Průvodce pro přípravu obcí na požadavky GDPR

Zpracovatel: Akademie GDPR – Svaz průmyslu a dopravy ČR
Zadavatel: Ministerstvo vnitra

Úvod do tématu

1 Co znamená GDPR?

GDPR – v plném anglickém znění General Data Protection Regulation neboli obecné nařízení o ochraně osobních údajů (dále jen „obecné nařízení“). Celý název předpisu je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, je nový právní předpis EU, kterým je zaváděna evropská reforma ochrany osobních údajů. V celé EU nabude GDPR účinnosti dnem 25. května 2018, je přímo závazné a má přednost před vnitrostátními zákony.

- ✓ **Jaký je cíl GDPR:** cílem je posílení práv subjektů osobních údajů jako fyzických osob-nositelů osobních dat v celé EU i při pohybu jejich osobních dat mimo Unii.
- ✓ **Prostředky využívané k dosažení cíle:** posílení práv subjektů údajů, aktualizace stávajících nebo zavádění nových povinností správců a zpracovatelů při zpracování osobních údajů.
- ✓ **Pro koho nařízení platí:** povinnosti vyplývající z obecného nařízení dopadají na všechny organizace, které kdekoli ve světě zpracovávají osobní údaje osob nacházejících se v EU. Nejde tedy pouze o organizace místně působící v EU, ale také o ty, které sídlí mimo EU, ale zpracovávají osobní údaje rezidentů EU.
- ✓ **Co budou nové požadavky znamenat pro obce a města:** pokud dodržují zákon o ochraně osobních údajů, nebude nových povinností mnoho. V souladu se systémovou analýzou, kterou zpracovalo Ministerstvo vnitra, lze doporučit zejména revizi toho, jaké údaje a pro jaké účely jsou zpracovávány, a dále nastavit pravidla pro zpracování a zabezpečení osobních údajů vzhledem k rizikovosti zpracování.

2 Vymezení základní rolí používaných v obecném nařízení

V této kapitole naleznete vysvětlení pojmů, které jsou v obecném nařízení používány pro možné role a postavení obcí a občanů při zpracování osobních údajů.

- ✓ Subjekt osobních údajů: je jakákoli identifikovaná nebo identifikovatelná fyzická osoba – tzv. nositel osobních údajů.

> ***Příklad:***
> *Subjektem údajů je Váš zaměstnanec, občan obce, případně fyzické osoby spolupracující s obcemi v rámci obchodních vztahů, tedy každý, jehož osobní údaje jsou zpracovávány. Vymezení pojmu zpracování osobních údajů naleznete v následující kapitole.*

- ✓ **Správce osobních údajů:** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který určuje účely a prostředky zpracování osobních údajů subjektů údajů, a to samostatně nebo v součinnosti s jiným správcem.

Příklad:
Správcem údajů je město nebo obec ve vztahu ke svým zaměstnancům či občanům a partnerům. Stává se jím v okamžiku převzetí údajů a s ním spojeným počátkem jejich zpracování.

- ✓ **Společný správce osobních údajů:** v případě, že účely a prostředky zpracování stanoví společně dva nebo více správců, stávají se společnými správci. Ti si mezi sebou transparentním ujednáním rozdělí odpovědnosti vyplývající z obecného nařízení (Kdo a jak bude vyřizovat požadavky subjektů na aplikaci jejich práv? Kdo bude plnit povinnost na transparentní poskytování informací? atd.) V případě podstatných prvků takového ujednání je o nich subjekt údajů informován. Subjekt má v případě společného správcovství možnost uplatňovat svá práva u kteréhokoliv ze společných správců.

Příklad:
Jsou-li osobní údaje spravovány více subjekty, například městským úřadem a určeným správcem městského bytového a nebytového fondu, může jít o tzv. společné správce, jejichž vztah je nutné smluvně upravit. Takové ujednání pokud každá z organizací samostatně určuje účel zpracování musí obsahovat definici jim společného účelu zpracování osobních údajů a jasné stanovení zodpovědností při jejich správě i plnění povinností vyplývajících z uplatnění práv subjektů podle obecného nařízení.

- ✓ **Zpracovatelem osobních údajů:** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatel samostatně neurčuje účel zpracování údajů a osobní údaje zpracovává pouze za účely, které mu vymezí příslušný správce.

Příklad:
Zpracovatelem údajů může být externí společnost, která pro obec zajišťuje svoz odpadu a udržuje evidenci odpadových nádob u rezidentů. Dalším příkladem je poskytování benefitů vlastním zaměstnancům, které zajišťuje externí firma. Jiným může být například správce základních registrů, který je však ve vztahu k obci jako správci osobních pouze jejich zpracovatelem. Ve všech těchto případech je obec správcem osobních údajů a zadává zpracování za konkrétními účely externí organizaci, která se tak stává zpracovatelem.

- ✓ **Příjemcem osobních údajů:** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje poskytnuty, ale dále je však nezpracovává ani neurčuje způsob jejich zpracování. Pokud příjemce údaje dále o své vůli zpracovává, stává se dalším správcem, ale to je z pohledu původního správce irelevantní. Příjemcem však není orgán veřejné moci, který údaje může získávat v rámci své činnosti.

Příklad:
Příjemcem údajů může být externí organizace poskytující obci IT služby v případě, kdy je tato organizace pověřena pouze k výkonu technické servisní služby nad systémy obce, ale není aktivně pověřena žádným zpracování osobních údajů. V kontextu výkonu této technické služby se však organizace může dostat k osobním údajům v průběhu výkonu servisu a stává je tak příjemcem osobních údajů.

- ✓ **Dozorový úřad v kontextu obecného nařízení:** dozorový úřad musí být nezávislým orgánem veřejné moci zřízeným daným členským státem EU; v případě ČR dozorovým úřadem Úřad pro ochranu osobních údajů. Dozorový úřad provádí konzultační a kontrolní činnost a zároveň slouží jako příjemce důvodných stížností na postup správců a zpracovatelů.

- ✓ **Evropský sbor pro ochranu osobních údajů**: každý a právě jeden dozorový úřad v každé z členských zemí EU bude mít po účinnosti obecného nařízení jednoho svého zástupce v Evropském sboru pro ochranu osobních údajů. Tento sbor bude monitorovat plnění požadavků GDPR v rámci celé EU, bude poradním orgánem Evropské komise a bude provádět výkladovou činnost. Zároveň bude jeho úkolem průběžně slaďovat postupy dozorových úřadů členských států, a to včetně případného přehodnocení výše udělené sankce.

