KPMG

GDPR

Dopady na business procesy a IT

Eva Štumpfová, Radek Koudela
KPMG Česká republika
Praha, 28. února 2017

GDPR – celofiremní aktivita

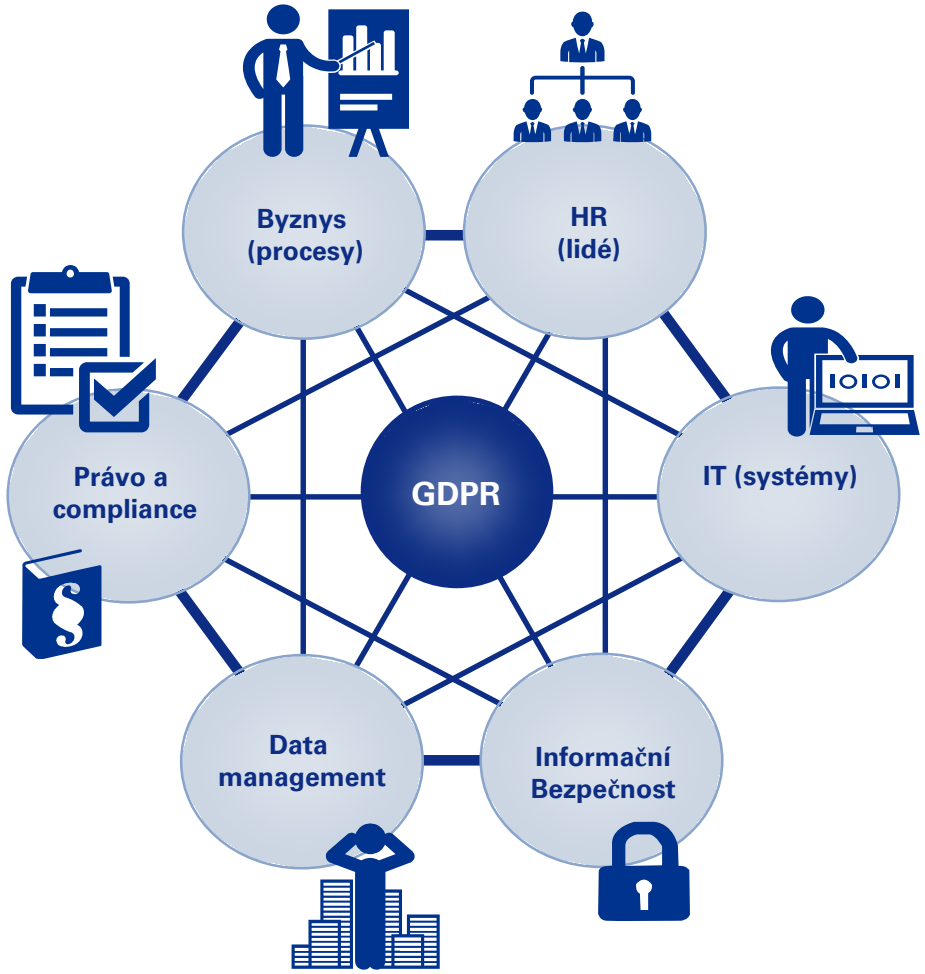
- **Přesah přes různá oddělení – je třeba řešit spíše projektově**
- **Zpracování automatizované i manuální**
- **Všechny „druhy“ osobních údajů včetně pseudonymizovaných (identifikovaná i identifikovatelná fyzická osoba)**

