

Správce osobních údajů – ZŠ a MŠ Brantice		
Vnitřní předpis		
Ochrana osobních údajů a Komerové systémy		
	Zrušuje předpis:	01.09.2018
	Autor/správce	Pověřenec/Ředitelka
	Schvaluje:	Ředitelka
	Správce ICT	Ředitelka
	Účinnost od:	01.11.2025
	Počet stran:	8
	Počet příloh:	4
Obsah:		
ČL. 1.	PŮSOBNOST	1
ČL. 2.	POJMY A DEFINICE	1
ČL. 3.	HLAVNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	2
ČL. 4.	ZÁKONNÉ DŮVODY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	2
ČL. 5.	PLNĚNÍ INFORMAČNÍ POVINNOSTI SPRÁVCE.....	3
ČL. 6.	SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ	3
ČL. 7.	ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A JEJICH VEDENÍ.....	3
ČL. 8.	POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ.....	4
ČL. 9.	HLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ – INCIDENT	4
ČL. 10.	PŘIDĚLOVÁNÍ OPRÁVNĚNÍ PŘI ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ.....	5
ČL. 11.	UPLATŇOVÁNÍ PRÁV SUBJEKTEM ÚDAJŮ.....	5
ČL. 12.	POUŽITÍ TISKOPISŮ A FORMULÁŘŮ.....	5
ČL. 13.	ZVÝŠENÁ RIZIKA, KAMERY, AUTOMATIZOVANÁ ZPRACOVÁVÁNÍ A AI	5
ČL. 14.	EXTERNÍ ZPRACOVATELÉ.....	6
ČL. 15.	POVINNOSTI ZAMĚSTNANCŮ A MLČENLIVOST PŘI ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ	7
ČL. 16.	KONTROLA OPATŘENÍ - REVIZE TÉTO SMĚRNICE A PROŠKOLOVÁNÍ	8
ČL. 17.	SEZNAM PŘÍLOH	8

Čl. 1. Působnost

- (1) **„Účelem směrnice“** je stanovit v podmínkách ZŠ a MŠ Brantice dále jen **„správce“** jednotný proces automatizovaného i neautomatizovaného zpracování osobních údajů při vzdělávání, a to v souladu s nařízením EU 2016/679 (GDPR), a zákonem č. 110/2019 Sb. o zpracování osobních údajů a metodických pokynů dozorového úřadu www.uouu.cz.
- (2) Tato směrnice je závazná pro všechny zaměstnance správce a osoby přistupující k osobním údajům, za které zodpovídá správce.

Čl. 2. Pojmy a definice

- (1) **„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 v jakékoliv jejich podobě,
- (2) **„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, subjektem údajů může být dítě, zaměstnanec, zákonný zástupce, rodič, občan, pacient, klient, zákazník, aj.,
- (3) **„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 behaviorální reklamy),

- (4) **„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 stavu či o sexuální orientaci fyzické osoby. Pro účely této směrnice je jednotně používán pojem osobní údaj i pro kategorii citlivých údajů,
- (5) **„profilováním“** jakákoli forma 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,
- (6) **„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,
- (7) **„anonymizace“** zpracování osobních údajů tak, že již nikdy nemohou být přiřazeny konkrétnímu subjektu údajů,
- (8) **„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,
- (9) **„zpracovatelem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje, za které je zodpovědný správce,
- (10) **„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 správcem jako **„Incident“**, (ztráta složky s osobními údaji, napadení databáze klientů hackerem, neoprávněné zveřejnění osobních údajů na webu organizace aj,)
- (11) **„dotčeným dozorovým úřadem“** dozorový úřad, který dozoruje zpracovávání osobních údajů v ČR dle zákona www.uoou.cz.

Čl. 3. Hlavní zásady zpracování osobních údajů

- (1) Správce a zaměstnanci při zpracování osobních údajů se mají povinnost řídit těmito zásadami:
 - 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, za slučitelné se považují účely pro řešení životních situací občanů,
 - 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 a zpracovávány přesně,
 - 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, důvěrnost a dostupnost** – technické a organizační zabezpečení osobních údajů, které zajistí, že nebude porušena integrita a důvěrnost osobních údajů.

Čl. 4. Zákonné důvody zpracování osobních údajů

- (1) Osobní údaj lze zpracovávat, pokud je předem přiřazen 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) Přiřazení zákonného důvodu musí být provedeno před samotným započítáním zpracovávání a po konzultaci s pověřencem viz bod Čl. 12.