3 Základní pojmy v obecném nařízení

Základní definice zůstávají shodné se současným zákonem o ochraně osobních údajů. GDPR tak nezavádí revolučně novou definici pojmů z oblasti ochrany osobních údajů oproti stávajícím platným přepisům. Jde především o jejich aktualizaci a doplnění. V této kapitole jsou důležité pojmy vyjmenovány a blíže vysvětleny.

- ✓ **Osobní údaj:** za osobní údaj jsou podle obecného nařízení považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat.
- ✓ **Zvláštní kategorie osobních údajů:** do této kategorie spadají osobní údaje, které jsou vysoce citlivé a jejich zneužití s sebou nese významné riziko pro základní práva a svobody subjektů údajů – například údaje o rasovém či etnickém původu, genetické a biometrické údaje, údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci, politické názory, náboženské vyznání, filosofické přesvědčení, ale i členství v odborech.
- ✓ **Zpracováním osobních údajů:** je jakákoliv automatizovaná nebo manuální operace, popřípadě soubor operací systematicky prováděných s osobními údaji nebo soubory osobních údajů. Mezi typy zpracování osobních údajů můžeme uvést jejich uložení, přepsání, přenos, obnovení, zveřejnění a další.

  Příklad:
  Jako příklad zpracování osobních je možné uvést vedení archivu, elektronické evidence, změnu osobních údajů občana na základě jeho změny trvalého bydliště, skartace osobní složky bývalého zaměstnance a další.
- ✓ **Evidence osobních údajů:** je strukturovaný soubor osobních údajů, který je přístupný na základě specifických kritérií. Jako příklady těchto typů přístupů můžeme uvést přístup centralizovaný, decentralizovaný nebo rozdělený podle zeměpisné polohy či funkce.
- ✓ **Zpracování osobních údajů, na které se obecné nařízení vztahuje:** nařízení se vztahuje na plně nebo částečně automatizované zpracování osobních údajů a také na plně manuální zpracování osobních údajů, které jsou součástí evidence nebo mají být do evidence zařazeny.
- ✓ **Zpracování osobních údajů, na které se obecné nařízení nevztahuje:** nařízení se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní účely a soukromé využití v domácnosti. Nevztahuje se také na orgány činné v trestním řízení (jejich činnost je upravena zvláštními právními přepisy) a na zpracování v rámci obrany a zajištění bezpečnosti ČR.
- ✓ **Třetí země:** je stát mimo Evropskou unii. Tento pojem je zásadní převážně pro přenos osobních údajů rezidentů EU do těchto třetích zemí. Předávání do třetích zemí je blíže vysvětleno dále v příručce.

Základní práva a povinnosti v oblasti ochrany osobních údajů

1 Zásady zpracování osobních údajů podle obecného nařízení

Obecné nařízení stojí na několika základních zásadách, které se aplikují jako obecné principy používané pro každé zpracování osobních údajů. Mezi tyto zásady řadíme:

- ✓ **Zákonnost zpracování**: osobní údaje musí být zpracovávány výlučně zákonným způsobem a ze zákonných důvodů. Zpracování je zákonné v případě, že je naplněn minimálně jeden legitimní právní titul uvedený v obecném nařízení (souhlas subjektu údajů, plnění jiné právní povinnosti, ochrana životně důležitých zájmů subjektu údajů, výkon veřejné moci nebo plnění úkolu ve ve veřejném zájmu, oprávněný zájem správce). V prostředí obcí bude nejčastějším právním titulem pro zákonnost zpracování osobních údajů velmi pravděpodobně plnění právní povinnosti a nebo výkon veřejné moci (v případě agend obce v přenesené působnosti) a nebo provádění úkolu ve veřejném zájmu (v případě agend obce v samostatné působnosti).
- ✓ **Korektnost a transparentnost zpracování:** veškeré informace o zpracování osobních údajů musí být jednoduše, transparentně a bez poplatků přístupné subjektům údajů. Tyto informace musí být předávány za použití srozumitelných jazykových prostředků a to ideálně v písemné podobě. V případech, kdy je to možné by k předání informací mělo docházet v elektronické podobě. V případě žádosti subjektu lze informace předat také ústně, ale správce by měl mít vždy na paměti případné plnění povinnosti doložit předání takových informací (vyhodnotit si, kdy je ústní předání vhodné a kdy nikoliv).
- ✓ **Zásada standardní ochrany osobních údajů:** tato zásada v sobě obsahuje kvantitativní, časové a účelové omezení zpracování osobních údajů, viz následující body.
  - **Účelové omezení zpracování osobních údajů**: osobní údaje mohou být zpracovávány pouze za předem stanovenými účely, za kterými byly nasbírány a pouze způsoby a prostředky, které jsou s těmito účely slučitelné.
  - **Časové omezení zpracování osobních údajů**: zásada určující, že osobní údaje mohou být zpracovávány pouze po dobu nezbytně nutnou pro dané zpracování.

  Příklad: V případě plnění právních povinností, které na agendu obce dopadají, je maximální doba zpracování určena v odpovídajícím právním přepisu a je shodná s požadovanou archivační lhůtou. Po uplynutí této lhůty by mělo být veškeré zpracování osobních údajů pro tento účel ukončeno.
- ✓ **Omezení rozsahu zpracovávaných osobních údajů:** zásada určující, že osobní údaje mohou být zpracovávány pouze v nezbytně nutném rozsahu pro daný účel zpracování.

Příklad: Osobní složka bývalého zaměstnance uložená v personálním archivu musí obsahovat pouze osobní údaje potřebné pro splnění právních povinností, případných závazků vůči zaměstnanci nebo údaje drženého na základě jiného právního titulu jakým je například souhlas pracovníka o zpracování jeho osobních údajů. Jakékoliv údaje, které tuto podmínku nesplní, nemohou být dále zpracovávány.

