

Implementácia GDPR: praktické tipy pre zabezpečenie súladu s GDPR



White & Case

Implementácia GDPR: praktické tipy pre zabezpečenie súladu s GDPR

Obsah

1. Úvod
2. Praktické rady
3. Indikatívny harmonogram compliance projektu
4. Otázky, diskusia



Úvod

Aplikovateľnosť Nariadenia, národná úprava

Nariadenie:

- **Uplatniteľnosť** – odklad vymožitelnosti požiadaviek zavádzaných Nariadením zo strany úradov
 - **25. mája 2018 ~ 8 mesiacov na zabezpečenie súladu s Nariadením**

Národná úprava:

- Nový zákon o ochrane osobných údajov – aktuálny stav: ukončené MPK, návrh zákona bude predložený parlamentu

**Nový sankčný režim – vysoká
motivácia okamžite začať so zabezpečovaním
súlady s GDPR**

Nový sankčný režim – vysoká motivácia okamžite začať so zabezpečovaním súladu s GDPR

- Nariadenie zavádza **výrazne vyššie** pokuty ako bola doterajšia európska prax
- Dvojstupňový režim ukladania pokút:
 - Až do výšky **10 000 000 EUR** (resp. **2%** z obratu) napr. porušenia v oblasti bezpečnosti údajov, posúdenia vplyvu, ustanovenia zodpovednej osoby
 - Až do výšky **20 000 000 EUR** (resp. **4%** z obratu) napr. porušenia základných zásad spracúvania, práv dotknutých osôb, porušenia povinností pri prenose do tretích krajín
- Pokuty ukladané podľa nariadenia majú byť **účinné, primerané, odrádzajúce**
- Pokuty **nie sú** ukladané **obligatórne** – široká diskrečná právomoc úradov
- **Kritéria** (či pokutu uložiť a v akej výške): povaha/závažnosť/trvanie, úmysel/nedbanlivosť, kroky na zmiernenie škody, predchádzajúce porušenia, kategória OÚ, ako sa úrad o porušení dozvedel, ...
- Otázne, ako bude Úrad pristupovať ku kontrolám/sankciám v období tesne po uplatniteľnosti GDPR

Praktické rady

Nastavenie *compliance* projektu

- Vytvorenie interných tímov zložených zo zástupcov príslušných oddelení (právo, IT, bezpečnosť)
- Definovanie priorít, na ktoré bude potrebné sa sústrediť / definovanie rizikového profilu spoločnosti
- Určenie pilotných subjektov, u ktorých sa bude testovať implementácia GDPR a jednotlivé riešenia
 - relevantné pre korporátne skupiny
- Zvýšenie povedomia o implikáciách GDPR v rámci spoločnosti
- Zvýšenie povedomia spolupracujúcich tretích osôb (riziko spoluzodpovednosti)
- Implementácia v rámci rozpracovaných a nových projektov

Fázy compliance procesu (príklad) I

1. **Vykonanie analýzy spracúvania údajov a potrebných zmien (*data mapping, gap analysis*)**
 - ✓ Určenie rozsahu spracúvania (dotazník, interná/externá analýza)
 - ✓ Úplný audit ako alternatíva
2. **Vypracovanie plánu projektu na zabezpečenie súladu s GDPR**
 - ✓ Konkrétne povinnosti súvisiace so zabezpečením súladu s GDPR v zmysle nastavených priorít a rizikového profilu
 - ✓ Nastavenie harmonogramu povinností pre zabezpečenie súladu
3. **Úprava zmlúv so zákazníkmi (fyzické osoby)**
 - ✓ Analýza zmlúv a identifikácia ustanovení, ktoré je potrebné upraviť/opätovne prerokovať
 - ✓ Vypracovanie upravených vzorových zmlúv

Fázy compliance procesu (príklad) II

4. Úprava zmlúv so sprostredkovateľmi

- ✓ Analýza zmlúv a identifikácia ustanovení, ktoré je potrebné upraviť/opätovne prerokovať
- ✓ Vypracovanie upravených vzorových zmlúv
- ✓ Implementácia prenosových mechanizmov

