IB-CONSULTING & POSTUP ZAVEDENÍ SYSTÉMU OCHRANY OSOBNÍCH ÚDAJŮ DLE „GDPR“

ÚVODNÍ ANALYTICKÁ ČÁST:

V této fázi je nezbytné zmapovat, jak se ve firmě zachází s osobními údaji. Je nutné zjistit:

1. jaký druh osobních údajů se zpracovává (např. citlivé údaje, údaje dětí);
2. kdo s nimi pracuje (např. zaměstnanci jednotlivých odborů, externí dodavatelé);
3. kde jsou uloženy (např. CRM, jiná elektronická či papírová evidence);
4. na základě jakého právního titulu se osobní údaje zpracovávají (např. souhlas, smluvní povinnost, zákonné povinnosti);
5. k jakému účelu jsou data zpracovávána (např. mzdová či personální agenda, marketingové služby);
6. po jakou dobu jsou data zpracovávána (např. zda společnost osobní data smaže po ukončení projektu);
7. kde a jak se osobní údaje archivují (např. interní / externí úložiště, cloudové služby).

Prakticky je třeba do interního auditu zapojit jak vedení firmy, tak všechny odpovědné osoby. Harmonogram auditu může být následující:

1. úvodní porada vedení firmy - představení problematiky a rozsahu GDPR;
2. vytvoření GDPR týmu – zástupci všech oddělení, která pracují s osobními údaji;
3. audit jednotlivých oddělení;
4. zpracování získaných informací;
5. vytvoření závěrečné zprávy pro vedení společnosti s upozorněním na rizika a navržení praktických opatření.

PRAKTICKÁ ČÁST :

Na základě vypracované analýzy by měl návrh řešení obsahovat:

A) úpravu vnitřních norem a procesů společnosti:

1. úprava vnitřních dokumentů;
2. připravit se na případné zpracování posouzení vlivu na ochranu osobních údajů;
3. zajistit potřebnou dokumentaci k záznamům o činnostech zpracování;
4. analýzovat rizika ztráty dat a nastavit řešení bezpečnostních incidentů;
5. připravit se na zvláštní podmínky při zpracování osobních údajů dětí;
6. zajistit školení zaměstnanců, kteří nakládají s osobními údaji.

B) určení, zda společnost potřebuje pověřence pro ochranu osobních údajů (GDPR nestanoví žádné podmínky pro vzdělání či certifikování pověřence. Důležité je, aby měl znalosti a praktické zkušenosti v oblasti ochrany OÚ). Posoudit zda, zpracovatel povede záznamy o činnostech zpracování, za něž odpovídá (nad 250 zaměstnanců).

C) zajištění bezpečnosti zpracování osobních údajů

1. osobní údaje musí být zabezpečeny podle kategorie např. osobní a citlivé údaje;
2. v závislosti na kategorii zpracování osobních údajů nutno vyhodnotit možná rizika a preventivní opatření;
3. připravit postupy pro případné porušení ochrany dat. Nově musí být tato povinnost oznámena do 72 hodin Úřadu pro ochranu osobních údajů, ale i dotčené fyzické osobě;
4. zavedení technických opatření jako např. pseudonymizace (osobní údaje fyzické osoby jsou označeny číslem/kódem, přičemž spojovací číslo je vedeno odděleně od osobních údajů) a šifrování osobních údajů (postup, který převádí informace do nečitelné podoby na základě klíče/šifry) Nejde však o povinné podmínky zpracování osobních údajů, jde o bezpečnostní prvky, které mohou pomoci správci či zpracovateli OÚ.

REALIZAČNÍ FÁZE:

1. REVIDOVAT SOUHLASY SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ:

Revidovat a podrobněji upravit získané souhlasy se zpracováním osobních údajů, aby byl každý potenciální zákazník konkrétně informován, k jakému účelu poskytuje svoje osobní data. Takto revidované souhlasy bude potřeba zajistit v případě nepřímého marketingu. U zaměstnanců, stávajících zákazníků a obchodních partnerů je možné využívat již udělené souhlasy formou oznámení o zpracování jejich osobních údajů, pokud budou odpovídat výše uvedeným podmínkám.

2. REVIDOVAT SMLOUVY :

Revidovat smluvní vztahy mezi správcem (např. zaměstnavatel) a zpracovatelem (např. externí účetní firmou). Smlouva musí jasně nastavit povinnosti a odpovědnost za případnou škodu každé ze smluvních stran. V případě outsourcingu doporučujeme mít smluvně upraveno, že externí dodavatel zpracovává osobní údaje v souladu se všemi obecně závaznými právními předpisy.

Předpisy GDPR tak přimějí firmu, aby si „udělala v osobních datech pořádek“ a:

1. získala jasný přehled o osobních datech, která vlastní;
2. zlegalizovala data, která spravují neoprávněně;
3. zbavila se dat, která nepotřebují;
4. nastavila procesy, které zabrání úniku dat a vzniku škod.

V Třebíči dne 25.5.2018