- ✓ **Zásada přesnosti osobních údajů**: v praxi znamená, že zpracovávány by měly být pouze přesné osobní údaje, které budou v případě potřeby aktualizovány a správce přijme veškerá opatření k opravě či výmazu údajů nepřesných.
- ✓ **Odpovědnost správce**: zahrnuje povinnost správce dodržet všechny povinnosti vyplývající ze zásad obecného nařízení a současně i povinnost správce prokázat dodržení shody všech svých postupů a procesů zpracování údajů s těmito zásadami.

2 Práva subjektů údajů

Práva subjektů údajů můžeme rozdělit na dvě základní skupiny. První z nich jsou práva, která jsou aplikována automaticky a není potřeba jejich vyžádání ze strany subjektu údajů (tato práva přímo odpovídají některým povinnostem správců osobních údajů). Druhou skupinou jsou práva, která se uplatní pouze na žádost subjektu údajů. Dále jsou do těchto skupin rozdělena a následně vysvětlena příslušná práva subjektů údajů:

2.1 Automaticky se uplatňující práva

- ✓ **Právo na informace o zpracování osobních údajů:** každý subjekt údajů, jehož osobní údaje přebírá správce ke zpracování přímo od subjektu údajů nebo nepřímo od jiného správce má právo být automaticky informován o veškerých podstatných náležitostech tohoto získání a zpracování. Obsahem tohoto předání informací musí být minimálně kontaktní údaje správce a jeho případného pověřence pro ochranu osobních údajů, rozsah získaných údajů, účel zpracování a legitimní titul zpracování včetně doby, do kdy je platný. Není nutné informovat o tom, co subjekt údajů ví. Pokud vyplňuje např. formulář, není nutné jej informovat o údajích, které právě vyplnil, ale jen o účelech zpracování, totožnosti správce a dalších náležitostech.
- ✓ **Právo nebýt předmětem automatizovaného rozhodnutí založeného na profilování:** toto právo znamená, že subjekt údajů nesmí být součástí rozhodování výhradně pomocí automatických prostředků, mj. např. na základě profilování subjektu údajů, pokud to pro subjekt údajů má právní účinky nebo se ho to dotýká obdobně významným způsobem – tedy podle automatizovaného vyhodnocování osobních údajů například na základě pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se subjekt údajů nachází, nebo jeho pohybu.

Výjimku z tohoto zákazu tvoří situace, kdy je takové rozhodnutí nutné ke splnění smlouvy mezi správcem a subjektem údajů, když k němu subjekt údajů dal souhlas nebo je přímo povoleno jiným právním předpisem.

- ✓ **Právo na výmaz („právo být zapomenut“):** by se mělo uplatnit automaticky tam, kde pro daný osobní údaj pominul účel zpracování, nebo pro další kompatibilní účel, nebo pokud například subjekt údajů odvolá svůj souhlas se zpracováním. Pokud by snad správce v takové situaci k výmazu nepřistoupil automaticky, má subjekt údajů možnost si realizaci tohoto práva vyžádat. Právo na výmaz však není možné realizovat tam, kde jsou údaje dále uchovávány či zpracovávány z důvodu plnění právní povinnosti, ochrany veřejného zdraví, archivace nebo například pro výkon, určení či obhajobu právních nároků

- ✓ **Právo obrátit se na pověřence na ochranu osobních údajů (DPO):** v případě, že zpracování osobních údajů probíhá v organizaci, která má povinnost jmenovat pověřence na ochranu osobních údajů, má subjekt údajů právo se na tohoto pověřence obrátit s dotazy či s žádostmi o vysvětlení nejasností. Kontakty na pověřence musí být zveřejněné a pro subjekty údajů snadno dosažitelné.
- ✓ **Právo na poskytnutí svobodného souhlasu se zpracováním osobních údajů a jeho odvolání:** v případech, kdy je zpracování osobních údajů založeno na souhlasu subjektu údajů, musí být správce schopný tento souhlas jasně doložit. Souhlas musí být jasně odlišitelný od jiných skutečností. Zároveň musí být souhlas svobodný a subjekt údajů musí mít možnost ho odvolat stejně snadno, jako ho udělil.
- ✓ **Právo na opravu či aktualizaci údajů:** je aplikováno automaticky, avšak subjekt údajů jej může uplatnit i na vlastní žádost v případě, že by správce k opravě či aktualizaci údajů nepřistoupil z vlastní iniciativy. Správce je v rámci tohoto práva povinen bez zbytečného odkladu opravit nepřesné osobní údaje, které se týkají daného subjektu. Subjekt údajů má současně právo na doplnění neúplných osobních údajů, například formou dodatečného prohlášení.

2.2 Práva subjektu údajů na vyžádání:

- ✓ **Právo získat od správce osobních údajů potvrzení o zpracování údajů:** každý subjekt údajů má možnost takovou žádost uplatnit u kteréhokoliv správce údajů a získat tak od správce potvrzení, zda daný správce jeho osobní údaje zpracovává či nikoliv.
- ✓ **Právo na přístup subjektu ke svým osobním údajům:** subjekt údajů má právo na přístup ke svým osobním údajům, která správce zpracovává. Na základě aplikace tohoto práva by měl subjekt údajů obdržet minimálně informace o rozsahu, účelu a době zpracování; příjemcích nebo kategoriích příjemců, kterým jsou osobní údaje předávány; zdroji, odkud byly osobní údaje získány; skutečnosti, zda dochází k automatizovanému rozhodování včetně profilování; zda probíhá předávání do třetí země a zda byly přijaty vhodné záruky v případě takového předání. Pokud firma provádí takové zpracování, že není schopna identifikovat subjekt údajů, který právo využil (např. snímá SPZ aut na firemním parkovišti), nemusí jen pro splnění žádosti sama získávat další osobní údaje, ale je na subjektu údajů, aby jí s identifikací pomohl (přijel jsem s touto SPZ v určitý čas) za účelem výkonu svého práva.
- ✓ **Právo získat kopii zpracovávaných osobních údajů:** je součástí práva na přístup k údajům, kterou lze uplatnit na žádost subjektu údajů. Správce je v případě požadavku subjektu údajů povinen poskytnout mu kopii zpracovávaných osobních údajů.
- ✓ **Právo na omezení zpracování:** subjekt údajů má v některých zvláštních případech právo na omezení zpracování za předpokladu, že je zapotřebí ověřit přesnost zpracovávaných osobních údajů, nebo jsou dány důvody pro výmaz, který však nelze z různých důvodů realizovat nebo kdy jsou údaje nutné pro obhajobu právních nároků a také v situaci, kdy subjekt údajů vznesl proti jejich zpracování námitku.
- ✓ **Právo na přenositelnost údajů:** tento bod znamená právo subjektu údajů na získání osobních údajů, které se jej týkají, od správce, který je zpracovává a možnost předání těchto údajů jinému správci. Údaje musejí být předány ve strukturovaném, běžně používaném a strojově čitelném formátu. Nesmí jít tedy o formát, který by licenčně zatížil příjemce osobních údajů. Další podmínkou pro realizaci přenositelnosti je, že se jedná o zpracování založené na souhlasu nebo smlouvě a současně jde o zpracování automatizované. Součástí práva na přenositelnost je i nárok subjektu údajů na to, aby předání údajů bylo realizováno přímo mezi správci údajů navzájem bez toho, aby se subjekt údajů musel sám na přenosu údajů podílet.

