

# Dopady GDPR do praxe

## Mgr. Klára Valentová

Praha, 31. 10. 2018

# GDPR v praxi organizace

- GDPR dopadá na veškeré oblasti činnosti organizace
  - zákazníci (současní, bývalí, potenciální)
    - problematika elektronického marketingu (antispamový zákon, e-Privacy nařízení)
  - zaměstnanci (současní, bývalí), uchazeči o zaměstnání
    - problematika sledování zaměstnanců (zákoník práce, zákon o inspekci práce)
  - dodavatelé (současní, bývalí, potenciální)
    - problematika elektronického marketingu
  - další osoby (rodinní příslušníci zaměstnanců, návštěvníci budovy, veřejnost)
- GDPR x ochrana osobnosti (občanský zákoník)

# Postup při implementaci GDPR

- Stanovení odpovědné osoby za implementaci GDPR
  - Primární odpovědnost – statutární orgán
  - Firemní právník, člen vrcholového vedení, vedoucí compliance oddělení nebo interního auditu...
- Sestavení realizačního týmu a jeho proškolení
  - Sestavit seznam oddělení a vybrat jednotlivé zástupce
  - Personalista, obchodní manažer, marketingový manažer, interní právník, IT specialista...
  - Úprava náplně práce
- Stanovení priorit, etap a termínu pro projekt

