Mateřská škola Včelička
U Školky 271
277 15 Tišice

Vnitřní předpis č. XX/2018 pro oblast ochrany osobních údajů

Verze 1

1. Úvodní ustanovení

Tento vnitřní předpis, v souladu s nařízením Evropského parlamentu a Rady 2016/679/EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR“) upravuje zpracování a nakládání s osobními údaji a jejich používání, uchovávání a předávání v případech, kdy správcem osobních údajů je Mateřská škola Včelička.

Tento vnitřní předpis je závazný pro všechny osoby v zaměstnaneckém či obdobném poměru a osoby pracující pro Mateřskou školu Včelička na základě smlouvy v případech, kdy přicházejí do styku s osobními údaji (dále jen „zaměstnanec“).

2. Vymezení pojmů

2.1. Osobní údaj – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

2.2. Zpracování – jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů jako je 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.

2.3. Shromáždění – systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější použití.

2.4. Omezení zpracování – označení uložených osobních údajů za účelem jejich zpracování v budoucnu.

2.5. Pseudonymizace – zpracování osobních údajů tak, že již nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně.

2.6. Evidence – jakýkoli strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií.

2.7. Správce – v případě mateřské školy mateřská škola Včelička jako právnická osoba, která určuje účely a prostředky zpracování osobních údajů.

2.8. Příjemce – subjekt, kterému jsou osobní údaje poskytnuty, s výjimkou orgánů veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právním předpisem (např. Mateřská škola Včelička).

2.9. Souhlas subjektu údajů – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává své svolení ke zpracovávání svých osobních údajů.

2.10. Porušení zabezpečení osobních údajů – porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů.

2.11. Zvláštní kategorie osobních údajů – údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení, členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby. Zpracování takových osobních údajů je zakázáno s výjimkami uvedenými v čl. 9 GDPR.

3. Zákonnost zpracování v jednotlivých oblastech

3.1. Mateřská škola Včelička zpracovává osobní údaje subjektů údajů – dětí navštěvujících mateřskou školu, jejich zákonných zástupců, popř. osob je vyzvedávajících.

3.2. Osobní údaje lze zpracovávat a uchovávat za předpokladu, že

a) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje, tj. zejména na základě zákona č. 561/2004 Sb., zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (např. stravování dítěte)

c) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (např. zajištění zdravotního ošetření v případě úrazu, alergie apod.)

d) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce

e) subjekt údajů udělil souhlas se zpracováním, přitom tento souhlas může kdykoli odvolat (např. identifikační údaje osob vyzvedávajících děti z mateřské školy).

3.3. Shromažďování osobních údajů může být prováděno pouze za účelem, pro který jsou osobní údaje zpracovávány.

3.4. Na zpracování osobních údajů se v Mateřské škole Včelička podílejí:

a) vedení mateřské školy,

b) učitelky.

3.5. Každý zaměstnanec, který pracuje s osobními údaji, je povinen zpracovávat pouze přesné osobní údaje, které získal v souladu s GDPR. Pokud zjistí, že zpracovávané osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaj opraví nebo doplní anebo zlikviduje v souladu se spisovým a skartačním řádem.

3.6. Při použití osobních údajů v rámci plnění pracovních úkolů jsou zaměstnanci povinni se chovat tak, aby nedošlo k porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (způsob zabezpečení osobních údajů obsahuje Čl. 32 GDPR).

3.7. Za ochranu dat a osobních údajů odpovídá každý zaměstnanec, který data a osobní údaje zpracovává. Za jejich ochranu odpovídá též přímý nadřízený těchto zaměstnanců. Ten je povinen provádět kontrolní činnost a při ní ověřovat, zda s osobními údaji je nakládáno podle GDPR a tohoto vnitřního předpisu.

3.8. Zpracování osobních údajů může být vykonáváno jen po nezbytně nutnou dobu, tj. zpravidla po dobu účasti dítěte na předškolním vzdělávání podle školského zákona. Pomine-li účel, pro který byly osobní údaje zpracovávány, zpracování musí být ukončeno. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely archivace, poté musí být zlikvidovány v souladu se spisovým a skartačním řádem. Zpracování musí být také ukončeno, pokud subjekt údajů odvolá svůj souhlas, který poskytl, nebrání-li tomu právní přepis.