Příklad: *Požadavku na aplikaci práva na přenositelnost se mohou v prostředí obcí týkat například všechny osobní údaje, které obec zpracovává na základě právního titulu souhlasu se zpracování osobních údajů získanému od subjektu osobních údajů.*

- ✓ **Právo vznést námitku:** subjekt údajů disponuje právem vznést námitku proti zpracování jeho osobních údajů, a to včetně profilování. Správce v takovém případě osobní údaje subjektu dále nezpracovává, pokud přímo neprokáže, že k danému zpracování má závažné a oprávněné důvody (např. jiný legitimní právní titul pro toto zpracování). Další případem, kdy je možné i přes námitku údaje dále zpracovávat jsou situace, kdy je zpracování nutné pro výkon a obhajobu právních nároků. Subjekt údajů musí být o tomto právu srozumitelnou formou informován, a to již při první komunikaci se správcem osobních údajů.

Příklad: *Obce mohou například na svých webových stránkách publikovat údaje o subjektech údajů na základě získaného souhlasu, který však vypršel. Pokud údaje na stránkách i přesto jsou stále uvedeny, může být na místě podání námitky proti takovému zpracování údajů.*

2.3 Povinnosti správců a zpracovatelů údajů

Organizace v roli správce údajů by si měla osvojit všechny své povinnosti, z nichž některé jsou v českém prostředí zcela nové. Jde zejména o tyto nové povinnosti:

- ✓ **Povinnost vést záznamy o činnostech zpracování:** každý správce údajů má dle obecného nařízení povinnost vést písemné záznamy o všech činnostech souvisejících se zpracováním údajů, které budou dostupné na vyžádání dozorovému úřadu.

☼ ***Vysvětlení:*** *Z povinnosti vést záznamy o činnostech zpracování platí jediná výjimka – neplatí pro organizace s počtem zaměstnanců do 250 zpracovávající osobní údaje pouze příležitostně, bezrizikovým způsobem a nezpracovávající citlivé osobní údaje. Jelikož v prostředí obcí je vyloučeno, aby zpracování osobních údajů probíhalo pouze příležitostně, je využití této výjimky pro obce de facto vyloučeno.*

- ✓ **Povinnost zajistit odpovídající zabezpečení osobních údajů:** správce i zpracovatel údajů musejí dle obecného nařízení přijmout s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, kontextu a rozsahu zpracování i k různě pravděpodobným a různě závažným rizikům všechna vhodná technická a organizační opatření k zajištění zabezpečení zpracování, kterými mohou být například šifrování, pseudonymizace (dočasná či přechodná anonymizace údajů pro účely určité fáze nebo určitého procesu jejich zpracování), zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb, schopnost obnovení údajů v případě bezpečnostních incidentů prostřednictvím racionálního systému jejich zálohování a automatizace procesů pro jejich obnovení a podobně.
- ✓ **Povinnost ohlašovat bezpečnostní incidenty na poli ochrany osobních údajů:** v případě jakéhokoli porušení zabezpečení údajů – tedy i v případech, kdy fyzicky nenastal únik dat, avšak pouze byla porušena jejich bezpečnost (dostupnost, důvěrnost, integrita) a je pravděpodobné riziko pro práva a svobody subjektu údajů – musí správce údajů bez zbytečného odkladu, nejpozději do 72 hodin hlásit tento incident dozorovému orgánu a v případě, že je pravděpodobné, že tímto incidentem vznikne vysoké riziko pro práva a svobody fyzických osob-subjektů údajů, pak je nutné oznámit jej i dotčeným subjektům údajů.
- ✓ **Povinnost provést posouzení vlivu na ochranu osobních údajů (DPIA):** před započetím nových zpracování údajů, které obnášejí vysoké riziko pro práva subjektů údajů, má správce v rámci procesu hodnocení dopadů povinnost posoudit jejich vliv

na ochranu údajů. To obnáší standardizovaný postup, který musí zahrnovat např. systematický popis zamýšlených operací zpracování a účely zpracování, posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů, posouzení rizik pro práva a svobody subjektů údajů a plánovaná opatření k řešení těchto rizik. Posouzení přitom není jednorázové, ale opakuje se kdykoli při zavedení nového procesu zpracování, který obnáší vysoké riziko, nebo při zvýšení míry rizika procesu již existujícího.

- ✓ **Povinnost realizovat předchozí konzultace s dozorovým úřadem:** tam, kde by mělo zpracování podle posouzení vlivů za následek vysoké riziko pro práva subjektů údajů, má správce povinnost přijmout opatření ke zmírnění tohoto rizika a tato opatření předběžně konzultovat s dozorovým orgánem. Tento konzultační proces má podle obecného nařízení závazné lhůty a pravidla.

  Příklad: Pokud obec vyhodnotí v rámci svého hodnocení dopadů určitý proces – např. může jít o zavedení nové technologie rozpoznávání vizuální podoby jednotlivých osob v rámci městského kamerového systému a sledování jejich pohybu v obci – za vysoce rizikový, má povinnost přijmout opatření ke zmírnění tohoto rizika (v daném případě by např. mohlo jít o zvýšené zabezpečení kamerového systému před kybernetickým útokem, zúžení okruhu osob, které mají přístup k záznamům z kamerového systému apod.) a tato opatření konzultovat s dozorovým úřadem.

