GDPR
Obecný metodický pokyn pro školství

Vydáno 19. 2. 2018

Zpracovala: Mgr. Eva Kleiberová

ÚVOD

Od 25. května 2018 je povinností každého statutárního orgánu organizace (ředitele školy) naplnit ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které spolu se zákonem o zpracování osobních údajů (jehož návrh je aktuálně v legislativním procesu) nahradí dosavadní právní úpravu, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů.

Co to tedy zajištění podmínek GDPR vlastně obnáší a co bude nutné provést?

1. ANALÝZA DAT - AUDIT

Účelem vstupního auditu je zjistit všechny parametry související se zpracováním osobních údajů jednotlivými zaměstnanci, případně dalšími externími subjekty. Pro zajištění těchto informací se nejčastěji využívá následujících šest otázek:

Proč?

Odpovědí na tuto otázku je účel (proč), pro který se osobní údaje v konkrétním případě zpracovávají. V případě školy jsou nejčastější

- **zákonné důvody**, tedy případy, kdy zákon vyžaduje, aby daný subjekt shromažďoval a zpracovával osobní údaje.
- Dále se zpracovávají **osobní údaje zaměstnanců** školy.
- Třetím důvodem pro zpracování osobních údajů mohou být **smlouvy** o pronájmu bytových či nebytových prostor, případně smlouvy o poskytování služeb, prodeji či nákupu.

Kde?

- oblast zabezpečení budov, tříd…
- IT oblast
- personální a platová oblast
- ekonomická oblast
- pedagogická oblast (základní a mateřské školy, školní družiny, školní knihovna)
- oblast spisové služby
- oblast školních jídelen
- oblast hospodaření a smluv

O kom?

Cílem je **identifikovat** tzv. **subjekt údajů**, tedy fyzickou osobu, jejíž osobní údaje se z konkrétního důvodu shromažďují. Jasně se tak určí osoba, která je oprávněna (sama, případně prostřednictvím pověřeného zástupce) získat informace o zpracování dat nebo žádat jejich výmaz či převedení k jinému správci (pokud to příslušná legislativa umožňuje).

Co?

Získané informace popisují:

- typ osobních údajů (např. jména a příjmení, telefonní číslo, e-mailová adresa, datum narození, stav atd.),
- jejich zdroj (subjekt osobních údajů, třetí strana, základní registry, vlastní evidence apod.), ~~a~~
- právní důvod pro shromažďování (platná legislativa, smlouva, kvalifikovaný souhlas jednotlivce atd.).

Kdy?

Výstupem jsou informace časového charakteru, konkrétně jde o následující údaje:

- **kdy** byly osobního údaje získány,
- **termín aktualizace** (jak často se musí informace ověřovat a případně upravovat),
- **doba uchování** v souladu s platnou legislativou (zejména zákon o archivnictví a spisové službě a jednotlivé speciální zákony.

Jak?

Cílem je popsat **způsob**, jakým se osobní údaje shromažďují, zpracovávají a ukládají. Výstupem není pouze informace o konkrétním nástroji (software, tištěný dokument, základní registry či jiné komunikační nástroje), ale i popis postupu zpracování osobních údajů.

Kdo?

Odpovědi identifikují:

- **kdo** osobní údaje primárně **zpracovává** (odpovídá za jejich aktuálnost a kvalitu),
- **komu** mohou být **zpřístupněny** (včetně důvodů, proč tato konkrétní osoba může údaje zpracovávat, za jakých podmínek, jakým způsobem a po jakou dobu).

2. ANALÝZA PROCESŮ

Na rozdíl od předchozí datové analýzy se v této části zaměříte na procesy, v jejichž rámci se osobní údaje zpracovávají. Cílem je identifikovat konkrétní činnosti a popsat, jakým způsobem se v současné době osobní údaje zpracovávají (například postup při předávání osobních údajů).

3. REVIZE stávajících SOUHLASŮ se zpracováním osobních údajů

Škola velkou většinou zpracovává osobní údaje dle zákona, tedy z tzv. zákonných důvodů (legislativa stanovuje důvody, proč se konkrétní osobní údaje shromažďují a zpracovávají, a správce tudíž nemusí žádat o souhlas se zpracováním subjekt údajů).

Při revizi souhlasů se zpracováním osobních údajů se proto pověření pracovníci mohou zaměřit především na specifické případy zpracování, jako jsou například smluvní vztahy či dobrovolné poskytnutí osobních údajů. V těchto případech je explicitně vyžadován kvalifikovaný souhlas subjektu údajů s jejich zpracováním. V případech, kdy škola souhlas se zpracováním získala v minulosti, je nezbytné prověřit, zda splňuje podmínky vyplývající z GDPR.

4. ANALÝZA RIZIK

Velmi důležitou roli v rámci příprav na zavedení GDPR do školy hrají rizikové analýzy, které identifikují nejrůznější hrozby plynoucí z případných chyb a nedostatků.
Jedná se například o:

- rizika pro osobní údaje fyzických osob,
- popis posuzované aktivity – definice, účel, charakteristika,
- klasifikace rizika (nízké / střední / vysoké),
- pravděpodobnost vzniku škody,
- klasifikace možné škody (malá / střední / velká),
- typizace škody
    - materiální (např. škoda na majetku zneužitím platebních údajů)
    - nemateriální (např. poškození dobrého jména, zneužití identity)
    - společenská (např. diskriminace),
- rizika vyplývající z občansko-právních sporů,
- potenciální pokuty,
- pracovně-právní spory,
- posouzení vlivu na ochranu osobních údajů.

