Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Co obce mohou udělat pro GDPR už nyní

Medlov, 23.10.2017
Mgr. Miroslava Sobková
sobkova@smocr.cz

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Aktuální otázky menších samospráv

- I. Úvod
- Stručný popis postupu při implementaci GDPR
- Vytvořit si přehledy se zdroji osobních údajů
- Co požadovat od dodavatelů SW produktů

Úvod

- Nařízení Evropského parlamentu 2016/679 je uveřejněno v plném znění na stránkách ÚOOÚ
- GDPR se týká všech osobních údajů jak v přenesené působnosti, tak i v samostatné působnosti
- Citlivé údaje jsou zvláštní kategorií osobních údajů

Úvod

Osobní údaje			
Jméno, příjmení	pohlaví	IP adresa	fotografie
Věk a datum narození	občanství	stav	RČ nebo jiný identifikátor vydaný státem
Email adresa	Telefonní číslo	Adresa bydliště , pracoviště	

Citlivé osobní údaje			
Etnický nebo rasový původ	Zdravotní stav	Náboženské vyznání	Tresty a odsouzení
Sexuální orientace	Politické názory	Členství o odborových organizacích	Osobní údaje dětí
Genetické informace	Biometrické informace		

II. Stručný popis postupu při implementaci

- Revize spojená s analýzou existujícího prostředí:
- Seznam procesů, kde jsou používány osobní údaje a určení důvodů pro sběr a zpracování osobních údajů
- Jak probíhá zpracování osobních údajů probíhá a kde se ukládají osobní údaje? (listinná forma, kartotéka, archiv, skříň, počítač a sw. produkt, databáze, lokální nebo síťová úložiště, cloudová služba, emaily, kamerové zařízení apod.)

II. Stručný popis postupu při implementaci

- 2. Závěry a doporučení na základě analýzy:
- doporučení se mohou týkat např.
  používání a zavedení nových procesů
  nebo nové technologie
- může dojít ke změně v IT infrastruktuře
- doplnění stávající a vytvoření nové dokumentace
- Vytvoření nové politiky pro ochranu dat

II. Stručný popis postupu při implementaci

- Doporučení na základě analýzy je nutné realizovat v praxi a vytvořit si plán postupu nasazení
- Pravidelná revize včetně vzdělávání a školení obsluhy

III. Jak na revizi vlastními silami

- Zaměřte se na činnosti které provádíte a na dokumenty, které při těchto činnostech vznikají. Tímto postupem by jste měli dojít k vytvoření přehledu, který bude základem pro Vaši další spolupráci s pověřencem pro ochranu osobních údajů a měli byste získat přehled o rizikovém zpracování osobních údajů
- 1. Je na ÚOOÚ nahlášena nějaká evidence osobních nebo citlivých údajů?

III. Jak na revizi vlastními silami

- ověřte, zda opatření, která budete pro ochranu osobních údajů používat jsou dostačující
- 2. Již existuje nějaké technicko - organizační opatření ve formě vnitřního předpisu k zajištění ochrany osobních údajů
- Obecní úřad mohl v minulosti vydat za určitým účelem nějaká technicko – organizační opatření, která mohou obsahovat osobní údaje

III. Jak na revizi vlastními silami

- např. pro komunikaci s bezpečnostní službou, odchodu z kanceláře, vytváření a úschovy kopií. Zajistěte, aby tato opatření byla v souladu s postupy popsanými v organizačním řádu.
- 3. Určit a zjistit si, kde se nacházejí osobní údaje (používané informační systémy a programy). Projít, které sw. produkty používáte, kdo je jejich dodavatelem (zpracovatelem) a o jaké osobní údaje se zde jedná

III. Jak na revizi vlastními silami

- 4. Prověřit veškeré listinné zdroje, v kterých se nacházejí osobní údaje tzn. projít veškeré evidence
- 5. Připravit platné pracovní smlouvy k revizi

Pro zpracování naprosté většiny osobních údajů není nutný souhlas zaměstnance, přesto je doporučeno tento souhlas vyjádřit a to buď v pracovní smlouvě nebo formou dodatku

III. Jak na revizi vlastními silami

- Pokud mzdy zpracovává jiná organizace (smluvní vztah k úřadu) měl by zaměstnanec vyjádřit souhlas vždy, protože jeho osobní údaje nezpracovává zaměstnavatel.
- 6. Zjistit a vytvořit seznam nařízení a pravidel úřadu, která jsou používána a jsou účinná.

