Grant Thornton

An instinct for growth™

Systémová analýza a opatření v rámci GDPR

Kraje a právnické osoby zřizované kraji

1. března 2018

Cíle systémové analýzy

Dne 25. května 2018 nabývá účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).

Cílem projektu bylo zpracovat analýzu současného stavu s ohledem na požadavky GDPR, což zahrnovalo následující témata…

Přehled zpracovávaných osobních údajů

Popis zpracování osobních údajů v informačních systémech v kontextu činnost krajů a právnických osob zřizovaných kraji.

Dopady nařízení GDPR

Popis dopadů obecného nařízení o ochraně osobních údajů na kraje a právnické osoby zřizované kraji.

Zhodnocení souladu s GDPR

Zhodnocení, zda stávající činnosti krajů a právnických osob zřizovaných kraji jsou či nejsou v souladu s obecným nařízením o ochraně osobních údajů.

Rizika zpracování

Zhodnocení rizika zpracování a v kontextu obecného nařízení o ochraně osobních údajů jejich kvalifikování.

Nápravná opatření

Návrh opatření k nápravě v případě, kdy stávající činnost je nesouladná s obecným nařízením o ochraně osobních údajů.

Pověřenec na ochranu osobních údajů

Doporučení kvalifikace, organizačního postavení a činnosti pověřence pro ochranu osobních údajů v kraji

Systémová analýza byla provedena na vzorku 3 krajů vybraných zadavatelem a vztahuje se ke všem agendám v přenesené působnosti krajů, tak k základním (všem krajům společným) agendám v samostatné působnosti.

Systémová analýza pokrývá také vymezené činnosti právnických osob zřizovaných kraji.

Typy organizací a jejich agend, které byly zahrnuty do analýzy

Kraje

- Doprava,
- Školství, mládež, tělovýchova,
- ŽP a zemědělství,
- Územní plánování, stavební úřad,
- Kultura a památková péče,
- Regionální rozvoj a cestovní ruch,
- Kontrola,
- Kancelář hejtmana a vnějších vztahů,
- Podpora řízení,
- Kancelář ředitele úřadu,
- Legislativa a právo,
- Krajský živnostenský úřad,
- Sociální věci,
- Zdravotnictví,
- Investice a majetek,
- Finance,
- Bezpečnost a krizové řízení,
- Dotace a projekty,
- Interní audit.

Škola a školské zařízení

- Personálně-mzdová agenda,
- Úsek ekonomicko-provozní,
- Agenda pedagogiky.

Zdravotnické zařízení

- Personálně-mzdová agenda,
- Úsek ekonomicko-provozní,
- Poskytování zdravotních služeb.

Zařízení sociálních služeb

- Personálně-mzdová agenda,
- Úsek ekonomicko-provozní,
- Poskytování sociálních služeb.

Kulturní

- Personálně-mzdová agenda,
- Úsek ekonomicko-provozní,
- Knihovnické a informační služby.

Oblast dopravní obslužnosti

- Personálně-mzdová agenda,
- Úsek ekonomicko-provozní,
- Agenda dopravní obslužnosti.

Vstupní podklady

Quick Check

Vyplňuje zpravidla zástupce bezpečnosti ve spolupráci s IT. Tento dotazník slouží pro zpracování souhrnné analýzy připravenosti.

Dotazník právní

Vyplňuje zpravidla zástupce za oddělení nebo danou agendu, je potřeba zpracovat pro každou agendu v rámci dané organizace (tj. krajského úřadu nebo příspěvkové organizace) zvlášť, a to jak v rámci výkonu samostatné působnosti, tak v rámci výkonu přenesené působnosti.

Přehled systémů

Vyplňuje zpravidla zástupce IT a techničtí zástupci aplikací (garant/vlastník aplikace). Tento dotazník slouží pro zjištění všech informačních systémů, které obsahují OÚ/COÚ, a jejich bezpečnostních parametrů.

