ZÁKLADNÍ ŠKOLA BRNO OTEVŘENÁ

Směrnice k ochraně osobních údajů

Údaje správce:

Základní škola Brno, Otevřená 20a, příspěvková organizace
IČO: 49466208
Otevřená 986/20a, 641 00 Brno

Směrnice je platná ke dni: 25.05.2018 a nahrazuje směrnice dříve přijaté.

Čl. 1

Předmět a účel směrnice

1. Směrnice pro ochranu osobních údajů upravuje k zajištění souladu činnosti Základní školy Brno, Otevřená 20a, (dále jen „správce“) s požadavky 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 jen „GDPR“ nebo „nařízení“).

Čl. 2

Vymezení základních pojmů

1. Pro účely této směrnice se rozumí:

   (a) auditním záznamem výpis záznamů o událostech prováděných v operačním systému počítače, respektive databáze/programu, které tento systém automaticky zapisuje a umožňuje jejich zpětnou kontrolu;

   (b) automatizovaným zpracováním zpracování, které zahrnuje operace:

      (i) ukládání informací na nosiče dat nebo jejich zpracování v databázích a programech,

      (ii) archivování informací jejich ukládáním na archivační paměťová média a v případě potřeby obnovování informací z archivních médií;

(c) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů (např. vzorek DNA, otisk prstu, obraz oční sítnice);

(d) manuálním zpracováním jakékoliv zpracování s výjimkou zpracování automatizovaného (listinná podoba, kartotéky, spisy);

(e) oprávněnými osobami pracovníci správce (dále jen „zaměstnanci“), kteří v rámci plnění pracovních povinností mají přístup k osobním údajům a dále je zpracovávají,

(f) pověřencem pro ochranu osobních údajů (dále jen „pověřenec“ nebo „DPO“) osoba jmenovaná správcem a zpracovatelem osobních údajů v souladu s článkem 37 GDPR;

(g) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za identifikovatelný, jestliže ho lze přímo či nepřímo identifikovat na základě konkrétních údajů nebo informací;

(h) příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny. Za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky nebo Evropské unie;

(i) správcem Základní škola Brno, Otevřená 20a;

(j) subjektem osobních údajů fyzická osoba, k níž se konkrétní osobní údaje vztahují;

(k) vedoucím zaměstnancem ředitelem;

(l) zpracovatelem každý subjekt, který na základě smluvního vztahu se správcem zpracovává osobní údaje;

(m) zpracováním osobních údajů jakákoliv operace s osobními údaji, a to provedená automatizovaně nebo manuálně. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče dat, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace;

(n) záznamem o činnostech zpracování záznamy vedené v souladu s článkem 30 GDPR;

(o) bezpečnostním incidentem jakékoliv porušení zabezpečení osobních údajů dle článku 33 GDPR;

(p) základními zásadami zpracování osobních údajů zásada zákonnosti, korektnosti a transparentnosti zpracováním, zásada účelového omezení zpracování na základě legitimního účelu, zásada minimalizace údajů, zásada přesného zpracování, zásada aktuálnosti údajů a zásada zabezpečeného zpracování.

Čl. 3

Postavení jednotlivých osob při zpracování osobních údajů a zajištění ochrany osobních údajů

1. Z pohledu ochrany osobních údajů existují v organizaci správce osoby s následujícím postavením:

   Pověřenec pro ochranu osobních údajů (DPO) – plní následující úkoly:

   (a) poskytování informací a poradenství zaměstnancům správce,

   (b) monitorování souladu činností správce s touto směrnicí, GDPR a dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s předpisy správce v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců zapojených do operací zpracování a souvisejících auditů;

   (c) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 GDPR;

   (d) spolupráce s dozorovým úřadem;

   (e) působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle článku 36 GDPR, a případně vedení konzultací v jakékoli jiné věci vztahující se k ochraně osobních údajů;

   (f) působení jako kontaktní místo pro subjekty údajů a dozorový úřad.

   Výkon funkce pověřence bude zajištěn externím dodavatelem na základě smluvního vztahu.

   Směrnice může dále definovat další úkoly pověřence, které mohou být rovněž obsahem smlouvy.

Vedoucí zaměstnanec (ředitel) – odpovídá za identifikaci rizik v oblasti ochrany osobních údajů. Případná zjištění konzultuje s DPO a je ve vztahu k němu hlavní komunikační osobou.