5. Úprava zmlúv/vzťahov s prevádzkovateľmi

- ✓ Analýza zmlúv a identifikácia ustanovení, ktoré je potrebné upraviť/opätovne prerokovať
- ✓ Ak klient a ďalší prevádzkovateľ konajú samostatne v pozícii prevádzkovateľa, bude potrebné upraviť ich vzťah zmluvou o zdieľaní údajov (*Data sharing agreement*)
- ✓ Ak klient a ďalší prevádzkovateľ konajú spoločne v pozícii prevádzkovateľa, bude potrebná zmluva o spoločnom spracúvaní údajov prevádzkovateľmi (*Joint controllership agreement*)

Fázy compliance procesu (príklad) III

6. Úprava interných predpisov o ochrane údajov a zásad používania cookies

- ✓ Analýza interného spracúvania údajov (t.j. predpisov o spracúvaní osobných údajov zamestnancov a pod.) a zásad používania cookies
- ✓ Analýza externého spracúvania údajov (t.j. predpisov o spracúvaní osobných údajov zákazníkov, dodávateľov a pod.)
- ✓ Vypracovanie/úprava predpisov a zásad

7. Zabezpečenie súladu s lokálnou a sektorovou legislatívou

- ✓ Zistenie potreby implementácie opatrení vyplývajúcich z lokálnej legislatívy (relevantné pre korporátne skupiny alebo cezhraničných spracovateľov) alebo sektorovej legislatívy
- ✓ Úprava príslušných interných predpisov a procesov

Fázy compliance procesu (príklad) IV

8. **Revízia zásad uchovávania údajov**

- ✓ Analýza existujúcich postupov uchovávania/likvidácie údajov
- ✓ Vypracovanie základného rámcového predpisu upravujúceho zásady uchovávania údajov resp. úprava existujúceho predpisu

9. **Určenie vedúceho dozorného orgánu**

- ✓ Určenie miesta „hlavnej prevádzkarne“ na účely spracúvania údajov v EÚ, podľa ktorého bude zároveň určené sídlo „vedúceho dozorného orgánu“ pre spracovateľské operácie
- ✓ Analýza zmien, ktoré bude potrebné implementovať
- ✓ Komunikácia s preferovaným dozorným orgánom o návrhu na jeho ustanovenie za „vedúci dozorný orgán“

10. **Analýza cezhraničných prenosov údajov**

- ✓ Analýza existujúcich mechanizmov prenosu údajov s porovnaním výhod/nevýhod
- ✓ Vypracovanie príslušnej dokumentácie podľa zvolenej stratégie
- ✓ Implementácia zvoleného mechanizmu prenosov

Fázy compliance procesu (príklad) V

11. Záznamy o spracúvaní údajov

- ✓ Analýza prípadných registračných povinností v príslušných jurisdikciách
- ✓ Analýza existujúcich registrácií/praxe vedenia záznamov
- ✓ Vypracovanie/úprava evidenčných formulárov a usmernení o vedení záznamov

12. Bezpečnosť údajov a pripravenosť v prípade porušenia ochrany údajov

- ✓ Analýza interných predpisov týkajúcich sa bezpečnosti údajov a ohlasovania porušenia ochrany osobných údajov
- ✓ Úprava interných predpisov týkajúcich sa bezpečnosti údajov
- ✓ Úprava/príprava interných predpisov o ohlasovaní porušenia ochrany, vrátane vzorov oznámenia porušenia dozorným orgánom a dotknutým osobám
- ✓ Voľba a implementácia primeraných postupov/interných procesov ohlasovania
- ✓ Realizácia „testovacích cvičení“