- ✓ **Povinnost jmenovat pověřence pro ochranu osobních údajů:** povinnost jmenovat pověřence na ochranu osobních údajů má každá organizace, která je orgánem veřejné moci nebo orgánem zřízeným zákonem, který plní zákonem stanovené úkoly ve veřejném zájmu. Dalším z parametrů, na základě kterých může vyvstat tato povinnost u soukromoprávních subjektů, je případ, kdy hlavní činnost podnikání organizace vyžaduje rozsáhlé, pravidelné a systematické monitorování subjektů údajů nebo rozsáhlé zpracování zvláštních kategorií osobních údajů.

Pověřenec pro ochranu osobních údajů

V této kapitole je podrobněji přiblížena nová role, kterou obecné nařízení zavádí, tzv. pověřenec pro ochranu osobních údajů (anglicky Data Privacy Officer, zkratka DPO). Zaměříme se především na možnosti jeho jmenování neboli ustanovení do funkce, na role pověřence, kvalifikaci, kritéria výběru kandidáta na tuto roli a jeho postavení v organizaci. Následně se budeme podrobněji věnovat konkrétním úkolům, pravomocem a odpovědnostem, které jsou s rolí pověřence přímo spjaty.

1 Způsoby, jakými může organizace jmenovat pověřence

- ✓ **Jmenování interního zaměstnance do role pověřence:** varianta, kdy organizace jmenuje stávajícího pracovníka s odpovídající kvalifikací do role pověřence. Toto přijetí agendy spojené s pozicí pověřence musí být provázeno také zajištěním nezávislosti pověřence, která je blíže vysvětlena dále v textu. Výhodou této varianty je, že umožní organizaci jmenovat pracovníka, který již má vysokou znalost interních procesů a zpracování osobních údajů v dané organizaci.
- ✓ **Jmenování externího pověřence:** obecné nařízení umožňuje zajištění role pověřence jako externí služby od fyzické nebo právnické osoby. V případě právnické osoby má tato varianta další podmínky a to především to, že daná právnická osoba musí rolí pověřence pověřit konkrétního zaměstnance, který prokáže potřebnou kvalifikaci (viz dále). V případě zastupitelnosti musí mít i zástupce potřebnou kvalifikaci stejně jako oficiálně pověřený zaměstnanec.
- ✓ **Jmenování společného pověřence pro více organizací:** skupinám organizací je také umožněno jmenovat jednoho společného pověřence. Podmínkou pro využití této varianty je nutnost zajistit, že daný pověřenec bude schopen plnohodnotně zastávat všechny své úkoly ve všech spravovaných organizacích.

2 Kvalifikace a odborné schopnosti pověřence

Obecné nařízení přímo nestanovuje konkrétní parametry výběru kandidáta pro roli pověřence. Není tedy vyžadována žádná konkrétní úroveň vzdělání nebo specializace. Nicméně existují doporučující parametry pro takový výběr:

- ✓ Pověřenec pro ochranu osobních údajů by měl být jmenován na základě odpovídajících profesních kvalit, a to zejména odborných znalostí praxe v oblasti ochrany osobních údajů, práva, procesního řízení a měl by disponovat i určitou hladinou technických znalostí.

  ☼ ***Vysvětlení:*** *Vzhledem k zařazení pověřence pro ochranu osobních údajů do katalogu prací ve veřejné správě vyplývá kvalifikace pověřence poskytující služby veřejnoprávní organizaci v rámci zaměstnaneckého poměru z jeho zařazení do platových tříd. V případě pověřence poskytujícího služby externě se však tato pravidla nepoužijí.*
- ✓ Základní kritériem výběru kandidáta na tuto pozici je jeho schopnost plnit požadované úkoly v organizaci, pro kterou byl jmenován. Požadavky na výkon role pověřence se mohou lišit především povahou a velikostí organizace.
- ✓ Úroveň odborných znalostí pak musí být přímo úměrná složitosti, citlivosti a rozsahu zpracování osobních údajů v dané organizaci.

> ***Příklad:*** *Odbornost pověřence v případě malé obce vykonávající pouze základní agendy zahrnující zpracování osobních údajů může být nižší než v případě většího města, kde je rozsah a složitost zpracování osobních údajů významně vyšší, a to včetně množství třetích stran, kterým jsou osobní údaje předávány.*

- ✓ Pověřenec by měl mít také odpovídající povědomí o národní i evropské legislativě týkající se ochrany osobních údajů a velmi dobrou znalost obecného nařízení.

3 Postavení pověřence v organizaci

Jmenování pověřence pro ochranu osobních údajů musí provázet i zajištění odpovídajících podmínek této pozice dle požadavků obecného nařízení. Podmínky jsou následující:

- ✓ **Zajištění nezávislosti** v praxi znamená, že pro splnění této podmínky měl mít pověřenec přístup přímo k nejvyššímu vedení obce (v ideálním případě přímo ke starostovi). Zároveň by od organizace neměl dostávat žádné pokyny, které se budou přímo týkat výkonu jeho úkolů pověřence (například by neměl být pověřen kromě výkonu úkolů pověřence také jinou agendou, kde by mohl ovlivnit účel zpracování osobních údajů). Pověřenec by však v každém případě měl být nezávislý a nesmí být ve střetu zájmů. V neposlední řadě by měl být seznámen s veškerým zpracováním osobních údajů v organizaci a měl by získat přímý nebo nepřímý přístup ke všem zdrojům informací potřebných pro výkon své agendy.

  > ☼ ***Vysvětlení:*** *Nepřímým přístupem k informacím je myšleno zajištění spolupráce a dostupnosti vlastníků daných informačních systémů nebo osob odpovědných za dané zpracování osobních údajů místo udělení přímého přístupu k informacím. Důvodem může být především zvýšení úrovně informační bezpečnosti.*

- ✓ **Zamezení střetu zájmů** je jedním ze zásadních požadavků pro jmenování nové role. Pověřenec se v průběhu plnění svých úkolů a případných dalších úkolů, které mu organizace uloží, nesmí dostat do situací, kdy by mohl přímo ovlivňovat účel zpracování osobních údajů, nebo kdy nebude dobře ošetřeno dělení odpovědností.