Zpracovatel – externí subjekt, který z titulu smluvního vztahu se správcem zpracovává osobně údaje, které mu svěřil správce. Podmínky spolupráce se zpracovatelem jsou definovány dále.

Čl. 4

Základní zásady a povinnosti při zpracování osobních údajů

1. Všichni zaměstnanci správce musí dodržovat základní zásady týkající se zpracování osobních údajů. Zaměstnanci jsou povinni dodržovat všechny zákonné normy, zejména pak ty, které se vztahují k výkonu jeho pracovních povinností, a dále vnitřní předpisy správce.
2. Zaměstnanci hlásí každý bezpečnostní incident přímo pověřenci pro ochranu osobních údajů a zároveň řediteli.
3. Zaměstnanci zpracovávají pouze přesné osobní údaje, přičemž je případě potřeby jsou schopni aktualizovat, dále je zpracovávají způsobem zajišťujícím zabezpečení před neoprávněným či protiprávním zpracováním, náhodnou ztrátou, zničením nebo poškozením. Zpracování údajů je možné pouze na základě právních důvodů. Osobní údaje je možné shromažďovat pouze pro určité účely, které jsou výslovně vyjádřené a jsou legitimní. Subjekt má právo vědět, které údaje správce zpracovává a kdo k nim má přístup, a to po jakou dobu. Je možné zpracovávat pouze osobní údaje, které jsou přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování.
4. Zaměstnanci musí být schopni doložit oprávněnost jimi prováděných operací zpracování osobních údajů a zdroje, prostřednictvím kterých údaje získali (tj. buď samotné subjekty údajů nebo jiný zdroj).
5. Při zpracování je nutné průběžně sledovat slučitelnost účelů, tedy zda jsou osobní údaje zpracovávány v souladu s účelem, ke kterému byly získány a zda je případně odlišný účel zpracování slučitelný s účelem původním.
6. Správce odpovídá za dodržení výše uvedených zásad a musí být schopen toto dodržení souladu prokázat.

Čl. 5

Pravidla pro nakládání s osobními údaji vedenými v listinné a elektronické podobě

1. Zaměstnanci užívající prostředky informačních a komunikačních technologií správce jsou povinni používat svěřené prostředky pouze k plnění svých pracovních povinností a v souladu s účelem, ke kterému byly určeny, neužívat osobní údaje subjektů údajů pro vlastní potřebu a zamezit neoprávněným osobám nahlížení do elektronických i listinných dokumentů.
2. Zaměstnanci jsou povinni zabezpečit svůj uživatelský účet a počítač přiměřeným heslem, které nesmí být nikde uloženo nebo napsáno, a ani sdělováno druhé osobě, a to ani osobě odpovědné za správu IT.
3. Při opuštění pracoviště musí zaměstnanci zabránit neoprávněnému použití PC, například okamžitým spuštěním spořiče obrazovky chráněného heslem, uzamknutím PC, standardním ukončením práce na PC apod. Po skončení pracovní činnosti jsou zaměstnanci povinni vypnout PC nebo jej uvést do režimu spánku tak, aby nemohla být činnost obnovena bez zadání hesla.
4. Při tisku, kopírování a skenování dokumentů zaměstnanci neponechávají v zařízení bez dozoru žádné dokumenty.
5. Osobní údaje je zakázáno sdělovat telefonicky a elektronickou poštou jakékoliv osobě bez relevantního ověření totožnosti a oprávněného nároku na sdělení údajů dle této směrnice a příslušných právních předpisů.
6. Zaměstnanci správce jsou povinni zabránit neoprávněnému přístupu, nežádoucím změnám, zcizení a zneužití všech údajů nebo informací, kterými správce disponuje v listinné nebo elektronické podobě. Informace ukládané v kancelářích, místnostech a prostorách správce musí být zabezpečeny proti náhodnému a nahodilému přístupu – všechny dokumenty obsahující osobní údaje a nosiče dat, jiné než osobní počítače, musí být zvlášť uzamčeny, to se netýká místnosti určené k plnění funkce archivu. Po opuštění pracoviště je každý zaměstnanec povinen zabezpečit všechny dokumenty umístěním do uzamčených skříní nebo trezoru, zaheslovat/vypnout počítače, zavřít okna a uzamknout dveře.
7. Při opuštění pracoviště musí být všechny dokumenty odstraněny z pracovní desky a uzamčeny nebo jinak uchovány ve smyslu výše uvedeného odstavce.
8. V případě využívání mobilního telefonu nebo jiného přenosného zařízení, které může obsahovat osobní údaje, musí být toto zařízení rovněž zabezpečeno přiměřeným heslem. Zaměstnanec musí dbát na to, aby nebylo mobilní zařízení ztraceno nebo zneužito.