Fázy compliance procesu (príklad) VI

13. Dohľad nad ochranou osobných údajov

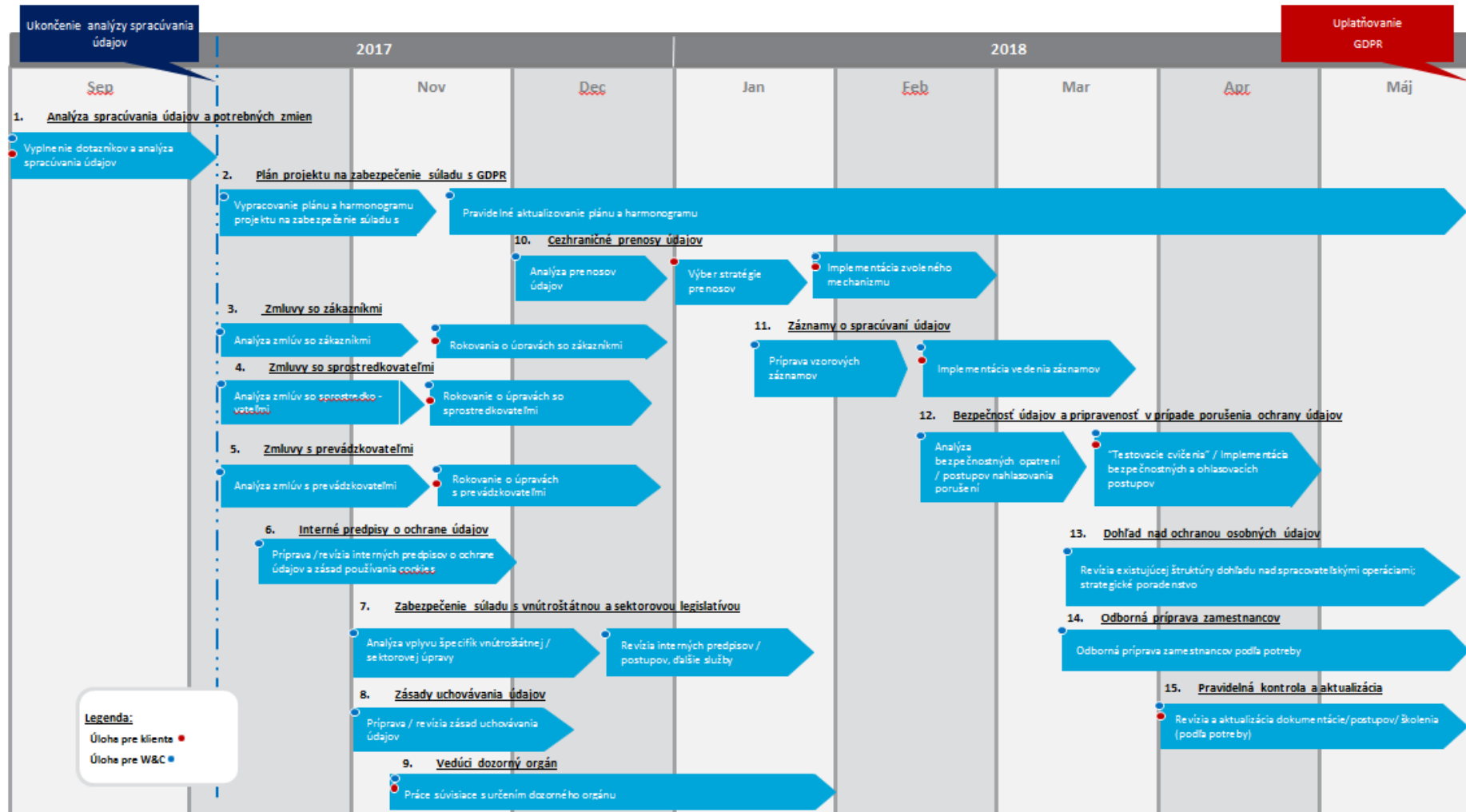
- ✓ Určenie zodpovedných osôb na lokálnej alebo funkčnej úrovni
- ✓ Zabezpečenie koordinácie odpovedí na žiadosti dotknutých osôb
- ✓ Implementácia princípu pravidelného posudzovania ochrany údajov a princípu špecificky navrhutej ochrany údajov (*privacy by design*)
- ✓ Zabezpečenie monitoringu zmien legislatívy a regulácie v oblasti ochrany osobných údajov

14. Odborná príprava zamestnancov

- ✓ Určenie rozsahu prípravy zamestnancov v súvislosti s implementáciou GDPR
- ✓ Realizácia školení

15. Pravidelná kontrola a aktualizácia

Indikatívny harmonogram



Otázky?

Ďakujeme za pozornosť

White & Case