Získané informace se uplatní především při zpracovávání posouzení vlivu konkrétních aktivit na bezpečnost osobních údajů. Využití však naleznou i při argumentaci pro zavádění vybraných opatření a nařízení v rámci školy.

5. ANALÝZA BEZPEČNOSTI

Zcela svébytnou oblastí, na kterou bude nutné se zaměřit, je bezpečnost informací zpracovávaných v rámci školy, ať už prostřednictvím vlastních informačních systémů či cloudových řešení nebo v papírové podobě. Stávající řešení obvykle poskytují jistou míru zabezpečení, nicméně lze předpokládat, že stávající stav nebude plně odpovídat požadavkům GDPR.

6. PRÁVNÍ AUDIT

Právní analýza vlivu GDPR má ukázat, do jaké míry je jednání vedení školy a jeho zaměstnanců, v oblasti ochrany osobních údajů, v souladu s požadavky nové legislativy.

V praxi to znamená:

- projít veškeré předpisy a směrnice, postupy a pravidla pro zacházení s dokumenty nebo vyřizování požadavků subjektů na poskytování informací,
- pokud zpracování osobních údajů vyplývá ze smlouvy, musí tato obsahovat konkrétní ustanovení včetně kvalifikovaného souhlasu se zpracováním osobních údajů (nepodmíněný platností samotné smlouvy). Pokud škola tento souhlas dosud nezískala, musí tak učinit v následujících měsících,
- nové smlouvy, které škola uzavírá s dodavateli nebo obchodními partnery. Pozor, když v původních smlouvách byl nějakým způsobem včleněn souhlas se zpracováním osobních údajů. Takové smlouvy bude nutné (změnou definice účelu a souhlasu se zpracováním osobních údajů) uzavřít kompletně znovu,
- nejpozději k datu účinnosti GDPR (25. 5. 2018) je třeba smluvně ošetřit také vztahy se subjekty, jimž škola poskytuje osobní údaje. Příkladem může být například smluvní vztah se zpracovatelem platů, účetnictví, BOZP, IT apod. Ti se bez základních osobních dat neobejdou,
- podobná situace panuje také ve vztahu k poskytovatelům cloudových služeb, na jejichž serverech jsou uloženy dokumenty obsahující osobní údaje. I když v tomto případě se musíte zaměřit spíše na smluvní podmínky konkrétní služby a posoudit způsob, jakým jsou osobní údaje zabezpečeny.

7. JMENOVÁNÍ POVĚŘENCE

Školy mají povinnost jmenovat nezávislého pracovníka pro ochranu osobních údajů, u něhož nedochází ke střetu zájmů (čl. 38 odst. 6 GDPR). Jeho hlavní povinností bude monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat. Pověřenec může být sdílený více školami a ve většině případů bude zajištěn zřizovatelem.

8. ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Bude nutné nastavit **pravidla vedení záznamu** o zpracování osobních údajů (viz čl. 30 GDPR). Správce a zpracovatel jsou povinni vést písemné záznamy (za písemné se považují i elektronické záznamy) o činnostech zpracování.

Povinné obsahové náležitosti záznamů prováděných správci jsou:

- jméno a kontaktní údaje správce,
- účely zpracování,
- popisy kategorií subjektů údajů a kategorií osobních údajů,
- kategorie příjemců,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
- plánované lhůty pro výmaz kategorií údajů (pouze pokud je to možné),
- obecný popis bezpečnostních opatření uvedených v čl. 32 odst. 1 (je-li to možné).

Správce je povinen písemné záznamy na vyžádání poskytnout dozorovému úřadu.

9. ZAJIŠTĚNÍ PROCESŮ

Je třeba **zajistit** jednotlivé procesy k naplnění všech požadavků GDPR.

10. KONTROLA DODRŽOVÁNÍ OPATŘENÍ

Je třeba **zkontrolovat,** zda všechna opatření vedla k zajištění ochrany osobních údajů dle nařízení GDPR.

11. ŠKOLENÍ ZAMĚSTNANCŮ

S přijatými opatřeními a metodickými pokyny je nutné **prokazatelně seznámit** všechny **zaměstnance**, kteří budou osobní údaje zpracovávat.

12. ZÁVĚREČNÁ ZPRÁVA

Závěrečná zpráva ukončuje fázi příprav a realizace změn a převádí celý projekt do praktického užívání.

Tento postup bude nutné neustále **opakovat** - GDPR je živá struktura, která se bude stále vyvíjet.

Máte-li k tomuto tématu jakékoliv dotazy, obraťte se na nás, rádi Vám pomůžeme.

Mgr. Eva Kleiberová
GDPR specialista

Sensio.cz s.r.o.
Infolinka: +420 737 299 398
E-mail: gdpr@sensio.cz
Web: www.GDPRproSKOLSTVI.cz