# GDPR a obec

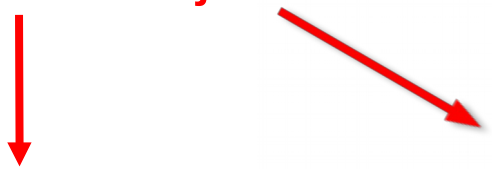
**Praha 12. 3. 2018**

**Mgr. Jan Vobořil, Ph.D.**

iure
...není nám to jedno

# GDPR

Jaké změny přicházejí s GDPR



Ve formě právní regulace

V obsahu právní úpravy

Nová práva a povinnosti

Stará práva a povinnosti nově upravená

# Hlavní novinky v obsahu právní úpravy

» úprava způsobů komunikace se SÚ (čl. 12 – ve vazbě na čl. 13, 14, 15-22, ad.)

» právo na omezení zpracování údajů (čl. 18 GDPR)

» právo na přenositelnost údajů (čl. 20 GDPR)

» právo vznést námitku proti zpracování osobních údajů (čl. 21 GDPR)

» vedení záznamů o činnostech zpracování (čl. 30 GDPR) x zrušena registrační povinnost

» povinné ohlašování případů porušení zabezpečení OÚ – (čl. 33 a 34 GDPR)

» posouzení vlivu na ochranu OÚ (čl. 35 GDPR)

» pověřenec ochrany osobních údajů (DPO) – (čl. 37 - 39 GDPR)

» sankce a náhrada újmy (čl. 82+83+84 GDPR)

# Právní důvod zpracování OÚ

» Každé zpracování OÚ musí být založeno na některém z právních důvodů

» Dnes koncept ZOOÚ **souhlas x výjimky**

» Fakticky dle směrnice i GDPR je souhlas jedním z rovnocenných důvodů

» Důvody zpracování:

1. Subjekt údajů udělil souhlas se zpracováním
2. Zpracování je nutné pro dodržení právní povinnosti správce
3. Zpracování je nezbytné pro plnění úkolu veřejného zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
4. Zpracování je nezbytné pro plnění nebo uzavření smlouvy, jejíž stranou je SÚ
5. Zpracování je nezbytné pro ochranu životně důležitých zájmů SÚ a tento nemůže vyslovit souhlas
6. Zpracování je nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby

» Samostatným důvodem už není, že se jedná o oprávněně zveřejněné OÚ

» Právní důvody nelze dodatečně měnit (např. uplatnit ochranu práv správce, když je problém s platností souhlasu)

» Zvláštní kategorie údajů – zpracování zakázáno – výjimky čl. 9 odst. 2

# Vedení záznamů o činnostech zpracování

(čl. 30)

- Kdy se vedou povinné záznamy:

  1) organizace s více než 250 zaměstnanci

  2) další organizace za podmínek že:

     - Je zde riziko při zpracování pro práva  a svobody SÚ
     - Nejde pouze o příležitostné zpracování
     - Zpracovávají se zvláštní kategorie údajů dle čl. 9 nebo údaje o rozsudcích v trestních věcech dle čl. 10

- Zdroje: Registr práv a povinností, přehledy zákonů dle IZ,
- V záznamech o činnostech zpracován jsou údaje o správci, účely, kategorie SÚ, příjemci, informace o předání OÚ do třetí země, lhůty pro výmaz, obecný popis technických, bezpečnostních a organizačních opatření
- Záznamy se na požádání poskytnou dozorovému úřadu
- Do jisté míry nahrazuje registrační povinnost
- Obce III. Typu – zhruba 160-180 agend v přenesené působnosti (agendy v samostatné působnosti)

# Příprava záznamů o zpracování

» Její zpracování by mělo být základním vstupem

» Analýza se týká klíčových otázek:

1. jaké osobní údaje jsou zpracovávány (co vlastně jsou osobní údaje? zvláštní kategorie údajů),
2. na základě jakých právních důvodů,
3. jakým způsobem jsou zpracovávány
4. kdo se na zpracování podílí
5. jaká pro zpracování platí pravidla (přístup, využívání, předávání dalším subjektům)
6. kdo ze zaměstnanců či externistů za zpracování odpovídá
7. jak jsou údaje zabezpečeny
8. jaká je rizikovost (riziko prolomení zabezpečení, rizika pro SÚ související s úniky)