  > ***Příklad:*** *Jako případ střetu zájmů můžeme uvést situaci, kdy je do role pověřence jmenován vedoucí pracovník oddělení IT, který má přímou možnost vstoupit a ovlivnit zpracování osobních údajů v informačních systémech a zároveň zastávat roli pověřence.*

- ✓ **Zabezpečení dostatečných zdrojů pro výkon funkce** je povinností organizace, která pověřence jmenuje, a to ať jde o zajištění pracovního prostředí, případného personálu a adekvátní výše mzdy. Zároveň musí mít zajištěnou dostatečnou časovou dotaci pro výkon svých úkolů a povinností v případě, že je organizací pověřen i dalšími úkoly.

4 Povinnosti a úkoly pověřence

V obecném nařízení je uveden minimální rozsah úkolů pověřence pro ochranu osobních údajů. Jeho úkoly jsou v této kapitole stručně vysvětleny.

- ✓ **Metodické vedení a poradenství:** role pověřence je především rolí poradní v tématu ochrany osobních údajů. Pověřenec by měl podporovat a metodicky vést dodržování zásad zpracování osobních údajů v organizaci.
- ✓ **Monitorování souladu s předpisy souvisejícími s ochranou osobních údajů:** pověřenec musí mít dlouhodobé povědomí o aktuálním stavu právních úprav, které se týkají ochrany osobních údajů a udržovat všechna jejich zpracování v souladu s těmito úpravami. Musí se tedy v této oblasti kontinuálně vzdělávat a být schopen na aktuální situaci reagovat.

- ✓ **Vedení záznamů o činnostech zpracování:** všem organizacím nad 250 zaměstnanců, které neprovádějí pouze příležitostné zpracování necitlivých osobních údajů s nízkým rizikem, de facto tedy i všem obcím, je v GDPR uložena povinnost vést záznamy o činnostech zpracování (viz předchozí výklad). Odpovědnost za vedení těchto záznamů nese správce osobních údajů nebo jeho případný zástupce. Pověřenec by ovšem měl průběh plnění této povinnosti minimálně kontrolovat, případně může vést katalog zpracovatelských operací nebo celou agendu vedení těchto záznamů. V případě organizace pod 250 zaměstnanců platí výjimka z této povinnosti, pokud jsou splněny všechny podmínky udávané v obecném nařízení.
- ✓ **Komunikace s dozorovým úřadem a subjekty údajů:** pověřenec je primární kontaktní osobou jak pro subjekty osobních údajů, tak pro dozorový úřad pro oblast ochrany osobních údajů. Jeho kontaktní údaje musí být zveřejněné a v případě potřeby jednoduše dostupné. V případě řešení stížností ze strany subjektů údajů nebo při případné kontrole zajišťuje pověřenec komunikaci s dozorovým úřadem.
- ✓ **Podpora při posouzení vlivu na ochranu osobních údajů:** pověřenec poskytuje správci posudek v jakých případech je nutné provést posouzení dopadu na soukromí subjektů údajů, metodicky toto posouzení může vést a následně přidat své vyjádření k jeho závěrům. Nesmí však toto posouzení sám přímo vykonávat tak, aby se předešlo střetu zájmů.
- ✓ **Budování povědomí o ochraně osobních údajů v organizaci:** dalším z úkolů pověřence je zajišťování nebo garance dlouhodobého a pravidelného vzdělávání a školení zaměstnanců o ochraně osobních údajů. Pravidelné vzdělávání a vyškolení zaměstnanců je jedním z nástrojů, jak snížit riziko porušení požadavků obecného nařízení v důsledku chyby lidského faktoru. Zároveň školení představuje dlouhodobě účinný nástroj pro budování všeobecného povědomí o informační bezpečnosti a ochraně soukromí v organizaci.

Předávání osobních údajů do třetích zemí

V této části příručky jsou vysvětleny základní otázky předávání osobních údajů do třetích zemí, v prostředí obcí se bude jednat například o systematickou spolupráci s partnerskými městy a opakované vysílání delegací nebo zaměstnanců obce do těchto zemí. K takovému předání osobních údajů může dojít pouze v případě, že organizace splní podmínky, které pro tento přenos obecné nařízení stanovuje. Možné záruky pro naplnění těchto podmínek jsou popsány níže.

- ✓ **Předávání založené na vhodných zárukách:** pokud neexistuje rozhodnutí Evropské komise podle článku 45 obecného nařízení (whitelist, blacklist), správce nebo zpracovatel mohou předat osobní údaje do třetí země pouze v případě, že přijímající správce nebo zpracovatel poskytne dostatečné záruky a je zajištěna vymahatelnost práv subjektů údajů. Pokud neexistuje zvláštní povolení dozorového úřadu, je vhodné záruky možné prokázat pomocí vhodných záruk, tedy závazných podnikových pravidel (která však v prostředí obcí nejsou použitelná), pomocí standardních doložek o ochraně údajů přijatých dozorovým úřadem nebo Evropskou komisí, dále pak schváleným kodexem chování, schváleným mechanismem pro vydání osvědčení či prostřednictvím smluvních doložek mezi správcem a zpracovatelem.
- ✓ **Závazná podniková pravidla:** závazná podniková pravidla jsou schvalována dozorovým úřadem za předpokladu, že jsou závazná a prosazovaná všemi podniky ve skupině podniků; přiznávají vymahatelná práva subjektům údajů; obsahují strukturu a kontaktní údaje skupiny organizací; obsahují popis předání údajů apod.
- ✓ **Předání či zveřejnění povolená právem EU:** rozhodnutím soudního orgánu a rozhodnutím správního orgánu třetí země, které po správci nebo zpracovateli požadují předání nebo zpřístupnění osobních údajů, lze předání či zveřejnění uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem, aniž jsou dotčeny jiné důvody pro převod.
- ✓ **Výjimky pro specifické situace:** pokud neexistuje rozhodnutí o odpovídající ochraně, ani vhodné záruky předání včetně závazných podnikových pravidel, existuje několik výjimek, v rámci kterých může předání do třetích zemí přesto proběhnout. Výjimky jsou popsány v čl. 49 obecného nařízení (příklad výjimek: předání je nezbytné pro plnění smlouvy mezi subjektem údajů a správcem; předání je nezbytné z důležitých důvodů veřejného zájmu apod.).