9. Každý zaměstnanec pracuje jen s takovými údaji, které odpovídají náplni jeho práce a jeho pracovnímu zařazení.

Čl. 6

Podmínky pro získání souhlasu subjektu údajů

1. Souhlas se získává v případě, že zpracování údajů není prováděno na základě jiného právního titulu. Zaměstnanci správce vždy konzultují s pověřencem definici souhlasů a stanovení účelu, pro který se souhlas získává.
2. Souhlas nesmí být součástí jiného dokumentu (přihláška, pracovní smlouva a podobně) a vždy musí být vyhotoven v samostatném dokumentu. Současně je vždy nutné posuzovat, zda není vyžadován nadbytečně.
3. V případě užití souhlasu jsou zaměstnanci oprávněni využít pouze závazný vzor schválený pověřencem.
4. V případě získávání souhlasů na dobu určitou musí odpovědný zaměstnanec vést registr souhlasů a hlídat dobu trvání poskytnutého souhlasu tak, aby operace zpracování nebyly prováděny po uplynutí této doby.
5. Souhlas musí být informovaný, tj. text souhlasu musí obsahovat rovněž plnění informační povinnosti nebo musí na text plnění informační povinnosti odkazovat; v takovém případě zaměstnanec ověří, zda se subjekt údajů poskytující souhlas s informační povinností seznámil.

Čl. 7

Transparentní informace, sdělení a postupy pro výkon práv subjektů údajů

1. Za plnění informační povinnosti dle článku 12 GDPR je odpovědný ředitel ve spolupráci s pověřencem.

1. Všeobecná informační povinnost je plněna zveřejněním na webových stránkách správce. Minimální požadavky jsou stanoveny v článku č. 8 této směrnice.
2. Soulad rozsahu a obsahu informační povinnosti kontroluje průběžně ředitel ve spolupráci s pověřencem.
3. Při výkonu práv subjektů údajů musí být vždy relevantně ověřena totožnost žadatele, aby bylo jednoznačně prokázáno, že má vztah ke zpracovávaným osobním údajům. Totožnost při vyřizování žádosti ověřuje pověřenec následovně:

(a) žádost v listinné podobě musí být doručena osobně a totožnost žadatele ověřena z platného dokladu;

(b) žádost v listinné podobě může být opatřena úředním ověřením pravosti podpisu, což nahrazuje osobní ověření identity žadatele;

(q) žádost zaslaná ve formě e-mailové zprávy musí být opatřena zaručeným elektronickým podpisem žadatele, což nahrazuje osobní ověření identity žadatele;

(r) žádost zaslaná datovou schránkou musí být odeslána výhradně z datové schránky žadatele, což nahrazuje osobní ověření identity žadatele.

4. Na žádost se odpovídá primárně ve stejné formě, v jaké byla podána. Je-li vyhověno žádosti o přístup, vyřídí se výhradně poštou do vlastních rukou subjektu údajů nebo jeho zástupce.

5. Při pochybnosti o identitě žadatele nemůže být žádosti vyhověno. Žadatel musí být o tomto vyrozuměn a musí mu být umožněno dodatečné prokázání totožnosti.

6. Při podání žádosti zmocněncem subjektu údajů musí zmocnění odpovídat obecným požadavkům právních předpisů s tím, že ověřena musí být jak totožnost zmocněnce, tak totožnost zmocnitele. Postupuje se analogicky k odst. 4. tohoto článku.

7. Žádosti se vyřizují bez zbytečného odkladu, nejpozději ve lhůtě stanovené článkem 12 odst. 3 GDPR (do jednoho měsíce od obdržení žádosti).

8. Veškeré žádosti se evidují v Registru žádostí subjektů údajů dle čl. 13 této směrnice, a to včetně popisu způsobu jejich vyřízení. Za evidenci je odpovědný pověřenec.

