Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Svaz měst a obcí SMO ČESKÉ REPUBLIKY

Připravte se na GDPR doporučenou revizí svého stavu

(v.1.0)

Obsah:

I. Úvod

GDPR je označení pro nařízení Evropského parlamentu a Rady EU č. 2016/679, obecné nařízení o ochraně osobních údajů. Zmíněná zkratka vychází z anglického názvu nařízení – *General Data Protection Regulation*. Protože se jedná o nařízení, představuje na rozdíl od směrnice Evropské unie přímo účinný právní předpis, tj. k jeho účinnosti jej není třeba implementovat českou právní úpravou. Na nařízení právně navazuje národní právní úprava, kterou v České republice představuje zákon č. 101/2000 Sb., o ochraně osobních údajů, v současné době se připravuje novelizace zákona, která bude odpovídat obecnému nařízení o ochraně osobních údajů. V navrhované právní úpravě budou pouze dílčí úpravy, které povoluje obecné nařízení upravit národní legislativou. Nařízení zpřesňuje ochranu osobních údajů a posiluje **právo fyzické osoby** na kontrolu zpracování osobních údajů. GDPR se týká všech osobních údajů. Takové údaje mohou být zachycené v listinné podobě, ale i v elektronické podobě, zejména v různých informačních systémech. Pro obce je rovněž typická jejich role zřizovatele dalších právnických osob, např. školských právnických osob, neziskových organizací, ale i organizací obchodněprávní povahy (např. akciových společností). Je tedy na obci, aby zajistila poučení o povinnostech v oblastech ochrany osobních údajů a implementaci odpovídajících procesů též u těchto subjektů. V této souvislosti je nutné též připomenout článek 8 týkající se souhlasu dítěte a související problematiky (typicky mateřské školy, ZŠ a podobně). Vzhledem k tomu, že u dětí je zvýšená ochrana poskytování osobních údajů a většinou tyto údaje spadají do zvláštní kategorie osobních údajů (citlivé údaje). Je nutné dbát, aby se vedly údaje pouze nezbytné pro výkon dané agendy (např. školský zákon), pokud školský zákon neobsahuje osobní údaje, které např. škola/školka potřebuje ke své činnosti, je nutný souhlas dle obecného nařízení.

II. Základní pojmy

Mezi **obecné osobní údaje** patří jakákoliv informace, která vede přímo či nepřímo k identifikaci.
U podnikajících fyzických osob se řadí mezi **osobní údaje i tzv. organizační údaje**, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

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	Síťový identifikátor

Zvláštní kategorie osobních údajů			
Etnický nebo rasový původ	Zdravotní stav	Náboženské vyznání	Tresty a odsouzení
Sexuální orientace	Politické názory	Členství v odborových organizacích	Osobní údaje dětí
Genetické informace	Biometrické informace	Ekonomická identita	

Nařízení Evropského parlamentu 2016/679 je uveřejněno v plném znění na stránkách UOOU. Stránka UOOU pro GDPR: https://www.uoou.cz/gdpr/ds-3938/p1=3938.

Zpracování osobních údajů:

Jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí nebo bez pomoci automatizovaných postupů spočívající v:

„shromažďování dat, zaznamenávání dat, uspořádání dat, strukturování dat, uložení dat, přizpůsobení nebo pozměnění dat, vyhledávání dat, nahlédnutí na data, použití dat, zpřístupnění dat přenosem, šíření dat nebo jakékoliv zpřístupnění, seřazení nebo zkombinování dat, omezení dat, výmaz nebo zničení dat“.

Zpracování osobních údajů podle obecného nařízení dopadá jak na zpracování osobních údajů ve společnosti správce nebo zpracovatele, tak i na zpracování osobních údajů v cloudu nebo v cloudových službách.

Správce – fyzická nebo právnická osoba, která sama nebo spolu s jinými určuje účel a způsoby zpracování osobních údajů, případně ten, kdo je určen jako správce zákonem. Mezi povinnosti správce patří:

- Zajistit, že zpracování osobních údajů bude odpovídat nařízení a zavést vhodná organizační a technická opatření;
- Musí být schopen doložit svoje opatření;
- Zajistit pouze takové zpracovatele, kteří jsou schopni splnit zpracování dle nařízení.