Zavádění obecného nařízení krok po kroku

V této kapitole Vám příručka stručně představí, kde začít s řešením požadavků obecného nařízení a jak postupovat při jejich zavádění do agend obce:

1 Posouzení současného stavu

1.1 Posouzení stávajícího stavu obce oproti požadavkům nařízení:

nejprve by si každá organizace měla projít výše popsané požadavky obecného nařízení a vyhodnotit, do jaké míry je v dané chvíli naplňuje. Na základě takového zhodnocení aktuálního stavu si pak obec stanoví první priority pro vytvoření plánu, jak efektivně jednotlivé požadavky obecného nařízení naplnit.

1.2 Zmapování zpracování osobních údajů (katalogizace a kategorizace):

po provedení tohoto kroku by měl být hotový kompletní přehled o zpracování osobních údajů, které v obci probíhá. Takový přehled by měl obsahovat minimálně následující informace ke každému zpracování osobních údajů:

- ✓ název zpracování osobních údajů,
- ✓ účel zpracování osobních údajů,
- ✓ právní titul, na jehož základě zpracování probíhá,
- ✓ typy osobních údajů, které jsou při zpracování zasaženy (jméno, příjmení, adresa ad.),
- ✓ datum vypršení legitimního titulu zpracování (např. vypršení archivační lhůty na základě jiné právní povinnosti),
- ✓ jméno osoby odpovědné za dané zpracování,
- ✓ Vstupní zdroje odkud osobní údaje přicházejí a následně informační systémy, kam vystupují.

V rámci kategorizace zpracování osobních údajů se vyhodnotí, zda jde o zpracování zvláštních kategorií osobních údajů (citlivé údaje) a případně, jestli nejde o nadbytečné zpracování.

Tento katalog by se měl následně dlouhodobě udržovat a aktualizovat, přičemž by měl sloužit jako nástroj pro podporu výkonu úkolů pověřence, ale i dozorového úřadu.

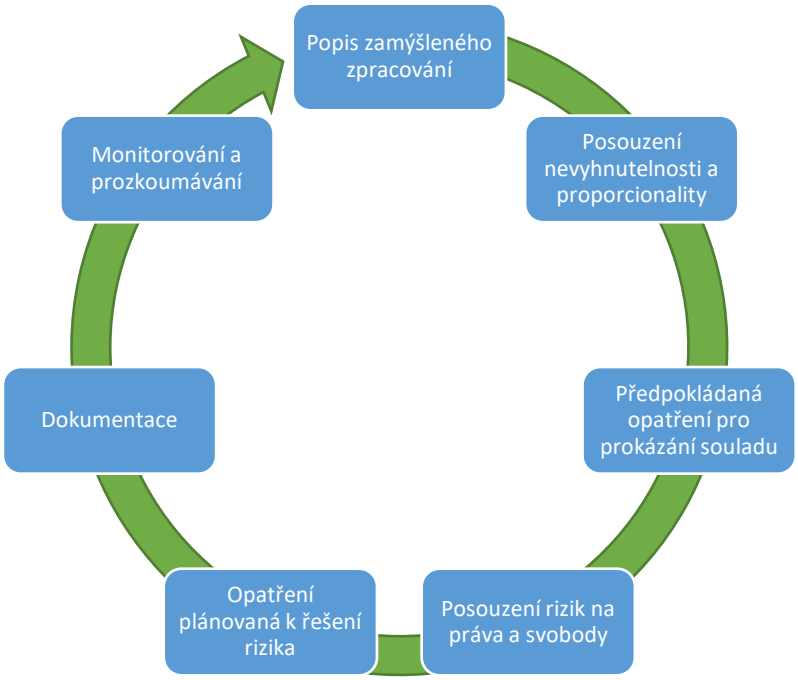
1.3 Revize zabezpečení zpracování osobních údajů:

dalším krokem by mělo být vyhodnocení stavu zabezpečení materializovaného (probíhajícího ve fyzické podobě) i elektronického zpracování osobních údajů. Výsledky této revize by měly být následně prioritizovány a to by mělo upozornit na oblasti, kde organizace musí zavést technická a organizační opatření nejdříve. Příklady nejdůležitějších oblastí, které by měly revidovány:

- ✓ fyzická bezpečnost (bezpečnost vstupů do budovy, uložení osobních údajů na pracovišti, zabezpečení archivu ad.),
- ✓ zabezpečení koncových zařízení (PC, laptopy, servery, mobilní telefony),
- ✓ autorizace (kdo má přístup k čemu a zda ho potřebuje) a autentizace (schopnost jednoznačně identifikovat uživatele),
- ✓ schopnost detekovat ohlásit případné porušení zabezpečení osobních údajů.

1.4 Provedení posouzení dopadu na ochranu soukromí v případě, kdy je nutné:

vyhodnocení potřeby posouzení dopadu na ochranu soukromí by mělo navazovat na předchozí kroky, aby bylo kvalifikované na základě stavu zpracování a zabezpečení zpracování. Postup provedení posouzení popisuje následující obrázek z výkladových stanovisek WP29.



Zdroj: Výkladová stanoviska WP29 pro DPIA

2 Právní kroky

2.1 Interní přepisy a smluvní vztahy

- ✓ **Revize smluvní dokumentace pro zaměstnance:** od pracovních smluv až po předávací protokoly upravující používání služební techniky apod. Vzhledem k tomu, že řada účelů zpracování v pracovněprávních vztazích vyplývá přímo ze zákona, není nutné jejich zahrnutí do smlouvy. Rozšíření smluvních ujednání naopak lze doporučit tam, kde dochází ke zpracování údajů například na základě oprávněného zájmu zaměstnavatele.