Čl. 5. Plnění informační povinnosti správce

- (1) Za účelem splnění informační povinnosti správce je na webových stránkách školy <https://www.zsbrantice.cz/> zveřejněn povinný dokument **„Informace ke zpracování osobních údajů, kamerovým systémům a uplatňování práv pro veřejnost a zaměstnance“ vedený jako příloha č. 1**. V případě jakéhokoliv získávání osobních údajů je zaměstnanec na žádost subjektu údajů povinen s tímto dokumentem seznámit, resp. předat jeho listinné vyhotovení nebo odkázat na jeho elektronickou verzi uveřejněnou na webu školy.
- (2) Za aktuálnost tohoto dokumentu je zodpovědná ředitelka ve spolupráci s pověřencem.

Čl. 6. Souhlas se zpracováním osobních údajů

- (1) Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování konkrétního osobního údaje pro konkrétního správce, k určitému účelu zpracování a na určitou jednoznačnou a nezaměnitelnou dobu, který musí být subjektu údajů zřetelně předem sdělen.
- (2) Zaměstnanec je povinen souhlas před prvním použitím konzultovat s ředitelkou a pověřencem.
- (3) 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.
- (4) Subjekt údajů má právo svůj souhlas kdykoli odvolat a musí být na to předem upozorněn. 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.
- (5) 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 a 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.
- (6) Za účelem zpracovávání osobních údajů při školní nebo mimoškolní činnosti, které nelze zpracovávat jiným zákonným způsobem, je veden a předkládán školou zákonným zástupcům **„Souhlas se zpracováním osobních údajů“, který je veden jako příloha č. 2 této směrnice.**

Čl. 7. Záznamy o činnostech zpracování osobních údajů a jejich vedení

- (1) Dle zákona Správce vede záznamy o zpracování osobních údajů (dále jen "záznamy"), ve kterých má zpracovány veškeré agendy, při kterých dochází ke zpracování osobních údajů subjektů údajů v rámci školní a mimoškolní činnosti.

- (2) Tyto záznamy (agendy) obsahují všechny tyto informace: kontaktní údaje správce, pověřence a správce záznamů, úsek nebo útvar, kde je agenda zpracovávána, název agendy, účel zpracování, kategorie subjektů údajů, kategorie osobních údajů, zvláštní kategorie osobních údajů, kategorie příjemců údajů, zákonné důvody zpracování, identifikaci právních předpisů zpracování upravujících, doba uchování, obecný popis technickoorganizačního zabezpečení, organizační zodpovědnost, technická zodpovědnost, používané analogové, elektronické nebo webové formuláře, informační systémy a cloudy ve kterých je agenda vedena.
- (3) Zodpovědnost za vedení záznamů a za jejich aktuálnost má ředitelka ve spolupráci s pověřencem. Záznamy se vedou po dobu 3 let zpětně.
- (4) Zaměstnanec má povinnost zpracovávat osobní údaje jen v souladu s těmito záznamy. Pokud zpracovávání osobních údajů neodpovídá záznamům nebo dochází ke změně agendy, informuje o tom bezodkladně ředitelku a pověřence
- (5) Za účelem aktuálnosti záznamů provede pověřenec s ředitelkou 1x do roka konzultaci k aktualizaci záznamů. Konzultace může být řešena emailem, online nebo osobně dle důležitosti změn. Struktura a záznamy jsou vedeny jako **Příloha č. 2 Záznamy o činnostech zpracování osobních údajů**.

Čl. 8. 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 jeho zaměstnanců. Současně přispívá k rozvoji a udržování zásad, postupů a procesů ochrany osobních údajů, konzultuje jejich aktualizaci, a ve spolupráci s ředitelkou provádí jejich průběžnou kontrolu.
- (2) Monitoruje soulad činností správce s platnými a přímo použitelnými normami Evropské unie a platnými obecně závaznými právními předpisy České republiky 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 dozorovým úřadem www.uoou.cz.
- (4) V případě incidentu doporučuje, zda je třeba jej hlásit dozorovému úřadu a subjektům údajů.
- (5) Ředitelka a zaměstnanci dbají, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.
- (6) 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 řádným plněním svých úkolů nesmí být správcem sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen ředitelce.
- (7) Subjekty údajů (občané, zaměstnanci) se mohou obracet na pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv.
- (8) Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů zákonem vázán mlčenlivostí a plní další úkoly stanovené smlouvou mezi pověřencem a správcem.

