Posouzení souladu nakládání a zpracování osobních informací s GDPR

Č.j.: 7ZŠ/0693/2018
Subjekt posouzení:
Základní škola a mateřská škola, Třinec, Kaštanová 412, příspěvková organizace
se sídlem Kaštanová 412, 739 61, Třinec - Dolní Lištná, IČ: 00847135
jednající Mgr. Ivetou Hudzietzovou, ředitelkou
(dále jen „školské zařízení" nebo „správce" nebo „zpracovatel")

Zpracovatel posouzení:
Mgr. Petr Letovanec, advokát
Se sídlem nám. Míru 551, 739 61 Třinec, IČ:

ČÁST I.
Základní informace

I.
Preambule

1) Toto posouzení je provedeno na základě požadavku správce a jeho účelem a smyslem je posouzení souladu nakládání a zpracování osobních informací správcem a s tím spojená analýza rizik zpracování osobních údajů v souvislosti s výkonem činností správce, jeho zaměstnanců, a dále posouzení ochrany získaných informací, jejich zabezpečení a dalších souvisejících způsobů nakládání, s nařízením 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 (dále jen nařízení GDPR nebo jen nařízení) a o zrušení směrnice 95/46/ES (GDPR), a dalšími obecně závaznými předpisy.

2) Při posouzení je vycházeno z analýzy nakládání s osobními informace a jejich zpracování, která byla provedena u správce za účelem sumarizace jím prováděných procesů nakládání s osobními informacemi a jejich zpracování, popisu jejich zabezpečení proti zneužití a přístupu jednotlivých skupin osob k těmto informacím (dále jen analýza).

3) Při posouzení, jakož i při provedené analýze, je vycházeno z informací poskytnutých výhradně správcem, pověřeným IT technikem a částečně z vlastních zjištění zpracovatele posouzení.

II.
Důležité základní pojmy

1) Osobními údaji jsou 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) Zpracováním jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

3) Evidencí je jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

4) 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

5) Zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

6) 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.

7) Údaji o zdravotním stavu osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.

8) Porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

9) Biometrickými údaji jsou osobní údaje 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.

III.
Zásady zpracování osobních údajů dle nařízení GDPR

1) Osobní údaje musí být:
   - ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem
   - shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný
   - přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány

- přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny
- uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením

2) Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit.

ČÁST II.
Posouzení souladu jednotlivých zásad

I.
Zásada zákonnosti zpracování

1) Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
   - subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů
   - 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
   - zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje
   - zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
   - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
   - zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě

2) Z provedené analýzy přesvědčivě vyplynulo, že správce jako zákonný důvod pro zpracování vychází převážně z toho, že zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje, a to na základě celé řady obecně závazných právních předpisů, dále pak je malá část zpracování osobních údajů umožněna na základě souhlasu se zpracováním a zpracování je v části také nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, což se týká smluvních závazků správce pro zajištění jeho provozních činností.

3) S ohledem na provedenou analýzu a zjištěné skutečnosti tak nebyl zjištěn žádný nesoulad správce se zásadou zákonnosti zpracování dle nařízení GDPR.

II.
Zásada transparentnosti

1) Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 nařízení GDPR a učinil veškerá sdělení podle článků 15 až 22 a 34 nařízení GDPR o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

2) Z provedené analýzy vyplynulo, že správce získává informace výhradně od subjektu údajů, resp. jejich zákonného zástupce a dále, že osobní informace používá výhradně za účelem stanoveným zákonem. S ohledem na skutečnost, že správce je veřejným školským zařízením, je rozsah jeho činnosti upraven zákonem, stejně jako jeho povinnosti, a tedy spadá do kategorie právnických osob, u kterých je subjektům známo, jaké informace správce má a v jakém rozsahu. Lze tedy ve vztahu ke správci aplikovat ust. článku 13 odst. 4 nařízení.

3) Co se týče ostatních informačních povinností správce, popř. informací, které nespadají pod aplikaci ust. článku 13 odst. 4 nařízení, pak správce zveřejnil na svých internetových stránkách dokument „Zásady ochrany osobních údajů“, včetně formuláře pro žádosti subjektů údajů, kde poskytl subjektům údajů veškeré relevantní informace, které požaduje čl. 12 odst. nařízení.

4) S ohledem na zjištění uvedená v odst. 2 a zpřístupnění informací způsobem uvedeným v odst. 3 tohoto článku lze konstatovat, že nebyl zjištěn žádný nesoulad správce se zásadou transparentnosti dle nařízení GDPR.

III.
Zásada účelového omezení a minimalizace údajů

1) Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nařízení nepovažuje za neslučitelné s původními účely. Osobní údaje musí být dále přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

2) Analýzou bylo zjištěno, že účel shromažďování a zpracování osobních údajů správcem je definován v v zák. č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), kdy jeho cíle jsou vymezeny v § 2 odst. 2, kdy se jedná zejména o rozvoj osobnosti člověka, který bude vybaven poznávacími a sociálními způsobilostmi, mravními a duchovními hodnotami pro osobní a občanský život, výkon povolání nebo pracovní činnosti, získávání informací a učení se v průběhu celého života. Rozsah získávaných a zpracovávaných osobních informací je pak konkrétně vymezen v těchto předpisech:
    - Zákon č. 561/2004 Sb., školský zákon
    - Zákon č. 89/2012 Sb., občanský zákoník

- Zákon č. 372/2011 Sb., o zdravotních službách
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení
- Zákon č. 337/1992 Sb., o správě daní a poplatků
- Zákon č. 280/2009 Sb., daňový řád
- Zákon č. 435/2004 Sb., o zaměstnanosti
- Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění
- Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí
- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 128/2000 Sb., o obcích
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek
- Vyhláška č. 14/2005 Sb., o předškolním vzdělávání

Analýzou nebyl zjištěn žádný přesah získávaných osobních informací mimo vymezený zákonný rámec a účel činnosti správce.

