Proč do toho jít s námi?

- Déle než rok se účastníme diskusí s **předními odborníky v oboru** a poskytujeme našim partnerům poradenství s přípravami na GDPR.
- Jsme členy **tří expertních skupin**, zabývajících se GDPR a ochranou osobních údajů.
- Připravujeme naše partnery na GDPR **napříč Evropskou unií** v rámci unikátních pilotních projektů.
- Našim cílem není změnit Vaše zavedené postupy, ale poskytnout Vám **rady pro** jejich **optimalizaci.**
- Komunikujeme s Úřadem pro ochranu osobních údajů
- Usilujeme o získání akreditace dle čl. 43 GDPR za účelem vydávání osvědčení ISO 17065

Co Vám můžeme nabídnout?

- V rámci úvodní konzultace Vám s pomocí těch správných otázek pomůžeme identifikovat **klíčové oblasti**, kde ve Vaší společnosti probíhá zpracovávání osobních údajů.
- Náš tým více než 10 expertů a členů pomocného týmu analyzuje identifikované klíčové oblasti a vyhodnotí jejich soulad s GDPR.
- Vytvoříme pro Vás jasnou a přehlednou zprávu, ze které se dozvíte:
  Které oblasti Vašeho podnikání podléhají regulaci GDPR
  Jaké požadavky na Vás GDPR klade
  Kde má Vaše společnost bezpečnostní mezery
- Na základě výstupní zprávy Vám dáme jednoduchá doporučení, jejichž implementace zajistí Vaši GDPR compliance.
- Profesní pojištění odpovědnosti ve výši 250 mil. Kč

© 2017 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena.

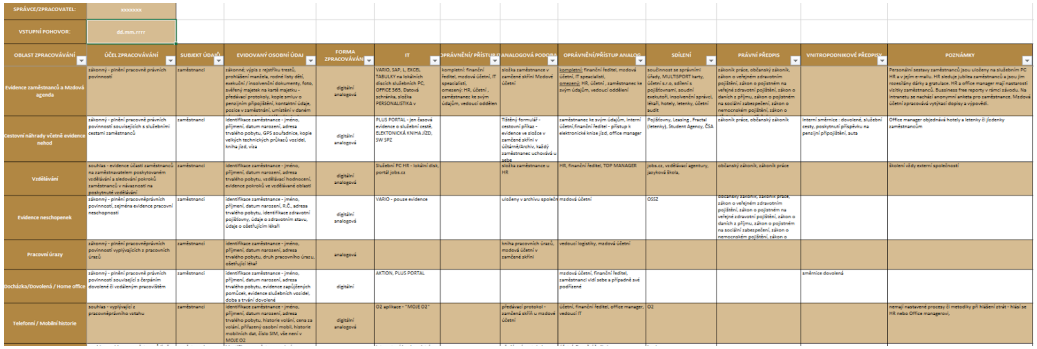
Vzorový průběhu GDPR auditu

1 Určení odpovědné osoby v rámci organizace

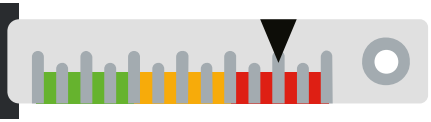
Před zahájením auditu je nutné ze strany organizace určit osobu, která bude za organizaci pověřena koordinací auditu a komunikací s advokátní kanceláří. Tato osoba bude odpovědnou osobou za audit za stranu organizace, bude předávat podkladovou dokumentaci a přebírat plnění od advokátní kanceláře.

2 Identifikace pracovních oddělení v organizaci

Společně s odpovědnou osobou organizace určíme jednotlivá oddělení v rámci organizace, která zpracovávají osobní údaje nebo se na zpracování podílejí, a vybereme zástupce těchto oddělení. Zástupci pomohou v průběhu auditu identifikovat jednotlivé procesy zpracování osobních údajů, ke kterým v organizaci dochází. Na základě naší metodiky bude sestaven přehled oddělení a jednotlivých kategorií oprávnění v rámci oddělení.



GDPR – Měřítko nutných změn



3 Osobní schůzka se zástupci jednotlivých oddělení

V rámci první části auditu se osobně setkáme se zástupci jednotlivých oddělení za účasti odpovědné osoby organizace, vysvětlíme jim, jak bude probíhat audit, jaké informace a podklady budeme potřebovat a proč. Cílem je, aby jednotliví zástupci odcházeli s vědomostmi nezbytnými pro řádné vypracování auditu. Organizace od nás obdrží tabulku pro sestavení přehledu evidencí a karet evidencí osobních údajů, včetně metodiky pro jejich zpracování a společně se pustíme do vypracování datového inventáře organizace.

