CO OBCE MOHOU UDĚLAT PRO GDPR UŽ NYNÍ?

Svaz měst a obcí ČESKÉ REPUBLIKY

Společně hájíme zájmy měst a obcí!

Praha, 5. prosince 2017

Ing. Tomáš Kejzlar, člen Komise pro informatiku, Svaz měst a obcí ČR

AKTUÁLNÍ OTÁZKY MENŠÍCH SAMOSPRÁV

- Problematika GDPR na obcích a související bezpečnost – připravte se na GDPR doporučenou revizí současného stavu v oblasti osobních údajů

I. Úvod
II. Stručný popis postupu při implementaci GDPR
III. Jak na revizi vlastními silami
IV. Vytvořit si přehledy se zdroji osobních údajů (rizikové zpracování osobních údajů)
V. Co požadovat od dodavatelů SW produktů

ÚVOD

- GDPR – evropská směrnice o ochraně osobních údajů fyzických osob „*General Data Protection Regulation*“
- Účinná od 25. května 2018
- Obec si musí zajistit pověřence pro ochranu osobních údajů
- Občan bude mít právo na výmaz a přenositelnost dat z evidencí a databází vedených obcí
- Pokud obec nezajistí bezpečnostní opatření – vysoké sankce

ÚVOD

- Zodpovědnost má politická reprezentace obce
- GDPR se týká všech osobních a citlivých údajů – nově zvláštní kategorie osobních údajů, které se vztahují k identifikované nebo identifikovatelné osobě. Takové údaje se vyskytují nejen v elektronické podobě, ale i v listinné formě.
- Nařízení Evropského parlamentu 2016/679 je uveřejněno v plném znění na stránkách ÚOOÚ

https://www.uoou.cz/gdpr/ds-3938/p1=3938

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 PŘI IMPLEMANTACI

- 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 vydat 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

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 VLASTNÍM 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 SI 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

VYTVOŘIT SI 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 SI 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 SI PŘEHLEDY S 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. CO POŽADOVAT OD DODAVATELŮ SW 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. CO POŽADOVAT OD DODAVATELŮ 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. CO POŽADOVAT OD DODAVATELŮ 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. CO POŽADOVAT OD DODAVATELŮ 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

Ing. Tomáš Kejzlar

Svaz měst a obcí
SMO
ČESKÉ REPUBLIKY