Čl. 8

Informace poskytované v případě, že osobní údaje jsou získány od subjektů údajů

1. Za řádné plnění informační povinnosti ve vztahu k subjektům údajů odpovídá pověřenec ve spolupráci s ředitelem. V případě získání údajů z jiného zdroje, než od subjektů údajů, je nutné posoudit využití výjimek z plnění informační povinnosti. Tyto výjimky je možné uplatnit pro situace, kdy je získávání nebo zpřístupnění osobních údajů výslovně stanoveno právem EU nebo členského státu nebo pokud poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí. Není-li možné některé z výjimek uplatnit, je nutné splnit informační povinnost vůči subjektu údajů dle čl. 14 GDPR.

9. Základní náležitosti informační povinnosti dle článku 13 GDPR tvoří nejméně:

(a) údaje správce;

(s) kontaktní údaje pověřence;

(t) účely zpracování a právní základ zpracování;

(u) oprávněné zájmy správce nebo třetí strany;

(v) údaje o případných příjemcích nebo kategorie příjemců;

(w) případný úmysl předat údaje do třetí země nebo mezinárodní organizaci;

(x) doba uložení údajů nebo kritéria pro její stanovení;

(y) poučení o jednotlivých právech subjektů údajů včetně poučení o možnosti obrátit se na dozorový orgán;

(z) poučení o možnosti odvolat kdykoliv souhlas;

(aa) skutečnost, zda je poskytnutí údajů zákonným nebo smluvním požadavkem.

Čl. 9

Právo subjektu údajů na přístup k osobním údajům

1. Za plnění povinností vyplývajících pro správce z uplatnění práva subjektů údajů na přístup dle článku 15 GDPR odpovídá pověřenec ve spolupráci s ředitelem. Pověřenec je povinen vyhotovit a zaslat žadateli vyjádření, zda jsou správcem zpracovávány jeho osobní údaje.

10. V případě existence zpracování osobních údajů žadatele správcem poskytne pověřenec tomuto žadateli zpracovávané osobní údaje a informace o zpracování. Na žádost budou rovněž poskytnuty kopie zpracovávaných údajů. Byla-li žádost podána elektronicky, poskytnou se informace primárně v elektronické formě.

11. V případě zpracování většího množství osobních údajů o subjektu bude žadatel vyzván k upřesnění, jaké informace konkrétně požaduje.

12. Žádosti subjektů údajů vyřizuje pověřenec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení. Detaily postupu upravuje čl. 7 této směrnice.

13. Právo na přístup nesmí být odepřeno ani omezeno. Omezení je možné pouze z důvodu ochrany obchodního tajemství, duševního vlastnictví, know-how nebo z důvodu ochrany osobních údajů třetích osob. Rovněž v případech, kdy by byl přístup žadatele k údajům omezen zvláštním právním předpisem.

Čl. 10

Právo na opravu

1. Za plnění povinností vyplývajících pro správce z uplatnění práva subjektu údajů na opravu údajů dle článku 16 GDPR odpovídá pověřenec ve spolupráci s ředitelem.
2. Při doručení žádosti o opravu pověřenec neprodleně zajistí aktualizaci nebo doplnění zpracovávaných údajů.
3. Žadatel bude pověřencem vyrozuměn o provedení opravy nebo doplnění osobních údajů.
4. Žádosti subjektů údajů vyřizuje pověřenec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení. Detaily postupu upravuje čl. 7 této směrnice.

Čl. 11

Právo na výmaz (právo být zapomenut)

1. Za plnění povinností vyplývajících pro správce z uplatnění práva subjektů údajů na výmaz (právo být zapomenut) dle článku 17 GDPR odpovídá pověřenec ve spolupráci s ředitelem.

14. Pověřenec neprodleně po doručení žádosti o výmaz posoudí, zda je požadavek oprávněný nebo zda existuje důvod k odmítnutí provedení výmazu dle článku 17 odst. 3 GDPR.
15. Pověřenec vyrozumí žadatele o tom, zda bylo žádosti vyhověno nebo zda byla odmítnuta. V případě odmítnutí musí být rozhodnutí náležitě odůvodněno.
16. Právo na výmaz se provede v listinné podobě fyzickou skartací všech dokumentů, v elektronické podobě pak výmazem ze všech databází a datových nosičů.
17. Žádosti subjektů údajů vyřizuje pověřenec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení. Detaily postupu upravuje čl. 7 této směrnice.

Čl. 12

Právo na omezení zpracování

1. Za plnění povinností vyplývajících pro správce z uplatnění práva subjektů údajů na omezení zpracování dle článku 18 GDPR odpovídá pověřenec ve spolupráci s ředitelem.

