Připravte se na GDPR doporučenou revizí svého stavu. (v.1.0)
Obsah:

**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 os. Údajů)
V. Co požadovat od dodavatelů softwarových produktů
VI. Pověřenec pro ochranu osobních údajů (DPO)**

# Úvod

V úvodu budou pouze vyjmenovány základní body, které říkají co je GDPR.
GDPR je označení pro nařízení Evropského parlamentu a Rady 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. Před nařízením byla účinná národní právní úprava, kterou v České republice představuje zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Protože byl tento zákon přijat dříve než nařízení, může dojít k situaci, kdy bude tento zákon v rozporu s nařízením, v takovém případě má nařízení aplikační přednost. Předpokládá se budoucí novelizace nebo nahrazení zmíněného zákona, tak, aby byla česká právní úprava v souladu s nařízením GDPR a aby jej neduplikovala. 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. Co vše jsou osobní údaje dle GDPR znázorňuje tabulka níže.

|  |
| --- |
| **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 (osobní údaje povahou zvláště citlivé)** |
| 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](https://www.uoou.cz/gdpr/ds-3938/p1%3D3938)

# II. Stručný popis postupu při implementaci GDPR

 1. Revize spojená s analýzou existujícího prostředí:
- Seznam procesů, kde jsou používány osobní údaje a určení důvodů pro zpracování osobních údajů
- Jak zpracování osobních údajů probíhá a kde se údaje ukládají (papírová forma, kartotéka, archiv, šanon a skříň, počítač a sw. produkt, databáze, lokální nebo síťová úložiště, používání cloudové služby, emaily, mobilní zařízení …)

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

3. Na základě analýzy a z ní vzešlých doporučení je nutné vytvořit si plán postupu nasazení a následně na základě tohoto plánu realizovat doporučení v praxi.

###  4. Pravidelná revize včetně vzdělávání a školení obsluhy

III. Jak na revizi 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 vaší další spolupráci s pověřencem pro ochranu OÚ a měli byste získat přehled o zpracování osobních údajů.

1. Je na ÚOOÚ nahlášena nějaká evidence osobních nebo citlivých údajů dle zákona 101/2000 Sb., ve znění pozdějších předpisů?
Jestliže máte takovou evidenci obsahující citlivé nebo osobní údaje a tato evidence byla nahlášena na ÚOOÚ a nadále tuto evidenci budete používat v nezměněné formě a rozsahu, potom ověřte, zda opatření, která budete pro ochranu osobních údajů používat jsou dostačující. Nebudete-li si jisti, že ochrana je dostatečná nebo pokud dojde k úpravě nebo rozšíření seznamu, potom by mohlo jít o rizikové zpracování osobních údajů a vy si nechte seznam znovu posoudit (tj. jeho oprávněnost používání a vámi navrhovaná opatření pro ochranu osobních údajů v seznamu obsažených (viz bod 5).

2. Již existuje nějaké technicko-organizační opatření ve formě vnitřního předpisu k zajištění ochrany osobních údajů? Jestliže takový předpis existuje, rozhodnout, zda jej budete používat i nadále a zda bude nutné provést jeho doplnění nebo úpravy dle vámi nově zjištěných skutečností.

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…). V každém případě zajistěte, aby tato opatření byla v souladu s postupy popsanými v organizačním řádu a provozním řádu informačního systému nebo zajistěte, aby tato opatření do těchto řádů byla doplněna.

 3. Určit a zjistit si elektronické zdroje, kde se nacházejí osobní údaje (používané informační systémy a programy).
Projít si, které sw. produkty používáte, kdo je jejich dodavatelem (zpracovatelem) a o jaké osobní údaje se zde jedná.

4. Zjistit si veškeré „papírové“ zdroje, kde se nacházejí osobní údaje (tj. projít veškeré evidence (šanony), kde se nacházejí nějaké dokumenty).