3) S ohledem na jasně, legislativně vymezený, a jednoznačně rozsahově daný rámec, sleduje shromažďování a zpracovávání osobních údajů správcem zcela legitimní účely a proto ani v tomto nebyl zjištěn žádný nesoulad správce se zásadou účelového omezení a minimalizace údajů dle nařízení GDPR.

IV.
Zásada přesnosti

1) Osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.

2) Analýzou bylo zjištěno, že aktualizace a správnost údajů subjektů hraje v činnosti správce velmi významnou roli, a to především při získávání informací o dětech, kdy sám správce svými interními postupy zjišťuje aktivně správnost zpracovávaných informací.

3) S ohledem na průběžně aktualizované evidence, kdy tato povinnost vyplývá pro správce ze zákona, nebyl zjištěn žádný nesoulad správce se zásadou přesnosti dle nařízení GDPR.

V.
Zásada omezení uložení

1) Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.

2) Analýzou bylo zjištěno, že správce je ze zákona povinen dodržet celou řadu lhůt pro uchování informací, jakož i skartaci dokumentů a tato zákonná úprava mu neumožňuje jinou možnost postupu ani vlastního uvážení.

3) S ohledem na zákonem jasně stanovené lhůty pro uložení a na průběžnou archivaci a skartaci u správce, kdy jeho povinnosti jsou striktně stanoveny zákonem, nebyl zjištěn žádný nesoulad správce se zásadou omezení uložení dle nařízení GDPR.

VI.
Zásada integrity a důvěrnosti

1) Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

2) Analýzou bylo zjištěno, že správce neposkytuje osobní informace žádným dalším příjemcům nebo kategoriím příjemců ve třetích zemích nebo v mezinárodních organizacích ani jiným subjektům soukromého práva, nemá-li k tomuto poskytnutí správce výslovný souhlas subjektu údajů nebo jeho zákonného zástupce, i v tomto případě se však jedná pouze o poskytnutí nezbytných informací pro naplnění účelu jeho činnosti. Osobní informace poskytuje správce pouze na základě vyžádání a zákonného zmocnění dohledovým orgánům, orgánům činným v trestním řízení, soudům a jiným orgánům veřejné správy, které mají právo požadovat osobní informace ze zákona a správce je povinen této žádosti vyhovět, případně poskytnutí těchto informací správcem je naplnění jeho zákonnou povinností. Správce zabezpečuje listinné dokumenty obsahující osobní informace subjektů primárně mechanickými prostředky, kdy úložiště dokumentů jsou zpřístupněna pouze zaměstnancům správce. Dokumenty obsahující osobní informace subjektů jsou uloženy v administrativních prostorách správce, kterými jsou prostory kanceláře ředitele, prostory sekretariátu, prostory kanceláří zaměstnanců správce a prostory archivu. Tyto prostory jsou umístěny mimo běžný přístup dalších osob, a to zejména dětí, jejich zákonných zástupců, osob externě spolupracujících se správcem či osob nahodile se vyskytujících ve školském zařízení. Uvedené prostory jsou zabezpečeny mechanickými uzamykatelnými zámky, k nimž mají klíče pouze zaměstnanci správce. Citlivé dokumenty, obsahující zvláštní kategorie osobních informací, jsou dále uloženy v uvedených prostorách v samostatně uzamykatelných skříních či stolech. Veškeré objekty správce jsou dále zajištěny elektronickým zabezpečovacím systémem, který je napojen na systém ochrany garantující včasný zásah složek Policie ČR v případě narušení objektu. Poskytované informace jsou v rámci zabezpečení předávány na externím disku, jehož obsah je šifrován.
3) Dále bylo zjištěno, že v elektronické podobě jsou veškeré osobní informace uchovávány na počítačovém síťovém serveru školy, který je umístěn v samostatně oddělené a zabezpečené místnosti, do které má přístup pouze ředitel školského zařízení a jím pověřený zástupce. Základní škola, jakož i obě mateřské školy mají oddělené vnitřní okruhy a nejsou vzájemně propojeny. Připojení dálkovým přístupem přes internet není ani pro zaměstnance možné. Vstup do programů, v nichž jsou uloženy osobní informace subjektů tak je možný pouze z počítačů vnitřní sítě správce, kdy každá oprávněná osoba má vlastní přístupové identifikační údaje nezbytné pro přístup do konkrétního počítačového programu. IT technik je smluvně zajištěn správcem pro správu, zabezpečení, uchování, obnovu, opravu a zajištění chodu a odstranění závad

počítačových sítí, programů a jiných souvisejících potřeb správce. Technik dále zajišťuje zálohu veškerých dat správce na svém vlastním zabezpečeném serveru, zajišťuje ochranu vstupu do sítě správce, obnovu hesel, odblokování účtu a ochranu před vnějšími vlivy, a to formou doménových kontrol, firewallů a kontroluje zabezpečení stávajícího softwaru proti virům a dalším škodlivým vlivům.

4) S ohledem na rozsah opatření aplikovaných správcem ve vztahu k zajištění ochrany před nežádoucími vlivy, jakož i před neoprávněným zásahem a náhodným zničením osobních informací, nebyl provedeným zkoumáním zjištěn žádný nesoulad správce se zásadou integrity a důvěrnosti dle nařízení GDPR.

5) S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, lze dále konstatovat, že správce je schopen zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování a minimalizovat rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.