Společní správci

Tento případ nastává při sdružování se obcí při různých příležitostech (např. výstavba kanalizačních sítí, rozsáhlejších projektů a podobně) bude docházet k situacím, kdy budou osobní údaje zpracovávány na základě pokynů od více správců.

Zpracovatel – fyzická nebo právnická osoba, která zpracovává osobní údaje jménem (tj. pro) správce. Správce a zpracovatel mají smluvní vztah, ve kterém je obsaženo:

- Předmět zpracování;
- Typy osobních údajů a kategorie subjektu údajů;
- Práva a povinnosti správce;
- Účel a dobu trvání zpracování.

Zákonnost zpracování osobních údajů:
Musí být splněna alespoň jedna z podmínek:

- Souhlas nebo smlouva se subjektem;
- Zákonná povinnost;
- Životně důležité zájmy subjektu dat;
- Veřejný zájem nebo oprávněné zájmy správce;
- Zpracování je nezbytné pro plnění smlouvy.

Souhlas subjektu musí být:

- **Svobodný** – odsouhlasení není podmínkou uzavření smlouvy či obchodu, není podepsán pod nátlakem, např. zaměstnavatele;
- **Konkrétní** – obsahuje jasně vymezený(é) účel(y) zpracování a je oddělený od ostatních prohlášení či obchodních podmínek;
- **Informovaný** – jednoduchým jazykem vysvětluje důsledky zpracování, kdo všechno údaje dostane, jak jej lze odvolat;
- **Jednoznačný** – osoba musí projevit svou vůli, nestačí „pokračování v používání webu“ či zaškrtnutí políčka s více účely.

U osoby mladší 16 let, musí být dán souhlas zákonného zástupce, věkovou hranici lze národní legislativou upravit. Naše navrhovaná národní legislativa snižuje věkovou hranici na 13 let.

Zvláštní kategorie osobních údajů lze zpracovávat, pokud:

- Subjekt údajů udělil výslovný souhlas;
- Zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany;
- Zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
- Zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
- Zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
- Zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů;
- Zpracování je nezbytné z důvodu významného veřejného zájmu;
- Zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.;
- Zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků;
- Zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

Pseudonymizace osobních údajů - proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Údaje kódované pomocí klíče jsou klasickým příkladem pseudonymizace. Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně. **Pseudonymizované osobní údaje nejsou anonymizovanými údaji, proto se na ně <u>vztahuje obecné nařízení.</u>**

Práva subjektů osobních údajů:
Před udělením souhlasu fyzické osoby se zpracováním jejím osobním údajům, musí být tato osoba poučena o tom, že má právo po správci, nebo zpracovateli požadovat:

- Záznamy o činnostech zpracování;
- Přístup k osobním údajům;
- Opravu dat;
- Výmaz nebo „právo být zapomenut“;
- Omezení zpracování dat;
- Přenositelnost údajů;
- Vznést námitku.

Vztahuje se na všechny osobní údaje včetně tzv. nestrukturovaných dat uložených například v přílohách emailů nebo na úložištích.

Pověřenec pro ochranu osobních údajů – DPO (*data protection officer*):
Kdo musí **povinně** zřídit funkci DPO:

- Orgány veřejné moci (obce, školy);
- Kdo provádí rozsáhlé systematické monitorování fyzických osob;
- Kdo zpracovává zvláštní kategorii osobních údajů, např. banky, nemocnice.

Úkoly pověřence pro ochranu osobních údajů:

- Spolupráce s dozorovým úřadem;
- Monitorování souladu s GDPR;
- Dohled nad činností ochrany dat;
- Školení pracovníků ve zpracování dat, poradenství;
- Provádění interních auditů.

Nařízení Evropského parlamentu 2016/679 je uveřejněno v plném znění na stránkách UOOU. Stránka UOOU pro GDPR: https://www.uoou.cz/gdpr/ds-3938/p1=3938.

