Úvod ke GDPR

Obecné nařízení

Obecné nařízení na ochranu osobních údajů neboli GDPR (General Data Protection Regulation) je uceleným souborem pravidel na ochranu dat v EU.
Cílem je hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji, dát jim větší kontrolu nad tím, co se s jejich daty děje.
GDPR se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, tedy i škol.
GDPR začne v celé EU platit jednotně **od 25. května 2018**. V Česku tak nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů.

Směrnice EU a nařízení EU

Nařízení platí v celém svém rozsahu v celé Evropské unii a je přímo použitelné.
Směrnice jako právní akt stanovující cíl, který musí všechny členské státy EU splnit, ponechává na členských státech, jak formulují vnitrostátní zákony a jak těchto cílů dosáhnou

Obecné nařízení a zákon

Doposavad pro ochranu osobních údajů platil zákon č. 101/2000 Sb., nyní se řídíme nařízením EU. Pokud jde o stanovení práv a povinností, není mezi nařízením a zákonem rozdíl, oba dva právní předpisy přímo adresátům stanovují povinnosti a práva.

Právní předpisy

Právní předpisy EU a ČR	Právní předpisy EU
Směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů	*Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů*
↓	↓
Zákon 101/2000 Sb., o ochraně osobních údajů	
↓	
Škola	**Škola**

Nejedná se o novou věc nebo zásadní změnu

Základní znak ochrany osobních údajů podle obecného nařízení je **kontinuita**.
Nařízení EU navazuje na Směrnici EU 95/46/ES podle které vznikl zákon 101/2000 Sb., o ochraně osobních údajů.
Například:

- jsou používány **stejné definice klíčových pojmů** (osobní údaj, subjekt údajů, zásady zpracování),
- pravidla jsou ale pro správce a zpracovatele **podrobnější** než ve směrnici,
- správcům jsou ukládány některé **nové povinnosti** (ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu, jmenování pověřence),
- nařízení reaguje také na nové **technické prostředky** a technologie (pseudonymizace a šifrování, obnova dostupnosti, pravidelné testování a hodnocení účinnosti zavedených opatření)
- **práva subjektu údajů** jsou zachována a nově upravena podrobněji.

Dodržovala-li škola zákon 101/2000 Sb., o ochraně osobních údajů, má většinu povinností daných nařízením EU již splněnu.

Nový přístup k ochraně osobních údajů

Lze hovořit o dvou nových přístupech, na kterých je Obecné nařízení založeno. Novými přístupy jsou:

- princip odpovědnosti správce (školy) a
- přístup založený na riziku.

Princip odpovědnosti znamená odpovědnost školy za dodržení zásad zpracování, které jsou uvedeny v článku 5 odst. 1 Obecného nařízení a zároveň musí správce být schopen tento soulad doložit.

Přístup založený na riziku uváděný pod anglickou zkratkou „RBA".

Tento koncept bude jakousi **náhradou stávajícího institutu ochrany osobních údajů - oznamovací povinnosti** podle § 16 zákona č. 101/2000 Sb. Ta ukládá správcům osobních údajů **oznámit písemně svůj záměr ještě před započetím samotného zpracovávání svému dozorovému úřadu** – v případě ČR tedy Úřadu pro ochranu osobních údajů. Má se tak předejít zahájení jakéhokoli zpracování osobních údajů, které může porušovat platné předpisy, tj. aktuálně v ČR povinnosti ze zákona č. 101/2000 Sb.

Nebezpečí porušování některých ustanovení tohoto zákona posuzuje daný dozorový úřad pro ochranu osobních údajů právě za použití rizik. Neboli - při tomto posouzení připravovaného zpracování osobních údajů **musí vzít v úvahu všechna rizika pro práva a svobody fyzických osob**. To samozřejmě zahrnuje i rizika v kontextu bezpečnostních opatření.

To, co je dosud zajišťováno aktivní činností dozorového úřadu, **přejde nyní z velké části na správce**. Ti budou hlavními nositeli úkonů zajišťujících provádění přístupu založeného na riziku, a to i v těch povinnostech podle GDPR, kde se definice „rizika pro práva a svobody lidí" výslovně neobjevuje.
Rizikovost totiž hraje roli už v naplňování samotných zásad zpracování osobních údajů podle čl. 5.

Snadno to lze ilustrovat na **zásadě přesnosti**; čím vyšší je (jakékoli) riziko plynoucí z nepřesnosti některého ze zpracovávaných osobních údajů, **tím větší jsou nároky na mechanismy aktualizace osobních údajů**. U zásady omezení uložení tento přístup předepisuje již samotná formulace zásady. Rovněž uzpůsobení každého zpracování zásadě korektnosti musí přihlížet k rizikům pro práva a svobody lidí.

