IMPLEMENTACE GDPR V PROSTŘEDÍ MĚSTSKÉHO ÚŘADU CHEB

Konference GDPR ve veřejné správě
16.5.2018, Praha

GDPR – (General Data Protection Regulation)

- **Nařízení** Evropského parlamentu a Rady (EU) **2016/679** o ochraně fyzických osob
- Přijato 27. 4. 2016 (po čtyřletém vyjednávání)
- Účinnosti nabude **25. 5. 2018** (i bez zapracování do legislativy ČR)
- Nahrazuje Směrnici **95/46 EC** a v ČR zákon č. **101/2000 Sb.,** o ochraně osobních údajů a o změně některých zákonů
- Jedná se o nařízení, dokument přijatý na úrovni EU, není potřeba národní implementace a je platné pro všechny
- Jedná se o přelomovou novou legislativu, přinášející zásadní posílení ochrany osobních údajů a řadu nových povinností nebo změny stávajících povinností pro všechny správce a zpracovatele.

GDPR – (General Data Protection Regulation)

- Správní pokuta za nedodržování 20 mil. Euro nebo 4 % z celkového obratu společnosti
- Výrazně povyšuje ochranu dat na úroveň evropského zákona a posiluje právo osob na lepší kontrolu nad jejich osobními údaji
- Představuje rovnováhu mezi legitimními zájmy správců a zpracovatelů dat s právem osob na soukromí

GDPR - CO JSME PODNIKLI

1) Jmenování pracovního týmu GDPR

- **Po zralé úvaze jsme zvolili širší a užší tým**
- **Širší tým je složen z jednotlivých vedoucích odborů, právníka a externího dodavatele informačního systému**
- **Užší tým pak z tajemníka úřadu, vedoucí oddělení interního auditu (DPO), vedoucího odboru správních činností a obecní živnostenský úřad, vedoucího odboru organizačního a vedoucího odboru informatiky**

GDPR - CO JSME PODNIKLI

2) Harmonogram

- **V týmu GDPR jsme stanovili a odsouhlasili harmonogram jednotlivých úkolů, prací, kontrol a dalších potřebných termínových opatření.**
- **Tento harmonogram se na jednotlivých schůzkách projektového týmu kontroluje, doplňuje a aktualizuje.**

GDPR - CO JSME PODNIKLI

3) Jmenování pověřence pro ochranu osobních údajů (DPO)

- **Po debatách na celostátní úrovni byla zvolena jako pověřenec vedoucí interního auditu**
- **Toto rozhodnutí se nám ale v poslední době snaží vyvrátit Stanovisko OCHJ Ministerstva financí**
  - **Požádali jsme tudíž o vyjádření přímo ÚOOÚ a Ministerstvo vnitra**
  - **K tomuto stanovisku máme i rozklad ze strany právníka našeho města**

GDPR - CO JSME PODNIKLI

- **Z rozkladu právníka úřadu**
- Nelze slučovat **GDPR** se **zákonem o finanční kontrole**. Předmětný zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, vymezuje svoji působnost v § 1 odst. 1 takto: „Tento zákon vymezuje uspořádání a rozsah finanční kontroly vykonávané mezi orgány veřejné správy, mezi orgány veřejné správy a žadateli nebo příjemci veřejné finanční podpory a uvnitř orgánů veřejné správy. Stanoví předmět, hlavní cíle a zásady finanční kontroly vykonávané podle tohoto zákona a podle zvláštních právních předpisů, pokud tak tyto předpisy stanoví.“

GDPR - CO JSME PODNIKLI

- Nařízení GDPR tedy stanovuje pověřenci zvláštní požadavky, zejména se jedná o dostatečnou kvalifikaci, absenci střetu zájmů a v neposlední řadě shora uvedený přístup k nejvyššímu vedení organizace. Dle našeho názoru jsou to zejména tyto požadavky, jejichž naplnění interní auditor splňuje a nevidíme v tomto případě ani žádný střet zájmů, když auditor vedle auditu dle zákona o finanční kontrole plní zároveň roli pověřence dle příslušného nařízení GDPR, kdy výkon této činnosti s finanční kontrolou vůbec nijak nesouvisí a nemůže s ní být tedy ve střetu zájmů ani v rozporu s nezávislým plněním úkolů stanovených internímu auditu nebo pověřenci.
- *Toto stanovisko Městského úřadu Cheb vychází ze shora uvedeného zákona, GDPR a stanovisek Úřadu pro ochranu osobních údajů a Ministerstva vnitra ČR.*