  > ***Příklad:*** *V případě, kdy může být zaměstnanec v rámci své pracovní náplně vyslán na služební cestu do partnerské obce v zahraničí, měl by mít v pracovní smlouvě tuto informaci zahrnutou a to včetně možnosti, že může dojít v průběhu takové služební cesty k předání jeho osobních údajů zmíněné obci.*

- ✓ **Revize metodických postupů, směrnic a jiných interních předpisů zaměstnavatele:** ať už těch, které přímo upravují práci s osobními údaji, nebo těch, které se týkají dalších firemních procesů zahrnujících i zpracování osobních dat.
- ✓ **Revize udělených souhlasů se zpracováním údajů:** pro případy, kdy je nutné získat pro zpracování osobních údajů, musí ho obec zajistit. V každém případě platí povinnosti poskytnout zaměstnanci všechny informace, jejichž poskytnutí ukládá obcím jako správcům údajů obecné nařízení.
- ✓ **Revize způsobu vysílání zaměstnanců k výkonu práce do zahraničí** – jednodušší situace bude sice při vysílání pracovníků v rámci Evropské unie, protože Obecné nařízení platí pro všechny členské země EU a navíc i pro země EHP (tedy Norsko,

Lichtenštejnsko a Island), komplikovanější ale naopak bude situace při vysílání do třetích zemí. V těchto situacích obecné nařízení rozlišuje země „bezpečné“ (jejichž výčet – whitelist - aktuálně zahrnuje 12 zemí nebo jejich částí, který vydává svým rozhodnutím o adekvátní ochraně Evropská komise) a současně i na „nebezpečné“ (jejichž výčet – blacklist - dosud nebyl publikován, avšak publikaci lze očekávat nejpozději s účinností obecného nařízení). Do zemí bezpečných lze osobní údaje zaměstnanců přenášet bez dalšího, pro ty další však platí přísná omezení. Pro bližší informace o této problematice doporučujeme část textu této příručky zabývající se přenosem osobních údajů do třetích zemí, případně doporučujeme konzultaci s Úřadem pro ochranu osobních údajů nebo se specializovaným poradcem.

2.2 Vztahy s externími subjekty

- ✓ **Revize smluv o zpracování osobních údajů s externími subjekty** – například se zpracovateli mzdové agendy, agenturami práce nebo náborovými agenturami, smluvními pracovními lékaři, firmami poskytujícími zaměstnanecké benefity jako jsou stravenky nebo programy výhod pro zaměstnance apod. V řadě případů ve smlouvách dosud není ochraně osobních údajů zaměstnanců věnována potřebná pozornost, což se může stát velmi problematickým, a to především z důvodu, že správce nese primární odpovědnost za zpracování osobních údajů subjektů a je na něm si zajistit odpovídajícími technickými, organizačními a právními prostředky, že zpracování vykonávané zpracovateli bude v souladu s obecným nařízením.

3 Technické a organizační kroky

3.1 Zavedení nových a optimalizace stávajících procesů vstupujících do zpracování osobních údajů

- ✓ **Nastavení procesů pro vyřizování požadavků subjektů údajů:** organizace musí zabezpečit svou schopnost v odpovídající lhůtě (1 měsíc, případně až 3 měsíce pokud je prokázána komplikovanost vyřízení požadavku). K tomu je nutné zajistit funkčnost potřebných procesů týkajících se sběru, výmazu, přenosu osobních údajů a příprava komunikačních kanálů, jak interně v organizaci, tak směrem k subjektům údajů a dozorovému úřadu.
- ✓ **Příprava interních procesů pro zajištění dodržování zásad podle obecného nařízení:** jde především o nastavení odpovídajících expiračních lhůt pro držení osobních údajů, přesnost a aktuálnost skartačního a archivačního řádu, stanovení odpovědných osob za jednotlivé informační systémy a agendy zpracování osobních údajů nebo o nastavení procesu ohlašování porušení zabezpečení údajů.
- ✓ **Procesy informační bezpečnosti:** pro zajištění odpovídající míry zabezpečení zpracování osobních údajů by měly být zavedeny nebo aktualizovány procesy řízení informační bezpečnosti (např. politika hesel, přístupů, politika čistého stolu atd.). Důležitým procesem je detekce a reakce na bezpečnostní incident, do kterého spadá i řešení již zmíněné povinnosti ohlášení narušení zabezpečení zpracování osobních údajů.
- ✓ **Procesy přenosu osobních údajů třetím stranám nebo do třetích zemí:** optimalizací, zrušení nebo naopak zavedením nových procesů musí projít i agenda výměny informací s externími subjekty.

3.2 Úprava stávajících informačních systémů, nasazení nových řešení:

je možné, že v některých případech bude nutné provést úpravu stávajících nebo nasazení nových informačních systémů, které zajistí dostatečnou úroveň bezpečnosti a schopnost dostát všem požadavkům obecného nařízení.

3.3 Dlouhodobé udržování aktuálnosti prostředí:

představuje potřebu pravidelně aktualizovat všechny dokumentace a procesy, případně včas reagovat na zavádění nových zpracování nebo povinností vyplývajících z právních předpisů upravujících ochranu osobních údajů.

- ✓ **Vyškolení a pravidelné vzdělávání zaměstnanců v oblasti ochrany osobních údajů:** je nezbytným předpokladem pro zajištění dlouhodobého souladu s požadavky obecného nařízení. Pravidelné vzdělávání zaměstnanců v této oblasti představuje také jeden z klíčových a dlouhodobě účinných nástrojů ke snižování rizik souvisejících se správou a zpracováním osobních údajů. Rozsah a forma školení by měly být adekvátní pracovní náplni daného zaměstnance.

Užitečné odkazy

- ✓ Oficiální text obecného nařízení v češtině: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016R0679
- ✓ Web Úřadu pro ochranu osobních údajů: www.uoou.cz
- ✓ Webová stránka Evropské komise věnované reformě pravidel EU pro ochranu osobních údajů v roce 2018: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_cs
- ✓ Newsroom Pracovní skupiny podle článku 29 Směrnice 95/46/ES (tzv. Article 29 Working Party neboli WP 29): http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- ✓ Informace Ministerstva průmyslu a obchodu ČR o obecném nařízení: https://www.mpo.cz/cz/podnikani/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr--228672/
- ✓ Informace Ministerstva vnitra ČR o obecném nařízení: http://www.mvcr.cz/gdpr/
- ✓ Metodika GDPR - ochrana osobních údajů při výkonu spisové služby, zejména v informačních systémech spravujících dokumenty u veřejnoprávních původců: http://www.mvcr.cz/gdpr/clanek/nova-metodika-k-gdpr-v-oblasti-spisovych-sluzeb.aspx
- ✓ Metodické doporučení k činnosti obcí k organizačně-technickému zabezpečení funkce pověřence pro OOÚ dle obecného nařízení o OOÚ v podmínkách obcí: http://www.mvcr.cz/gdpr/clanek/aktualizovana-metodika-k-poverencum-pro-ochranu-osobnich-udaju.aspx