
Seznam dokumentů ke GDPR, které by obce měly mít připraveny k 25. květnu 2018

Seznam dokumentů, které budou muset obce mít postupně připraveny a zpracovány podle nároků vyplývajících z účinného obecného nařízení k ochraně osobních údajů (GDPR). Bude doplňován podle nejnovějších informací a stanovisek za věc odpovědných orgánů.

- **Organizační řád** - obce ho budou muset upravit, doplnit do něj funkci pověřence a další věci dle obecného nařízení.
- **Pracovní řád**
- **Spisový a skartační řád** – vzor jsme již zveřejnili na webu SMO ČR (<http://smocr.cz/cz/oblasti-cinnosti/gdpr/vzor-spisoveho-a-skartacniho-radu-obce.aspx>).
- **Směrnice pro práci s osobními údaji** – vzor jsme již zveřejnili na webu SMO ČR (<http://smocr.cz/cz/oblasti-cinnosti/gdpr/vzor-vnitriho-predpisu-smernice-obce-pro-praci-s-osobnimi-udaji.aspx>).
- **Provozní řád výpočetní techniky**
- **Systémová příručka k IS**
- **Revize stávajících souhlasů** – souhlasy získané v minulosti – prověřit, zda splňují podmínky obecného nařízení.
- **Informovaný souhlas dle obecného nařízení**
- **Dodatky ke smlouvám s dodavateli software a zpracovateli osobních údajů** – stanovení požadavků ze strany správce (mlčenlivost, závazání dalšího zpracovatele, odpovědnost zpracovatele, stanovení sankcí za porušení povinností atp.)
- **Dohoda o mlčenlivosti s externími pracovníky** - pro obce v mnoha oblastech pracují externisté. Obec by měla uzavřít dohodu o mlčenlivosti např. s externím pracovníkem IS (IT správce), externí účetní, externí mzdovou účetní atd.
- **Evidence** – vytvoření evidence kódů elektronického zabezpečovacího zařízení (EZS), evidence razítek, evidence klíčů (komu byly přiděleny), evidence souhlasů, evidence všech přenosných paměťových médií (flash disk, CD, externí disk atp.), evidence výpočetní techniky, úložišť dat a programového vybavení používaných ke zpracování osobních údajů. U přenosné výpočetní techniky a úložišť dat se eviduje též osoba odpovědná za využívání přenosného zařízení a za jeho ochranu před neoprávněným přístupem.

- **Seznam osob s přístupem** k základním registrům, k osobním datům ze základních registrů a k Czech Pointu.
- **Analýza (revize) osobních údajů, rizik a procesů** – dobrovolná, ale velmi užitečná. Z analýzy se vychází při zpracování dokumentace k prokázání souladu s GDPR, např. záznamů o činnostech zpracování.
- **Záznamy o činnosti zpracování** – povinné pro prokázání souladu s GDPR, dle čl. 30 obecného nařízení.
- **Technicko - organizační opatření** – obec vede evidenci opatření k zabezpečení osobních údajů. Pokud existuje vnitřní předpis upravující ochranu osobních údajů (např. pro komunikaci s bezpečnostní službou, odchodu z kanceláře, vytváření a úschovy kopií dat atp.) - provést jeho revizi a doplnit či změnit.
- **Řízení přístupů** – udělování oprávnění pracovníkům a jejich poučení o ochraně osobních údajů. Vést např. na kartě „Pověření k přidělení přístupových práv pracovníka k jednotlivým SW aplikacím v rámci informačního systému obce“.
- **Popis a definice postupu při narušení zabezpečení osobních údajů** – pravidla pro oznamování bezpečnostního incidentu ÚOOÚ, určení osoby odpovědné za ohlášení BI.
- **Ustanovení pověřence** pro ochranu osobních údajů (včetně smluvního vztahu), zveřejnění kontaktních údajů pověřence.