III. Stručný popis postupu při implementaci GDPR

1. Určit pracovníka (lépe více pracovníků), který bude řešit implementaci GDPR do praxe úřadu;
2. Audit dat a stanovení účelu jejich zpracování;
3. Analýza procesů;
4. Analýza rizik;
5. Analýza bezpečnosti informací a zabezpečení osobních údajů;
6. Právní dopady na chod úřadu;
7. Smlouvy:
    - nové smlouvy;
    - již uzavřené smlouvy;
    - úprava smluv se zpracovateli osobních údajů;
8. Dohoda společných správců při zpracování osobních údajů;

9. Předávání dat do 3 zemí;

10. Zajištění procesů k naplnění požadavků GDPR:

- Záznamy o činnostech zpracování;
- Práva subjektu na informace;
- Mazání údajů;
- Právo na výmaz;
- Právo vznést námitku;
- Právo na omezení zpracování os. údajů;
- Právo na opravu;
- Právo na přenositelnost údajů;

11. Vlivy požadavků na provozované IT systémy;

12. Vytvoření plánu naplnění požadavků GDPR;

13. Doplnění a vytvoření pravidel a dokumentace včetně jejich další vedení;

14. Popis a definice postupu při narušení zabezpečení os. údajů;

15. Jmenování a spolupráce s pověřencem pro ochranu os. údajů;

16. Pravidelná revize, monitorování včetně vzdělávání a školení obsluhy.

IV. Implementace GDPR vlastními silami

Zaměřte se na činnosti, které provádíte a na dokumenty, se kterými je v rámci těchto činností nakládáno. Dále si vytvořte, nebo pokud existují, projděte a doplňte základní dokumenty úřadu – organizační řád, řád nebo směrnice pro provoz výpočetní techniky a spisový řád. Dále se zaměřte na dokumentaci k provozovaným softwarovým produktům. Tímto postupem byste měli dojít k vytvoření přehledu, který bude základem pro vaši další spolupráci s pověřencem pro ochranu OÚ a měli byste získat přehled o zpracování osobních údajů.

1. Určit pracovníka (lépe více pracovníků),

který bude řešit implementaci GDPR do praxe úřadu. Výsledkem činnosti této skupiny by mělo být zvládnout vlastními silami. Před revizí osobních údajů doporučujeme připravit si:

- Audit dat – seznam agend, které obec vykonává a kde jsou používány osobní údaje fyzických osob;
- Analýzu procesů;
- Vytvoření nebo pouze doplnění předpisů a nařízení, např. Organizační řád, řád pro provoz výpočetní techniky, spisový řád, směrnice o ochraně osobních údajů, včetně zajištění přístupu k osobním údajům;
- Jednání správce a stanovení jeho požadavků vůči dodavateli informačních systémů, které pracují s osobními údaji. Správce a zpracovatel se dohodnout na stanovení minimálních požadavků na bezpečnost práce na PC a všech síťových připojení (vnitřní, externí);
- Revize všech smluv, např. dodavatelské, odběratelské, pracovní;

- Plán práce k zajištění povinností plynoucí z obecného nařízení;
- Ustanovení pověřence pro ochranu osobních údajů (včetně smluvního vztahu);
- Předpokládaný odhad finanční náročnosti implementace GDPR v souvislosti s rozpočtem obce.

2. Co si připravit?

Pro přípravu revize osobních údajů, stanovení účelu jejího zpracování, analýzu procesů a analýzu rizik je potřebné si připravit následující informace a podklady:

- Dokumenty v listinné i elektronické formě, které obsahují osobní údaje fyzických osob, včetně pracovníků, kteří s nimi pracují;
- Souhlasy se zpracováním osobních údajů, např. rozesílání sms informací, dotazníky, seznamy kulturních a sportovních akcí;
- Smlouvy, včetně pracovních smluv, smluv s dodavateli SW, externími správci informačních systémů, provoz EZS (elektronické zabezpečovací zařízení) a s bezpečnostní službou, provoz kamerového systému (nezapomeňte na pracovní smlouvy, smlouvy s dodavateli SW, externími správci informačních systémů, provoz EZS a s bezpečností službou, provoz kamerového systému);
- Faktury a licenční smlouvy vážící se k licencím provozovaných SW produktů;
- Pokud existuje případ předávání os. údajů do 3 zemí (pracovníci, kteří předávání realizují);
- Vnitřní předpisy, směrnice a nařízení, např. řád spisové služby, organizační řád, směrnice pro provoz výpočetní techniky.

