

**Ako nastaviť vo firme efektívny  
GDPR compliance systém?**

**eFOCUS**

---

# NASTAVENIE SÚLADU S PRAVIDLAMI GDPR / COMPLIANCE



Požiadavky



Pravidlá



Interné politiky



Transparentnosť



Právo



Nariadenia



Štandardy

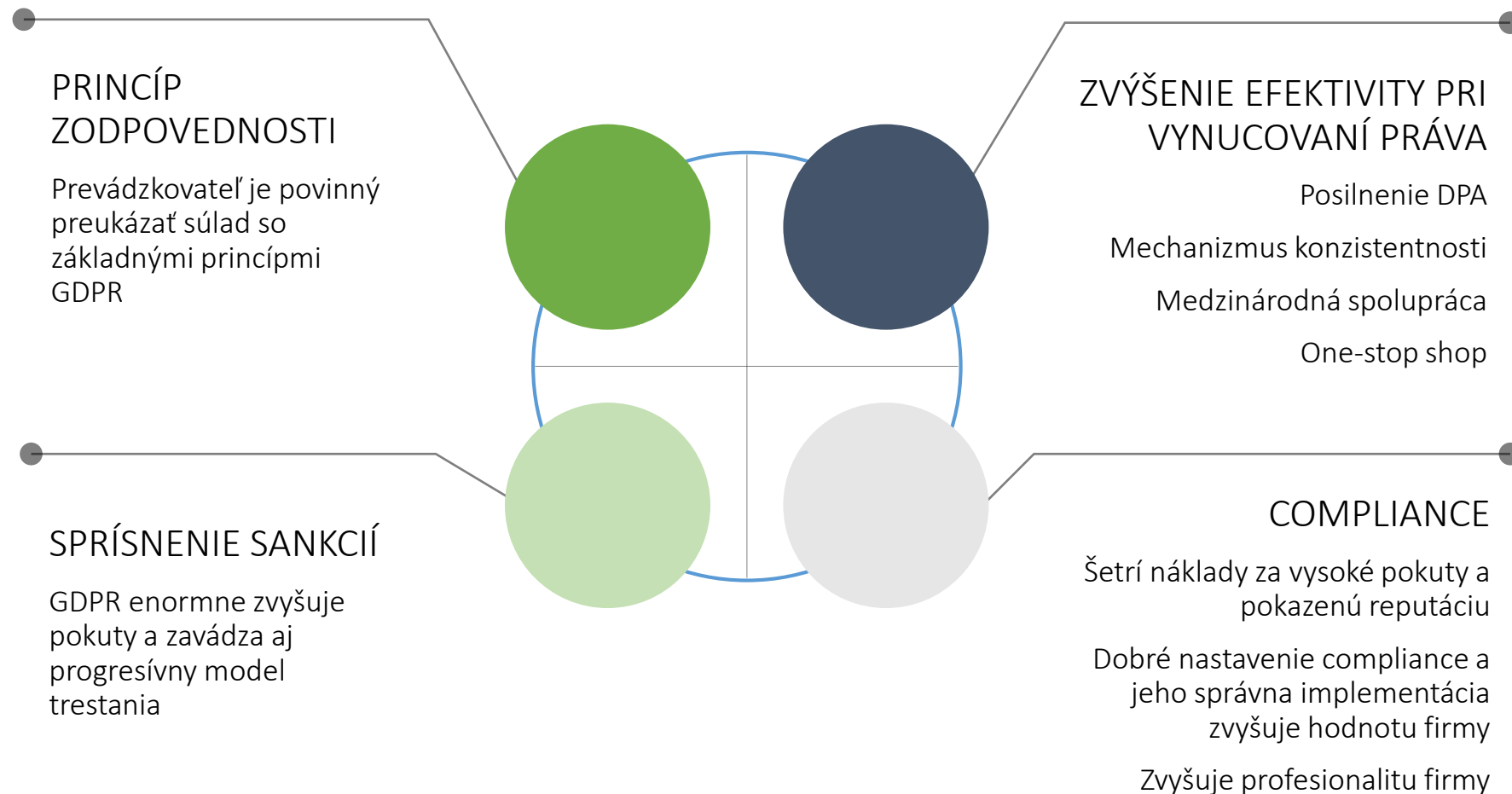


Riadenie



**Steiniger** | *law firm*

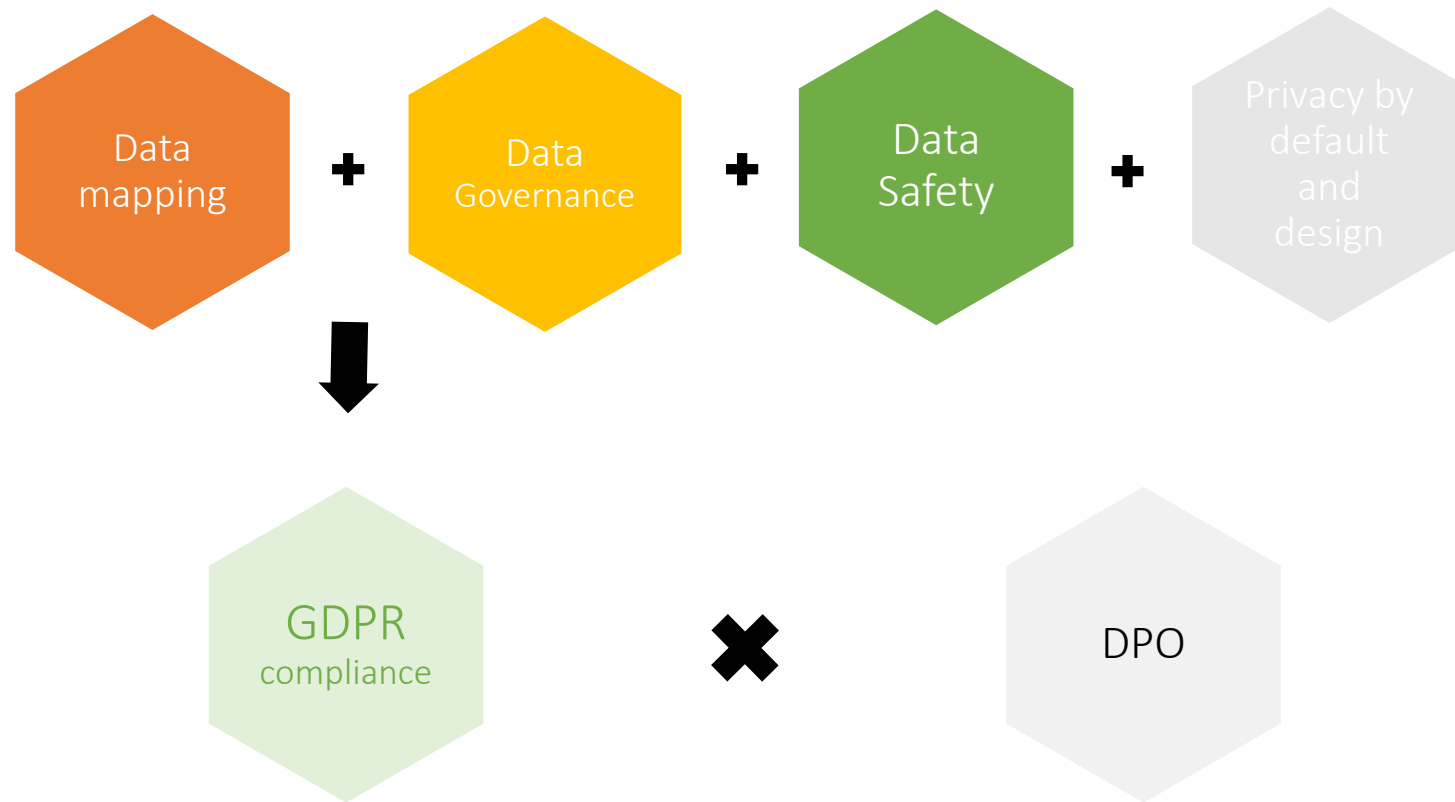
# DOBRÁ INTERNÁ PRÁVNA A BEZPEČNOSTNÁ DOKUMENTÁCIA JE ZÁKLADNÝM PREDPOKLADOM PRE ZNÍŽENIE A ELIMINÁCIU COMPLIANCE RIZIKA