3.9. Osobní údaje musí být zpracovávány korektně, zákonným a transparentním způsobem v souladu s čl. 5 GDPR.

4. Záznamy o činnostech zpracování osobních údajů

4.1. Každý zaměstnanec odpovědný za ucelenou agendu zpracovává ve spolupráci s pověřencem obce Tišice záznamy o činnostech zpracování podle čl. 30 GDPR.

4.2. Každý zaměstnanec odpovědný za ucelenou agendu prověřuje nutnost změny záznamů o činnostech zpracování v návaznosti na změny právních předpisů.

4.3. Aktualizace záznamů o činnostech zpracování osobních údajů jsou předávány ředitelce mateřské školy.

4.4. Tyto záznamy tvoří přílohu tohoto vnitřního předpisu, příloha je průběžně aktualizována s uvedením data zpracování záznamu.

5. Získávání souhlasu subjektu údajů

5.1. Nestanoví-li nařízení o ochraně osobních údajů nebo zvláštní zákon jinak, mohou být osobní údaje zpracovávány pouze s výslovným souhlasem subjektu údajů. V tomto případě musí být subjekt údajů srozuměn s tím, jaké osobní údaje, za jakým účelem a na jak dlouhou dobu jsou poskytovány. Souhlas subjektu údajů musí být správce schopen prokázat po celou dobu zpracování.

5.2. Subjekt údajů musí být seznámen s tím, že má právo na

a) Přístup k osobním údajům
b) Výmaz (podle čl. 17 případy, kdy osobní údaje již nejsou třeba, došlo k odvolání souhlasu, dojde k oprávněné námitce, osobní údaje byly zpracovány neoprávněně)
c) Opravu nebo doplnění
d) Omezení zpracování (podle čl. 18 v případě, že subjekt osobních údajů popírá přesnost osobních údajů, zpracování je protiprávní, ale subjekt údajů nepožaduje výmaz, osobní údaje nejsou potřeba, ale subjekt údajů je požaduje, do doby vyřešení námitky subjektu údajů)
e) Přenositelnost
f) Vznést námitku
g) Nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, tj. právo nebýt předmětem rozhodnutí s uvedenými účinky bez účasti lidského faktoru.

5.3. Subjekt údajů má právo svůj souhlas kdykoli odvolat, o čemž musí být při udělení souhlasu poučen.

5.4. Pokud jsou osobní údaje získávány prostřednictvím formulářů, musí každý formulář obsahovat doložku. V textu doložky musí být informace o účelu, za jakým jsou osobní údaje získávány, jakým způsobem budou využívány a prohlášení o tom, že získané osobní údaje nebudou využívány k jiným účelům. Další součástí doložky bude souhlas se zpracováním

osobních údajů a seznámení s právy subjektu údajů. Souhlas musí být podepsán subjektem údajů.

5.5. Zpracování informací týkajících se telefonů a e-mailových adres subjektů údajů za účelem zasílání informací je možné jen na základě jejich souhlasu.

6. Zpracování zvláštních kategorií osobních údajů

6.1. Mateřská škola Včelička zpracovává zvláštní kategorie osobních údajů pouze v případě, kdy

a) subjekt údajů udělil výslovný písemný souhlas (např. pro účely zveřejňování na webu, vyzvedávání dítěte jinou osobu než zákonným zástupcem) nebo

b) tak stanoví právní předpis (např. v oblasti přenosných nemocí v souvislosti s karanténou).

7. Provozování kamerového systému

Mateřská škola Včelička neprovozuje kamerový systém.

8. Informace pro výkon práv subjektu údajů

8.1. V případě získání osobních údajů od subjektu údajů, musí příslušný zaměstnanec sdělit subjektu údajů (zpravidla zákonnému zástupci dítěte)

a) kontaktní údaje Mateřské školy Včelička

b) účely zpracování a právní základ

c) případné příjemce osobních údajů (např. obec Tišice)

d) dobu, po kterou budou osobní údaje uloženy, je-li to nezbytné

e) existenci práva požadovat přístup k osobním údajům, jejich opravu nebo výmaz, popř. omezení zpracování a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů

f) existenci práva odvolat souhlas se zpracováním osobních údajů

g) poučení o právu obrátit se na Úřad pro ochranu osobních údajů.

8.2. Obdobně se postupuje v případě, že nebyly osobní údaje získány od subjektu údajů, navíc nad rámec informací podle předchozího odstavce je třeba sdělit zdroj, ze kterého osobní údaje pocházejí.