Pokud již existuje nějaké technicko-organizační opatření ve formě vnitřního předpisu k zajištění ochrany osobních údajů, je nutné jej revidovat a případně doplnit. Např. obecní úřad mohl v minulosti za určitým účelem vydat nějaká technicko-organizační opatření, která mohou nebo nemusí obsahovat osobní údaje, např. pro komunikaci s bezpečnostní službou, odchodu z kanceláře, vytváření a úschovy kopií dat:

- seznam SW (software) produktů provozovaných obecním úřadem, kde se zpracovávají nebo evidují osobní údaje, např. na jakém PC, notebooku, tabletu SW instalován a kdo jej používá a kdo je také dodavatelem SW;
- dokumentaci – uživatelskou a systémovou příručku pro provozovaný informační systém a další SW prostředky;
- zjistit, zda jsou nějaká data obsahující osobní údaje uložena v cloudu a jestli ano, tak, o která data se jedná a kdo je provozovatelem tohoto úložiště;
- Připravit se seznam osob, které mají přístup k osobním údajům ze základních registrů, a osoby, které mají přístup k osobním údajům ze ZR obyvatel a osoby, které mají přístup k CzechPOINTu, např. formou tabulky, viz vzor níže:

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

- 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			

Doporučení pro vzory vnitřních směrnic:

- **Organizační řád**
  - *vzor na stránkách SMO:* http://www.vzdelanyzastupitel.cz/docTemplates/Default.aspx?dirID=8;
- **Provozní řád inf. systému**
  - *příloha Vzor Provozní řád informačního systému*;

Pro členy SMO a CSS viz webové stránky Svazu měst a obcí ČR:

- **Spisový řád** (měl by obsahovat i seznam razítek)
  - *vzor na stránkách MVČR:* http://www.mvcr.cz/clanek/vzory.aspx.

3. Audit dat a stanovení účelu jejich zpracování

Výsledkem této činnosti je zjištění všech důležitých parametrů, které souvisejí se zpracováním osobních údajů na úřadě, ale i zpracováním osobních údajů jinými externími subjekty. Výsledky analýzy zaznamenejte do vzoru Agendového listu osobních údajů.

Součástí tohoto doporučení je prázdná šablona Agendovy_list_sablona.docx a předvyplněný seznam agendových listu Agendove_listy_vyplnene.docx

4. Analýza procesů

Analýza procesů je analýza zaměřená na postup práce od jednoho člověka k druhému, přičemž popisuje vstupy, výstupy, jednotlivé kroky a případně také spotřebu zdrojů. Zjednodušeně řečeno, je analýza procesů o tom, "jak se co dělá" či "jak co probíhá". Může se jednat o analýzu jednoho konkrétního procesu nebo komplexní analýzu všech procesů organizace.

Analýza procesů pomáhá jednotlivé procesy identifikovat, popsat a dát do vzájemných souvislostí. Může poskytnout jak detailní, tak přehledový obrázek o procesech na úřadě a pomůže zjistit nedostatky či problémy při zpracování osobních údajů.
Popis procesu se bude realizovat pomocí karty procesu. Karta procesu je šablona, která obsahuje textový popis zdrojů, vstupu, vlastního popisu, výstupu a řídící dokumentace procesu.
Popisovat se budou procesy pro potřeby naplnění nařízení 679/2016 , které se týkají pouze zpracování osobních údajů.

Revize stávajících souhlasů se zpracováním osobních údajů.
V případech, kdy úřad souhlas se zpracováním získal v minulosti, je nezbytné prověřit, zda splňuje podmínky obecného nařízení.