Čl. 9. Hlášení porušení zabezpečení osobních údajů – Incident

- (1) Každý zaměstnanec (nebo externí zpracovatel) je povinen bezodkladně nahlásit i podezření na jakékoliv porušení zabezpečení osobních údajů (incident) ředitelce a pověřenci na e-mail edum@edum.eu a na telefonní číslo pověřence +420 602553813.
- (2) Po vyhodnocení závažnosti porušení zabezpečení osobních údajů pověřencem s výsledkem, že se jedná o porušení ochrany osobních údajů, ředitelka s pověřencem vyplní formulář **Hlášení incidentu**, který je součástí **přílohy č. 1** této směrnice.
- (3) V případě, že bude pověřencem doporučeno nahlášení incidentu dozorovému úřadu a subjektům údajů, provede ředitelka nebo jím pověřená osoba toto nahlášení do 72 hodin od nahlášení incidentu zaměstnancem.

- (4) Ředitelkou podepsané hlášení Incidentu vede ředitelka a pověřenec v evidenci po dobu 3 let zpětně.

Čl. 10. Přidělování oprávnění při zpracovávání osobních údajů

- (1) Za účelem zpracování osobních údajů v různých informačních systémech, jsou jednotlivým zaměstnancům přidělovány přístupová oprávnění, a to na základě jejich požadavků na ředitelku. Zaměstnanci jsou povinni bezodkladně ohlásit jakékoliv požadavky na změnu přístupových oprávnění ředitelce. Skutečnostmi, které mohou vyvolat požadavek změny přístupových oprávnění, jsou zejména vznik nebo ukončení pracovního poměru, vznik nebo zánik práva zpracovávání osobních údajů změnou pracovního zařazení nebo přístupů do agend a registrů.
- (2) Písemný požadavek (email) musí obsahovat jméno a příjmení zaměstnance, jeho pracovní pozici dle organizačního řádu, určení sw aplikací a datových uložišť a analogových evidencí, do kterých má být umožněn přístup a požadovaný rozsah přístupových oprávnění.
- (3) Přístupová oprávnění schvaluje ředitelka a na jeho pokyn nastavuje ICT specialista.

Čl. 11. Uplatňování práv subjektem údajů

- (1) Zaměstnanec je povinen usnadňovat výkon práv subjektu údajů. Výkon práv je prováděn jen na základě žádosti Subjektu údajů. Zaměstnanec je povinen přijatou žádost řešit s ředitelkou a pověřencem. Vyřizování žádosti se řídí pravidly stanovenými **v příloze č. 1** této směrnice, která obsahuje kompletní výčet všech práv, způsob podání a vyřízení žádosti.
- (2) Za vyřízení a evidenci žádostí souvisejících s uplatněním práv je zodpovědný zaměstnanec který má příslušné osobní údaje ve své agendě.

Čl. 12. Použití tiskopisů a formulářů

- (1) Pokud je při získávání osobních údajů použito tiskopisu, formuláře (analogový, elektronický nebo webový) nebo jiného dokumentu například smluv, vyhlášek, interních postupů a týká se zpracování osobních údajů, jehož tvorba je plně v kompetenci správce (dále jen "vlastní formulář"), musí být předem odsouhlasen ředitelkou a schválen a revidován pověřencem.
- Na formuláři musí být uvedeny totožnost a kontaktní údaje správce a jeho případného zástupce (název správce, adresa organizace, název odboru (útvary), tel., email, adresa podatelny, datová schránka).
 - Účely zpracování, pro které jsou osobní údaje určeny a právní základ a zákonné důvody ke zpracovávání dle Čl. 4 této směrnice.
 - Text a webový odkaz na informace poskytované správcem. **"Ostatní práva a povinnosti při zpracovávání osobních údajů" naleznete na webových stránkách školy <https://www.zsbrantice.cz/>.**
 - Pokud jsou formuláře součástí právní povinnosti správce, použijí se v takovém znění, které vyplývá z obecně závazných právních předpisů. Pokud je použito formuláře nebo tiskopisu, za který zodpovídá jiný správce, oznámí zaměstnanec tuto skutečnost subjektu údajů.