5. Připravit si smlouvy včetně všech pracovních smluv k revizi.
Pro pracovní smlouvy platí, že zpracování naprosté většiny osobních údajů není nutný souhlas zaměstnance. Přesto je doporučeno tento souhlas vyjádřit buď v pracovní smlouvě nebo nějakou formou dodatku k pracovní smlouvě. Pokud mzdy zpracovává jiná organizace (smluvní vztah úřadu) měl by zaměstnanec souhlas vyjádřit vždy, protože jeho osobní údaje nezpracovává zaměstnavatel.

6. Zjistit a vytvořit si seznam nařízení a pravidel úřadu, která jsou používána a jsou platná.

Mělo by se minimálně jednat o:
- **Organizační řád***příloha Vzor na organizační řád (stránky SMO ČR, odpovědný zastupitel)*

**- Provozní řád informačního systému**

*příloha Vzor Provozní řád informačního systému*- **Spisový řád** (měl by obsahovat i seznam razítek)
*příloha Vzor spisového a skartačního řádu (ze stránek MV)*

- **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 Czech POINTu (CzP) např. formou tabulky – viz vzor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Základní registry/CP** | **Zpracovatel (pracovní místo)**  | **Příjemce** | **Opatření pro bezpečné zpracování** |
| *Přístup k registru – názevPřístup 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 (formou tabulky)

|  |  |  |  |
| --- | --- | --- | --- |
|  **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* |  |  |  |

- **Pravidla pro přijímání petic a vyřizování stížností**

7. Pro elektronické zdroje (= informační systémy a programy) ověřit:
- existenci dokumentace k IS a programům, které obecní úřad používá. Mělo by se jednat o **uživatelskou a systémovou příručku**.
Ověřit si, že systémová příručka obsahuje:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz). Jedná se o popis jak provozních, tak i nutných organizačních podmínek.
2. Licenční podmínky.
3. Popis podpory uživatele (hot-line, postupy při pomoci).
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních.
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal.
7. Pokud úřad používá cloudové služby, potom by měl mít seznam aplikací, kde jsou osobní údaje a mít smluvní dokumenty s poskytovatelem cloudových služeb.

Dle novely zákona č. 181/2014 Sb., ve znění pozdějších předpisů o kybernetické bezpečnosti mají orgány veřejné moci také povinnost si ve smlouvách s poskytovateli digitálních služeb cloud computingu zajistit, že budou dodržována bezpečnostní pravidla stanovená Úřadem (Národní úřad pro kybernetickou bezpečnost. Tento zákon stanovuje nezbytné náležitosti, které musí takové smlouvy obsahovat a obecná pravidla, která by měla být řešena v rámci bezpečnostních opatření zakotvených ve smlouvách s poskytovateli digitálních služeb cloud computingu. Obecně zákon zpřísnil požadavky na zabezpečení a výběr dodavatelů informačních systémů a požadavky na smluvní dokumentaci vážící se k vybraným systémům a službám.

Všechny smluvní vztahy, které nesplňují požadavky dle zákona o kybernetické bezpečnosti, musí být uvedeny do souladu s novými požadavky zákona do 1. srpna 2018, což může pro mnohé, zejména tedy orgány veřejné moci, znamenat **úpravu uzavřených smluv anebo uzavření smluv nových**.

Dále upozorňujeme na nutnost dodržení povinností při předávání osobních údajů do zemí mimo EHP (Evropský hospodářský prostor) nebo do třetích zemí, které nemají srovnatelnou úroveň záruk a také mezinárodním organizacím. Výše uvedené body s informacemi uvedenými v systémové příručce jsou důležité pro pověřence pro ochranu osobních údajů a jeho činnost. Zvláštní pozornost a důraz by měl být na dostupné a čitelné logy.

# IV. Vytvořit si přehledy a seznamy:

1. vytvořit si seznam zdrojů s výskytem osobních údajů.
Seznam by měl sloužit k přehledu, kde jsou a jak jsou používány osobní údaje na obecním úřadu.
 Dále by měl obsahovat zdroje, které mohou být rizikovým zpracováním osobních údajů. Pokud na základě kritérií jako je způsob a operace zpracování, povaha údajů (zvláštní kategorie osobních údajů), možnosti zabezpečení, je potřebné takové zpracování konzultovat dotazem na ÚOOÚ.