8.3. Informování podle předchozích bodů písm. a), b), c), d) se nepoužijí, pokud Mateřská škola Včelička již tyto údaje má, poskytnutí takových informací není možné z důvodu veřejného zájmu, získání je uloženo právním předpisem nebo osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat mlčenlivost.

9. Přístup k osobním údajům

9.1. Subjekt údajů má právo získat potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány. Mateřská škola Včelička poskytne na žádost bezplatně jednu kopii zpracovávaných osobních údajů. Další kopie se zpoplatňují poplatkem.

9.2. Obdobně se postupuje při uplatnění práva na přenositelnost podle čl. 20 GDPR.

9.3. Získáním kopie nesmějí být nepříznivě dotčena práva a svobody jiných osob, pro tyto účely se jejich osobní údaje a informace o nich začerní.

9.4. Lhůta k vyřízení žádosti subjektu údajů je jeden měsíc od přijetí žádosti.

10. Zveřejňování osobních údajů

10.1. Osobní údaje lze zveřejnit jen se souhlasem subjektu údajů nebo na základě povinnosti stanovené právním předpisem (např. na nástěnce nebo webových stránkách mateřské školy).

10.2. Zveřejnit lze v omezeném rozsahu i osobní údaje např. v souvislosti s životním jubileem dětí. Za účelem blahopřání lze zveřejnit pouze jméno a příjmení a uvedení důvodu „životní jubileum“. K uvedení konkrétního data narození, bydliště je však třeba souhlas subjektu údajů.

10.3. Nelze zveřejnit zvláštní osobní údaje dětí (např. zdravotní stav, národnost apod.).

11. Zabezpečení osobních údajů

11.1. Dokumenty s osobními údaji v listinné podobě podléhají režimu spisového a skartačního řádu. Při práci s nimi musí zaměstnanci obce dbát zvýšené opatrnosti. K dokumentům mají přístup jen ti zaměstnanci, kteří přístup k těmto dokumentům nezbytně potřebují k výkonu svých pracovních činností.

11.2. Dokumenty musí být zabezpečeny proti odcizení a prohlížení nepovolanými osobami, a to zejména uchováváním v uzamčených skříních, neponecháním v nezamčené místnosti bez přítomnosti odpovědného zaměstnance[1].

11.3. Porušení zabezpečení osobních údajů může spočívat v

a) porušení důvěrnosti – neautorizované nebo náhodné prozrazení (zveřejnění) nebo neautorizovaný přístup k osobním údajům
b) porušení dostupnosti – náhodná ztráta či zničení osobních údajů
c) porušení integrity – nežádoucí či neautorizovaná změna osobních údajů.

11.4. Ochrana osobních údajů v informačních systémech je zajištěna přidělováním přístupových oprávnění a používáním přístupových hesel, které jsou jednotlivým zaměstnancům přidělena. Dále musí být zajištěny následující požadavky:

a) Je zakázáno zasílat osobní údaje e-mailem.
b) Pokud aplikace umožňuje pořizování záznamů o přístupech k osobním údajům, musí být funkce aktivní (auditní stopa) a je zakázáno záznamy o přístupech mazat nebo jakkoli upravovat.
c) Při pořizování nového softwaru je třeba požadovat funkci pro pořizování auditní stopy zahrnující informaci o uskutečněném vyhledání osobních údajů s identifikací uživatele, datem a časem a rozsahem prohlížených osobních údajů.
d) Uchovávání externích datových nosičů obsahujících osobní údaje, které již nebudou používány, je zakázáno. Takové nosiče se musí předat osobě odpovědné za skartaci, která zajistí jejich likvidaci. Výjimkou jsou datové nosiče, které jsou součástí archivu, ty se řídí spisovým a skartačním řádem.
e) Zaměstnancům jsou vytvořeny přístupy do IS a k jednotlivým aplikacím v souladu se zásadami upravujícími oblast IT. Při skončení výkonu funkce jsou přístupy přenastaveny nebo zrušeny.

11.5. Každý zaměstnanec na svém pracovišti musí učinit vhodná a přiměřená opaření k ochraně osobních údajů. Jestliže mu v tom brání technické nebo organizační překážky, které nemůže sám vyřešit, informuje neprodleně ředitelku mateřské školy.

[1] Např. při úklidu kanceláří

11.6. Každý zaměstnanec si musí nastavit mechanismy, aby pokud možno zjistil porušení zabezpečení osobních údajů sám.

11.7. Porušení zásad zabezpečení osobních údajů se považuje za porušení pracovní kázně. Zpřístupnění osobních údajů nebo jejich ztráta se považuje za závažné porušení pracovní kázně.