— Všechny druhy médií: electronická, papírová, video, hlas

— Všechny zainteresované strany: zaměstnanci, zákazníci, dodavatelé

— Všechny lokality, pobočky, třetí strany

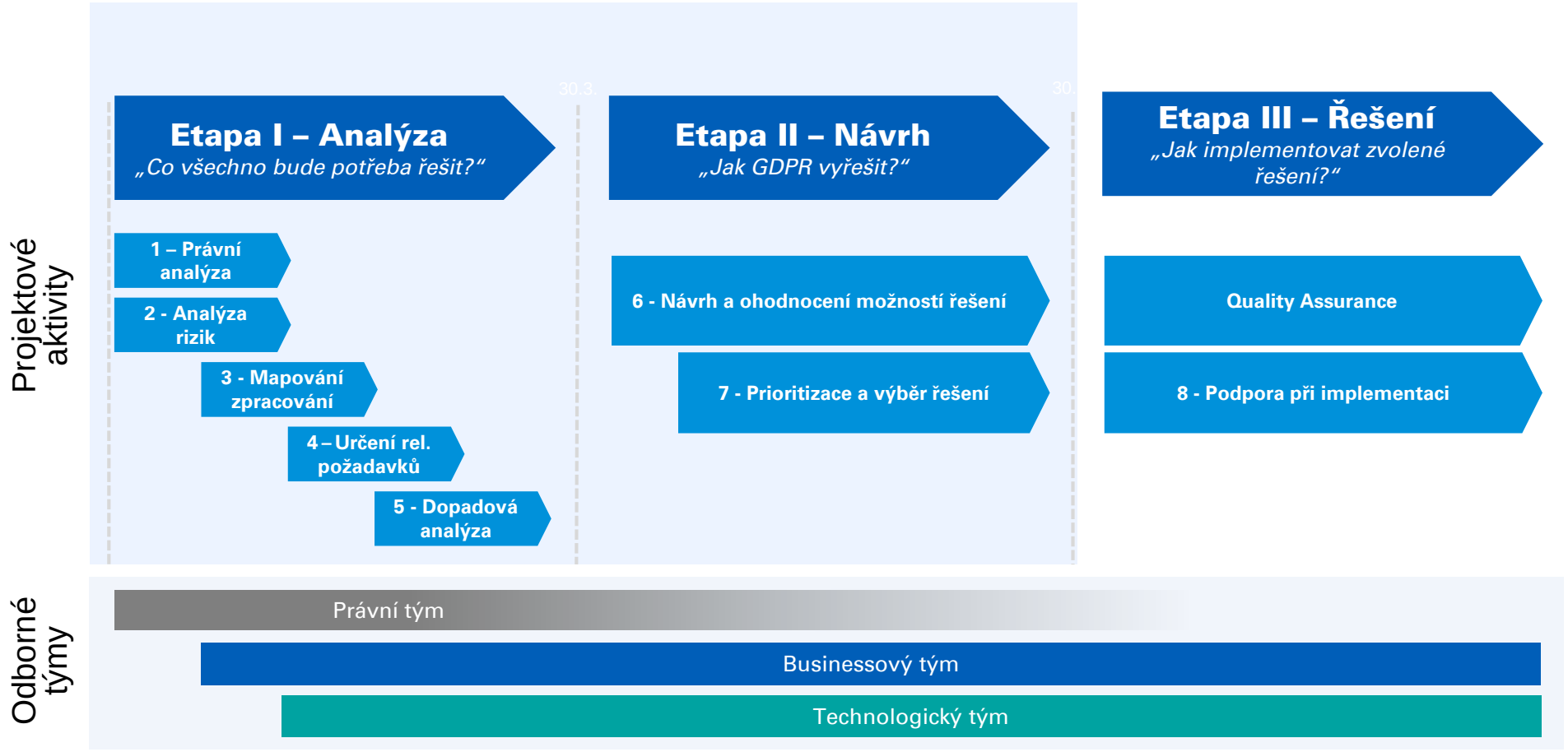
- **Rizika:**
  - Finanční – business
  - Reputační, negativní publicita
  - Smluvní
  - Právní a regulatorní



KPMG

Náš přístup k implementaci GDPR

Obecná metodika - standardní projekt



Přístup KPMG – compliance vs. příležitost

- KPMG chápe GDPR nejen jako právní a compliance aspekt, ale vzhledem ke znalosti procesů a podnikání klientů jsme přesvědčeni, že lze využít tuto regulaci jako business příležitost
- Nejen checklist
- Navázání na úspěšné projekty NOZ a MCD – stejný koncept
- Využití zkušeností ze zemí, které začaly řešit dříve

