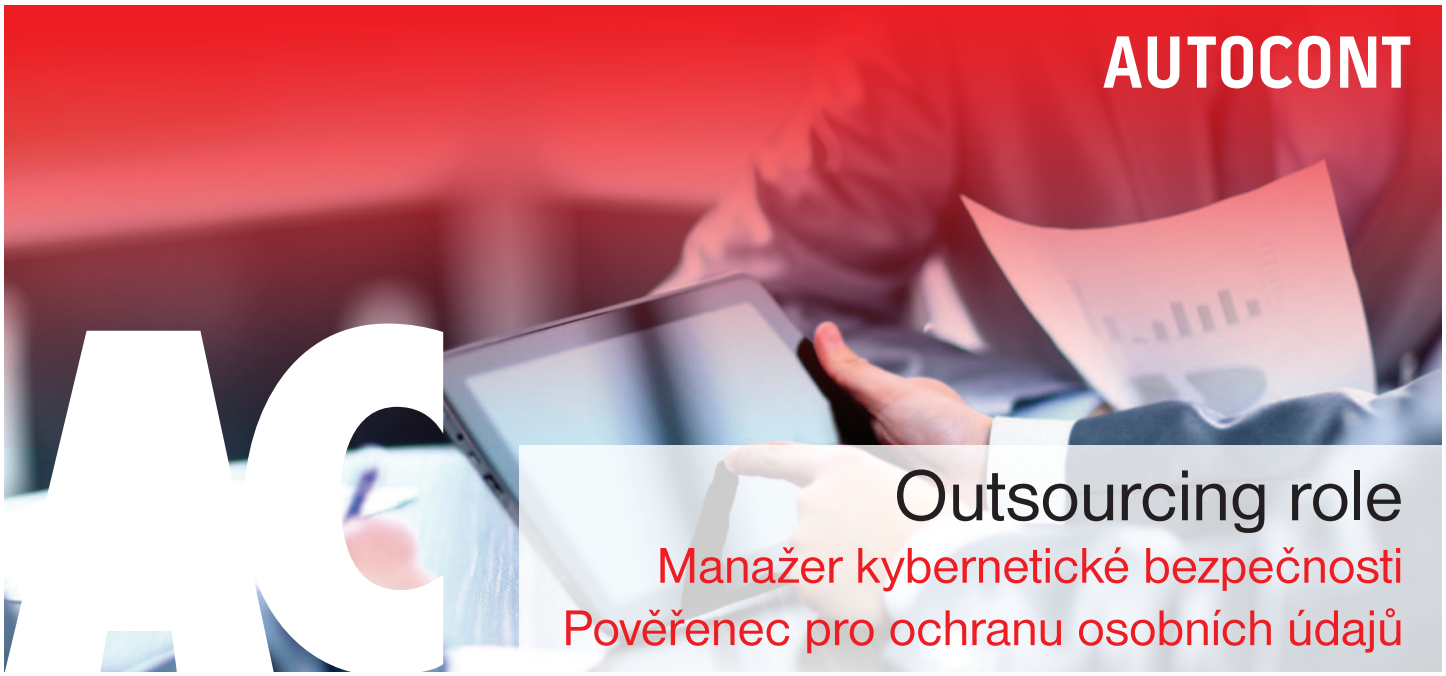


AUTOCONT

Outsourcing role

Manažer kybernetické bezpečnosti

Pověřenec pro ochranu osobních údajů

POŽADAVEK NAŘÍZENÍ GDPR ZAJISTIT ROLI POVĚŘENCE PRO OCHRANU OÚ MŮŽE PRO ORGANIZACE ZNAMENAT TENTÝŽ PROBLÉM, JAKO V PŘÍPADĚ MANAŽERA KYBERNETICKÉ BEZPEČNOSTI. EXTERNÍ OBSAZENÍ OBOU TĚCHTO ROLÍ SICE ORGANIZACI NIKDY NEZBAVÍ ZODPOVĚDNOSTI, ALE ZÍSKÁ TAK ZKUŠENÉHO SPECIALISTU.

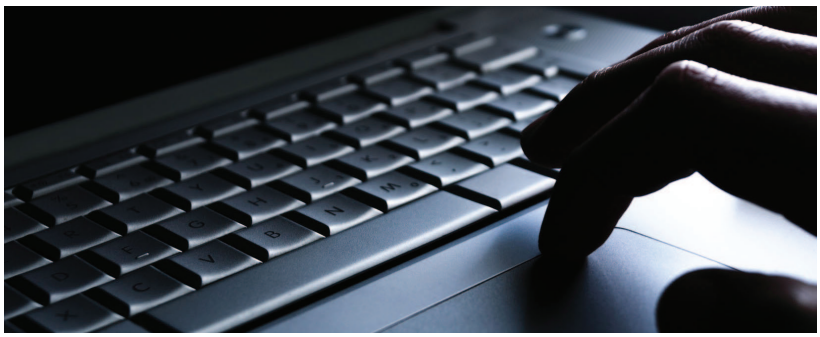
Manažer kybernetické bezpečnosti

Práce externího manažera KB zahrnuje především tzv. „měkké dovednosti“, jako je poradenství, metodické vedení, školení, ale i odborné konzultace na aktuální témata, řešení otázek kybernetické bezpečnosti, revize a dokumentování, případně navrhování změn interních procesů, úpravy a aktualizace bezpečnostních předpisů zákazníka, kontrolní činnosti týkající se dodržování stanovených bezpečnostních pravidel, licenční politiky, zvládání rizik či incidentů, změnového řízení atd.