12. Opravy a doplnění osobních údajů, omezení zpracování osobních údajů

12.1. Příslušný zaměstnanec neprodleně opraví nebo doplní chybné nebo nepřesné osobní údaje, pokud to zjistí sám nebo ho na to upozorní subjekt údajů (zákonný zástupce dítěte) nebo jiný zaměstnanec.

12.2. V této souvislosti může přicházet v úvahu i omezení zpracování osobních údajů, v takovém případě postupuje příslušný zaměstnanec podle zásad uvedených výše.

13. Likvidace osobních údajů

13.1. Pomine-li účel, pro který byly osobní údaje zpracovávány, provede odpovědný zaměstnanec jejich likvidaci podle zásad stanovených ve spisovém a skartačním řádu.

13.2. Data uchovávaná na datových nosičích jsou po uplynutí archivační doby likvidována, o likvidaci je sepsán zápis.

13.3. Data z přepisovatelných datových nosičů musí být po ukončení zpracování vymazaná, nosiče, u kterých nelze tuto operaci provést, musí být fyzicky zničena tak, aby nebyla možná jejich rekonstrukce. O zničení musí být sepsán zápis.

14. Odpovědnost zaměstnanců a ohlašování porušení zabezpečení osobních údajů

14.1. Každý zaměstnanec odpovídá za řádné zpracování osobních údajů ve své působnosti v souladu s GDPR a tímto vnitřním předpisem.

14.2. Zaměstnanci jsou povinni zachovávat mlčenlivost o osobních údajích, k nimž mají přístup nebo o nichž se dozvěděli.

14.3. Předávání spisů s osobními údaji v případě déletrvající nepřítomnosti zaměstnance se děje podle zásad pro zastupování.

14.4. Namátkovou kontrolu dodržování této směrnice a skutečnosti, zda zaměstnanci mají v rámci IS přístup jen k takovým agendám s osobními údaji, ke kterým mají oprávnění, kontroluje ředitelka mateřské školy.

14.5. Při porušení zabezpečení osobních údajů musí příslušný zaměstnanec, který porušení zjistil nebo se o něm dověděl, nejpozději do 5 hodin informovat ředitelku mateřské školy a porušení zdokumentovat (stručný popis události a např. otisk obrazovky). Zároveň neprodleně učiní potřebná opatření k zabránění pokračování tohoto porušení (např. vypnutím aplikace) a v případě potřeby vyzve ke spolupráci osobu odpovědnou za IT.

14.6. Krádež dat je třeba oznamovat neprodleně po zjištění.

14.7. Není třeba řešit porušení dostupnosti osobních údajů v důsledku dočasného výpadku elektřiny.

15. Ředitelka mateřské školy a spolupráce s dozorovým úřadem

15.1. Za dodržování GDPR odpovídá ředitelka mateřské školy, v případě její nepřítomnosti zástupkyně ředitelky.

15.2. Ředitelka mateřské školy plní následující povinnosti:

a) analyzuje procesy a rizika mající dopad na zpracování osobních údajů

b) má v gesci vnitřní předpis pro oblast ochrany osobních údajů

c) ohlašuje za Mateřskou školu Včelička případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů

d) je kontaktní osobou pro komunikaci s Úřadem pro ochranu osobních údajů.

15.3. Ředitelka mateřské školy po metodické stránce v oblasti GDPR spolupracuje s pověřencem obce, kterého lze kontaktovat jednak prostřednictvím sekretariátu obce, jednak na e-mailové adrese poverenec@tisice.cz.

15.4. Pověřenec obce se podílí na školení zaměstnanců mateřské školy, šetření případů porušení zabezpečení osobních údajů a oznamování porušení Úřadu pro ochranu osobních údajů ve lhůtě a za podmínek stanovených čl. 33 GDPR.

16. Podněty a stížnosti subjektů údajů

16.1. Podněty a stížnosti subjektů údajů jsou předávány ředitelce mateřské školy ve lhůtě jednoho týdne od jejich přijetí se stanoviskem odpovědného zaměstnance.

16.2. Ředitelka mateřské školy nebo jí pověřený zaměstnanec zpracuje odpověď subjektu údajů.

Tento vnitřní předpis byl schválen dne 21. května 2018.

Vnitřní předpis nabývá účinnosti dne 25. května 2018

Pověřena řízením Mateřské školy Včelička: ……

Veronika Kovářová