GDPR není pouze restriktivní, ale podporuje usnadnění (a zároveň zabezpečení) přenosu osobních údajů

- Příklad 1) Zlepšení kvality dat v důsledku GDPR – možnost jejich dalšího, efektivnějšího a účelnějšího využití pro byznys rozhodnutí
- Příklad 2) Přenositelnost dat – velká příležitost pro snadnější přechod klientů, nabízení dalších služeb
- Příklad 3) …

Přístup KPMG – Data Protection Framework

ZDROJE OSOBNÍCH ÚDAJŮ

Organizace získává osobní údaje od různých subjektů. Způsob získání a zpracování osobních údaje se pak liší dle business potřeby.

Při zpracování impakt analýzy vyjdeme z existujících projektových streamů a zajistíme, že se na žádný aspekt nezapomene.

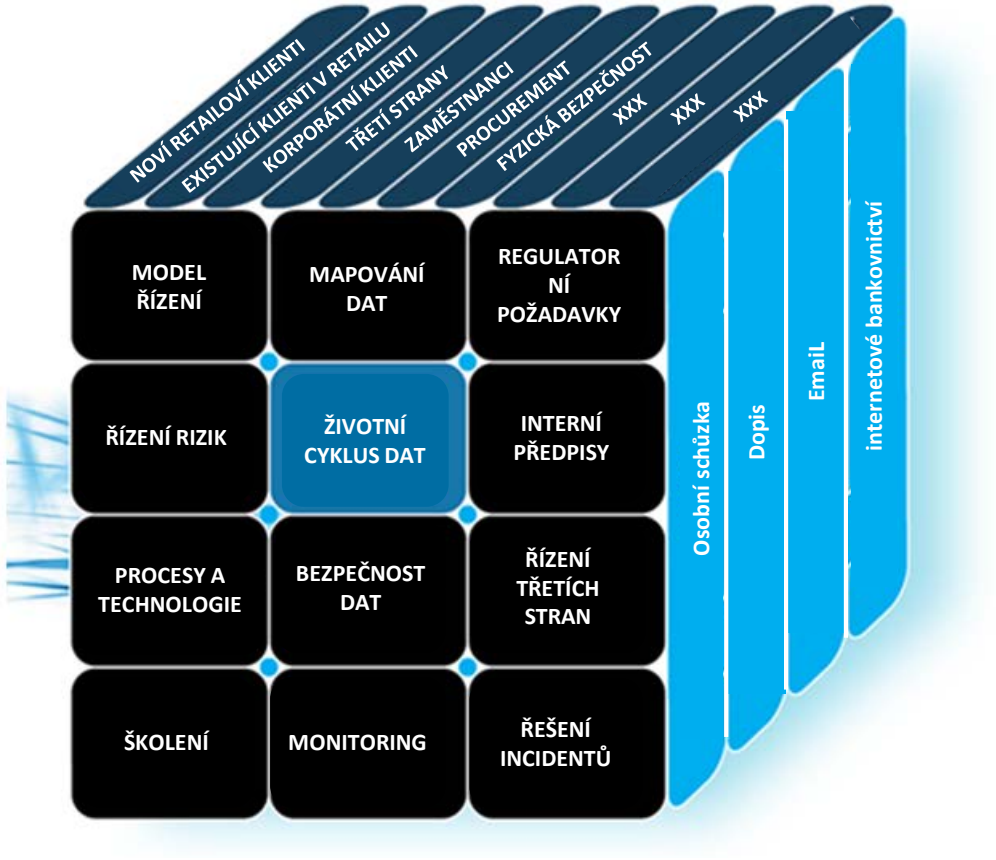
ZPŮSOB ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ

Při zpracování impakt analýzy budeme respektovat kanály, prostřednictvím kterých ČS sbírá osobní data.

RÁMEC PRO ŘÍZENÍ OCHRANY OÚ

Analýzu vypracujeme s ohledem na všechny aspekty řízení ochrany osobních údajů a soukromí v souladu s požadavky GDPR.

Identifikujeme dopady do jednotlivých komponent rámce pro řízení ochrany osobních údajů, které následně poskytnou praktickou a pragmatickou strukturu pro každodenní řízení a dohled nad ochranou osobních údajů.