5. Analýza rizik (informační systém)

Před zahájením analýzy rizik je stanoven a zdokumentován účel a rozsah analýzy, které určují její podrobnost. Co nejpřesněji jsou také formulovány předpoklady a omezující podmínky, např. architektura informačního systému, prostředí apod.
Také je provedena identifikace požadavků na ochranu informací a bezpečnostní opatření, které mohou vyplynout ze zákonných požadavků, interních předpisů a charakteru informačního systému.
Realizaci analýzy rizik je vhodné si ponechat zpracovat včetně popsání závěrů a doporučení.

V. Co požadovat od dodavatelů programů a IS a doplnění vnitřních předpisů:

1. Písemně se dotázat dodavatele IS a programů, zda jeho systémy budou včas na nařízení připraveny a zda je připraven spolupracovat s pověřencem pro ochranu osobních údajů. Toto prohlášení doporučujeme v písemné formě, dodavatel může mít toto prohlášení zveřejněné i na svých www stránkách. Je vhodné si s dodavateli vyjednat tyto body:
    - Závazek spolupracovat s pověřencem pro ochranu osobních údajů;
    - Splnění dostupnosti údajů a informací o zpracování pro subjekt;
    - Bude realizováno právo subjektu na opravu a výmaz osobních údajů;
    - Bude realizováno právo na omezení zpracování;
    - Doporučujeme umožnit poskytnutí kopie zpracovávaných osobních údajů subjektu těchto údajů;
    - Realizace práva na přenositelnost údajů (subjekt má právo získat osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu);

- Podpora logování v čitelné formě a s takovým rozsahem, že bude možné jednoznačně prokázat denní činnosti informačního systému (nebo programu) s vazbou na uživatele a jeho činnost.

2. Provedení revizi smluv se zpracovateli. Tato smlouva by měla obsahovat článek o tom:

- Zajištění mlčenlivosti u osob oprávněných zpracovávat os. údaje;
- Zajistit splnění podmínky pro zapojení dalšího zpracovatele dle obecného nařízení pro ochranu osobních údajů;
- Jakým způsobem budou zajištěna práva subjektu (informace o vedených údajích, výdej kopií dat, výmaz;
- Součinnost s pověřencem pro ochranu osobních údajů, např. Kontrola, sledování, výpisy, dohledání incidentu a problému;
- Ujednání o náhradě škody včetně regresních nároků zpracovatele (možnost sjednání pojištění odpovědnosti zpracovatele za škodu);
- Zajistit podmínky ukončení smlouvy a co bude nutné při ukončení s dodavatelem zajistit nebo odstranit např. (odstranit kopie, zničit nebo předat osobní údaje.

3. Ověřit a doplnit do příslušných dokumentací a nařízení, jak budou provedena opatření na zabezpečení dat dle čl. 32 obecného nařízení a zajistit, aby níže uvedené body byly součástí systémové příručky

- Pseudonymizace a šifrování osobních údajů – zajistit aby popis byl součástí systémové příručky;
- Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- Zajistit aby popis byl součástí systémové příručky a provozního řádu inf. systému.

4. Zajistit, aby bylo uvedeno v provozním řádu:

- Schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- Proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování – zajistit, aby popis provedených testů dodavatel byl součástí systémové příručky a aby kontrola a realizace procesu součástí provozního testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření byla uvedena v provozním řádu inf. systému.

Obecní úřad je povinen zřídit funkci pověřence pro ochranu osobních údajů. Popis problematiky a možných postupů je uvedeno v dokumentu **Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí,** které je uveřejněno na stránkách MVČR: http://www.mvcr.cz/odk2/.

Zdroje:

- UOOÚ (webové stránky)
- MVČR (webové stránky)
- Management Mania (webové stránky)
- Krajský úřad Karlovarského kraje – karta procesu
  Catania Group s.r.o (webové stránky)
- Microsoft (webové stránky, Metodika analýzy rizik)
- GDPR praktický průvodce implementací (Luděk Nezmar)