18. Pověřenec posoudí oprávněnost obdrženého podání a vyrozumí žadatele o tom, zda bylo žádosti vyhověno nebo zda byla odmítnuta.
19. V případě oprávněnosti žádosti pověřenec ve spolupráci s ředitelem vhodným způsobem zajistí omezení zpracování.

20. V případě odmítnutí žádosti musí být takové rozhodnutí náležitě odůvodněno, a v případě, že bylo zpracování po dobu vyřizování žádosti subjektu omezeno, musí být subjekt údajů předem upozorněn na to, že bude omezení zpracování zrušeno.

21. Omezení zpracování musí být vyznačeno v databázi, ve které jsou údaje vedeny. V případě vedení údajů v listinné podobě musí být upozorněním na omezení zpracování označen příslušný spisový materiál.

22. Žádosti subjektů údajů vyřizuje pověřenec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení. Detaily postupu upravuje čl. 7 této směrnice.

Čl. 13

Registr žádostí subjektů údajů a registr bezpečnostních incidentů

1. Pověřenec vede registr žádostí subjektů údajů a registr bezpečnostních incidentů (dále také jen „registry“).

2. Registry slouží pro vnitřní kontrolu správce a pro účely prokázání náležitého plnění povinností vyplývajících z Nařízení ve vztahu k subjektům údajů a k dozorovým orgánům.

3. V registru incidentů musí být uvedeny veškeré dostupné informace o incidentu, zejména pak popis jeho průběhu, datum a čas zjištění, přesný čas poskytnutí informace o incidentu pověřenci, způsob ohlášení, účinky a přijatá nápravná opatření.

4. V případě, že nebyl bezpečnostní incident hlášen dozorovému úřadu, bude v registru rovněž uvedeno odůvodnění tohoto postupu.

5. V případě nedodržení lhůty pro ohlášení bude v registru rovněž uvedeno náležité odůvodnění.

6. V případě, že nebyl bezpečnostní incident hlášen subjektům údajů, bude v registru rovněž uvedeno náležité odůvodnění tohoto postupu.

7. V registru žádostí subjektů se uvede, kdy byla žádost doručena, k uplatnění kterého práva směřovala a způsob a lhůty jejího vyřízení. U každé žádosti musí být rovněž uvedeno náležité odůvodnění způsobu vyřízení. Každá operace se žádostí subjektu bude označena datem, kdy byla provedena, aby bylo možné prokázat splnění jednotlivých lhůt.

8. Údaje z registru předloží pověřenec na vyžádání správci.

Čl. 14

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

1. Za splnění oznamovací povinnosti dle článku 19 GDPR odpovídá pověřenec ve spolupráci s ředitelem. V rámci plnění této povinnosti oznamuje správce jednotlivým příjemcům, jímž byly osobní údaje zpřístupněny, veškeré opravy, výmazy nebo omezení zpracování s výjimkou případů, kdy se to ukáže jako nemožné nebo vyžadující nepřiměřené úsilí.

23. Všechny postupy dle čl. 16 (právo na opravu), 17 (právo na výmaz) a 18 (právo na omezení zpracování) GDPR oznamuje pověřenec všem příjemcům, jímž byly správcem dotčené osobní údaje poskytnuty.

Čl. 15

Právo vznést námitku

1. Za plnění povinností vyplývajících pro správce z uplatnění práva subjektů údajů na podání námitky dle čl. 21 GDPR odpovídá pověřenec ve spolupráci s ředitelem.

24. Pověřenec neprodleně po doručení námitky posoudí její přiměřenost a důvodnost. Během tohoto hodnocení musí být zpracování omezeno na rozsah odpovídající účelu určení, výkonu nebo obhajoby právních nároků.

25. V případě vyhovění námitce bude zpracování údajů neprodleně ukončeno.

26. Žádosti subjektů údajů vyřizuje pověřenec bez zbytečného odkladu, nejpozději do jednoho měsíce od doručení.

Čl. 16

Odpovědnost správce

1. Správce odpovídá za zpracování údajů v souladu se základními zásadami dle článku 5 GDPR, dalšími právními předpisy a touto směrnicí. Kromě této směrnice může být bezpečnost zpracování osobních údajů a informací všeobecně upravena v ostatních interních předpisech správce.

27. Odpovědnost správce dle předchozího odstavce vykonává ředitel. Pravidelně, ve spolupráci s pověřencem, monitoruje soulad této směrnice a dalších vnitřních předpisů správce s platnými předpisy a je povinen sledovat aktuální změny právní úpravy, rozhodovací praxi a proces tvorby nové právní úpravy v oblasti ochrany osobních údajů.