GDPR - CO JSME PODNIKLI

4) Nastavení pravidelných schůzek jednání týmu GDPR

- **Užší tým se schází v pravidelných intervalech po 14 dnech**
- **Informace o jednání týmu a stavu rozpracovanosti problematiky GDPR v prostředí úřadu a příspěvkových organizací předkládáme radě města.**
- **Z každé schůzky je sepsán zápis s úkoly, jejich termínem plněním a dalšími náležitostí, které z této schůzky vzniky.**
- **Tým si na své jednotlivé schůzky zve vedoucí jednotlivých odborů, městského právníka, nebo jinak dotčené osoby.**

GDPR - CO JSME PODNIKLI

5) Vstupní analýza a vzhled tabulek, které vyplnili vedoucí jednotlivých odborů a samostatných oddělení

- **Pro každý jednotlivý odbor a samostatné oddělení jsme připravili k vyplnění následující tabulku, díky které jsme chtěli zjistit, jaké OÚ údaje a v jaké formě na jednotlivých místech zpracováváme**

Kategorie	osoby zprac. OÚ	Přehled účelů zpracování osobních údajů									
		ve smyslu nařízení Evropského parlamentu a Rady EU č. 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 (obecné nařízení o ochraně osobních údajů), které se stane přímo účinné a aplikovatelné ode dne 25. května 2018.									
		Odbor:				Vedoucí odboru:				Stránka:	
		Poř. číslo	Účel zpracování	Zákonná norma	Kategorie osobních údajů	Kategorie subjektu údajů	Kategorie příjemců	Doba uchování	Způsob uchování	Místo uchování	Uzamykatelné prostory

GDPR - CO JSME PODNIKLI

6) Vstupní analýza a zpracování tabulek

- **Po zpracování tabulek vedoucími jednotlivých oddělení přišla na řadu kompletace jednotlivých částí, kontrola odevzdaných zpracování a vlastní řešení zpracování OÚ přímo v prostředí jednotlivých odborů, samostatných oddělení a MP, jednotlivými členy užšího týmu GDPR.**
- **K jednotlivým zpracováním OÚ byla stanovena kategorizace zpracování a osoby, kteří zpracovávají.**
- **Na základě zjištěných údajů z dotazníků, došlo i k místním šetřením na jednotlivých odborech s cílem zjistit nutnost dalšího zabezpečení skříní, regálů a místností, kde jsou OÚ uloženy.**

GDPR - CO JSME PODNIKLI

6) Vstupní analýza a zpracování tabulek - kategorizace

KAREGORIE	1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
I.	e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
II.	c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
III.	b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
IV.	a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
V.	d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
VI.	f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.
C	čl. 9. Jedná se o takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Ve školském prostředí se pak můžeme setkat zejména s těmi údaji ze zvláštní kategorie, které souvisejí se zdravotním stavem dítěte (např. nemoc nebo zdravotní postižení), náboženským vyznáním, sociální situací či s etnickým původem. K osobním údajům z této zvláštní kategorie je pak třeba přistupovat specificky,

GDPR - CO JSME PODNIKLI

6) Vstupní analýza a zpracování tabulek – zpracovávající osoby

2. Osoby zpracovávající osobní údaje		
V = Vedoucí	P = Pověřen./odpovědn. zaměstn.	Z = Všichni pracovníci odboru

GDPR - CO JSME PODNIKLI

7) Výstup z analýzy a následné šetření

- **Zjištění, které vyplynulo z analýz je to, že každý z nás zpracovává velké množství osobních údajů. Je však potřeba přistoupit k tomuto zpracování velmi svědomitě. Ne každý osobní údaj, který v dnešní době požadujeme, je pro naší práci nutný a potřebný.**
- **Například: když potřebuji pro ztotožnění osoby občanský průkaz, nepotřebuji nikde mít zapsáno jeho číslo, stačí poznamenat, že jsem ověřil dle OP.**
- **Na jednotlivých odborech leží mnoho spisů a dokumentů, které již mohou být skartovány nebo předány do archivu.**