**Steiniger**

*law firm*

# GDPR = KONIEC STATICKEJ A FORMÁLNEJ PRÁVNEJ DOKUMENTÁCIE ?



**Steiniger**

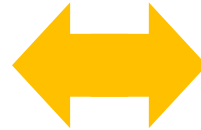
| *law firm*

# AKO ODPOVEDAŤ NA VÝZVY, KTORÉ PRINÁŠA GDPR?



1

Treba vytvoriť robustný a „živý“ compliance systém tvorený právnou dokumentáciou a dokumentáciou bezpečnostných opatrení, ktorý bude dostatočne individuálne zohľadňovať potreby a podmienky konkrétnej organizácie.



2

Treba implementovať systém do praxe a dbať na jeho kontinuálne dodržiavanie, vynucovanie, kontrolovanie a prehodnocovanie v kontexte podstatných udalostí, legislatívnych zmien, či nového vývoja s dopadom na ochranu údajov, a to v správny čas, správnymi prostriedkami, vhodným personálom a dobre nastavenými procesmi.



**Steiniger**  
— law firm —

# ČO ZOBRAŤ PRI NASTAVENÍ INTERNÉHO PROSTREDIA NAJVIAC DO ÚVAHY Z HĽADISKA ZMIEN, KTORÉ PRINÁŠA GDPR?

- Rozšírenie konceptu osobných údajov ako regulovanej kategórie dát a prepojenie s e-Privacy, najmä pri marketingových aktivitách
- Potvrdenie Opt in formy pri súhlase dotknutej osoby
- Prítomnosť osobných údajov detí
- Zmeny v obsahu povinných informácií určených dotknutým osobám
- Zmeny v požiadavkách na obsahové náležitosti zmluvy so sprostredkovateľom
- Prítomnosť spoločného prevádzkovateľa
- Prvky cezhraničného spracúvania v rámci EÚ a one-stop shop pravidlá
- Zvážte, či je subjekt organizačne a technicky pripravený vybavovať agendu práv dotknutých osôb v kontexte nových zmien.
- Spravte zmapovanie informačných tokov, v ktorých sú prítomné osobné údaje, skontrolujte právne základy, účely a dodržiavanie základných zásad vo vzťahu ku každej jednotlivej spracovateľskej operácii v rámci ktorej dáta do organizácie prichádzajú ako aj odchádzajú.
- Analyzujte dopady na cezhraničné prenosy do tretích krajín mimo EÚ.
- Analyzujte dopady na bezpečnosť spracúvania osobných údajov a pripravenosť na manažment bezpečnostných incidentov.
- **Analyzujte vznik povinnosti poveriť DPO.**
- Analyzujte povinnosť vykonať posúdenie vplyvu na ochranu údajov a predchádzajúcu konzultáciu s DPA.
- Analyzujte vznik povinnosti vedenia záznamov o spracovateľských operáciách.