Čl. 13. Zvýšená rizika, Kamery, Automatizovaná zpracovávání a AI

- (1) Pokud správce zpracovává osobní údaje, kde mohou vznikat významná rizika například: na základě "oprávněného zájmu" nebo "ve veřejném zájmu" nebo zpracovává osobní údaje bez souhlasu, bez dostatečné právní opory, **(např. GPS v autech, ověřování formou biometrie, kamerové systémy, jiné záznamové systémy dat, kvalita a efektivita práce zaměstnanců, informační bezpečnost apod.)** nebo zpracovává osobní údaje při výuce, kde dochází k plně automatizovanému vyhodnocování osobních údajů pomocí vyspělých SW systémů nebo umělé inteligence (AI), nebo při zpracovávání mohou být významná rizika tak:
- (2) O zpracování uvedeném v odst. (1) tohoto článku informuje zaměstnanec předem pověřence a vyžádá si stanovisko ke zpracovávání osobních údajů.

- (3) Veškeré zpracovávání osobních údajů na základě oprávněných zájmů, ve veřejném zájmu, automatizované rozhodování nebo s významnými riziky bude uveřejněno pro zaměstnance a občany v rámci veřejného dokumentu na webu města v Příloze č. 1. Ke každému takovému zpracovávání bude v souladu se zákonem nebo metodikou Úřadu pro ochranu osobních údajů www.uoou.cz, vypracován "**test proporcionality**", zda zpracovávání osobních údajů správcem nepřevyšuje oprávněné zájmy subjektu údajů. Tyto testy, by měly obsahovat ve stručném rozsahu následující:
- Systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce.
 - Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu a alternativním postupům.
 - Posouzení rizik pro práva a svobody subjektů údajů.
 - Plánovaná opatření ke snížení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob a legislativě.
- (1) Za vypracování testů je odpovědný zaměstnanec, do jehož příslušnosti dané zpracovávání osobních údajů spadá, a to ve spolupráci s pověřencem. Za tímto účelem ředitelka poskytne a zajistí pověřencem požadované veškeré informace. Evidenci testů proporcionality vede zaměstnanec v kopii pověřenec.
- (2) Ředitelka ve spolupráci s pověřencem doplní povinné transparentní informace o zařízeních a systémech pro veřejnost do přílohy č. 1 této směrnice a dále s pověřencem konzultují obsah a vhodnost umístění informační tabulek na vstupu do monitorovaných objektů a prostor.
- (3) Předávání záznamů z kamer provádí jen ředitelka nebo jím pověřená osoba na základě protokolu, který je v příloze č. 1 této směrnice.

Čl. 14. Externí Zpracovatelé

- (1) Je-li v rámci schválené agendy ke zpracování osobních údajů použito externího zpracovatele, provede zaměstnanec konzultaci s pověřencem tak, aby zpracování osobních údajů zpracovatelem bylo řádně ošetřeno smluvním ustanovením, která mimo jiné bude upravovat tyto povinnosti zpracovatele:
- a. Zpracovatel zpracovává osobní údaje pouze na základě prokazatelných pokynů správce.
 - b. Zpracovatel zajišťuje, aby se osoby oprávněné pro něj zpracovávat osobní údaje zavázaly k mlčenlivosti.
 - c. Zpracovatel dle zákona přijme technická a organizační opatření nezbytná či pro zabezpečení a zpracování osobních údajů.
 - d. Zpracovatel, v případě možného zapojení dalšího zpracovatele, neprodleně informuje o této skutečnosti správce a vyžádá si od něj souhlas k takovému zpracování.
 - e. Je-li to možné, je zpracovatel povinen být správcem nápomocen prostřednictvím vhodných technických a organizačních opatření k naplnění povinností správce při zabezpečování uplatňování práv subjektem údajů a zajišťování souladu s výkonem povinností správce při hlášení porušení zabezpečení osobních údajů dozorovému úřadu a v případě jakéhokoliv porušení zabezpečení osobních údajů, postupovat dle Čl. 9.
 - f. Po ukončení poskytování služeb spojených se zpracováním osobních údajů zpracovatel v souladu s rozhodnutím správce všechny předané osobní údaje buď vymaže, nebo je prokazatelně předá zpět správci a vymaže existující kopie, pokud mu jiná právní povinnost neukládá osobní údaje nadále uchovávat.
 - g. Zpracovatel poskytne správci, na vyžádání, veškeré informace (postupy, směrnice, vnitřní předpisy) potřebné k prokázání toho, že byly splněny povinnosti stanovené v tomto článku a ve smlouvě se zpracovatelem.