GDPR - CO JSME PODNIKLI

GDPR - CO JSME PODNIKLI

7) Výstup z analýzy a následné šetření

- **Z těchto šetření tedy vyplývá to, že je potřeba skutečně pořádně „UKLIDIT SE STOLU“ . Přebrat dokumenty, které nejsou již potřeba.**

GDPR - FÁZE IMPLEMENTAČNÍ

Zjištění organizačně-technického zabezpečení

- **Zmapování systému přístupů a uzamykatelných prostor v jednotlivých budovách MěÚ a doplnění zámečku na skříně, popř. výměna nábytku za uzamykatelný.**
- **Zjišťování stavu manipulace s klíči a přístupovými kartami – přesný přehled kdo od čeho má klíče a kam se s nimi dostane.**
- **Revize přístupů k EZS (elektronických zabezpečovacích systémů) a EPS (elektronických požárních systémů). Kdo může odkódovat prostory úřadu.**

GDPR - FÁZE IMPLEMENTAČNÍ

Revize souhlasů se zpracováním OÚ

- **V součinnosti s právníkem města provedli vedoucí odborů, samostatných oddělení a městské policie revizi používaných souhlasů se zpracováním osobních údajů**
- **Dále proběhla revize smluv s dodavateli, uzavřenými jednotlivými odděleními a odbory města**
- **Dalším bodem byla revize zpracovatelských smluv s dodavateli, kteří pro město zpracovávají OÚ. V tomto případě se jedná třeba i o firmy, které pro nás poskytují e-learningové školení a vystavují certifikáty z těchto školení.**

GDPR - FÁZE IMPLEMENTAČNÍ

Revize souhlasů se zpracováním OÚ – příklad textu pro Senior dopravu

- Žadatel souhlasí, v souladu s ustanovením zákona č. 101/2000 Sb. v souladu s ustanoveními 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 (obecné nařízení o ochraně osobních údajů - dále v textu jen „Nařízení“), se zpracováním osobních údajů, kterými jsou v tomto případě:
- jméno, příjmení, datum narození, trvalý pobyt, číslo občanského průkazu popřípadě informace
- o zdravotním stavu žadatele (ZTP/ZTP/P),
- pro účely vyřízení žádosti o vydání průkazu SENIOR DOPRAVA CHEB. Zpracováním osobních údajů se dle čl. 4 Nařízení, rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů (shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení). Žadatel prohlašuje, že byl informován o účelu (vyřízení žádosti o vydání průkazu SENIOR DOPRAVA CHEB, včetně prověření žadatele zda vůči němu nemá město Cheb neuhrazené pohledávky po lhůtě splatnosti) a době zpracování osobních údajů (po dobu vyřizování žádosti, případně platnosti následně vydaného průkazu, maximálně po dobu tří měsíců po zániku platnosti předmětného průkazu nebo rozhodnutí o jeho nevydání) a dále i o správci – zpracovateli, který bude s osobními údaji nakládat (město Cheb dále v textu jen „správce“) i o skutečnosti, že uvedený správce má pověřence pro ochranu osobních údajů (Ing. Květa Balgová, e-mail: balgova@cheb.cz, tel.: 354 440 285).
- Tento souhlas byl udělen svobodně a vědomě, po splnění informační povinnosti správcem podle Nařízení. Žadatel výslovně souhlasí s tím, že správce si k této záležitosti vyžádá stanoviska ostatních odborů a oddělení MěÚ Cheb a souhlasí s tím, aby dotčené odbory informace vyžádané správcem (včetně osobních údajů ve výše uvedeném rozsahu a k uvedenému účelu) poskytly.
- Žadatel byl poučen, že může svůj souhlas s poskytnutím osobních údajů odvolat. Odvolání souhlasu musí být písemné. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Žadatel bere na vědomí, že odvolání souhlasu se zpracováním osobních údajů před rozhodnutím o žádosti způsobí okamžité přerušení řízení o žádosti a bude mít za následek záporné vyřízení žádosti, nebo způsobí zánik již vydaného průkazu. V případě nevyřízených závazků žadatele vůči správci může být odvolání souhlasu se zpracováním osobních údajů účinné až od okamžiku vyrovnání všech závazků.