**Steiniger**

| *law firm*

# EFEKTÍVNY INTERNÝ SYSTÉM OCHRANY OSOBNÝCH ÚDAJOV

## Hodnotenie

- Analýza podmienok spracúvania osobných údajov a identifikácia problémov
- Kontinuálna činnosť DPO
- Definovanie cieľov a bezpečnostných zámerov
- Úprava procesov s cieľom posudzovať dopady na ochranu osobných údajov pri všetkých rizikových aktivitách

## Prevenia

- Systémy na detekcie bezpečnostných incidentov
- Implementácia bezpečnostných opatrení
- Vzdelávanie a tréning zamestnancov zapojených do spracúvania osobných údajov
- Evidencia záznamov o preventívnych aktivitách
- Preverovanie sprostredkovateľov



## Reakcia

- Aktualizácia dokumentácie
- Revízia bezpečnostných opatrení
- Managment bezpečnostných incidentov
- Reporting DPO vedeniu firmy
- Výkon práv dotknutej osoby
- Budovanie vzťahu s DPA a konzultácie problémov
- Právna obhajoba v prípade problémov

## Sledovanie

- Interné audity
- Kontrolné mechanizmy zamestnávateľa aplikované na zamestnancov
- Monitoring legislatívy a aktuálnych trendov v oblasti ochrany osobných údajov (soft law, rozsudky CJEU, činnosť DPA)

# PRAKTICKÝ PRÍSTUP K PRINCÍPU ZODPOVEDNOSTI



## Interné politiky a akty riadenia určené na preukazovanie súladu s GDPR

- Bezpečnostné smernice bližšie vysvetľujúce a vynucujúce dodržiavanie prijatých bezpečnostných opatrení smerom k personálu
- Compliance smernice určené na interné usmernenie personálu na správny postup pri plnení regulačných povinností
- Transformácia písomných záznamov o poučení oprávnenej osoby na pokyny pre príjemcov osobných údajov (zamestnancov)
- Zakotvenie postavenia DPO v organizácii s ohľadom na stanovené právne požiadavky a rešpektovanie jej činnosti ovplyvňujúcej organizáciu.

## Budovanie firemnej kultúry orientovanej na ochranu súkromia

- Minimalizácia spracúvania údajov
- Snaha o kontinuálne dodržiavanie základných zásad zákonného spracúvania OÚ
- Interné kontroly a systém vzdelávania
- Spôsob využívania sociálnych sietí
- Zrozumiteľnosť prijatých pravidiel a ochota vysvetľovania záležitostí spojených so spracúvaním a ochranou osobných údajov
- Etický a zákonný prístup k profilovaniu dotknutej osoby
- Transparentná a proporcionálna aplikácia kontrolných mechanizmov na zamestnancov

