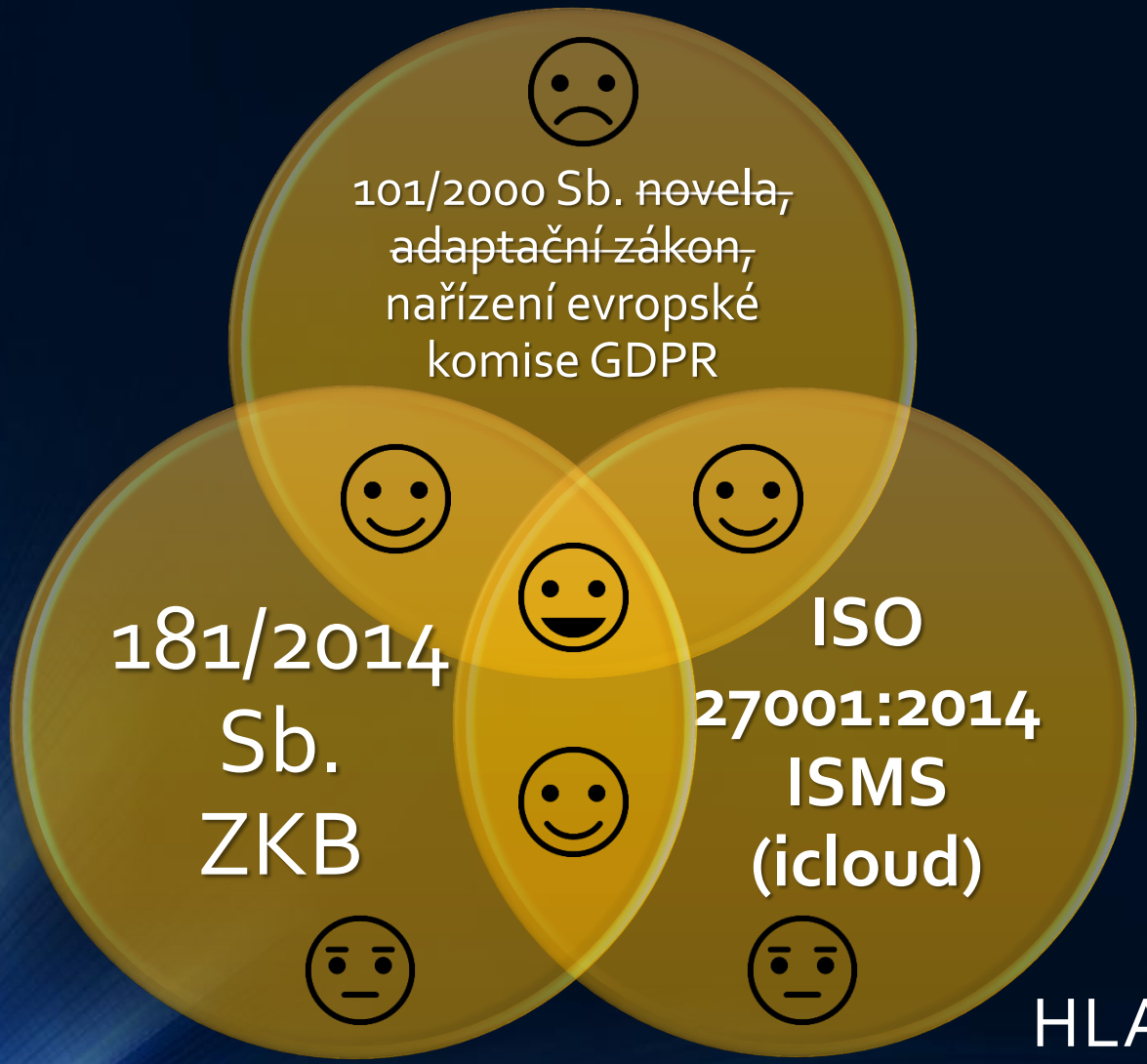
GDPR - *příklad z praxe*

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**

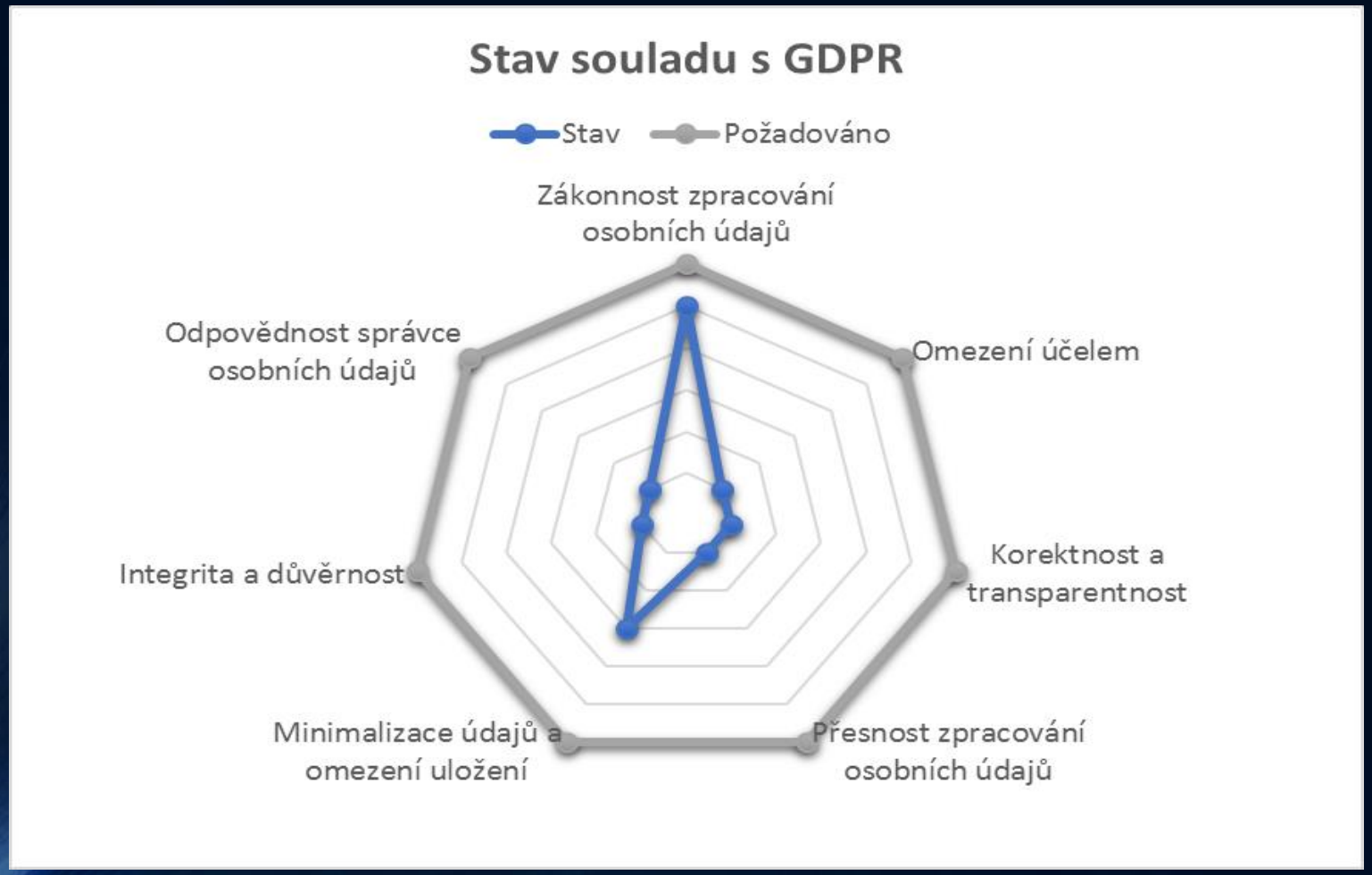
Stanovení rozsahu	Srovnávací analýza	Analýza rizik	Plán opatření	Implementace opatření	Kontrolní audit
• Legislativní rozsah • Organizační rozsah • ICT rozsah • Fyzický rozsah • Odpovědnost za GDPR projekt • Odhad náročnosti • Školení	• Analýza stavu plnění právních, procesních a technických požadavků 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

ANALÝZA RIZIK

WP248, iso29151, iso29134

40.474

SROVNÁVACÍ ANALÝZA
(graf budoucích požadavků)



NEJČASTĚJŠÍ NESHODY

Neznalost rozsahu zpracovávání osobních údajů

kde jsou uloženy, jak jsou zpracovávány, na základě jakých právních základů, ukládají se déle než je nutné