Činnosti externě zastávané role manažera KB nebo pověřence pro ochranu OÚ jsou upraveny formou harmonogramu, který definuje jednotlivé požadované, ať už jednorázové, nebo pravidelně se opakující činnosti ve vhodné frekvenci.

Pověřenec pro ochranu osobních údajů

Činnost pověřence pro ochranu OÚ se v mnohém prolíná s činností manažera kybernetické bezpečnosti, zvláště pokud jde o bezpečnost dat. Výkon této role je však více zaměřen na konzultační činnost v oblasti právních předpisů a poskytování informací. Pověřenec dle požadavků organizace zajišťuje také posouzení vlivu na ochranu OÚ. Osoba v této roli by proto měla být zapojena do veškerých záležitostí souvisejících s ochranou OÚ, včetně auditu, a samozřejmě je v souvislosti s výkonem svých úkolů vázána tajemstvím nebo důvěrností.



AC

PŘÍNOSY

- V první řadě vyřešení personálního obsazení „povinných“ rolí
- Splnění požadavků zákonů, norem a standardů
- Získání erudovaného specialisty pro oblast řízení kybernetické bezpečnosti nebo ochrany OÚ (případně obojí) a know how jak v řízení bezpečnosti, tak při zpracování OÚ

U činností můžete definovat:

- rozsah,
- četnost/frekvenci,
- formu a způsob vedení záznamů/ evidence,
- formu a způsob reportingu,
- kontaktní a zodpovědné osoby.

Pověřenec je nápomocen zákazníkovi převážně svými doporučeními, návrhy a pokyny při zavádění vhodných postupů a opatření, a také při vedení záznamů spojených se získáváním, zpracováním, ukládáním, přenosem a likvidací OÚ s cílem prokázat soulad s požadavky GDPR na dokumentované procesy. Na pověřence se také mohou obracet subjekty OÚ ve všech záležitostech souvisejících se zpracováním jejich OÚ a výkonem jejich práv.

Žádný z požadavků GDPR Vám nebrání využívat externího specialistu v jedné osobě pro obě role, tzv. dva v jednom, pokud to budete potřebovat. Jedinou podmínkou je, aby žádný z přidělených úkolů a povinností nevedl ke střetu zájmů těchto rolí.

Samozřejmou činností obou rolí je pravidelný reporting určeným odpovědným osobám vedení organizace v dohodnutých intervalech nebo na vyžádání.

Měli byste mít na zřeteli, že žádný externí manažer (KB nebo ochrany OÚ) v žádném případě nepřebírá odpovědnost za zákazníka. Tomu ostatně odpovídá i charakter této outsourcované role, neboť ta primárně není (a zřejmě nebude pověřena) žádnou rozhodovací pravomocí. Povinností těchto rolí je v tomto směru pouze sledovat, kontrolovat, vyhodnocovat, navrhovat, doporučovat, reportovat a upozorňovat management na anomálie, nedostatky, nesoulad, hrozby, zranitelná místa či vzniklá rizika ohrožující bezpečnost informací, včetně osobních údajů.

NA JAKOU DOBU SI SLUŽBU POŘÍDIT?

Služba outsourcingu role manažera KB nebo pověřence pro ochranu OÚ (případně 2v1) je na počátku standardně nabízena na 1 rok s možností prodloužení dle potřeb organizace. Celkový minimální rozsah prací je však značně individuální, a proto také velmi variabilní. Vždy dbáme na to, aby naše služby byly efektivní a jejich minimalizace nebyla na škodu skutečným potřebám a cílům zákazníka.
Pro představu o obvyklém rozsahu Vám mohou posloužit následující informace:

- Po dobu prvních 6 měsíců se práce mohou pohybovat v rozsahu např. 1 člověkoden měsíčně u zákazníka (tzv. „on site“) a 1 člověkoden měsíčně vzdáleně (tzv. „off site).
- Po „usazení“ činností a skutečných potřeb jsou pak zajišťovány činnosti v rozsahu 1 člověkoden za 2-3 měsíce „on site“ a 1 člověkoden za 2-3 měsíce vzdáleně.
- Celkově předpokládáme v prvním roce poskytování této služby v rozsahu minimálně 12-24 člověkodnů (v závislosti na požadované roli).
- Další činnosti mohou být vykonávány na vyžádání nebo v případě bezpečnostního incidentu či plánovaného auditu.