Čl. 17

Záměrná a standardní ochrana osobních údajů

1. Správce průběžně, dle momentální potřeby, aktualizuje technická a organizační opatření k zajištění ochrany osobních údajů.

28. Záměrnou ochranou se rozumí zohlednění a zapracování ochrany osobních údajů do přípravy nových postupů a opatření. Postupy ochrany osobních údajů začleňuje ředitel ve spolupráci s pověřencem do přípravy všech procesů, v rámci kterých by mohly být zpracovávány osobní údaje.

29. Standardní ochranou osobních údajů se rozumí udržování zavedeného standardu ochrany, kdy zaměstnanci správce uplatňují zásady a principy ochrany osobních údajů při všech prováděných operacích zpracování. Tím se rozumí zejména dodržování povinností stanovených nejen touto směrnicí, ale rovněž GDPR a dalšími právními předpisy.

Čl. 18

Záznamy o činnostech zpracování

1. Správce vede záznamy o činnostech zpracování dle článku 30 GDPR. Záznamy o činnostech se vedou jednotlivě každým zaměstnancem pro agendu jím zpracovávanou. Dle potřeby jsou aktualizovány pověřencem ve spolupráci s ředitelem a příslušným zaměstnancem. Záznamy o činnostech budou na vyzvání předloženy příslušným zaměstnancem ke kontrole pověřenci.

Čl. 19

Zabezpečení zpracování

1. Zabezpečení zpracování údajů dle článku 32 GDPR kontroluje pověřenec ve spolupráci s ředitelem.

30. Pověřenec dohlíží na aktuálnost organizačních a technických opatření k zabezpečení zpracování a uložení/archivace osobních údajů.

31. Pravidelně, nejméně však 1x do roka, kontroluje pověřenec na všech pracovištích správce dodržování této směrnice, dalších vnitřních předpisů, GDPR a souvisejících předpisů.

32. Pravidelně, nejméně však 1x do roka, kontroluje pověřenec ve spolupráci s ředitelem aktuálnost této směrnice a dalších vnitřních předpisů, zejména s přihlédnutím k prováděným operacím zpracování, stavu techniky a možným rizikům pro práva a svobody subjektů údajů.

Čl. 20

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Pověřenec provádí hlášení případů porušení zabezpečení osobních údajů (tzv. bezpečnostních incidentů) dozorovému úřadu dle článku 33 GDPR.

33. V případě vzniku bezpečnostního incidentu o něm zaměstnanec nebo zpracovatel, který incident zaznamená, neprodleně informuje pověřence a sdělí mu veškeré potřebné informace. Pověřenec neodpovídá za hlášení, resp. nenahlášení bezpečnostních incidentů, které mu nebyly oznámeny.

34. Pověřenec vyhodnotí, zda může mít za následek riziko pro práva a svobody fyzických osob.

35. V případě podezření na takové riziko ohlásí incident dozorovému úřadu v rozsahu stanoveném GDPR.

36. Pokud pověřenec neprovede hlášení bezpečnostního incidentu dozorovému orgánu, řádně odůvodní, proč tento incident vyhodnotil jako nikoliv rizikový pro práva a svobody subjektů údajů.

37. Pověřenec dbá na to, aby byla dodržena lhůta 72 hodin pro nahlášení. Lhůta se počítá od okamžiku zjištění bezpečnostního incidentu správcem. V případě, že hlášení nebude provedeno do 72 hodin, odůvodní pověřenec důvody zpoždění.

Čl. 21

Ohlašování případů porušení zabezpečení osobních údajů subjektům údajů

1. Pověřenec provádí hlášení bezpečnostních incidentů subjektům údajů dle článku 34 GDPR.

2. Pověřenec v případě bezpečnostního incidentu vyhodnotí okolnosti tohoto incidentu a jeho možný vliv na práva a svobody subjektů údajů. V případě vysoké rizikovosti vyhodnotí rovněž aplikovatelnost výjimky dle článku 34 odst. 3 GDPR. Výjimky se uplatní v případě, že správce zavedl náležitá technická a organizační opatření ve vztahu k údajům dotčeným porušením zabezpečení, zavedl následné opatření k vyloučení možného rizika pro subjekty údajů, při nepřiměřeném úsilí apod. Aplikaci výjimky je pověřenec povinen pečlivě zvážit a náležitě odůvodnit.

