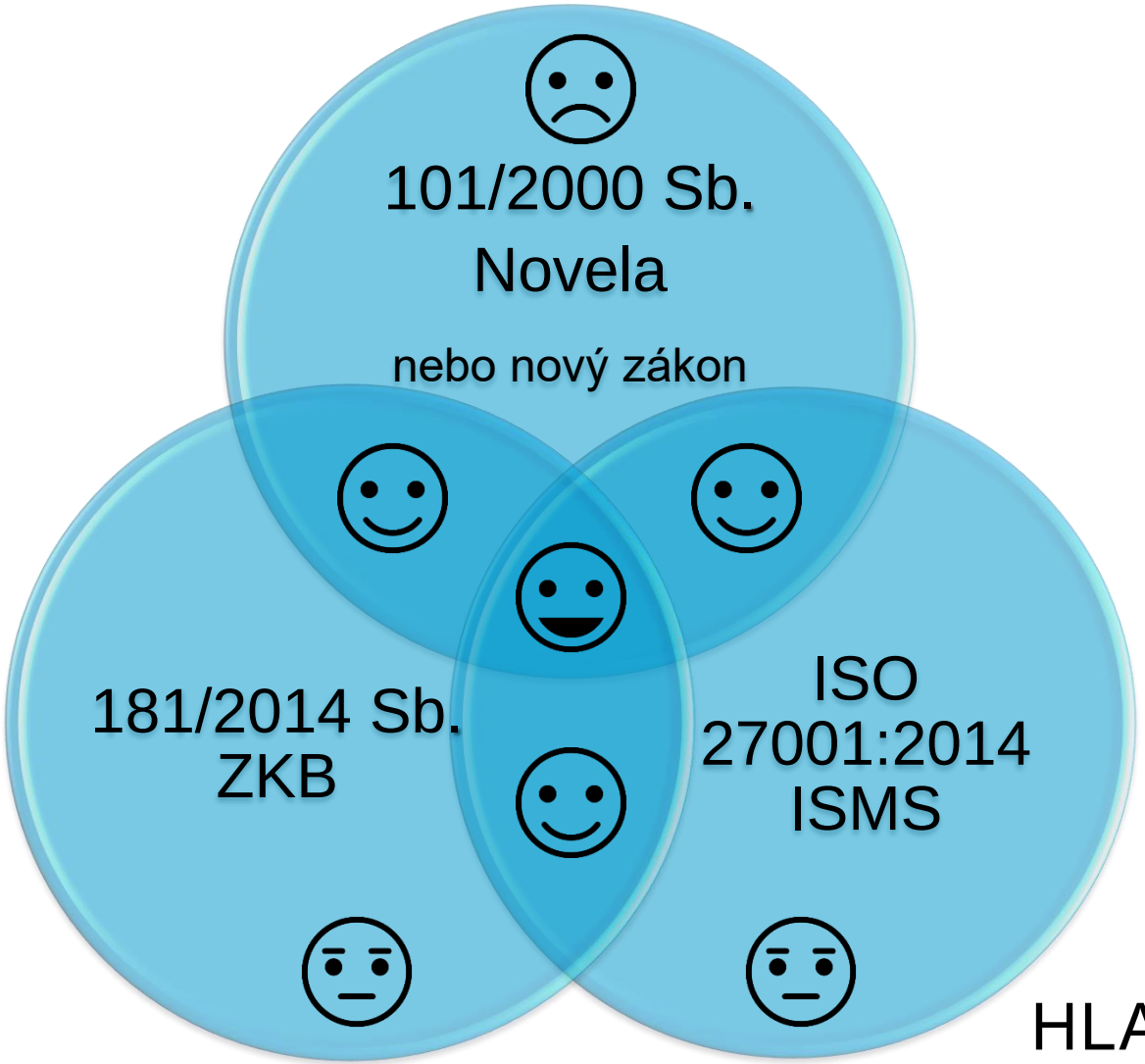
GDPR – příklad z praxe

MICHAL KOPECKÝ

TAJEMNÍK ÚMČ P2

VYUŽITÍ EXISTUJÍCÍCH SYSTÉMŮ



ICT

- Řízení přístupu
- Ukládání dat
- Logování
- IDS/IPS
- SIEM/SOC
- Kryptografie
- Sítě
- Mobilní zařízení
- Fyzická bezpečnost ICT
- Zálohování
- Antivirová ochrana
- Řízení kontinuity
- CCTV
- …

PROCESY

- Pořizování OÚ
- Odstraňování OÚ
- Změny OÚ
- Přenos OÚ
- Hlášení incidentů
- Pověřenec pro ochranu osobních údajů
- Posouzení vlivu na ochranu OÚ
- Spolupráce s dozorovým úřadem
- …