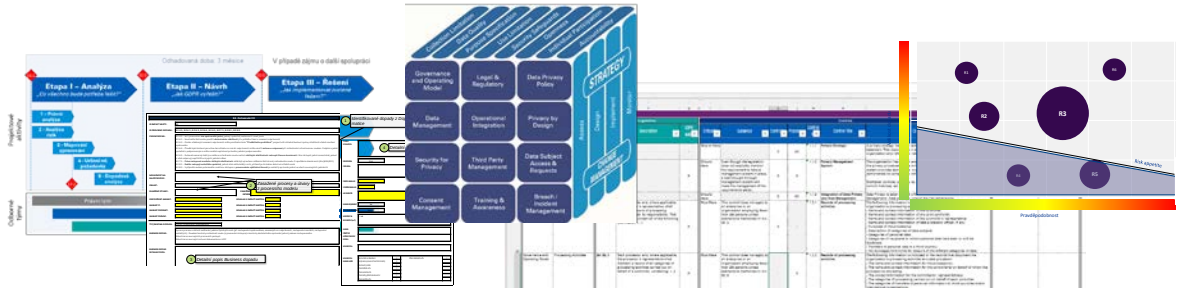


KPMG

KPMG aktiva pro GDPR

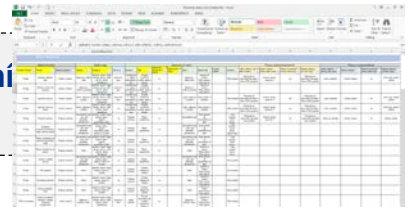
KPMG aktiva a akcelerátory pro GDPR

Metodika KPMG, Data Privacy Framework

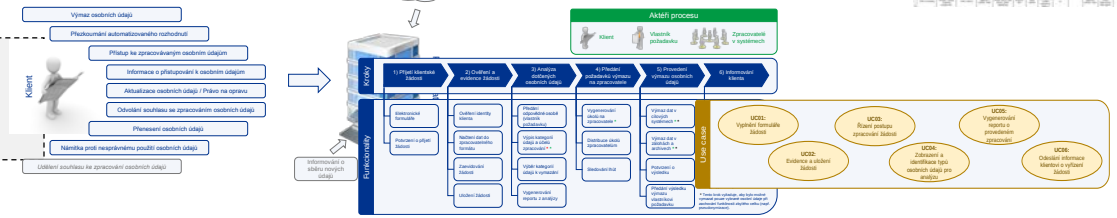


Referenční dopadová matice GDPR

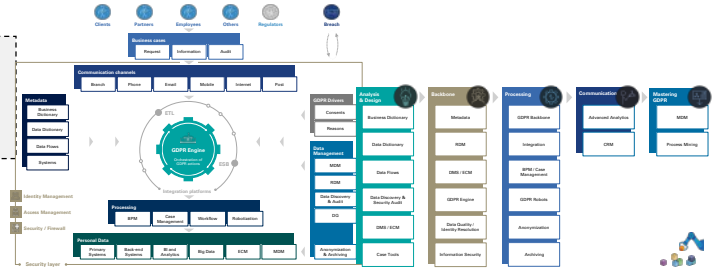
Referenční mapa zpracování osobních údajů



Návrh obslužných procesů, funkcionalit a datového modelu pro obsluhu GDPR agend



Architektura GDPR nástrojové podpory



Interní audit GDPR

— Nutnost pro interní auditory seznámit se s požadavky GDPR a riziky, kterým je organizace v souvislosti s GDPR vystavena

Schopnosti:

— Má náš interní audit odpovídající schopnosti a znalosti (ochrana osobních údajů, právo, IT)?

— Máme připravené nástroje pro auditování GDPR?

— Máme jistotu, že je organizace schopna odhalit incident související s osobními údaji?

Strategie:

— Je ochrana osobních údajů zařazena do auditního plánu?

— Máme zmapovaná rizika plynoucí z GDPR, víme jaké kontroly jsou nejdůležitější?