Čl. 15. Povinnosti zaměstnanců a mlčenlivost při zpracovávání osobních údajů

- (1) Každý zaměstnanec je odpovědný za obsahovou správnost, úplnost a ochranu jím zpracovávaných osobních údajů a je povinen zachovávat mlčenlivost o osobních údajích a zařízeních, s nimiž se při výkonu své práce seznámí i o bezpečnostních opatřeních k jejich ochraně, a to i po skončení pracovní činnosti. Za účelem naplnění tohoto požadavku, každý zaměstnanec nebo osoba v pracovním kontextu přicházející do styku s osobními údaji, za které zodpovídá správce, podepisuje prohlášení o mlčenlivosti. Za uplatnění, podepsání a evidenci **„Souhlasů - Informace a prohlášení ke zpracovávání osobních údajů pro zaměstnance dohodáře, praktikanty a stážisty“, který je veden jako příloha č. 4** Jakákoliv diferenciace od vzoru prohlášení musí být odsouhlasena ředitelkou a pověřencem.
- (2) Bezpečně zpracovávat a ukládat analogové a digitální dokumenty které obsahují osobní údaje a při používání ostatních informačních kanálů (elektronická pošta, telefon) postupovat tak, aby nemohla být narušena jejich důvěrnost a integrita a dostupnost. V případě analogových (papírových) dokumentů používat listinná úložiště (uzamykatelné šuplíky, kontejnery a skříně, trezory apod.).
- (3) V maximální míře, pokud to situace a zákon vyžaduje, provádět pseudonymizaci a anonymizaci osobních údajů ve zveřejňovaných dokumentech.
- (4) Pořizovat a využívat pomocnou analogovou a elektronickou dokumentaci (tabulky, seznamy, výpisy), obsahující osobní údaje sloužící k provoznímu zabezpečení pracovního výkonu zaměstnance tak, že musí být dostatečně chráněna, aby nedocházelo k neoprávněnému přečtení, kopírování nebo skenování a po skončení účelu provést skartaci nebo vymazání, pokud není dokumentace součástí zákonné evidence.
- (5) Ředitelka zajistí, aby kritická pracoviště, kde dochází ke zpracování osobních údajů byla uspořádána vhodným rozmístěním stolů a pracoviště tak, aby nedocházelo k narušení důvěrnosti zpracovávaných osobních údajů a zařízení a analogová nebo elektronická evidence byla zabezpečena mechanickým nebo elektronickým zabezpečením. (uzamykatelný nebo kódovaný prostor, kancelář, skříň) s řízeným přístupem dle čl. Čl. 10.
- (6) Zaměstnanec dbá, aby nebyly narušeny zásady ochrany osobních údajů, a to tak, že zejména při jednání s občany, (klienty) dodržuje zásadu prázdného stolu a prázdné obrazovky. Pravidelně uzamyká při odchodu z pracoviště počítač (svůj účet) tak, aby nedocházelo k neoprávněnému přístupu ke zpracovávaným osobním údajům.
- (7) Zaměstnanec má povinnost v případě vytvoření média s předávanými daty – záznamy z kamer, uchovávat nosné médium způsobem znemožňujícím neoprávněný či nahodilý přístup neoprávněných osob, a to vhodným zabezpečením, kryptováním nebo heslem
- (8) Zaměstnanec má povinnost neumožnit neoprávněným osobám sledovat na zobrazovacích zařízeních záběry z kamer nebo osobní nebo jiná data a požadavky na předání záznamů řešit pouze přes ředitelku.
- (9) Jakékoliv výtisky obsahující osobní údaje musí být tištěny na sdílených síťových tiskárnách jen pro potřebu zpracovávání osobních údajů v rámci pracovní činnosti. Musí být bezodkladně vyzvednuty a neponechány v tiskových frontách tiskových zařízení.
- (10) Zaměstnanec si je vědom, že jakékoliv neoprávněné zpracování osobních údajů, zejména svévolné pořizování kopií zaznamenaných záběrů kamer a dat (např. prostřednictvím mobilního telefonu nebo jiných záznamových zařízení), může být ze strany správce monitorováno a kontrolováno a je porušením povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci.
- (11) Zaměstnanec ukládá osobní údaje na prostředcích správce jen pomocí SW aplikací a zařízení, které jsou k tomu určeny a správcem ICT schváleny 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, ukládá zaměstnanec osobní údaje do samostatných souborů na určená úložiště, u kterých lze zajistit řízení přístupových práv a evidenci změn jen na úrovni souboru. Řízení přístupových práv k takovým souborům a adresářům podléhá stejnému schválení jako dle Čl. 10.