Čl. 22

Postavení pověřence pro ochranu osobních údajů

1. Pověřenec pro ochranu osobních údajů je externím poskytovatelem na základě smlouvy.

38. V souvislosti s výkonem této funkce musí mít přístup k osobním údajům a operacím jejich zpracování v míře nezbytně nutné k plnění jeho úkolů.

39. Správce zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu úkolů v oblasti zpracování osobních údajů.

40. Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení.

41. Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán mlčenlivostí v souladu s právem Unie nebo České republiky.

42. Pověřenec pro ochranu osobních údajů může plnit i jiné úkoly a povinnosti na základě jiného smluvního vztahu. Pověřenec nesmí být z titulu plnění jiného smluvního vztahu ve středu zájmů.

43. Kromě úkolů uvedených v čl. 3 plní pověřenec i následující úkoly:

    (a) zpracovává veškeré podněty a žádosti subjektů údajů a reaguje na ně ve lhůtách stanovených GDPR, jinými závaznými předpisy nebo interními lhůtami, zejména pak:

        (i) řeší žádosti subjektů údajů o přístup k osobním údajům;

        (ii) řeší žádosti subjektů údajů o opravu osobních údajů;

        (iii) řeší uplatnění práva na výmaz (práva být zapomenut) ze strany subjektů údajů;

        (iv) řeší uplatnění práva na omezení zpracování osobních údajů;

        (v) řeší doručené námitky proti zpracování osobních údajů;

    (bb) plní oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování osobních údajů;

    (cc) je odpovědný za splnění ohlašovací povinnosti dle 33 a 34 GDPR;

    (dd) je odpovědný za vedení registru žádostí subjektů osobních údajů a registru bezpečnostních incidentů.

44. Správce zveřejní kontaktní údaje pověřence v následujícím v rozsahu:

    (a) jméno a příjmení nebo obchodní firma;

(ee) telefonní číslo;

(ff) poštovní adresa;

(gg) adresa elektronické pošty.

a tyto údaje rovněž sdělí dozorovému úřadu.

45. Kontaktní údaje pověřence budou rovněž uvedeny v informační povinnosti a případně v dalších dokumentech týkajících se osobních údajů.

Čl. 23

Mlčenlivost

1. Zaměstnanci jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
2. Zaměstnanci jsou povinni upozornit ředitele na případné nedostatky v zabezpečení osobních údajů, nejedná-li se přímo o bezpečnostní incident dle této směrnice, respektive příslušného ustanovení GDPR.

Čl. 24

Přístup k osobním údajům v informačních systémech a prostředcích ICT

1. Přístup k osobním údajům (a veškerým dalším datům a údajům) v informačních systémech a počítačích je možný pouze na základě přístupových a uživatelských práv ke konkrétnímu informačnímu systému nebo počítači. Své uživatelské jméno ani heslo nesvěří zaměstnanec třetí osobě ani jinému zaměstnanci.

Čl. 25

Obnova dat ze záloh

1. Při obnově dat ze záloh je nutné provést aktualizaci osobních údajů podle aktuálního stavu. Při obnově zálohy nesmí dojít k obnovení osobních údajů, které byly dříve vymazány.

Čl. 26

Postup při řízení rizik ochrany osobních údajů

1. Cílem provedení analýzy rizik je identifikovat a posoudit možné hrozby a zranitelnosti v oblasti zpracování a ochrany osobních údajů a navrhnout přiměřená opatření pokrývající zjištěná rizika.

46. S ohledem na rozsah zpracování osobních údajů v instituci správce a počet zaměstnanců se možná rizika posuzují automaticky v rozsahu agendy zpracovávané konkrétním zaměstnancem s tím, že o tom nemusí být proveden písemný záznam. V písemné podobě bude posouzení rizik provedeno pouze tehdy, pokud to bude ukládat právní předpis.