Paušální časově nekonkrétní souhlasy

Neschopnost adekvátně reagovat na požadavky subjektů údajů

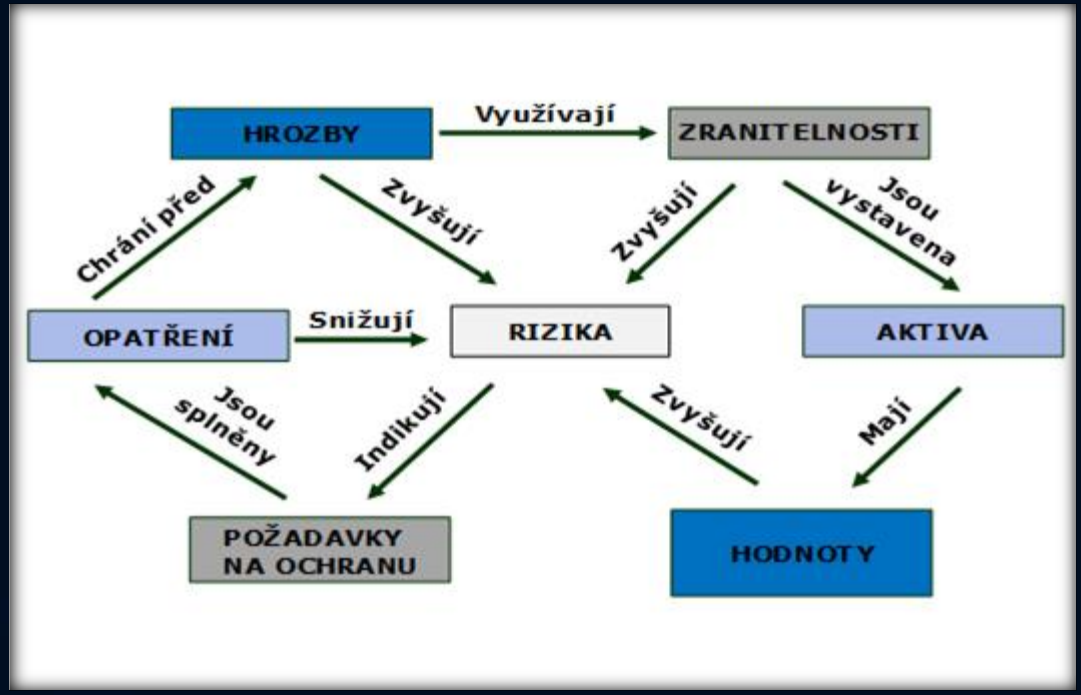
Nejednotná pravidla pro uzavírání smluv

Neexistence záznamů

Neexistující nebo zastaralá dokumentace

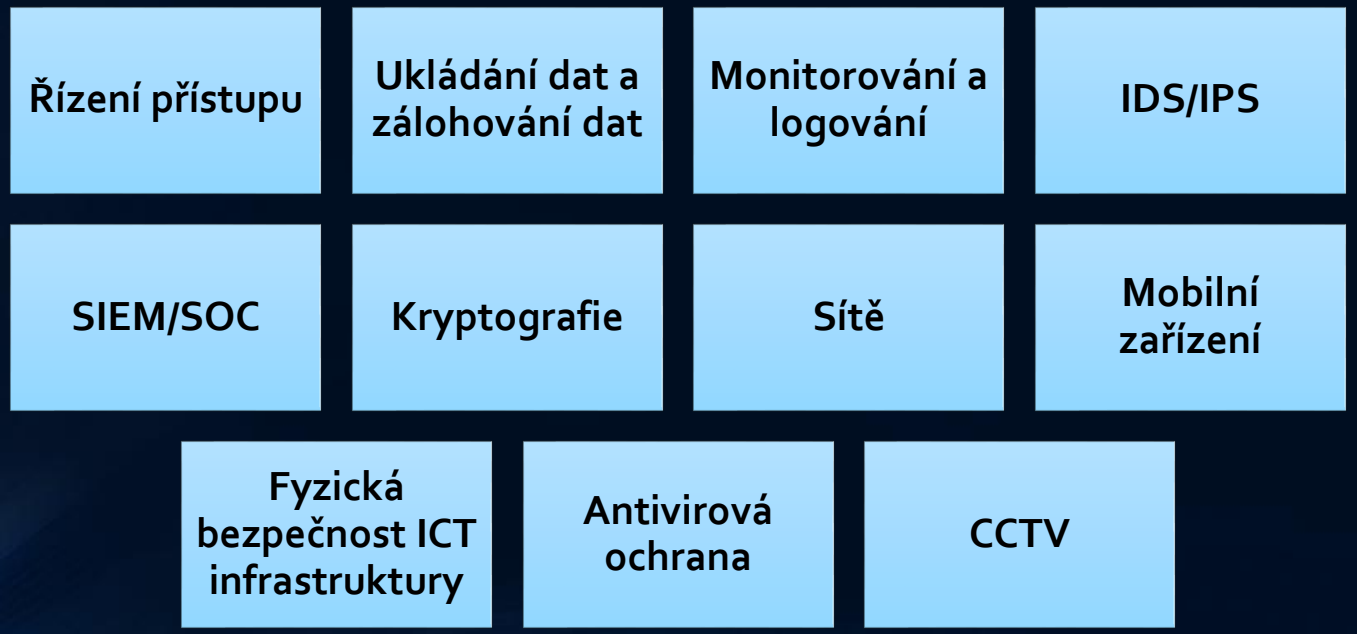
POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