**Mapování zpracování osobních  
údajů**

**Koncepce ochrany osobních  
údajů**

**Bezpečnostní opatření**

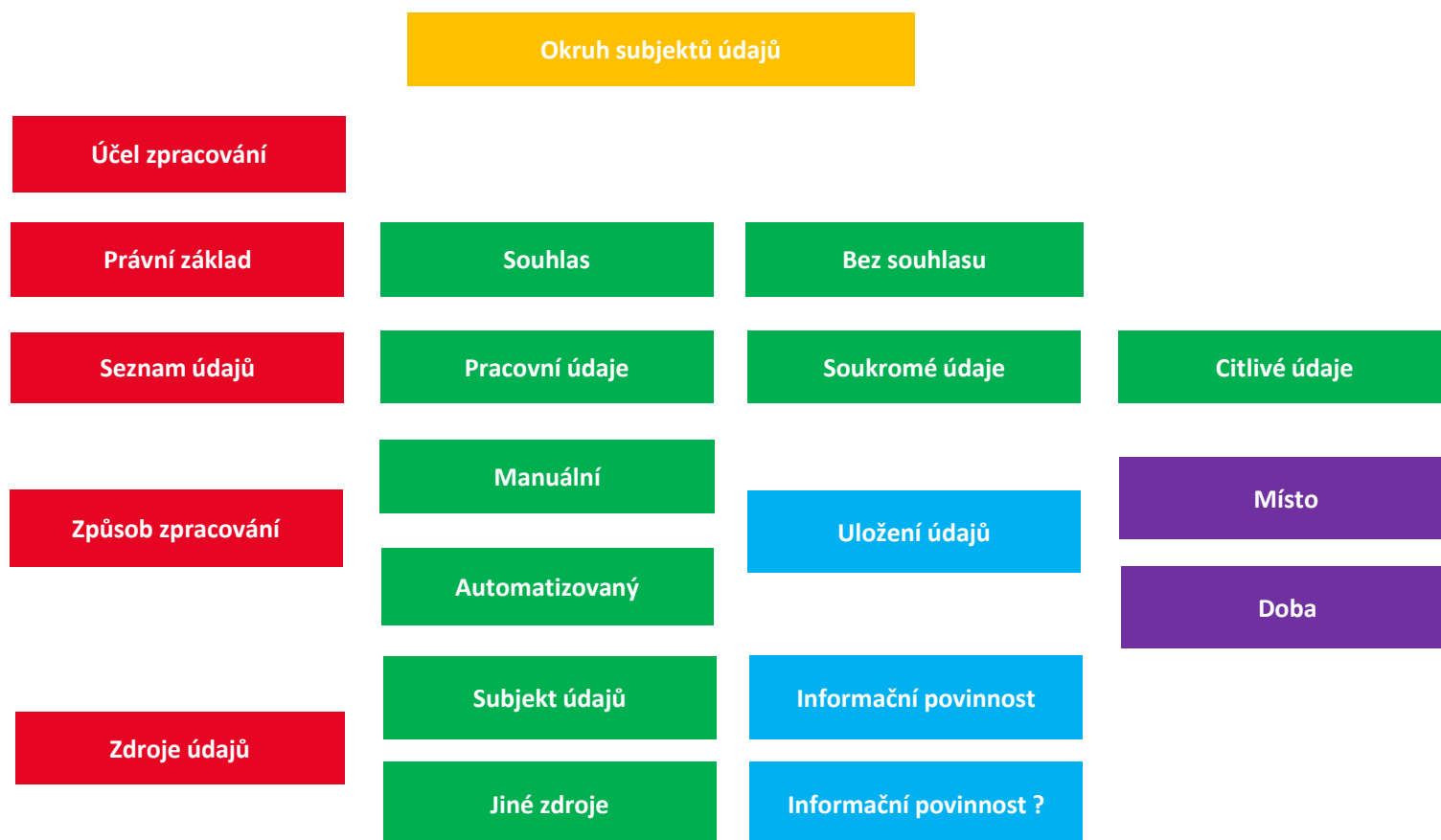
**Revize/příprava dokumentů**

**Nastavení interních procesů**

**Úpravy v IT systému**

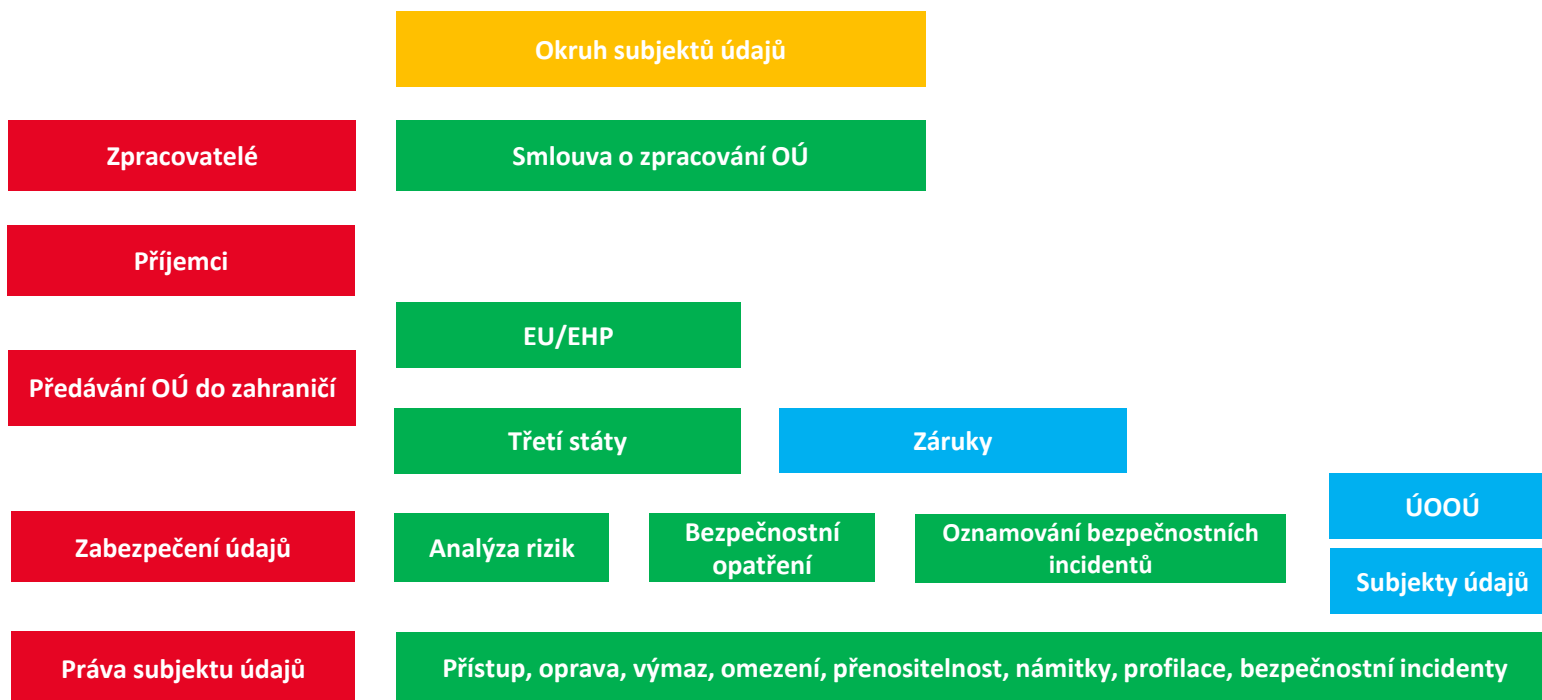
# Postup při implementaci GDPR

## Analýza zpracování osobních údajů – mapování



# Postup při implementaci GDPR

## Analýza zpracování osobních údajů – mapování



# Praktické problémy a chyby

- **Kdy a jak získávat souhlas?**
  - jen když není možnost zpracovávat osobní údaje z jiného právního titulu (např. plnění zákonné nebo smluvní povinnosti)
  - svoboda souhlasu – pozor na souhlas v pracovněprávních vztazích!
- **Jak a kdy plnit informační povinnost?**
  - vždy při získávání osobních údajů od subjektu údajů
  - zatím individuálně ve všech případech
  - pozor na obecná a obsáhlá informační memoranda
  - stručné, srozumitelné a transparentní informace

