externí vzdálené úložiště, které není pod zpracovatelskou smlouvou, jen se souhlasem manažera osobních údajů.

(10) Manažer osobních údajů a zodpovědná osoba za příslušnou agendu zpracovávání osobních údajů zodpovídají za fyzické zabezpečení zařízení a archívů používaných při zpracovávání osobních údajů, vhodným mechanickým nebo elektronickým zabezpečením (dveřní a zásuvkové zámky).

(11) Zaměstnanec je povinen před každým předáváním osobních údajů do zahraničí o tomto informovat manažera osobních údajů a svého nadřízeného, pokud není toto již součástí schválené, agendy v rámci **„registru zpracovávání osobních údajů“** a postupovat jen v souladu s pokyny manažera osobních údajů a pověřence.

(12) Pokud má zaměstnanec povoleno ukládat a zpracovávat na prostředcích správce osobní údaje pro svou osobní potřebu, oddělí tyto údaje od pracovních do složek s názvem **„Osobní“**.

(13) Pokud má zaměstnanec dovoleno používat ke zpracovávání osobních údajů vzdálený přístup do vnitřní sítě správce, formou vzdálené obrazovky nebo vzdáleného přístupu, nebo používá mimo vnitřní síť zařízení správce (NTB, mobil, tablet, aj.), na kterém zobrazuje osobní údaje, za které zodpovídá správce, je povinen dodržovat tuto směrnici a zabezpečit důvěrnost zobrazovaných osobních údajů stejným způsobem jako by byl na pracovišti správce.

(14) Pokud má zaměstnanec povoleno zpracovávat osobní údaje na prostředcích, které má ve svém osobním vlastnictví, provádí toto zpracovávání jen se souhlasem manažera osobních údajů a se schválením vedoucího IT nebo IT specialisty a je povinen dodržovat tuto směrnici a zabezpečit důvěrnost zobrazovaných osobních údajů stejným způsobem jako by byl na pracovišti správce a je povinen dodržovat všechna organizační a technická zabezpečení tak, jako by to bylo zařízení správce.

Čl. 16. Zpracovatelé

(1) Je-li v příslušné agendě ke zpracovávání osobních údajů použito externího zpracovatele (např. zpracování mezd, zajištění stravovacích služeb, obědy pro děti), zajistí manažer osobních údajů ve spolupráci se zodpovědnou osobou za příslušnou agendu, aby zpracovávání osobních údajů zpracovatelem bylo pod smlouvou, která mimo jiné bude obsahovat následující body, zpracovatel:

a) Zpracovává osobní údaje pouze na základě doložených pokynů správce. Pokud zpracovatel zpracovává osobní údaje mimo pokyny, informuje o tom správce, ledaže by právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

b) Zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

c) Přijme všechna opatření požadovaná pro technické a organizační zabezpečení zpracování.

d) V případě možného zapojení dalšího zpracovatele informuje neprodleně správce a vyžádá si od něj souhlas.

e) Je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti při zabezpečení „**uplatňování práv subjektem údajů“**

f) Je správci nápomocen při zajišťování souladu s povinnostmi při „hlášení porušení zabezpečení osobních údajů dozorovému úřadu“ a v případě jakéhokoliv porušení zabezpečení osobních údajů, za které zodpovídá správci, toto neprodleně hlásí správci. K nahlášení incidentu použije zpracovatel email reditel@zstyrfren.cz nebo telefonní číslo 556 835 038 na kontaktní osobu správce pro řízení incidentů a poté zpracovatel s manažerem osobních údajů vyplní formulář „hlášení incidentu“.

g) V souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud jiná právní povinnost nepožaduje uložení osobních údajů.

h) Poskytne správci veškeré informace (postupy, směrnice, vnitřní předpisy) potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku.

Čl. 17. Závěrečná ustanovení

(1) Směrnice nabývá účinnosti dne 25. 5. 2018.

Ve Frenštátě pod Radhoštěm dne 24. 5. 2018

……
RNDr. Zdeňka Murasová, ředitelka školy

Čl. 18. Seznam příloh

Příloha č. 1 Ochrana osobních údajů – Informace poskytované správcem.
Příloha č. 2 Hlášení Incidentu.
Příloha č. 3 Registr a záznamy o činnostech zpracovávání osobních údajů.
Příloha č. 4 Žádost – Uplatňování práv subjektem údajů.