Minimálně by měla obec mít:

- **Organizační řád** (vzor bude zveřejněn na webových stránkách Svazu)

III. Jak na revizi vlastními silami

- **Provozní řád informačního systému**
- **Spisový řád**, který by měl obsahovat i seznam razítek
- Seznam osob, které mají přístup k osobním údajům ze ZR obyvatel a popis opatření, dle kterých lze určit, komu byly a jsou tyto údaje předávány. Osoby, které mají přístup k CzP např. formou tabulky

III. Jak na revizi vlastními silami

Vzor tabulky – přístup k ZR

Základní registry/CP	Zpracovatel (pracovní místo)	Příjemce	Opatření pro bezpečné zpracování
Přístup k registru – název Přístup k CP	*Při jaké činnosti v jaké agendě se používá*	*Určení příjemce údajů ze ZR /CP*	*Postupy a opatření při práci se ZR/CP*

III. Jak na revizi vlastními silami

- Seznam klíčů k budově a komu byly přiděleny

Klíč	Jméno příjmení	Datum převzetí	Podpis
Identifikace klíče (číslo, název,...)			

- Seznam kódů k elektronickým zabezpečovacím zařízením

Kód EZS	Jméno příjmení	Datum převzetí	Podpis
Kód EZS			

III. Jak na revizi vlastními silami

- Pravidla pro přijímání petic a vyřizování stížností

7. Pro elektronické zdroje resp. informační systémy a programy je nutné ověřit:

- existenci dokumentace k IS a programům, které obecní úřad používá – **uživatelská a systémová příručka**
- ověřit, zda systémová příručka obsahuje:
- ✓ popis implementovaného systému nebo programu

III. Jak na revizi vlastními silami

- ✓ licenční podmínky
- ✓ popis podpory uživatele (hot-line, postupy při pomoci)
- ✓ bezpečnostní podmínky
- ✓ popisy systémem vytvářených logů
- ✓ zprávy a výsledky testů a certifikací
- ✓ pokud úřad používá cloudové služby, měl by mít seznam aplikací, které obsahují osobní údaje

III. Jak na revizi vlastními silami

- ✓ smluvní dokumenty s poskytovatelem cloudových služeb

Výše uvedené body s informacemi uvedenými v systémové příručce jsou důležité pro činnost pověřence pro ochranu osobních údajů

IV. Vytvořit přehledy a seznamy

1. Vytvořit si seznam zdrojů s výskytem osobních údajů

seznam by měl sloužit k přehledu, kde a jak jsou používány osobní údaje. Měl by také obsahovat rizikové zpracování osobních údajů

Seznam by měl obsahovat:

- název zdroje např. doklad, evidence
- účel zpracování

IV. Vytvořit přehledy a seznamy

- osobní údaje vyskytující se ve zdroji
- zákonnou normu, která opravňuje k evidenci a zpracování
- příjemce osobních údajů

2. Z elektronických i listinných zdrojů vytipovat ty, které obsahují osobní údaje a nejsou zpracovávány na základě zákonné normy nebo výkonu veřejné moci - rizikové zpracování

IV. Vytvořit přehledy a seznamy

- účel nebo účely zpracování
- kategorii osobních údajů
- příjemce nebo kategorie příjemců, kterým budou osobní údaje sděleny
- popis přijatých opatření pro zajištění bezpečnosti zpracování

IV. Vytvořit přehledy a seznamy

Evidence dokumentů a seznamů obsahující osobní údaje

Dokument / seznam	Účel zpracování a zpracovatel	Údaje	Příjemce	Zákon	Komentář	Rizikový?
Specifikace dokladu nebo seznamu názvem.	*Při jaké činnosti v jaké agendě se používá. Zparacovatel/Název pracovního místa, kde dokument seznam vznikl*	*Osobní údaje, které se zde objevují.*	*Pro koho je dokument nebo seznam vytvářen.*	*Zákon, dle kterého je dokument nebo seznam vytvářen a zpracováván.*	*Doplňující informace k popisu.*	*Ano nebo Ne.*

V. Dodavatelé SW a IS a doplnění vnitřních předpisů

1. Písemně se dotázat dodavatele IS a programů, zda jeho systémy budou včas na nařízení připraveny a že je připraven spolupracovat s pověřencem pro ochranu osobních údajů

Dodavatelé by měli určitě zabezpečit:

- závazek spolupracovat s pověřencem pro ochranu osobních údajů
- zajistit splnění dostupnosti údajů a informací o zpracování pro subjekt údajů

V. Dodavatelé SW a IS a doplnění vnitřních předpisů

2. Provést revizi smluv se zpracovateli

Smlouva by měla obsahovat:

- jak budou zajištěny osoby oprávněné zpracovávat osobní údaje a jejich mlčenlivost
- jaké jsou podmínky pro zapojení dalšího zpracovatele dle nařízení 679/2016
- jakým způsobem budou zajištěna práva subjektu

V. Dodavatelé SW a IS a doplnění vnitřních předpisů

- podpora pověřence pro ochranu osobních údajů např. dohledání incidentu
- ukončení smlouvy a co bude potřebné při ukončení zajistit např. předat osobní údaje

3. Ověřit jak budou provedena opatření k zabezpečení dat dle čl. 32

- pseudonymizace a šifrování osobních údajů – zajistit, aby byl popis součástí systémové příručky

V. Dodavatelé SW a IS a doplnění vnitřních předpisů

- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů (nahlášení incidentu 72 hodin na ÚOOÚ)
- proces pravidelného testování