JAK ZAČÍT S GDPR V PODMÍNKÁCH MALÉ OBCE

Svaz měst a obcí ČESKÉ REPUBLIKY

Společně hájíme zájmy měst a obcí!

Ing. Luděk Galbavý, Alis spol. s r.o.- komise informatiky SMO

KISMO

- Komise pro informatiku SMO ČR
- Poradní orgán Předsednictva SMO ČR

  Je složena z IT odborníků i politiků z měst a obcí, zasedá zpravidla 10 krát ročně a úzce spolupracuje s informatiky Asociace krajů ČR, se Sdružením tajemníků a s poslanci Parlamentu ČR.
- Spolupráce při zavádění projektů MV ČR
- Připomínkování legislativy a vládních koncepcí
- Zástupci – Praha, Brno, Kladno, Děčín, Vyškov, Karviná, Vodňany, Velké Meziříčí, Milevsko, Nymburk a další města a obce.

DŮVOD VZNIKU MATERIÁLU

- Členy komise jsou i zástupci (starostové) malých obcí, kteří vyslovili silné obavy, že nebudou schopni naplnit požadavky Nařízení Evropského parlamentu 2016/679.
- Z diskuse jasně vyplynul požadavek na dokument, který by jim umožnil (nejlépe) pomocí vlastních sil provést minimálně přípravu na splnění požadavků GDPR v prostředí malé obce.
- Mají potřebu odhadnout finanční náročnost pro sestavení rozpočtu na rok 2018.

OVĚŘENÍ STAVU V TERÉNU

Provedli jsme návštěvu několika malých obcí:

- Minimální (žádná) povědomost o GDPR.
- Chybějí základní dokumenty a směrnice (organizační řád, směrnice pro práci s výpočetní technikou, spisový řád, dokumentace pro provoz a implementace sw. produktů).
- Jsou provozovány systémy a vedeny evidence, které podléhají ohlašovací povinnosti dle zákona 101/2000 Sb.
- Existují listinné dokumenty a pracovní a příruční seznamy, které obsahují osobní údaje.

CO JSME TEDY VYTVOŘILI

- Připravili jsme popis možného postupu pro provedení revize současného stavu na obci s určením, jaká činnost je vykonávána dle jakého zákona.
- Šablony (tabulky) pro záznam tohoto stavu.
- Doporučení vytvořit nebo doplnit si vnitřní směrnice a řády (minimálně OŘ, Provozní řád inf. systému, Spisový řád).
- Doporučení, co požadovat od dodavatelů sw (příručky, implementační popisy, doplnění smluv, úpravy sw, závazek spolupráce s pověřencem).

Toto vše budou základní informace a dokumenty pro činnost pověřence na obci.

ÚVOD

GDPR je nařízení Evropského parlamentu a rady EU 2016/679 schválené Evropským parlamentem a v České republice nahrazuje zákon 101/2000 Sb. o ochraně osobních údajů.

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		

STRUČNÝ POPIS POSTUPU PŘI IMPLEMENTACI GDPR

➢1. 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 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.).

STRUČNÝ POPIS POSTUPU PŘI IMPLEMENTACI GDPR

➢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.
  Tuto fázi již ve spolupráci s pověřencem.

STRUČNÝ POPIS POSTUPU PŘI IMPLEMENTACI

3. Doporučení a postupy na základě analýzy je nutné realizovat v praxi a vytvořit si plán postupu nasazení.

4. Pravidelná revize včetně vzdělávání a školení obsluhy.

Tuto fázi již ve spolupráci s pověřencem.

JAK NA REVIZI VLASTNÍMI SILAMI

- Zaměřte se na činnosti, které provádíte a na dokumenty, které při těchto činnostech vznikají. Tímto postupem byste 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?

JAK NA REVIZI VLASTNÍMI SILAMI

Jestliže existuje, 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.

Např. pro komunikaci s bezpečnostní službou, činnosti při odchodu z kanceláře, vytváření a úschovy kopií.
Zajistěte, aby tato opatření byla v souladu s postupy popsanými např. v organizačním řádu.

JAK NA REVIZI VLASTNÍMI SILAMI

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.

JAK NA REVIZI VLASTNÍMI SILAMI

4. Prověřit veškeré listinné zdroje, ve 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. Pokud mzdy zpracovává jiná organizace (smluvní vztah k úřadu), měl by zaměstnanec vyjádřit souhlas vždy, protože jeho osobní údaje nezpracovává zaměstnavatel.

JAK NA REVIZI VLASTNÍMI SILAMI

Minimálně by měla obec mít:

- ✓ Organizační řád (vzor zveřejněn na webových stránkách Svazu).
- ✓ 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.

JAK NA REVIZI VLASTNÍMI SILAMI

Vzor tabulky pro přístupy k ZR a CzP

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*

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			

JAK NA REVIZI VLASTNÍMI SILAMI

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:

JAK NA REVIZI VLASTNÍMI SILAMI

- popis implementovaného systému nebo programu,
- 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,

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.

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

VYTVOŘIT SI 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.*

VYTVOŘIT SI PŘEHLEDY A SEZNAMY

Svaz měst a obcí SMO ČESKÉ REPUBLIKY

Evidence dokumentů a seznamů obsahující osobní údaje

Doklad	Účel zpracování	Údaje	Příjemce	Zákon	Komentář	Riziko vý
Daňové doklady, faktury	Ekonomické agendy	Jméno, příjmení, adresa	Dodavatel Odběratel	Zákon č. 563/1991 Sb., o účetnictví	Vytváří se na PC a tiskne ou se, zakládají	NE
Smlouvy	Evidence smluv	jméno, příjmení, adresa, datum narození	Smluvní strana	Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník	o dílo, pronájmy, ... Vytváří se na PC a tiskne ou se, zakládají	NE
Žádosti	Správní rozhodování obce	jméno, příjmení, adresa	Žadatel	Zákon č. 114/1992 Sb., o ochraně přírody a krajiny (dřeviny); zákon č. 183/2006 Sb., stavební zákon (sjezdy k domu)	kácení stromů, sjezdy k domu, diary	NE






VYTVOŘIT SI PŘEHLEDY A SEZNAMY

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.

Seznam by měl obsahovat:

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

VYTVOŘIT SI PŘEHLEDY A SEZNAMY

Seznam rizikových zpracování a evidencí k vyjádření UOOU

Seznam	Účel zpracování	Údaje	Příjemce	Důvod zpracování	Opatření
Program <název> , na PC starosty a v dohledovém centru technické pomoci . Jedná se o zobrazení seznamu občanů připojených na obecní wifi	On line pomoc připojeným občanům při technických problémech.	Jméno, příjmení, adresa, IP adresa, identifikace modemu	1. Starosta obce. 2.Pracovník firmy zajišťující technickou pomoc na dohledovém centu	Občané jako první kontaktují starostu obce a konzultují s ním problém. Starosta obce je schopen provést restart modemu a tímto se odstraňuje 90% problémů. Pokud starosta problém vlastními silami nevyřeší , potom občan kontaktuje dohledové centrum.	1. Seznam je dostupný pouze na počítači starosty. 2. Přístup na počítač starosty je zabezpečen jménem a heslem při přihlášení. 3. S dohledovým centrem je smluvním vztahem určen pracovník a pravidla pro provoz (viz systémová příručka). Smlouva obsahuje ujednání o mlčenlivosti. 4. Přístupy do systému jsou logovány. Log je archivován.

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,

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. Luděk Galbavý

Svaz měst a obcí
SMO
ČESKÉ REPUBLIKY