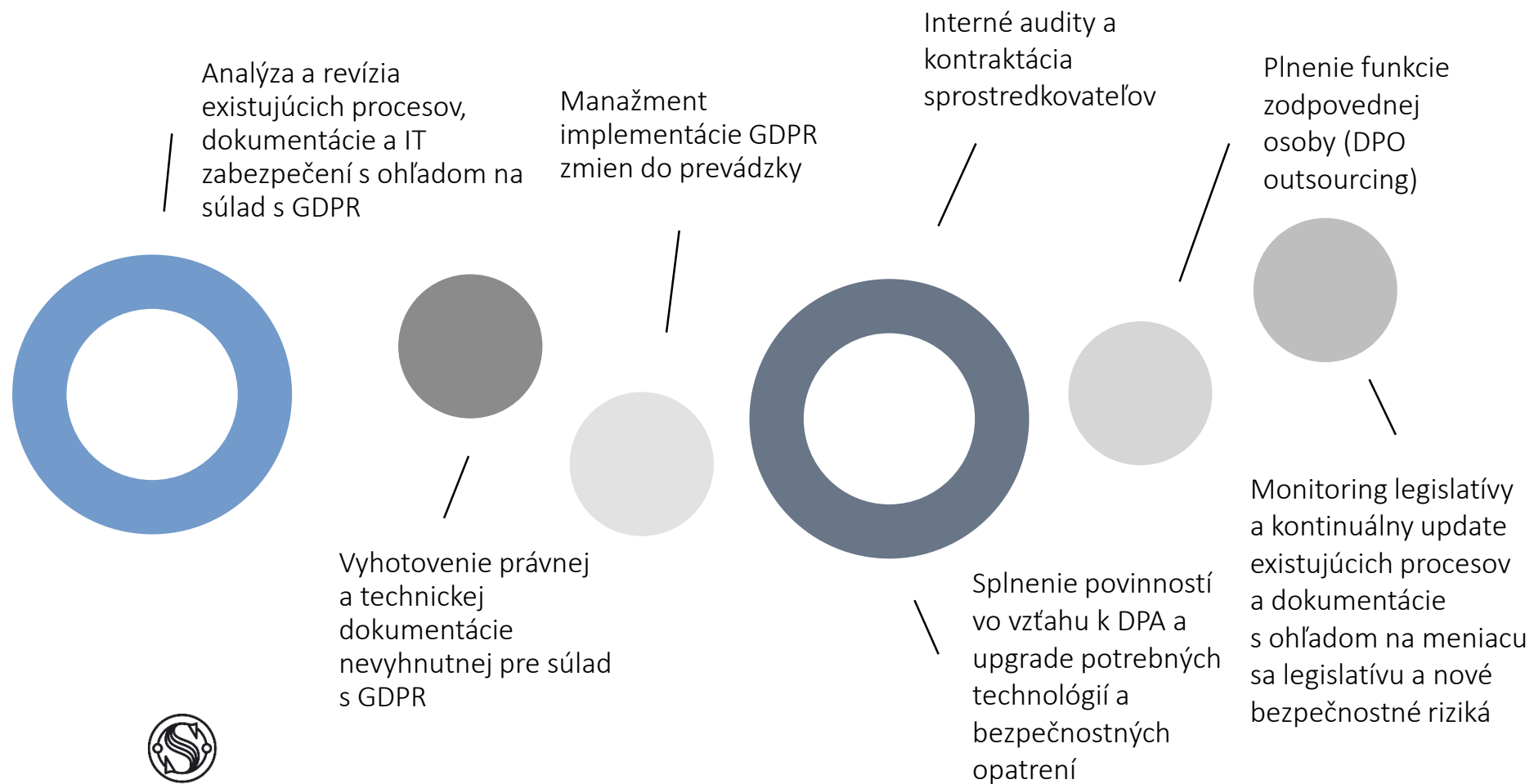
# PRAKTICKÝ PRÍSTUP K PRINCÍPU ZODPOVEDNOSTI



## Dôsledné plnenie regulačných povinností a vzťah s DPA

- Racionálne koncipovaná bezpečnosť spracúvania osobných údajov rešpektujúca požiadavky právnej úpravy článkov 25 a 32 GDPR
- Kontraktácia a audity sprostredkovateľov
- Správne používané a formulované súhlasy dotknutej osoby
- Vykonávanie DPIA a v prípade potreby aj na to nadväzujúce konzultácie s DPA
- Zodpovedné posudzovanie detekovaných bezpečnostných incidentov a ich oznamovanie DPA a dotknutým osobám
- Záznamy o spracovateľských činnostiach
- Určenie DPO
- Osobitné právne záruky pre cezhraničné prenosy do tretích krajín
- Certifikácia a kódexy správania

# AKÉ SLUŽBY SA POSKYTUJÚ PRI GDPR COMPLIANCE?



# SPÔSOBY REAKCIE TRHU NA DOPYT PO GDPR SLUŽBÁCH

## DRAFTOVÉ RIEŠENIE

Vzorové dokumenty  
Limitovanie na legal compliance  
Slabá individualizácia, žiadna implementácia

*Výsledok: Nízka cena za návod  
často pochybnej kvality*

## PROJEKT

Gap analýza  
Zohľadnenie individuálnych potrieb  
Manažment implementácie na  
všetkých úrovniach  
Kvalifikované právne posúdenie a  
detailné riešenie

*Výsledok: Komplexné riešenie s  
najväčšou istotou, garanciami a  
finančnými nákladmi*

## „EKOSYSTÉM“

Platforma na migráciu procesov a  
dát do zabezpečeného prostredia  
Zaujímavá možnosť, ktorá nie je  
vhodná pre každého