- 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**.
- Nástroj pro řízení rizik pro práva subjektu údajů



NÁVRH ICT OPATŘENÍ

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



ZMĚNY SMLUV A JINÝCH PRÁVNÍCH UJEDNÁNÍ

- GDPR se dotýká se vztahů s občany, dodavateli, kontrolními orgány a dalšími stranami.
- Změny ve smluvních a dalších právních vztazích prováděné v rámci dodažení shody s požadavky GDPR mohou zahrnovat například:
  - Souhlas subjektů údajů
  - Zaměstnanecké smlouvy
  - Smlouvy se zpracovateli OÚ
  - Smlouvy s dodavateli služeb a servisními organizacemi
  - Smouvy o zachování důvěrnosti informací
    a další

ROLE POVĚŘENCE

- Pověřenec musí být organizací jmenován, pokud:
  - zpracování provádí **orgán veřejné moci či veřejný subjekt** (bez ohledu na to, jaká data jsou zpracovávána)
  - hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, rozsahu nebo účelu, vyžadují **rozsáhlé pravidelné a systematické monitorování subjektů údajů**
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém **zpracování zvláštních kategorií údajů** a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

DOKUMENTY K GDPR

interní směrnice pro soulad s GDPR	souhlas se zpracováním osobních údajů /zrušením	informace poskytované subjektu údajů	potvrzení o zpracování osobních údajů	oznámení o opravě, výmazu nebo omezení zpracování OÚ
upozornění na zrušení omezení zpracování	oznámení o porušení zabezpečení subjektu údajů	informace o neschopnosti identifikovat subjekt údajů	informace o důvodech nepřijetí opatření vyžádaných subjektem údajů	předání osobních údajů subjektu údajů pro případ přenosu údajů jinému správci
upozornění na právo vznést námitku	souhlas s předáním osobních údajů do třetí země	oznámení o porušení zabezpečení dozorovému úřadu	balanční test	dokumenty upravující vztah s třetími stranami – zpracovatelská smlouva

činnosti pro příspěvkové organizace.	vypracování posouzení vlivu (DPIA).

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:

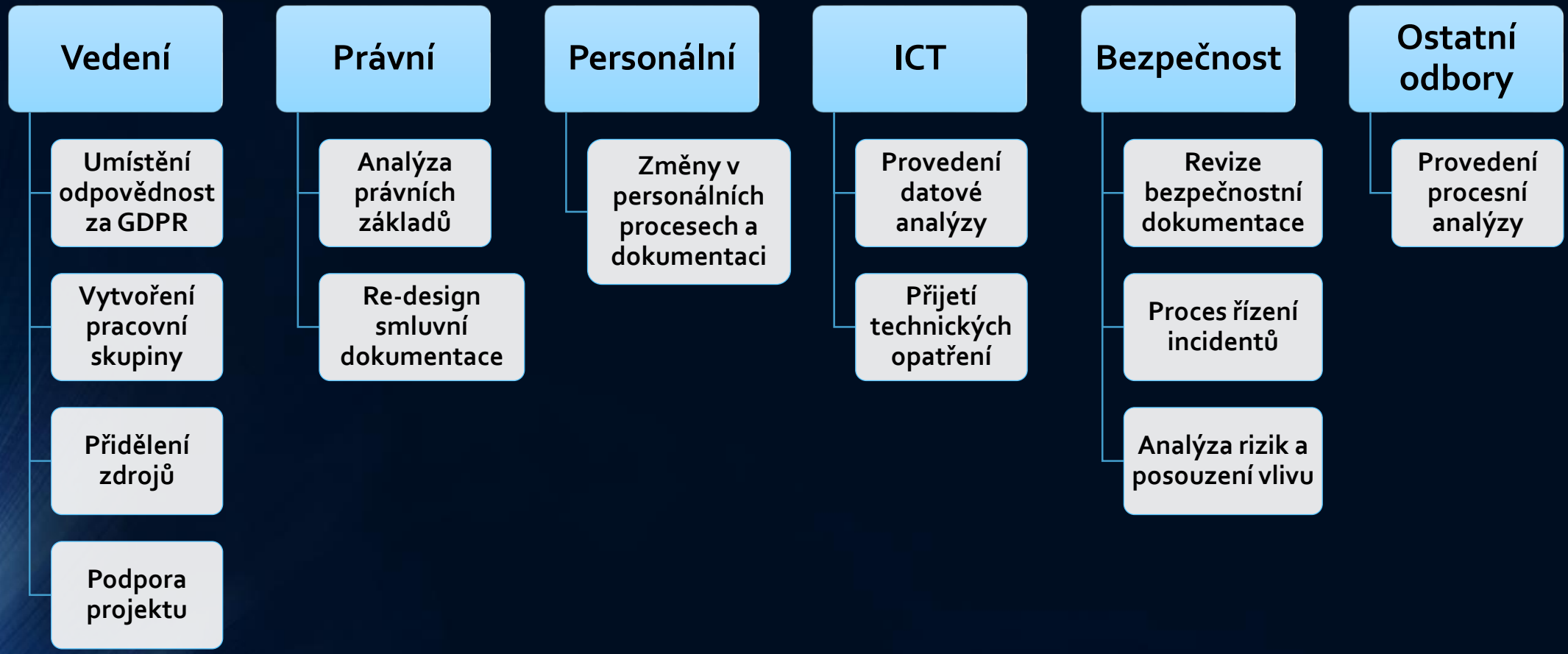
- znalost národního a unijního práva v oblasti ochrany dat a hluboké znalosti Obecného nařízení (GDPR)
- praktické zkušenosti aplikace požadavků ochrany dat
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat
- znalost dané oblasti podnikání a organizace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

- Výkon Pověřence je možno řešit plně dodavatelsky...