PRÁVNÍ

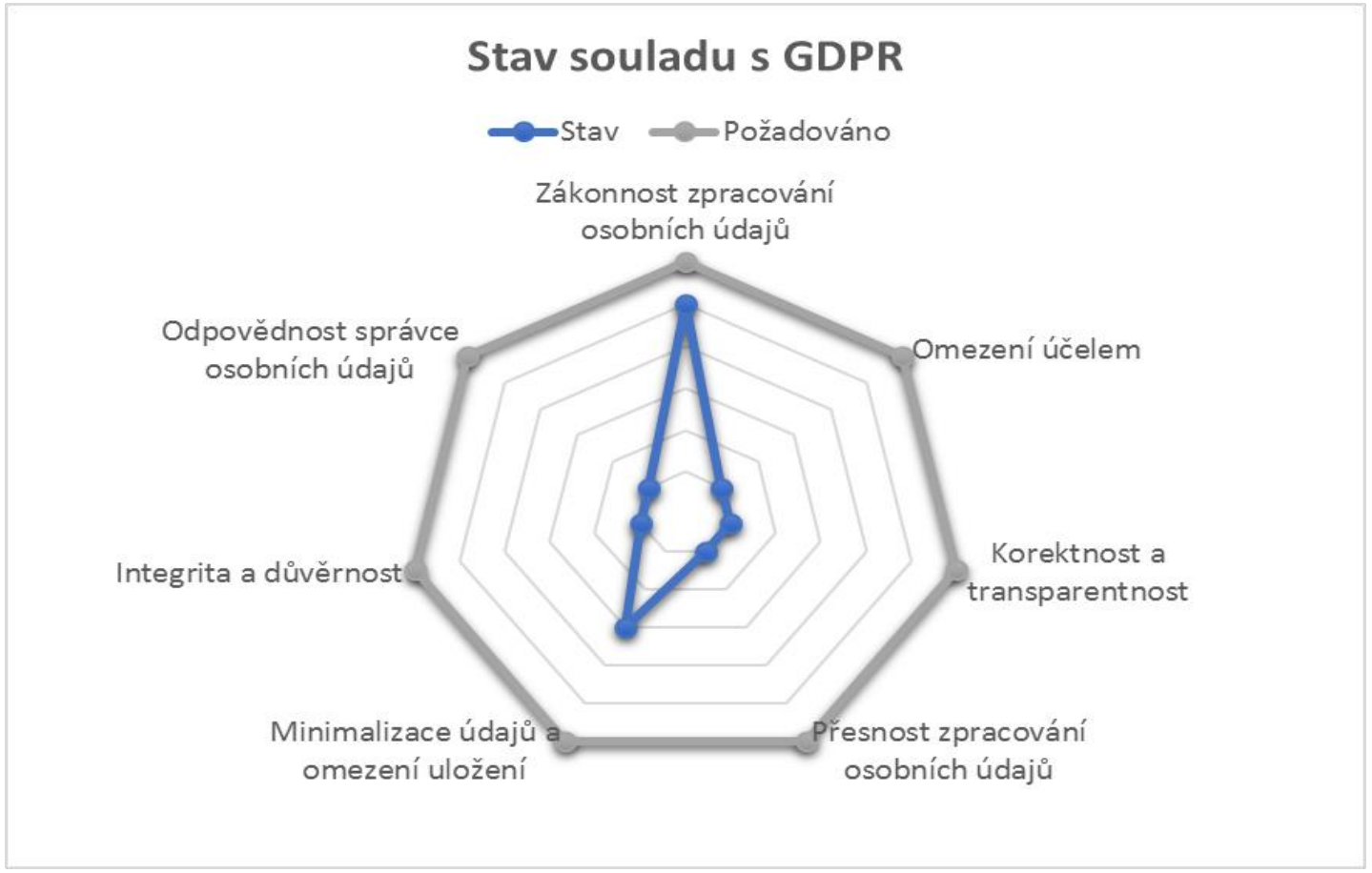
- Souhlas subjektů
- Zaměstnanecké smlouvy
- Smlouvy s dodavateli
- Smlouvy se zpracovateli OÚ
- NDA
- …
- …

HLAVNÍ OBLASTI DOPADU **GDPR**

Klasický POSTUP DOSAŽENÍ SOULADU S **GDPR**

Stanovení rozsahu	Srovnávací analýza	Analýza rizik	Plán opatření	Implementace opatření	Kontrolní audit
• Legislativní rozsah • Organizační rozsah • ICT rozsah • Fyzický rozsah • Odpovědnost za GDPR projekt • Odhad náročnosti • Školení	• Analýza stavu plnění právních, procesních a technických požadavků GDPR	• Analýza rizik bezpečnosti informací/OÚ • Prioritizace • Posouzení vlivu	• Plán opatření • Harmonogram • Nároky na zdroje • Interní/Externí • Součinnost	• Změny dokumentace dle právních základů zpracování • Obsazení rolí • Změny procesů zpracování OÚ a procesů souvisejících • Přijetí ICT opatření • Školení	• Ověření plnění požadavků GDPR interním/externím auditem