# Praktické problémy a chyby

- **S kým uzavírat smlouvu o zpracování osobních údajů?**
  - pouze se zpracovatelem
  - ne každý dodavatel je zpracovatel
  - zpracování musí být podle pokynů správce a jeho jménem
- **Co je to přímý marketing a kdy je třeba získávat souhlas?**
  - způsob marketingové komunikace, při které se oslovují zákazníci přímým adresním oslovením (např. e-mailem, poštou, telefonicky nebo i osobně)
  - GDPR – oprávněný zájem správce (bez souhlasu), subjekt údajů má právo na námitku
  - Antispamový zákon – zvláštní pravidla pro elektronický marketing (zákazník x potenciální zákazník)



# Praktické problémy a chyby

- **Lze předávat osobní údaje ve skupině společností?**
  - ano, ale jen pro určitý účel
  - vnitřní administrativní účely – oprávněný zájem – bez souhlasu subjektů údajů
  - postavení jednotlivých společností při zpracování osobních údajů
  - pozor na předávání osobních údajů mimo EHP
- **Co je to oprávněný zájem správce?**
  - v každém případě individuální posouzení
  - balanční test – zájem správce na zpracování osobních údajů převáží nad právy a svobodami subjektu údajů
  - např. provozování kamerového systému z důvodu ochrany majetku

# Praktické problémy a chyby

- **Co jsou to záznamy o činnostech zpracování?**
  - evidence jednotlivých zpracování osobních údajů
  - každý typ (účel) zpracování má svůj evidenční list
  - namísto registrace u Úřadu pro ochranu osobních údajů
  - povinnost platí fakticky pro všechny správce a zpracovatele
- **Musí mít všichni správci pověření?**
  - Ne, pouze všechny orgány veřejné moci a veřejné subjekty
  - Soukromý sektor – pouze výjimečně při splnění stanovených podmínek (např. nemocnice, velké pojišťovny)
- **Co je to posouzení vlivu na ochranu osobních údajů?**
  - zvláštní analýza vyžadovaná u některých rizikových zpracování osobních údajů
  - seznam operací, které nevyžadují posouzení vlivu

# Výkladová pravidla

- Pokyny Evropského sboru pro ochranu osobních údajů (dříve Pracovní skupina 29)
  - Pokyny pro určení vedoucího dozorového úřadu pro správce nebo zpracovatele
  - Pokyny týkající se pověřenců pro ochranu osobních údajů
  - Pokyny týkající se práva na přenositelnost údajů
  - Pokyny k posouzení vlivu na ochranu osobních údajů a ke stanovení, zda zpracování bude „pravděpodobně mít za následek vysoké riziko“
  - Pokyny k automatizovanému individuálnímu rozhodování a profilování podle GDPR
  - Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle GDPR
  - Pokyny k uplatňování a stanovování správních pokut pro účely podle GDPR
  - Pokyny k transparentnosti podle GDPR

# Výkladová pravidla

- Pokyny Evropského sboru pro ochranu osobních údajů (dříve Pracovní skupina 29)
  - Pokyny k souhlasu podle GDPR
  - Pokyny 2/2018 k výjimkám podle článku 49 GDPR
  - Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti
- Zdroj: <https://www.uoou.cz/pokyny-sboru/ds-4728/p1=4728>
- Metodická doporučení ÚOOÚ

# e-Privacy nařízení

- Návrh nařízení EU o soukromí a elektronických komunikacích
- Účinnost – 2019?
  
- Nová pravidla pro využívání cookies
- Nová pravidla pro elektronický marketing (spamming)

# Dotazy?



**Mgr. Klára Valentová, advokát  
Vilímková Dudák & Partners,  
advokátní kancelář, s.r.o.**

Karolinská 661/4, 186 00 Praha 8

Tel.: +(420) 222 814 911

Fax: +(420) 222 814 915

[klara.valentova@vilimkovadudak.cz](mailto:klara.valentova@vilimkovadudak.cz)

[www.vilimkovadudak.cz](http://www.vilimkovadudak.cz)

Děkuji za pozornost!

© 2018 Mgr. Klára Valentová

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání

Střelničná 1861/8a, Praha 8

tel: +420 251 115 576

fax: +420 251 512 422

[office@forum-media.cz](mailto:office@forum-media.cz)

[www.forum-media.cz](http://www.forum-media.cz)