» formulář záznamu – viz Analýza

# Navazující činnosti

- Úprava interních předpisů a směrnic
  - Co, kdo, kdy a jak?
  - Práva SÚ(např. informace, přístup, výmaz atd.)
  - Zabezpečení
  - Incidenty
- Školení zaměstnanců, kteří pracují s OÚ
- Úprava IT systémů
  - omezení účelem zpracování,
  - minimalizace rozsahu údajů,
  - omezení doby
- Změny smluv – zejména se zpracovateli

# Pověřenec pro ochranu osobních údajů

(čl. 37 - 39)

» Pověřence jmenuje správce i zpracovatel v následujících případech:

1. Zpracování provádí orgán veřejné moci
2. Hlavní činnost správce či zpracovatele spočívá
   A. v rozsáhlém, pravidelném a systematickém monitorování SÚ
   B. V rozsáhlém zpracování zvláštních kategorií údajů nebo údajů týkajících se trestních rozsudků

» Pověřenec nemusí mít formální kvalifikační předpoklady, ale musí mít zkušenosti s OOÚ, s právem a musí být schopen plnit povinnosti dle čl. 39

» Vhodné je, aby měl přiměřené znalosti v oblasti práva, IT technologií i chodu a procesů v organizaci

» Může jít o zaměstnance (i na kratší pracovní úvazek), může jít o spolupráci na základě smlouvy o poskytování služeb, může být jeden pověřenec pro více institucí (např. škol)

» Správce i zpracovatel by měli zveřejnit kontaktní údaje pověřence a sdělit je ÚOOÚ

# Postavení pověřence

» Nezávislost: Pověřenec by neměl dostávat žádné pokyny týkající se plnění úkolů. Nelze v souvislosti s plněním úkolů pověřence propustit či sankcionovat. Jiné úkoly nesmí být ve střetu zájmů

» Správce i zpracovatel musí podporovat pověřence při plnění jeho úkolů, poskytují mu nezbytné zdroje a součinnost. Pověřenec je podřízen vrcholovému vedení.

» SÚ se může obracet na pověřence ve všech záležitostech, které souvisí se zpracováním OÚ

» Povinnost mlčenlivosti bude upravena v implementačním zákoně

# Úkoly pověřence

» Poskytování informací a poradenství o povinnostech – správcům, zpracovatelům, zaměstnancům

» Průběžné monitorování souladu s Nařízením a dalšími předpisy týkajícími se OOÚ.

» Zvyšování odborné přípravy osob, které se podílí na zpracování OÚ

» Spolupráce s ÚOOÚ, působí jako kontaktní místo pro ÚOOÚ

# Zabezpečení OÚ

Správce i zpracovatel musí přijmout taková technická a organizační opatření, aby zajistili vysokou úroveň zabezpečení OÚ

Porušením zákona může být

- Zneužití OÚ třetí osobou (např. hacknutí databází, krádež klientských spisů)
- Zneužití údajů osobami, které k údajům mají přístup (např. zaměstnanci)
- Sdělení údajů neoprávněné osobě (rodinní příslušníci, státní orgány, ztráta či nedostatečná likvidace spisu atd.)

# Zabezpečení OÚ II.

Nastavení zabezpečení v závislosti na

- stavu techniky
- nákladům na provedení
- povaze, rozsahu, kontextu a účelům zpracování
- rizicích (pravděpodobnost zneužití + dopad do práv a svobod)

V závislosti na rizicích může být v různé míře potřebné

- data pseudonymizovat či šifrovat (zejména na externích zařízeních – např. notebooky apod.) – může mít vliv třeba na povinnost oznamovat incidenty
- zajišťovat důvěrnost, dostupnost a odolnost systémů a zpracování
- v případě fyzických či technických incidentů být schopen data obnovit
- pravidelné testování, posuzování a hodnocení přijatých opatření pro zajištění bezpečnosti zpracování

Povinnost hlásit incidenty (ÚOOÚ, SÚ)

# Sankce a náhrada újmy

» Nastupují v případech porušení povinností

» čl. 82 – náhrada škody a nemajetkové újmy pro SÚ ze strany správce či zpracovatele -

» čl. 83 – úprava sankcí za porušení

» Ukládání sankcí - účinné, přiměřené a odrazující

» až 20 mil Euro či 4% ročního celosvětového obratu

» čl. 83 odst. 7 státy mohou stanovit v jakém rozsahu se pokuty vztahují na orgány veřejné moci

- Dle návrhu implementačního zákona 10 mil Kč

» Vedle sankcí je třeba počítat i s nápravnými opatřeními, náklady spojenými s dosažením souladu s právními předpisy

Děkuji za pozornost

voboril@iure.org