SROVNÁVACÍ ANALÝZA
(graf budoucích požadavků)



NEJČASTĚJŠÍ NESHODY

Neznalost rozsahu zpracovávání osobních údajů

kde jsou uloženy, jak jsou zpracovávány, na základě jakých právních základů

Paušální časově nekonkrétní souhlasy

Neschopnost adekvátně reagovat na požadavky subjektů údajů

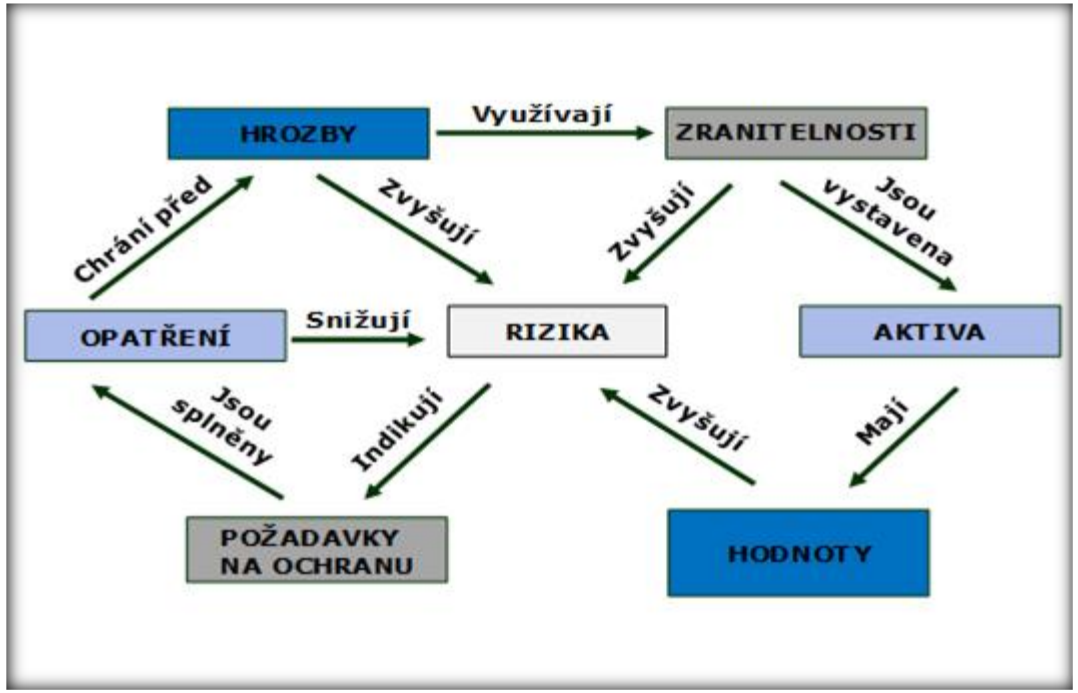
Nejednotná pravidla pro uzavírání smluv

Neexistence záznamů

Neexistující nebo zastaralá dokumentace

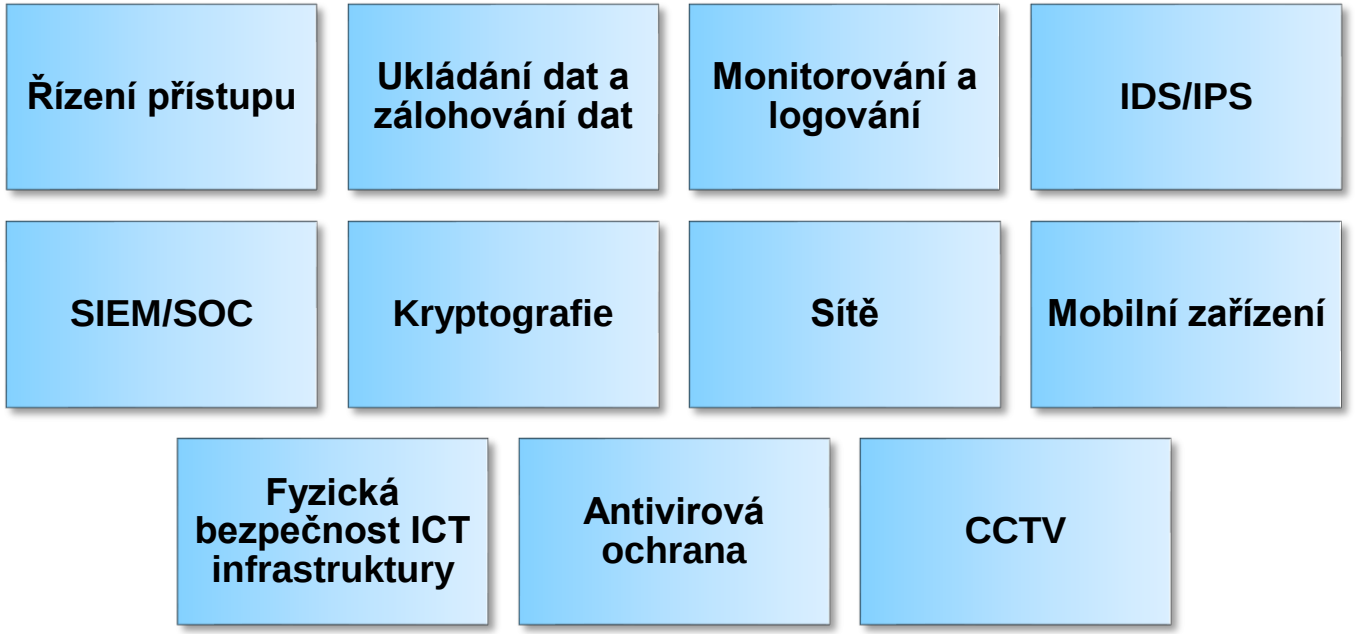
POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

- Jedním z klíčových požadavků GDPR je provádět posouzení nezbytnosti a přiměřenosti operací zpracování osobních údajů z hlediska účelů a posouzení rizik pro práva a svobody subjektů údajů.
- GDPR přímo stanoví i odpovědnosti za takové posouzení v rámci organizace a předpokládá se, že se bude jednat o jednu z **nejvíce kontrolovaných povinností**.



NÁVRH ICT OPATŘENÍ

- Změna infrastrukturu informačního systému organizace tak, aby byla schopna realizovat technická opatření nezbytná pro naplnění požadavků GDPR.



ROLE POVĚŘENCE

GDPR pro obsazení role Pověřence stanovuje, že *"…musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39."*, což obnáší:

- znalost národního a unijního práva v oblasti ochrany dat a hluboké znalosti Obecného nařízení (GDPR)
- praktické zkušenosti aplikace požadavků ochrany dat
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat
- znalost dané oblasti podnikání a organizace
- schopnost propagovat kulturu ochrany dat v organizaci

- Výkon Pověřence je možno řešit plně dodavatelsky

  ale ! :

- **Odpovědnost** je nepřenositelná a zůstává vždy na organizaci

