# Jak se jednoduše, rychle a správně rozhodovat, zda osobní údaj spadá pod ochranu GDPR

**Ing. Pavel Fencl**

**Veřejná informační služba, spol. s r.o.**

Cílem tohoto článku je vyčlenit některé momenty vnitro-organizační směrnice, která by v každé organizaci měla upravovat zpracování osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Nařízení" resp. „GDPR"), které jsou spojené s rozhodováním, zda konkrétní údaj spadá pod ochranu GDPR, či se na něj GDPR nevztahuje. Jaká je tedy základní logika Nařízení? Které údaje je třeba chránit dle tohoto Nařízení a na které se Nařízení nevztahuje?

Základní rozhodovací logika, která musí v organizaci proběhnout při zavádění směrnice GDPR do praxe musí obsahovat tyto základní kroky:

1. Jde o osobní údaj?
2. V případě, že jde o osobní údaj, dochází k jeho zpracování?
3. V případě, že jde o osobní údaj, který zpracovávám, znám účel (právní důvod) jeho zpracování?

Podívejme se nyní podrobněji, co jednotlivé kroky praxi nejenom v praxi školských zařízení znamenají.

**Krok 1 – Jde o osobní údaj?**

Podle znění nařízení platí, že osobním údajem jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě a dále, že 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). Ochrana podle Nařízení GDPR se tak vztahuje pouze na údaje, které jsou tzv. osobním údajem dle výše uvedené definice.

Co z výše uvedené definice vyplývá a co je nutné na tomto místě připomenout, že **ne každý údaj je osobním údajem**. Kde je tedy ta pomyslná hranice? Zjednodušeně lze říci, že osobním údajem jsou ty údaje, podle kterých dokážete „ukázat" (identifikovat) určitou osobu. Údaj o výši platu na pozici kuchařka v konkrétní školní jídelně, která zaměstnává 10 kuchařek, tak zcela jistě není osobním údajem – nedokážete podle tohoto údaje identifikovat konkrétní osobu. Údaj o výši platu vedoucí ŠJ v konkrétní školní jídelně však již je osobním údajem, neboť vedoucí ŠJ je vždy jen jedna osoba a tudíž dokážete podle toho údaje identifikovat konkrétní osobu. Jak z výše uvedeného plyne, ne každý údaj je údajem osobním, byť může jít stále o tentýž údaj a silně závisí na kontextu, v jakém se daný údaj nachází. Zároveň tento údaj vůbec nemusí být spojen s pro každého jasnými osobními údaji typu jméno, rodné číslo, datum narození, adresa apod., ale může jít o zcela obecný údaj (výše platu).

**Krok 2 – V případě, že jde o osobní údaj, dochází k jeho zpracování v organizaci?**

V případě, že jsem údaj identifikoval jako osobní údaj podle kroku 1, dalším rozhodovacím krokem je rozhodnutí, zda vůbec dochází ke zpracování tohoto osobního údaje v organizaci. Podle recitálu 15 Nařízení GDPR by se ochrana fyzických osob měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Podle recitálu 18 se toto nařízení se nevztahuje na zpracování osobních údajů fyzickou

osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností.

Z výše uvedené definice nařízení vyplývá, že **ne každé nakládání s osobním údajem je zpracováním osobního údaje ve smyslu GDPR**!

Ke zpracování osobního údaje dochází vždy a pouze tehdy, pokud:

- s osobní údajem nakládáte systematicky (opakovaně, stále stejným způsobem, ve stejném rozsahu apod.),
- je jedno, zda osobní údaje evidujete v PC (automatizované zpracování) nebo v sešitě, šanonu (neautomatizované zpracování),
- osobní údaj zakládáte do nějaké evidence (strukturovaný soubor),
- osobní údaje zpracováváte za organizaci z profesních nebo obchodních důvodů (aspekt oficiality) nikoliv pro soukromé účely,
- pro zpracování má organizace jasně vytyčený účel tj. potřebuje jej pro plnění svých povinnosti nebo pro účel své existence.

Z těchto hledisek tedy v praxi vyplývá, že:

- do evidence GDPR nespadají osobní údaje, které si evidujete pro soukromé účely (svůj soukromý adresář či telefonní seznam apod.)
- do evidence GDPR nespadají osobní údaje, které nemáte v žádné strukturované evidenci (letáky od dodavatelů materiálu či zboží, na kterých jsou kontakty na obchodní zástupce, osobní údaje z razítek jiných subjektů, jmenovky na dveřích školy či ŠJ, vizitky, nahodilé seznamy žáků nebo strávníků, fotografie ze zaměstnaneckého večírku pro účely účastníků apod.)

**Krok 3 - V případě, že jde o osobní údaj, který v organizaci zpracovávám, znám účel jeho zpracování?**

Na základě předchozích kroků, kdy jsem identifikoval údaj jako osobní, který v organizaci zpracovávám, je třeba se rozhodnout, zdali je znám účel (neboli mám právní důvod) zpracování tohoto údaje. Podle Nařízení GDPR totiž platí, že organizace musí mít minimálně jeden právní důvod, aby mohla osobní údaj zpracovávat, jinak jej zpracovávat nesmí. Zároveň platí, že jakmile v organizaci pomine poslední právní důvod zpracování osobního údaje, má organizace povinnost osobní údaj zlikvidovat. Možnosti právních důvodů zpracování jsou vždy podle Nařízení GDPR tyto:

- Splnění smlouvy (vždy dodavatelsko-odběratelské vztahy)
- Splnění právní povinnosti (vždy na základě zákona – například školní matrika apod.)
- Ochrana životně důležitých zájmů subjektu
- Splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci (vždy na základě zákona)
- Oprávněné zájmy správce (vždy, kdy organizace potřebuje osobní údaj pro výkon své činnosti)
- Souhlas subjektu údajů (vždy, kdy organizace nenajde právní důvod zpracování v předchozích bodech a zpracovávat osobní údaj potřebuje)

Z výše uvedeného tak platí, že pokud organizace zpracovává osobní údaj a nezná jeho účel zpracování, resp. nemá právní důvod pro jeho zpracování dle výše uvedených bodů, zpracovává tento osobní údaj nezákonně a tento osobní údaj musí zlikvidovat a dále nezpracovávat, případě zjednat nápravu například ve formě souhlasu ze zpracováním od fyzické osoby.

Dotazy týkající se GDPR v oblasti hromadného a školního stravování můžete zdarma položit odborníkům pomocí aplikace na stránkách www.gdprexperti.cz. Zde také naleznete celou řadu vzorových dokumentů, komentovaných zákonů a organizačních směrnic, které přináší komplexní řešení GDPR pro všechny školské organizace i organizace malého a středního podnikání.