Směrnice, řády, vzory smluv

- Vzor pracovní smlouvy (i DPP, DPČ)
- Vzor dodavatelské smlouvy
- Vzor souhlasů o zpracování OÚ
- Směrnice na ochranu OÚ
- Bezpečnostní směrnice/politika - fyzická a IT/ICT
- Organizační řád
- Skartační řád
- Pracovní řád

Výstupy systémové analýzy

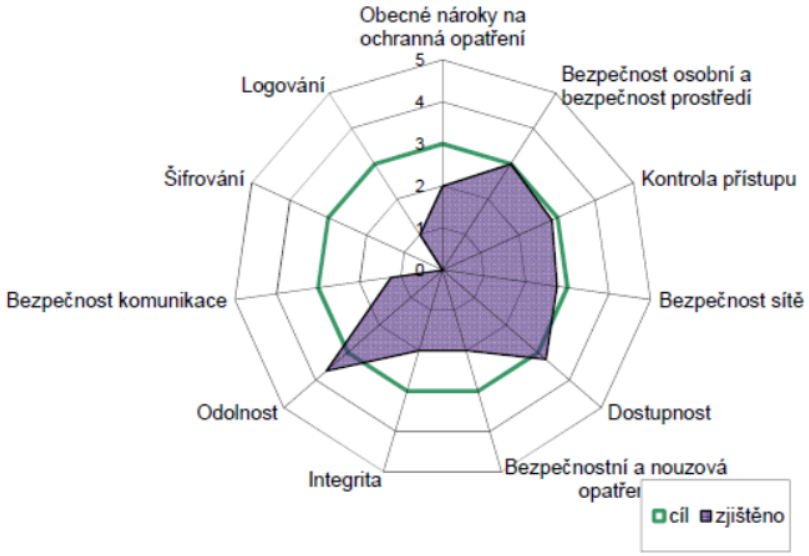
Obecné dopady GDPR	Zpracovávané osobní údaje	Přehled osobních údajů v IS	Analýza rizik	Přehled nesouladů s GDPR a návrh opatření	Pověřenec pro ochranu osobních údajů (DPO)	Výstupy pro jednotlivé organizace
• Popis dopadů GDPR na kraje a subjekty zřizované kraji	• Přehled zpracovávaných osobních údajů dle jednotlivých agend • Identifikace rolí, účelů zpracování, odpovědností, doby uchování osobních údajů • Přehled agend s uvedením jejich právních základů	• Přehled osobních údajů v identifikovaných typech informačních systémů	• Zhodnocení rizik zpracování včetně jejich významnosti, dle jednotlivých agend	• Přehled identifikovaných nesouladů s GDPR • Návrh organizačních a technických opatření	• Doporučení kvalifikace osoby a jejího organizačního začlenění • Přehled činností DPO	• Vyhodnocení Quick Check dotazníků

Základní vyhodnocení připravenosti krajů

Níže uvedené grafy představují vyhodnocení základního dotazníku „Quick Check“. Grafy znázorňují aktuální stav připravenosti procesů a organizačních opatření (vlevo) a technických opatření (vpravo) na GDPR.