- (12) Zaměstnanec ukládá a poskytuje osobní údaje na externí vzdálená úložiště (cloudy) jen se souhlasem správce ICT, nepodléhá-li takové zpracování osobních údajů konkrétnímu smluvnímu ujednání správce a zpracovatele pod zpracovatelskou smlouvou nebo postupem dle zákona.
- (13) Zaměstnanec má povinnost změny nastavení kamer a zařízení (např: změna počtu kamer, záběru, místa ukládání, rozsahu dat) provádět tak, aby bylo respektováno právo na ochranu soukromí všech osob nacházejících se v monitorovaných prostorech. Pro naplnění tohoto požadavku jsou možné změny řešeny jen se souhlasem ředitelky a po konzultaci s pověřencem.
- (14) Pokud má zaměstnanec dovoleno používat ke zpracování osobních údajů vzdálený přístup do vnitřní sítě správce, formou vzdálené obrazovky, nebo používá mimo vnitřní síť správce zařízení (notebook, mobil, tablet, aj.), na kterém zobrazuje osobní údaje, je povinen dodržovat tuto směrnici a zabezpečit důvěrnost zobrazovaných osobních údajů stejným způsobem jako by byl na pracovišti správce.
- (15) Pokud má zaměstnanec dovoleno používat ke zpracování osobních údajů osobní soukromé zařízení (notebook, mobil, tablet, aj.), na kterém zobrazuje osobní údaje je povinen dodržovat tuto směrnici a zabezpečit důvěrnost zobrazovaných osobních údajů stejným způsobem jako by byl na pracovišti správce, a to za bezpečnostních podmínek stanovených správcem ICT a se souhlasem zaměstnance, který má zařízení ve svém osobním vlastnictví.
- (16) V případě, že zaměstnanec zjistí technický nebo organizační nesoulad v provozu kamerového systému nebo jiného sběrného zařízení dat s touto směrnicí nebo informacemi na webových stránkách organizace, informuje o tom neprodleně ředitelku.

Čl. 16. Kontrola opatření - revize této směrnice a proškolení

- (1) Za účelem pravidelného prověřování fungování zavedených technických, organizačních a bezpečnostních opatření při zpracování osobních údajů je ředitelkou v rámci jeho působnosti dle organizačního řádu prováděna kontrola dodržování této směrnice.
- (2) Za účelem zajištění trvalé a plnohodnotné ochrany osobních údajů při jejich zpracování je správce povinen provádět nebo umožnit proškolení zaměstnanců v této oblasti. Školení na podnět pověřence může být dle situace a potřeby a dle rozhodnutí ředitelky provedeno prezenčně, online nebo odkazem na video prezentaci.
- (3) Do 12 měsíců od nabytí účinnosti této směrnice bude provedeno ředitelkou ve spolupráci s pověřencem.
 - a. Proškolení relevantních zaměstnanců.
 - b. Revize všech relevantních formulářů a Souhlasů a doplnění všech testů proporcionality u relevantních zpracovávání osobních údajů.
 - c. Revize a doplnění všech záznamů o činnostech.
 - d. Kontrola a doplnění všech relevantních zpracovatelských smluv.
 - e. Revize všech přístupových oprávnění k osobním údajům v relevantních SW oprávněních.

Čl. 17. Seznam příloh

- Příloha č. 1 Informace ke zpracování osobních údajů, kamerovým systémům a uplatňování práv pro veřejnost a zaměstnance.
- Příloha č. 2 Souhlas se zpracováním osobních údajů.
- Příloha č. 3 Záznamy o činnostech zpracovávání osobních údajů.
- Příloha č. 4 Vzor prohlášení o mlčenlivosti.

.....
ředitelka