*Výsledok: Zabezpečíte data safety a  
data governance pre komplexné  
procesy, zostane vyriešiť vlastné  
administratívno-právne povinnosti*

## SOFTWARE

Bezpečnostné opatrenia  
Log manažment / šifrovanie  
Pomôcky pre DPO  
Automatizované DPIA

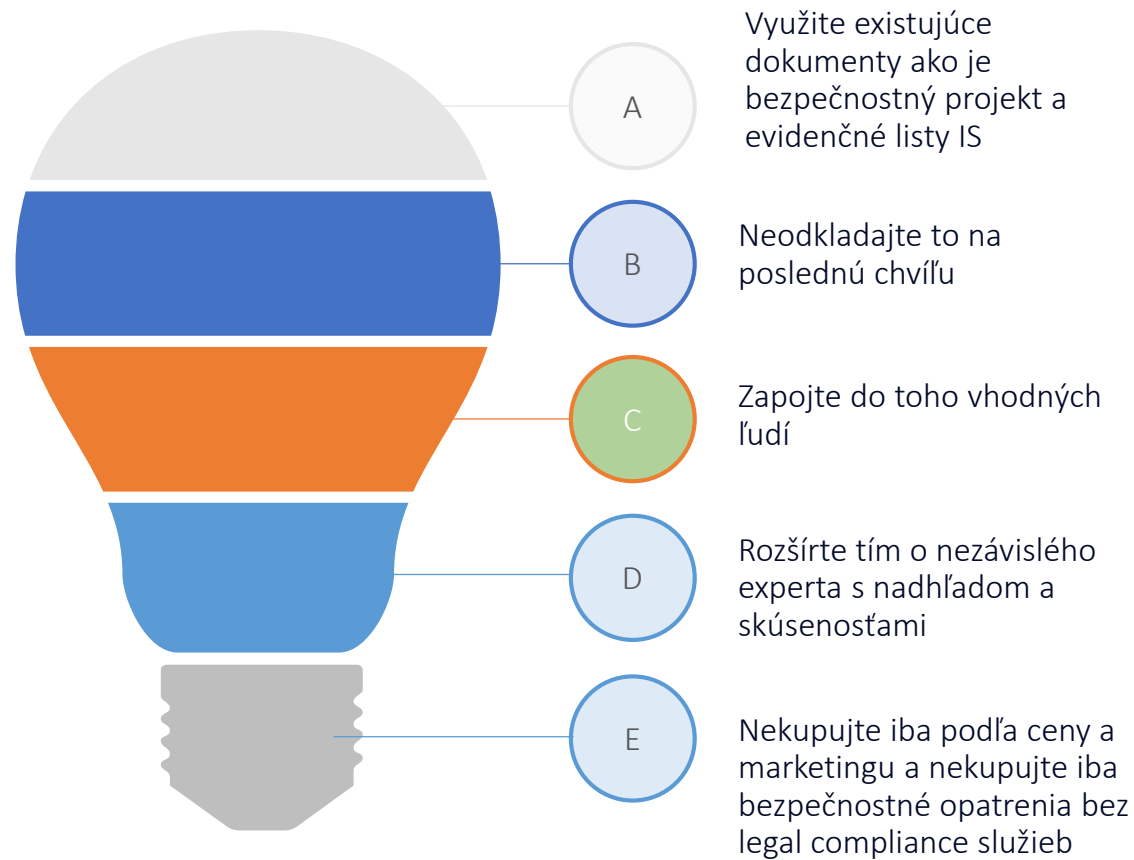
*Výsledok: Vyriešite parciálnu  
záležitosť, nie však súlad s GDPR*



**Steiniger**

law firm

# ODPORÚČANIA





# Q & A



**Steiniger** | *law firm*



Ďakujem. Kontaktujte ma.

## JUDr. Ondrej Zimen

Právnik / Data protection specialist

+421 948 589 666

[o.zimen@steiniger.org](mailto:o.zimen@steiniger.org)



Ďakujem za pozornosť.