4 Analytická část

Po skončení první části auditu bude z naší strany vyžádána podkladová dokumentace a informace pro analýzu gdpr compliance organizace. V této fázi se zapojuje náš expertní tým IT, který posuzuje organizační a technické zabezpečení IT infrastruktury společnosti a klíčové podnikové systémy. Po obdržení všech potřebných podkladů a informací analyzujeme, jak organizace zpracovává osobní údaje v porovnání s požadavky gdpr. V rámci analytické části:

- **4.1** analyzujeme, jaké evidence osobních údajů společnost vede, jaké jsou v nich osobní údaje a kde jsou uloženy;
- **4.2** posuzujeme právní základ společnosti pro jednotlivé kategorie zpracování osobních údajů;
- **4.3** sestavujeme datový inventář organizace, ze kterého jsou patrné jednotlivé nedostatky vedení evidencí;
- **4.4** posuzujeme, ke kterým evidencím je organizace povinna vést záznamy o zpracování;
- **4.5** vyhodnocujeme správnost organizací připravených posouzení vlivů (DPIA) nebo doporučujeme, ke kterým kategoriím zpracování osobních údajů je organizace povinna zpracovat DPIA;
- **4.6** v případě, že organizace provádí profilování, zkoumáme jeho zákonnost a splnění informačních a dalších povinností podle GDPR;
- **4.7** vyhodnocujeme zavedená bezpečnostní opatření při zpracování osobních údajů;
- **4.8** analyzujeme vnitropodnikové předpisy na poli ochrany osobních údajů;
- **4.9** posuzujeme správnost smluv partnery organizace, kteří jsou správci či zpracovatelé osobních údajů, s ohledem na požadavky čl. 28 GDPR;
- **4.10** analyzujeme nastavení IT systému z pohledu tzv. best practice, omezení přístupu, minimalizace zpracování osobních údajů a celkového nastavení;
- **4.11** prověřujeme, zda organizace dodržuje princip privacy-by design, pokud jako součást auditu posuzujeme vývojový proces nových procesů (volitelná služba nad rámec cenové nabídky).

© 2017 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena.

Vzorový průběh GDPR auditu

4 GAP analýza

GAP analýza dává ucelený přehled o tom, v jakém stavu je ochrana dat v organizaci v porovnání s požadavky GDPR.

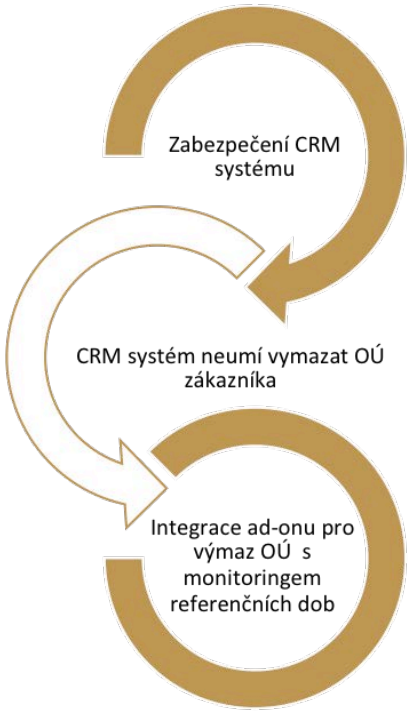
5 ROAD MAP kroků

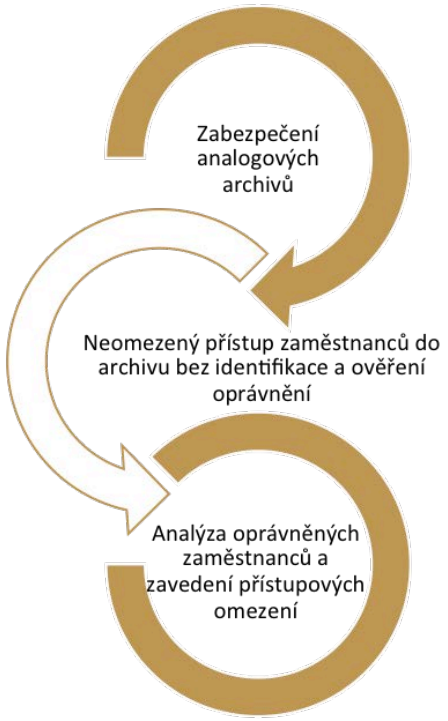
Na základě GAP analýzy bude vytvořena roadmapa kroků, kterými musí organizace projít, aby získala osvědčení pro účely prokázání souladu s GDPR. ROAD MAP se primárně bude týkat těchto oblastí:

1. Oblast bezpečnosti.
2. Oblast systému řízení ochrany osobních údajů.
3. Oblast samotného zpracování osobních údajů.
4. Oblast interních předpisů organizace.
5. Školení v rámci organizace.
6. Oblast řízení rizika třetích stran.

Ukázka výstupů GAP analýzy:

OBLAST	ODKAZ NA USTANOVENÍ GDPR	PRÁVNÍ OBLAST	ZNĚNÍ USTANOVENÍ	SOUČASNÝ STAV	IDENTIFIKOVANÝ NESOULAD S GDPR	MÍRA NEDOSTATKU	
Odpovědnost správce	čl. 24 (3)	Povinnosti správce; Kodexy	3. Jedním správců, jimiž se dotčí, že správce plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42.				
Odpovědnost správce	čl. 25 (1)	Ochrana údajů	1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež zakládá zpracování, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlení do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.				
Odpovědnost správce	čl. 25 (2)	Ochrana údajů	2. Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.				