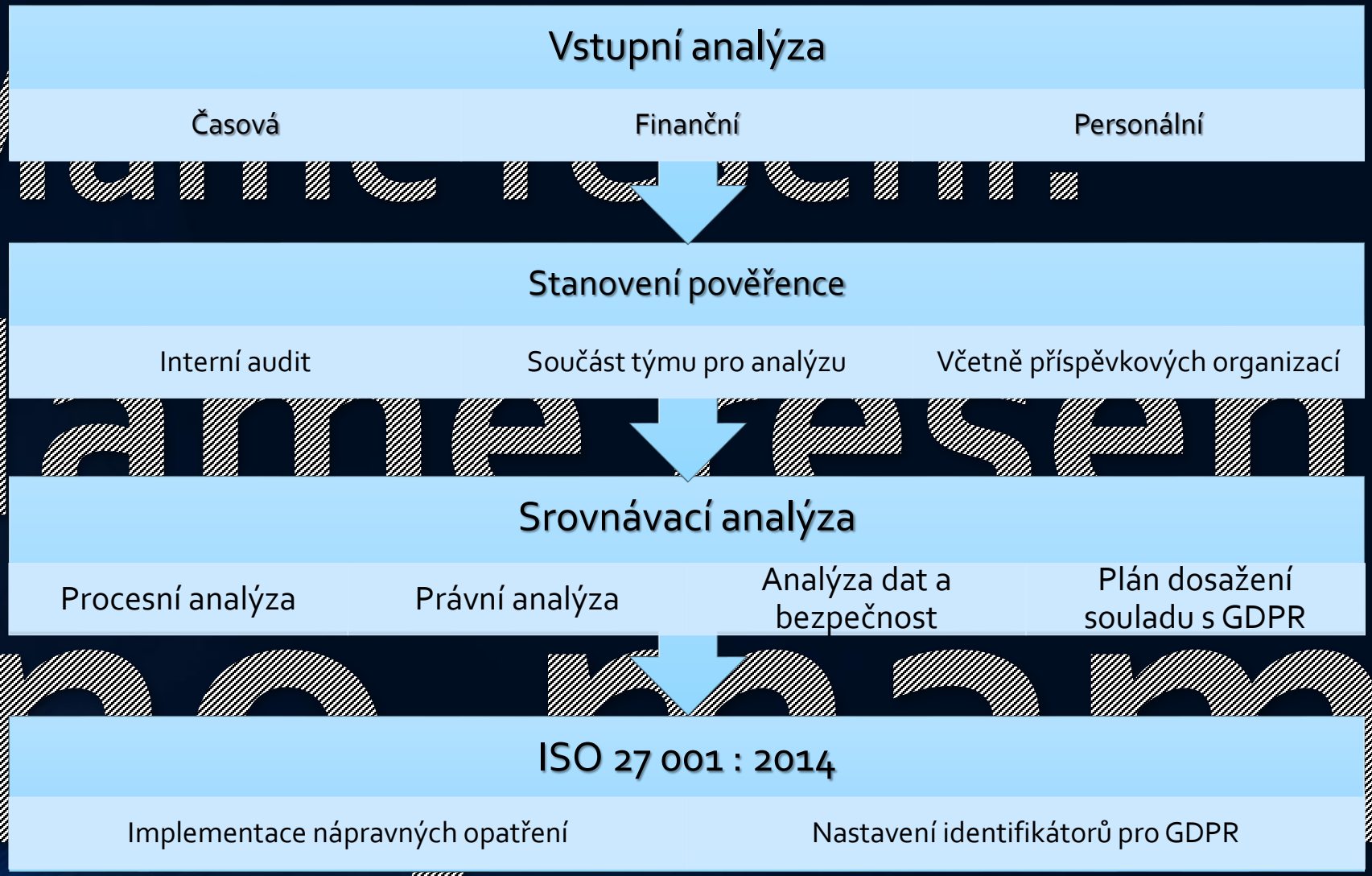
  ale:

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

DOPADY PODLE STRUKTURY ORGANIZACE



Máme řešení?


Vstupní analýza
Časová
Finanční
Personální
listopad 2017
Stanovení pověřence
Interní audit
Součást týmu pro analýzu
Včetně příspěvkových organizací
listopad 2017
Srovnávací analýza
Procesní analýza
Právní analýza
Analýza dat a bezpečnost
Plán dosažení souladu s GDPR
květen 2018
ISO 27 001 : 2014
Implementace nápravných opatření
Nastavení identifikátorů pro GDPR
září 2018

VZOROVÁ ANALÝZA připomínky

- *Neúplnost popisů procesů jednotlivých typů obcí*
- *Formulace opatření na vysoké technické úrovni – není možné realizovat bez bližších znalostí řízení bezpečnostních opatření - nutno přiblížit reálnému stavu v oblasti řízení obcí. Vše vztaženo na malé obce a to jak první nastavení, tak samotná revize v pravidelných cyklech*
- *Nepostihuje rozdílnost zákona č. 131/2000 Sb. o hlavním městě Praze a specifickém postavení jednotlivých typů MČ*
- *Zavádění nových činnosti spojených se zajištěním periodických prověřovacích činností, které nejsou v dokumentu uvedené a jsou nutné k řádnému zajištění složitějších operací nebo činností k definování a ověřování zpracování osobních údajů :*
  - *stanovení projektového týmu pro ochranu OÚ*
  - *stanovení klasifikaci aktiv*
  - *definování a realizace balančních testů zpracování osobních údajů*
  - *definování a realizace testů slučitelnosti zpracování osobních údajů*
  - *tvorba a ověřování posouzení vlivu na ochranu osobních údajů*
- *Finanční zatížení úřadů, a to jak v oblasti mzdových tak i v oblasti nákladů na služby - pro malé obce likvidační*
- *Nutnost vytvoření celé řady nových směrnic (pokynů) pro oblast řízení zpracování OÚ*
- *V procesech kde jsou obce zpracovatelem pro jednotlivá ministerstva je nutno dát k dispozici aktuální dokumentaci k jednotlivým procesům zpracování. (základní registry, evidence obyvatel, doklady…)*

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. P*<u>ředpoklad naplnění Nařízení EU k GDPR pro Prahu 2 je částka do velikosti malého rozsahu!</u>