- V Chebu dne: _____ Podpis žadatele: _____

GDPR - FÁZE IMPLEMENTAČNÍ

Vytvoření katalogových listů

- **Každý vedoucí odboru, samostatného oddělení a Městské policie dostali za úkol pro vést revizi jimi zpracovávaných údajů a doplnění údajů: správce / zpracovatel, odpovědná osoba.**
- **Poté byla tabulka opět zkompletována, aby z ní mohlo dojít ke zpracování jednotlivých katalogových listů zpracování OÚ.**

Číslo	Odbor	Kategorie	osoby zprac. OÚ	Poř. číslo	Účel zpracování	Zákonná norma	Kategorie osobních údajů	Kategorie subjektu údajů	Kategorie příjemců	Doba uchování	Způsob uchování	Místo uchování	Uzamykatelné prostory	Zpracovatel / Správce	Zodpovědná osoba

GDPR - FÁZE IMPLEMENTAČNÍ

Vytvoření katalogových listů

Záznam o činnosti zpracování dle článku 30 nařízení GDPR

Datum zpracování: 28.03.2018
Datum aktualizace:

Číslo záznamu	1		
Správce osobních údajů			
Správce osobních údajů	Městský úřad Cheb Náměstí Krále Jiřího z Poděbrad 1/14 350 20 Cheb IČO: 00253979 DIČ: CZ00253979 ID datové schránky: a8gbnyc	**Zástupce správce osobních údajů**	Mgr. Václav Sýkora, MBA Tajemník Městského úřadu Cheb sykora@cheb.cz tel.: 354 440 106
Statutární zástupce	Starosta města, pověřený usnesením Zastupitelstva města	**Odpovědný útvar**	**INF**
Pověřenec pro ochranu osobních údajů	Ing. Květa Balgová	**Zpracovatel/Správce osobních údajů**	**S**
Činnost zpracování			
Název činnosti zpracování osobních údajů	Evidence EZS		
Zodpovědná osoba	Bc. Martin Trnka		
Kategorie subjektu osobních údajů	všichni zaměstnanci		
Kategorie osobních údajů	Jméno, příjmení, titul		

GDPR - FÁZE IMPLEMENTAČNÍ

Vytvoření katalogových listů

Kategorie osobních údajů	Jméno, příjmení, titul
Kategorie příjemců osobních údajů	Odbor INF, na vyžádání odbor ORG
Zpracování osobních údajů pouze v rozsahu nutném pro dosažení primárního účelu	ANO
Předání osobních údajů do třetí země nebo mezinárodní organizaci	NE
Zákonnost zpracování	
Zákonná norma nebo důvod zpracování	
Lhůty	
Doba uchování	po dobu platnosti pracovněprávního vztahu zaměstnance
Místo uložení	
Uloženo kde	DB EZS ústředny

GDPR - FÁZE IMPLEMENTAČNÍ

Aktualizace směrnic MěÚ

- **Projektový tým GDPR vytipoval jednotlivé směrnice, které je nutné aktualizovat.**
- **<u>Jedná se o tyto nejdůležitější směrnice:</u>**
  - **Organizační řád**
  - **Spisový a skartační řád Městského úřadu Cheb a Městské policie Cheb**
  - **Provozní řád objektů, v nichž sídlí Městský úřad Cheb**
  - ***Směrnice pro práci s osobními údaji***
  - **Směrnice k ochraně osobních údajů v kamerovém systému města Cheb**
  - **Zveřejňování informací na oficiálních webových stránkách města Chebu**