Procesy a opatření ochrany dat

Opatření informační bezpečnosti

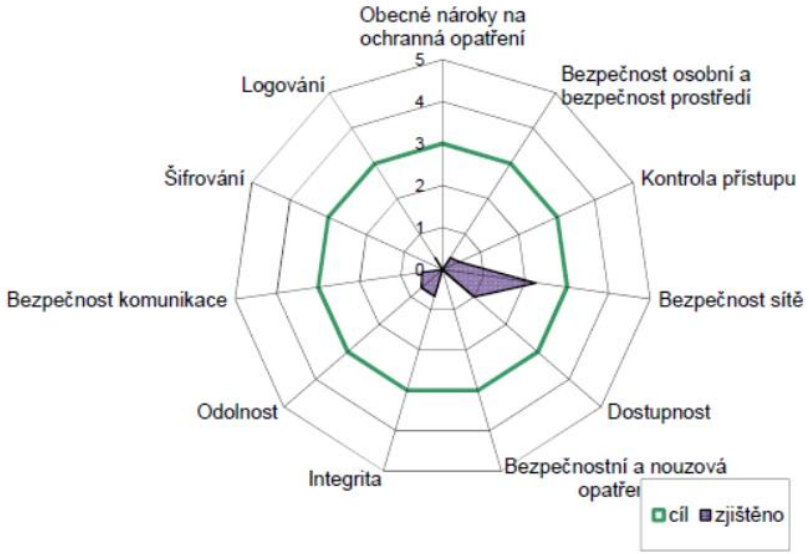


Základní vyhodnocení připravenosti právnických osob zřizovaných kraji

Níže uvedené grafy představují vyhodnocení základního dotazníku „Quick Check“. Grafy znázorňují aktuální stav připravenosti procesů a organizačních opatření (vlevo) a technických opatření (vpravo) na GDPR.

Procesy a opatření ochrany dat

Opatření informační bezpečnosti

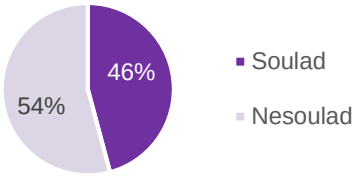


Organizační, procesní a právní doporučení

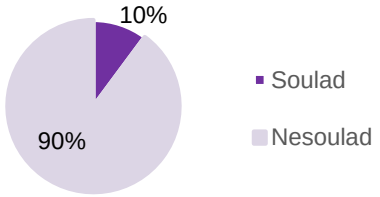
- Provedení revize interních předpisů (zejména za účelem vymezení rolí a odpovědností ve vztahu ke každé činnosti vykonávané v rámci organizace),
- Stanovení účelů zpracování a rozsahu zpracovávaných osobních údajů,
- Revize stávajících právních titulů, včetně udělených souhlasů,
- Zavedení mechanismů za účelem výkonu práv subjektů údajů,
- Zpracování či revize výstupu s informacemi pro subjekt údajů,
- Vedení záznamů o činnostech zpracování,
- Jmenovaní pověřence pro ochranu osobních údajů,
- Stanovení podmínek pro zapojení zpracovatele,
- Zavedení postupu pro ohlášení/oznámení porušení zabezpečení osobních údajů,
- Vedení záznamů o udělených souhlasech, vedení záznamů o splnění informační povinnosti, dokumentace případů porušení zabezpečení osobních údajů.

Doporučená technická opatření

Kraje



Právnické osoby zřizované kraji



Následující doporučení platí pro většinu posuzovaných systémů:

Zpracování analýzy rizik

Zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti

- vedení auditních záznamů (logů),
- zajištění přenosu dat šifrovanou komunikací,
- napojení na centrální monitoring (SIEM).

Obnova dostupnosti OÚ a přístupu k nim včas v případě incidentu (plán obnovy po havárii)

Pravidelné testování, posuzování a hodnocení účinnosti zavedení opatření pro zajištění bezpečnosti (obnova po havárii, vyhodnocování incidentů, obnova záloh)

Pseudonymizace

- zavedení těchto opatření zvážit na základě výsledku analýzy rizik a posouzení nákladů,
- pro nově nakupované systémy doporučujeme jako standard.

Pověřenec pro ochranu osobních údajů

Doporučení ke kvalifikaci

- žádný požadavek na dosažené vzdělání či certifikaci,
- jmenování na základě profesních kvalit, zejména odborných znalostí práva a praxe v oblasti ochrany osobních údajů a své schopnosti plnit úkoly stanovené v čl. 39 GDPR,
- dostatečná znalost prostředí a prováděných procesů zpracování.

Doporučení k organizačnímu začlenění

- přímé podřízení vrcholovým řídícím pracovníkům,
- „interní“ či „externí“ pověřenec,
- zamezení střetu zájmů,
- výkon funkce a plnění povinností a úkolů nezávislým způsobem.

Doporučení k činnosti

- monitoring,
- poradenství a konzultace,
- kontrola,
- kontaktní místo.