DOPADY PODLE STRUKTURY ORGANIZACE

- **Vedení**
  - Umístění odpovědnost za GDPR
  - Vytvoření pracovní skupiny
  - Přidělení zdrojů
  - Podpora projektu
- **Právní**
  - Analýza právních základů
  - Re-design smluvní dokumentace
- **Personální**
  - Změny v personálních procesech a dokumentaci
- **ICT**
  - Provedení datové analýzy
  - Přijetí technických opatření
- **Bezpečnost**
  - Revize bezpečnostní dokumentace
  - Proces řízení incidentů
  - Analýza rizik a posouzení vlivu
- **Ostatní odbory**
  - Provedení procesní analýzy

Máme řešení?

Vstupní analýza

listopad 2017

- Časová
- Finanční
- Personální

Stanovení pověřence

listopad 2017

- Interní audit
- Součástí týmu pro analýzu
- Včetně příspěvkových organizací

Srovnávací analýza

únor 2018

- Procesní analýza
- Právní analýza
- Analýza dat a bezpečnost
- Plán dosažení souladu s GDPR

ISO 27 001 : 2014

březen 2018

- Implementace nápravných opatření
- Nastavení identifikátorů GDPR
- Definování překrytu 90/10

Finále

- Je chybou vyrábět teorie dřív, než jsou shromážděna všechna fakta. *Sir Arthur Ignatius Conan Doyle*
- *Ale i:*
- Evansův zákon: jestliže zůstáváš klidný, zatímco ostatní ztrácejí hlavu, je to neklamná známka toho, že jsi problém nepochopil.
- *Prakticky by však mělo platit:*
- *Nikdo z nás si nemůže dovolit investovat do řešení této směrnice více než je potřeba, někteří ji vidí jako bublinu, která je uměle živena těmi, kteří v tom vidí dobrý obchod, ale takhle to pro veřejnou správu myšleno nebylo.* Náš předpoklad naplnění Nařízení EU k GDPR je částka do velikosti malého rozsahu!