GDPR - FÁZE IMPLEMENTAČNÍ

Provedení analýzy rizik IT

- **Vedoucí odboru informatiky ve spolupráci s DPO provedl analýzu rizik pro jednotlivé části informačních systémů.**
- **Rizika byla zvolena dle modelu analýzy MV ČR.**

GDPR - FÁZE IMPLEMENTAČNÍ

Provedení analýzy rizik IT

Město Cheb

Odbor: **Odbor Informatiky**
Jméno: **Bc. Martin Trnka**

Evidenční list rizika

Pojmenování rizika: 1. Informační systém spisové služby

Hodnocení rizika: 1. Vnější útoky 2. Technické chyby 3. Lidský faktor 4. Narušení integrity OÚ 5. Neoprávněný přístup 6. Narušení dostupnosti 7. Ztráta osobních údajů 8. Narušení práv a svobod subjektu údajů.

číslo rizika	Hodnocení rizika		přijatá opatření	Hodnocení po opatření		datum hodnocení	předpokl. termín dalšího hodnocení
	pravděp.	dopad		pravděp.	dopad		
1.	2	3	Zlepšení stávajícího zabezpečení, provedení penetračních testů - Výzva č. 10 Kyberbezpečnost	2	2	18.04.2018	18.04.2019
2.	2	2	Pravidelná instalace aktualizací	2	2	18.04.2018	18.04.2019
3.	3	3	Přechod na přihlášení se synchronizací s AD	2	2	18.04.2018	18.04.2019
4.	2	3	Pravidelné aktualizace systému, provádění nesmazatelných záloh, Výzva č. 10 Kyberbezpečnost	2	2	18.04.2018	18.04.2019
5.	1	3	Přechod na přihlášení se synchronizací s AD	2	2	18.04.2018	18.04.2019

GDPR – A PŘÍSPĚVKOVÉ ORGANIZACE

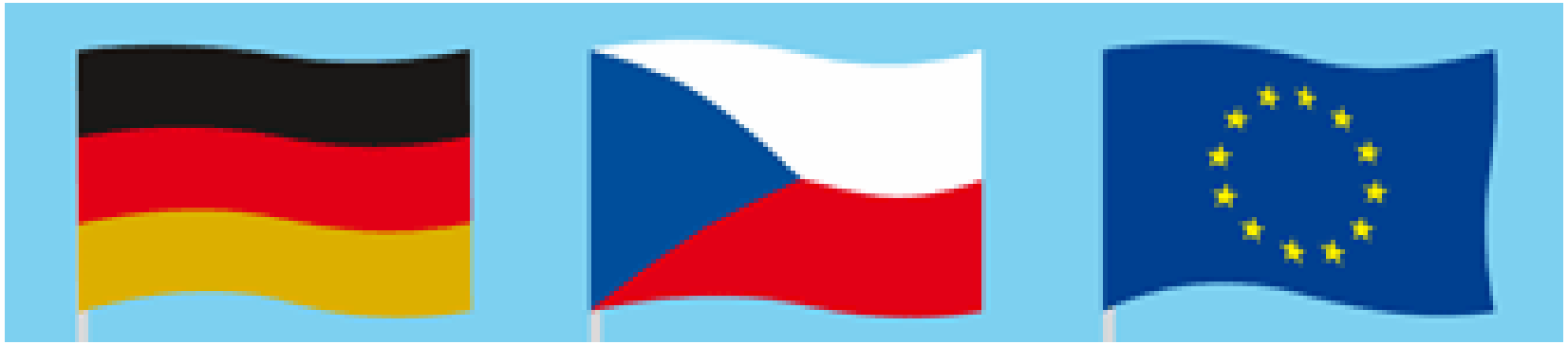
- **Byla zvolena a radou města schválena varianta, že se o naše organizace postaráme a danou problematiku jim pomůžeme vyřešit.**

GDPR – A PŘÍSPĚVKOVÉ ORGANIZACE

Nastavení GDPR v příspěvkových organizacích města

- **Poptávkovým řízením byla vybrána firma, která zpracovává problematiku GDPR na jednotlivých příspěvkových organizacích.**
- **V dubnu 2018 proběhla kompletní analýza v jednotlivých organizacích.**
- **Do konce května by měla být hotova implementace vlastního dle nařízení GDPR.**