Role IA:

— Nutnost implementovat robustní kontroly a opatření. Interní závislost na IA pro odhalení rizik a kontrolních neefektivit týkajících se GDPR. Klíčová role IA v prevenci vysokých pokut a dalších hrozeb

Nástroje pro interní audit GDPR

a) **Quick scan a zhodnocení vyspělosti – Privacy maturity assessment (obdoba CMM – zhodnocení procesů na škále 1-5)**

b) **GDPR katalog kontrol**

Data Privacy Framework - Control Catalog

Section		Legislation			Controls						
Domain	Sub Domain	Article	Description	GDPR audit	Criticality	Guidance	Controller	Processor	Control N°	Control Title	Control Description
Data Subject Access & Requests	Right to Restriction of Processing	Art. 18	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: […]	X	Must Have	-	X	-	9.3.1	**Procedures for the Restriction of processing of personal data**	Procedures are in place to timely and adequately respond to requests and execute the restriction of processing of their personal information.
Data Subject Access & Requests	Right to Object	Art. 21	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on those	X	Must Have	-	X	-	9.4.1	**Procedures for the Objection of the processing of personal information**	Procedures are in place to timely and adequately respond to requests from data subjects to object to the processing of their personal information.
Data Subject Access & Requests	Right to Rectification	Art. 16	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. […]	X	Must Have	-	X	-	9.5.1	**Procedures for the Rectification of personal data**	Procedures to, in a timely and adequately manner, respond to requests from data subjects to update or correct their personal data.
Data Subject Access & Requests	Right to Erasure	Art. 17, 1	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: […]	X	Must Have	-	X	-	9.6.1	**Procedures for the Erasure of personal data**	Procedures are in place to provide individuals the right to erasure where one of the following grounds applies: - the personal data are no longer necessary; - the data subject withdraws consent; - the data subject objects to the processing; - the personal data have been unlawfully processed; - the personal data have to be erased for compliance with a legal obligation;

IT Aktivity vyplývající z implementace GDPR

Pořízení souhlasu

Změny v IT prostředí

- Front-end úpravy (systémy, el. kanály)
- Úpravy workflow
- Sign-pady
- Integrace do datového úložiště
- Úpravy aplikačních rozhraní
- Evidence souhlasů a žádostí o úpravy

Evidence

- Evidence souhlasů a žádostí o úpravy

Mapování dat

Master Data Management

- IT architektura
- Business architektura – Profilování
- Klasifikace a segmentace
- Unifikace záznamů, business pravidla

Evidence kontextuálních informací

- Historie
- Vlastnictví
- Přístupy
- Data (platnosti)
- Pravidla archivace

Podpůrné komponenty

- Datový katalog
- Data Profiling Tool
- DQ katalog
- Business slovník

Analýza dopadů, bezpečnost

Nástroj pro monitoring

- Kontrola využití dat a souhlasu
- Integrace nástroje a systémů
- Monitoring a hodnocení ICT architektury
- Proces klasifikace

Řízení rizik a incidentů

- Evidence a klasifikace
- Scénáře zneužití
- Vyhodnocení, alerty a nápravná opatření

Case management

- Hlášení incidentů
- Správa požadavků a změn
- Výmaz dat

Jste připraveni na GDPR?

- Víte, pro jaké vaše produkty potřebujete souhlasy se zpracováním osobních údajů?
- Jaké osobní údaje skutečně potřebujete zpracovávat?
- Kde (v jakých systémech) jsou tyto osobní údaje uloženy?
- Máte správně nastaveny procesy spouštěné klientem?
- Jak jsou zabezpečeny systémy v nichž jsou osobní údaje uloženy a zpracovávány?
- Mohou s těmito osobními údaji pracovat jen zaměstnanci, kteří je potřebují ke své práci?

Eva Štumpfová
Senior Manager

Kontakt:
T +420 222 123 746
M +420 724 734 573
estumpfova@kpmg.cz

Radek Koudela, CISA, CRISC
Associate Manager

Kontakt:
T +420 222 123 624
M +420 607 256 537
rkoudela@kpmg.cz