🗁 Sdělení ÚOOÚ k přístupu založenému na riziku

Novinky v ochraně osobních údajů

- Úprava postupu, jakým se může subjekt údajů (žák, zákonný zástupce, …) obracet na správce (školu) či zpracovatele dle čl. 12 GDPR
- Vedení záznamů o činnostech zpracování dle čl. 30 GDPR
- Ohlašování případů porušení zabezpečení osobních údajů dle čl. 33 a 34 GDPR
- Zavedení institutu pověřence dle čl. 37 -39 GDPR
- Zpřísnění podmínek předávání osobních údajů do ciziny dle čl. 44 a násl. GDPR
- Právo na informace a přístup k osobním údajům čl. 14-16 GDPR
- Právo na přenositelnost údajů dle čl. 20 GDPR
- Právo vznést námitku při zpracování dle čl. 21 GDPR
- Výslovná úprava práva být zapomenut dle čl. 17 odst. 2 GDPR
- Souhlas se zpracováním osobních údajů může ve vymezených případech vyjádřit i dítě

Specifika v ochraně osobních údajů pro školy

- Spravování osobních údajů o dětech (v určitých situacích bude potřeba nabýt práva ke zpracování od zákonných zástupců).
- Spravování zvláštních kategorií osobních údajů tzv. citlivé údaje (data o zdravotním stavu dětí, např. psychologické posudky pro IVP).
- Kombinaci osobních údajů více subjektů (děti, zákonní zástupci, další zmocněnci žáka, pedagogičtí pracovníci, pracovníci družin, klubů a jídelen atd.).
- Kombinaci různých právních titulů zpracování (plnění právní povinnosti, úkol ve veřejném zájmu, plnění smlouvy, oprávněný zájem, ….).
- Povinnosti poskytovat osobní údaje či výstupy z nich dalším veřejným orgánům (ČŠI, MŠMT, zřizovatel).

Zabezpečení osobních údajů

Obecné nařízení neukládá povinnost použít pro zabezpečení zpracování osobních údajů některá specifická opatření (například šifrování).
Je třeba vždy vycházet:

- z konkrétních podmínek školy (typ školy, velikost, …),

· stav techniky
· náklady na přijetí a provedení jednotlivých technických a organizačních opatření,

Při posuzování úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování (náhodné nebo protiprávní zničení, ztráta, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům).

Uložení sankcí

Obecné nařízení stanoví, že za jakékoliv porušení obecného nařízení by měly být uloženy sankce včetně správních pokut, a to vedle nebo místo opatření uložených dozorovým úřadem. Zatímco v některých členských státech včetně České republiky dozorové úřady pokuty ukládají, v jiných členských státech EU (např. Dánsko) tomu tak dosud není. Horní hranice správních pokut, které ukládá Úřad pro ochranu osobních údajů, je v současné době 10 000 000 Kč, přičemž v minulosti (do 31. prosince 2004) dosahovala dvojnásobku. Nejvyšší dosud uložená pokuta za zjištěné a prokázané porušení povinností, za které se pokuty ukládají, nedosáhla ani polovinu sazby.
Horní hranice pokut je nová, ale jak je opakovaně v preambuli k obecnému nařízení uváděno, pokuty mají být v každém jednotlivém případě účinné, přiměřené a odrazující. Obecné nařízení současně respektuje zásady správního trestání, včetně kritérií pro stanovení výše pokut i podmínek pro určení odpovědnosti i vyvinění se (z trestu).

Cíle výchovy a vzdělávání

Škola musí především plnit cíle výchovy a vzdělávání, které jsou dány:
· školským zákonem (§ 2),
· zřizovací listinou,
· školním vzdělávacím programem.
Vedle této základní povinnosti plní i další úkoly:
· bezpečnost dětí a žáků,
· pracovně právní problematika zaměstnanců,
· ochrana osobních údajů.
Žádná z těchto dalších povinností nemůže překrýt nebo omezit plnění hlavního cíle. Proto je potřeba vytvořit takový systém ochrany osobních úkolů, aby plnění zákonných povinností v oblasti ochrany osobních údajů nebylo na úkor výchovy a vzdělávání.

Příklady:
· obavy vytvářet seznamy žáků,
· neustálé požadování souhlasu zákonných zástupců,
· minimalizace údajů na úkor přehlednosti (kódy místo jmen žáků, …),
· škola bez fotografií,
· čas určený výchově a vzdělávání je spotřebován na zabezpečení ochrany údajů,
· …

Ochrana osobních údajů ve škole nemůže být zabezpečena jednotlivými dokumenty, jednotlivým plněním úkolů, ale musí vytvářet systém, který ve svém celku a provázanosti zajistí ochranu osobních údajů dle požadavků GDPR.

🗁 *Systém školy k zabezpečené ochrany osobních údajů dle nařízení EU*