Čl. 27

Zveřejňování a předávání osobních údajů

1. Osobní údaje dětí mohou být zveřejněny pouze se souhlasem zákonných zástupců nebo osob vykonávajících rodičovskou odpovědnost dle rozsahu uděleného souhlasu. V případě nedostatečnosti souhlasu je nutno vyžádat souhlas nový.
2. Osobní údaje dětí ani zákonných zástupců nebo osob vykonávajících rodičovskou odpovědnost nesmí být vyvěšeny v prostorách školy vyjma odůvodněných případů (například rozpis dětí do tříd při zahájení docházky ve vestibulu školy, dietní opatření v prostorách školní jídelny přístupných jen zaměstnancům apod.) s tím, že je vždy nutné posuzovat jak odůvodněnost, tak přiměřenost rozsahu zveřejněných údajů.
3. Zákonní zástupci poskytují souhlas na období vzdělávání jejich dítěte na této základní škole a na zákonem stanovenou dobu nezbytnou pro jejich zpracování, pro vědecké účely, a účely archivnictví. Škola se zavazuje zpracovávané údaje zabezpečit před neoprávněným nebo nahodilým přístupem a zpracováním, před změnou a zničením, zneužitím či ztrátou. Zákonní zástupci berou na vědomí, že v případě specifických případů mohu být požádáni o individuálně vymezený souhlas ke konkrétní akci, bude-li jeho povaha takový souhlas vyžadovat.
4. Zákonní zástupci byli seznámeni se skutečností, že škola běžně pořizuje ilustrativní fotografie (video ze školních akcí, ze kterých není možné určit totožnost dítěte, například celkové fotografie a záběry ze třídy, z akce, kde nejsou děti zobrazeny s podrobným portrétem a/nebo se neuvádí více, než křestní jméno; v těchto případech nejde o zachycení podoby ve smyslu § 84 občanského zákoníku a nepodléhá souhlasu. Zároveň jsou si vědomi toho, že škola využívání ve společných prostorách v rámci bezpečnosti žáků a ochrany majetku kamerový systém. Zákonní zástupci byli seznámeni se skutečností, že odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním.
5. Osobní údaje dětí mohou být předány smluvnímu zpracovateli nebo při plnění povinností podle zvláštního právního předpisu.
6. Osobní údaje zaměstnanců mohou být zveřejněny pouze se souhlasem nebo v případě, že jejich pracovní náplni odpovídá nutnost zveřejnění jména, příjmení a kontaktních údajů.

Vždy však může být zveřejněn pouze pracovní e-mail a pracovní telefonní číslo. Takové zveřejnění je v souladu s oprávněným zájem správce a nevyžaduje souhlas zaměstnance jako subjektu údajů.

7. Osobní údaje zaměstnanců mohou být předány smluvnímu zpracovateli (např. při vedení mzdového účetnictví), v jiných případech potom při plnění povinnosti podle zvláštního právního předpisu.

Čl. 28

Spolupráce se zpracovatelem osobních údajů

1. V případě uzavření smluvního vztahu se zpracovatelem musí být splněny požadavky článku 28 GDPR.
2. Smlouva se zpracovatelem musí být písemná a obsahovat předmět a dobu trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, práva a povinnosti správce. Zpracovatel musí mít za povinnost zpracovávat údaje výhradně na základě pokynů správce a musí mít za povinnost zajistit, aby osoby údaje zpracovávající byly vázány smluvní nebo zákonnou mlčenlivostí. Zpracovatel musí být smluvně zavázán přijmout opatření k zabezpečení údajů dle čl. 32 GDPR, k dodržování podmínek pro zapojení dalšího zpracovatele, zohledňovat povahu zpracování a být správci nápomocen při plnění povinností při uplatňování práv subjektů údajů. Zpracovatel musí být smluvně zavázán k provedení všech požadovaných operací, zejména pak k realizaci práva na opravu, výmaz, přístup či omezení zpracování. Zpracovatel musí být rovněž smluvně zavázán k umožnění auditů a inspekcí prováděných správcem.
3. Pokud již smluvní vztah se zpracovatelem existuje, kontroluje namátkově ředitel ve spolupráci s pověřencem dodržování podmínek ochrany osobních údajů ze strany zpracovatele.

Čl. 29

Posouzení vlivu na ochranu osobních údajů (DPIA)

1. Pokud je pravděpodobné, že určitý druh zpracování osobních údajů ve správcem bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

2. Z posouzení může vyplynout nutnost předchozí konzultace s ÚOOÚ. Provedení posouzení je nutné provádět v součinnosti s pověřencem. Rovněž je nutné zohlednit zákonnou výjimku z povinnosti posouzení provádět pro takové operace zpracování, které zákon ukládá provést.

Čl. 30

Skartace a archivace dokumentů

1. Skartace a archivace dokumentů se řídí zvláštním předpisem správce.

Brno 22.05.2018

Mgr. Dagmar Šenbergerová

ředitelka školy