© 2017 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena.

Vzorový průběh GDPR auditu

6 Implementace

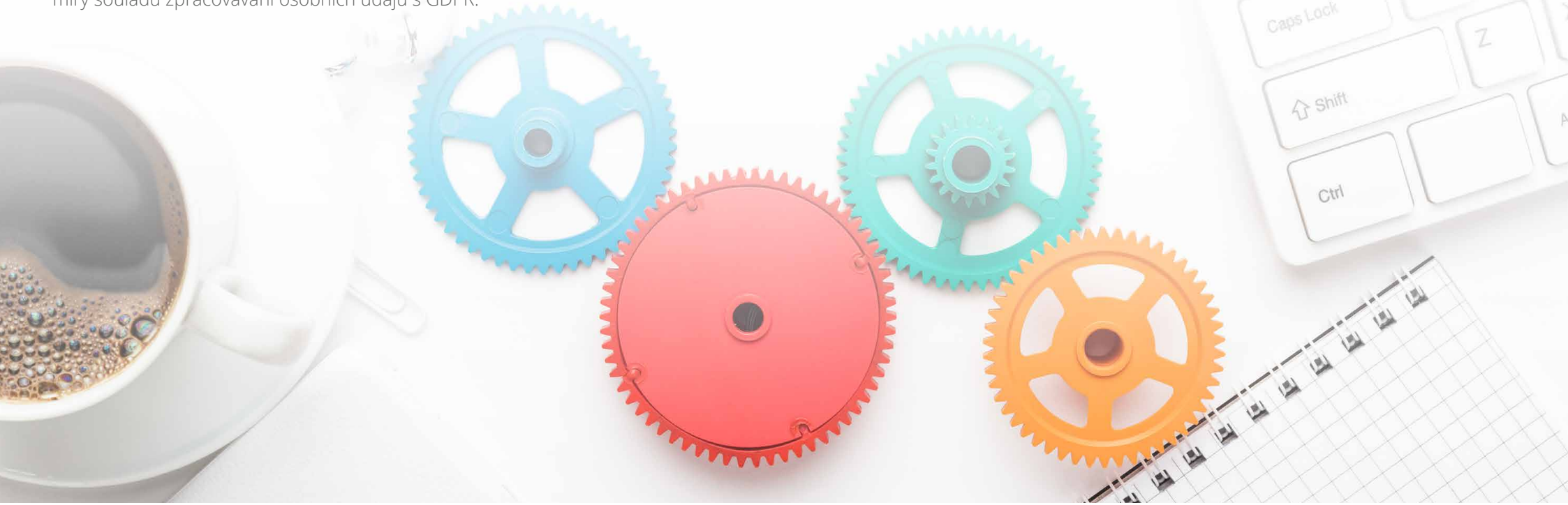
Organizaci je dán prostor pro implementaci doporučení uvedených v GAP analýze.

7 Reaudit

Po implementaci je proveden reaudit zpracovávání osobních údajů za účelem zjištění míry souladu zpracovávání osobních údajů s GDPR.

8 Záverečná zpráva

Na základě GAP analýzy a následné implementace od nás **organizace obdržíte závěrečnou zprávu, která slouží jako tzv. paper trail** – seznam opatření přijatých v rámci nastavení a udržení ochrany osobních údajů a jejich zpracování. GAP analýza a závěrečná zpráva slouží k prokázání **GDPR compliance** před dozorovým orgánem a je podkladem pro veškeré budoucí zpracování osobních údajů.



© 2017 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena.

Reference

Výroba a e-commerce

Více než 20 dokončených analýz nakládání s osobními údaji podle GDPR ve společnostech zaměřujících se na B2B.

Více než 15 ukončených GDPR auditů u společností s koncovými zákazníky - fyzickými osobami.

Zkušenost s GDPR audity se zahraničním přesahem - GDPR audit v rámci mezinárodního holdingu vlastněného českou matkou zastřešující dvanáct společností v rámci EU.

Zdravotnictví

GDPR audit pro skupinu zdravotnických klinik v Moravskoslezském kraji.

Audity soukromých lékařských praxi, včetně zubních ordinací.

GDPR audit holdingu, který zastřešuje zdravotnická zařízení napříč Českou republikou (kliniky, polikliniky, laboratoře a lékárny).

Veřejný sektor

GDPR školení a workshop pro čtvrtou největší vysokou školu v České republice. GDPR školení zaměstnanců správních úřa-dů, muzeí a divadel.

IT

Posouzení GDPR readiness softwarových řešení, například jedné z největších světových on-line marketingových platforem. Spolupráce s vývojáři na nových funkcionalitách pro podporu správců a zpracovatelů.

Posouzení GDPR readiness ITSM řešení u koncového zákazníka.

Více než 6 měsíců zkušeností s přípravou zpracovatelských smluv pro zákazníky.

© 2017 SEDLAKOVA LEGAL s.r.o. Všechna práva vyhrazena.