Seznam by měl obsahovat:
- název zdroje (doklad, evidence, …),
- účel zpracování,
- osobní údaje vyskytující se ve zdroji,
- zákonnou normu, která opravňuje k evidenci a zpracování,
- příjemce osobních údajů (pokud by se předpokládalo předávat údaje do třetích zemí, je nutné tuto skutečnost uvést).
*(vzor viz Seznam evidencí a dokumentů)*

Pokud se v seznamu vyskytují činnosti a evidence osobních údajů, které bude nutné používat, potom doplnit i popis přijatých opatření pro zajištění bezpečnosti zpracování.

2. Z elektronických i „papírových“ zdrojů vytipovat ty, které obsahují osobní údaje a jsou zákonnou normou nebo výkonem veřejné moci neobhájitelné (=neexistuje) nebo problematicky obhajitelné.
Takové zdroje by mohly být právě rizikovým zpracováním osobních údajů. U těchto zdrojů zpracovat (popsat) a vytvořit seznam jako podklad pro dotaz na ÚOOÚ, případně vytvořit oznámení k posouzení legality a legitimity budoucího zpracování:

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

## Co udělat jako první věc!

**Vytvořte si seznam(-y):**Seznam ve tvaru s těmito sloupky:
**Evidence dokumentů a seznamů obsahující osobní údaje.** (Vzorový dokument je v další příloze.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dokument/****seznam** | **Účel zpracování a zpracovatel** | **Údaje**  | **Příjemce** | **Zákon**  | **Komentář** | **Rizikový?** |
| *Specifikace dokladu nebo seznamu názvem.* | *Při jaké činnosti v jaké agendě se používá.**Zpracovatel /Název pracovního místa, kde dokument nebo 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.*  |

Pokud je ve sloupci Rizikový uvedeno ano, potom bude vytvořen další dokument, který bude zaslán na UOOU jako dotaz na legální zpracování a na dostatečný rozsah bezpečnostních opatření při zpracování osobních údajů. (viz dokument *Seznam případů pro ÚOOÚ.docx*)

 *(vzor viz Seznam evidencí a dokumentů)*

# 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 že je připraven spolupracovat s pověřencem pro ochranu osobních údajů. Takové prohlášení je vhodné mít písemně nebo dodavatel může mít toto prohlášení zveřejněné i na svých www stránkách.
Dodavatelé by měli určitě zabezpečit:
- závazek spolupracovat s pověřencem pro ochranu osobních údajů
- že bude splněna dostupnost údajů a informací o zpracování pro subjekt údajů
- bude realizováno právo subjektu na opravu a výmaz údajů
- bude realizováno právo na omezení zpracování
- bude možnost subjektu poskytnout kopii zpracovávaných osobních údajů
- bude realizováno právo 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. Provést revizi smluv se zpracovateli. Tato smlouva by měla obsahovat článek o tom:
- 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 (informace o vedených údajích, výdej kopií dat, výmaz),
- podpora pověřence pro ochranu osobních údajů (kontrola, sledování, výpisy, dohledání incidentu a problému, ...),
- ujednání o náhradě škody včetně regresních nároků (vhodné je doplnit i ujednání o pojištění odpovědnosti zpracovatele za škodu)
- o ukončení smlouvy a co bude nutné při ukončení zajistit (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.
 a) pseudonymizace a šifrování osobních údajů – zajistit aby popis byl součástí systémové příručky
 b) schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zajistit aby popis byl součástí systémové příručky a provozního řádu informačního systému
 c) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů – zajistit aby popis byl součástí systémové příručky a provozního řádu informačního systému
d) proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování – zajistit aby popis provedených testů byl součástí systémové příručky a aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření a byla uvedena v provozním řádu informačního systému

# VI. Pověřenec pro ochranu osobních údajů (DPO):

Orgány veřejné moci, mezi které náleží i obce jsou povinny zajistit si 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,** je uveřejněno na stránkách MVČR a tvoří také přílohu tohoto doporučení.
<http://www.mvcr.cz/odk2/>