GDPR - EXKURZE



GDPR – SPOLEČNÉ, PŘESTO ROZDÍLNÉ

- Návštěva chebského týmu v partnerském městě Hof (Bavorsko)
- Nařízení platí pro celou EU, proto jsme chtěli zjistit stav přípravy u sousedů
  - Zákon existuje na úrovni spolku – připravuje se modifikace zákona roku 1982. Spousta ustanovení je stejná i v nařízení GDPR, myšlenka je stejná.
  - Spolkový zákon je platný pro soukromé podniky a firmy a dále pro spolkové úřady. Bavorský zákon pouze pro veřejnou správu v Bavorsku.
  - Na kontrolu dodržování zákona je stanoven pověřenec na úrovni Bavorska.
  - Pro privátní sféru je definován spolkový kontrolor.
  - Ministerstvo vnitra pro Bavorsko připravuje příručky, metodiky a další návody pro práci s GDPR

GDPR – SPOLEČNÉ, PŘESTO ROZDÍLNÉ

- V Hofu nemají žádnou vnitřní směrnici ani předpis pro implementaci zákona. Zákon je platný a definuje, jak smí být využívány a zpracovány osobní údaje. Tato pravidla jsou dostačující, a proto není nutné tvořit další směrnici. Jednotlivé úřady jsou odpovědné za jeho dodržování.
- Pověřenec pro ochranu osobních údajů:
  - Dává rady
  - Zabývá se kontrolou zákona
  - Vede seznam řízení, kde jsou uvedena veškerá data, včetně lhůt pro výmaz, komu se zprostředkovávají, kdo je zpracovává.
  - Vyřizuje žádosti pro přezkum zpracování osobních z jednotlivých oddělení pro nové případy zpracování.
- V Bavorsku nejsou předpokládány žádné pokuty pro obce.
- Stát má pomáhat, ne pokutovat.
- Každý úřad v Bavorsku má svého pověřence.
- Pro firmy od 10 zaměstnanců je povinný také DPO, v současnosti jej ale nemají a je to pokutováno.

GDPR – POVĚŘENEC V BAVORSKU

- Může to být zaměstnanec interního auditu (IA), určuje si to sám úřad.
- Na oddělení IA je v současnosti 5 zaměstnanců.
- Vedoucí oddělení IA je současně i DPO.
- Při zavádění zabrala tato funkce cca 50 % času, dnes už max. 20 %.
- DPO je potřebný i v případě zavádění nových procesů, zavádění nových aplikací.
- Nadřízeným pracovníkem DPO v Hofu je přímo primátor města.
- DPO města komunikuje s přímo nadřízeným DPO v Bavorsku.
- Zatím ještě DPO neměl potřebu se obracet na kontrolní orgán a hlásit pochybení na úřadě.
- Kontrolní orgán většinou přijde sám na podněty žadatelů.
- DPO se setkávají cca 2x ročně pro výměnu informací.
- Je velmi dobré, když DPO je interní auditor, jelikož má velmi silnou pozici v úřadě a také dobře zná úřad.

GDPR – POUŽITÉ ZDROJE

Ke zpracování prezentace bylo použito:

- **zápisy ze schůzek týmu GDPR MěÚ Cheb,**
- **volně dostupné zdroje MV ČR,**
- **výstup z analýzy GDPR MV ČR,**
- **Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob,**
- **vlastní zkušenosti s aplikací nařízení GDPR do praxe úřadu.**

GDPR – UŽITEČNÉ ODKAZY

Odkazy

- **Modelové situace**
  - http://www.mvcr.cz/gdpr/clanek/modelove-situace.aspx
- **Chatbot GDPR**
  - https://www.spcr.cz/chatbot-gdpr
- **Problematika GDPR na ÚOOÚ**
  - https://www.uoou.cz/gdpr/ds-3938/p1=3938

DĚKUJI ZA POZORNOST

Mgr. Václav Sýkora, MBA, tajemník Městského úřadu Cheb
sykora@cheb.cz