Ministerstvo financí
České republiky

STANOVISKO

ODBORU CENTRÁLNÍ HARMONIZAČNÍ JEDNOTKA
Č. 1b/2018

Dotaz

Může interní auditor vykonávat zároveň funkci pověřence pro ochranu osobních údajů (DPO) v rámci agendy GDPR?

ZAŘAZENÍ DOTAZU

PRÁVNÍ PŘEDPIS	• zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)
SOUVISEJÍCÍ PRÁVNÍ PŘEDPISY	• 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
KLÍČOVÁ SLOVA	interní audit; GDPR ; pověřenec pro ochranu osobních údaj; DPO
DATUM ZPRACOVÁNÍ	vydáno 13. dubna 2018; aktualizováno 21. září 2018
ZPRACOVATEL	oddělení 4701 – Harmonizace interního auditu

Stanovisko

Interní auditor, který vykonává interní audit podle zákona o finanční kontrole, nemůže být jmenován pověřencem pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů. Pověřenec pro ochranu osobních údajů nemůže být organizačně začleněn do útvaru interního auditu nebo podřízen vedoucímu útvaru interního auditu nebo internímu auditorovi.

Odůvodnění:

Interní audit je definován v ustanovení § 28 odst. 2 zákona o finanční kontrole jako nezávislé a objektivní přezkoumávání a vyhodnocování operací a vnitřního kontrolního systému orgánu veřejné správy. Hlavním úkolem interního auditu je dávat doporučení ke

zdokonalování kvality vnitřního kontrolního systému, k předcházení nebo ke zmírnění rizik a k přijetí opatření k nápravě zjištěných nedostatků (srov. § 28 odst. 3 zákona o finanční kontrole). Aby interní audit mohl plnit své úkoly v souladu s požadavky zákona o finanční kontrole, musí být funkčně nezávislý a organizačně oddělen od řídicích výkonných struktur. Tento požadavek je zakotven v ustanovení § 29 odst. 1 zákona o finanční kontrole. Ustanovení § 29 odst. 4 zákona o finanční kontrole tyty požadavky ještě upřesňuje a výslovně stanoví, že útvar interního auditu nelze pověřovat úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.

Interní auditor by měl mít přístup ke všem informacím, záznamům, dokladům, systémům, operacím, zaměstnancům a k veškerému majetku orgánu veřejné správy. V rámci své činnosti vytváří auditní stopu, ve které zpracovává osobní údaje. Příkladem této auditní stopy jsou zápisy ze schůzek, dotazníky, zprávy o vykonaném interním auditu. Dále je mu umožněno nahlížet do informačních systémů, smluv, faktur a další dokumentace orgánu veřejné správy, které obsahují osobní údaje. Interní auditor tudíž shromažďuje, zaznamenává, ukládá, používá, zpřístupňuje a šíří osobní údaje. Interní auditor je zpracovatelem osobních údajů.

Základní úkoly pověřence pro ochranu osobních údajů jsou stanoveny v čl. 39 obecného nařízení o ochraně osobních údajů. Jde zejména o poskytování poradenství, ověřování souladu s právními předpisy upravujícími ochranu osobních údajů, posuzování vlivu připravovaných opatření na ochranu osobních údajů a spolupráci s dozorovým úřadem. V případě sloučení funkce interního auditora a pověřence pro ochranu osobních údajů se pověřenec dostává do střetu zájmu, protože jako interní auditor plní úkoly, u kterých v široké míře zpracovává osobní údaje a jeho činnost by měla být podřízená nezávislému a objektivní posouzení pověřence pro ochranu osobních údajů. Ve sloučené pozici může mít pověřenec zájem jako interní auditor na určitém způsobu zpracování osobních údajů. Jeho poradenská činnost a doporučení v tomto případě nebude naplňovat požadavek obecného nařízení plnit své povinnosti a úkoly nezávislým způsobem.

I když na první pohled, v důsledku použité terminologie, může vymezení úkolů pověřence pro ochranu osobních údajů evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze je zaměňovat. Naplňování povinností vyplývajících orgánu veřejné správy z právních předpisů upravujících ochranu osobních údajů, včetně plnění úkolů pověřence pro ochranu osobních údajů, jsou součástí vnitřního kontrolního systému.

Vnitřním kontrolním systémem v rámci orgánu veřejné správy je souhrn nástrojů, procesů a opatření, které jsou zavedeny v organizaci k ošetření rizik, která ohrožují dosažení stanovených cílů. Jedná se tedy o jakýkoliv řídicí kontrolní mechanismus, včetně výkonu funkce pověřence pro ochranu osobních údajů. Interní auditor podle § 28 odst. 2 zákona o finanční kontrole objektivně a nezávisle přezkoumává vnitřní kontrolní systém a dává doporučení ke zdokonalování jeho kvality. Podle § 29 odst. 4 zákona o finanční

kontrole nelze interního auditora pověřit úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů. V praxi může nastat situace, že činnost pověřence pro ochranu osobních údajů bude prověřována interním auditorem a dle názoru interního auditora nebude pověřenec postupovat v souladu s právními předpisy nebo vnitřními směrnicemi orgánu veřejné správy. V tomto případě interní auditor předloží vedoucímu orgánu veřejné správy doporučení k přijetí opatření k nápravě zjištěných nedostatků. Bude-li funkce pověřence a interního auditora sloučena, ověření interního auditora nebude objektivní a nezávislé, tak jak to stanoví § 28 odst. 2 zákona o finanční kontrole. Zároveň bude porušeno ustanovení § 29 odst. 4 zákona o finanční kontrole, které zakazuje pověřovat interního auditora úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.

Právní úprava zaručuje internímu auditorovi a pověřenci pro ochranu osobních údajů nezávislé postavení a vylučuje střet zájmů. Tato nezávislost je zaručená pro tyto funkce samostatně. V případě jejich sloučení nebude požadavek na zajištění nezávislosti naplněn ani u jedné z nich.

Výkon funkce pověřence pro ochranu osobních údajů interním auditorem nebo zařazení pověřence do útvaru interního auditu je v rozporu s ustanoveními zákona o finanční kontrole, které upravují funkční nezávislost a postavení interního auditora (zejména ustanovení § 28 odst. 2 a 3, § 29 odst. 1 a 4 zákona o finanční kontrole).

Neslučitelnost funkce pověřence pro ochranu osobních údajů a interního auditora se vztahuje jen na orgány veřejné správy, které zřídily útvar interního auditu nebo výkonem interního auditu zvlášť pověřily zaměstnance podle § 28 odst. 1 zákona o finanční kontrole. Neslučitelnost funkcí se tudíž nevztahuje na obce do 15 000 obyvatel, které dle zákona nahradily interní audit přijetím jiných opatření podle § 29 odst. 6 zákona o finanční kontrole. Z celkového počtu obcí se neslučitelnosti funkcí pověřence pro ochranu osobních údajů a interního auditora vztahuje jen na 89 obcí, které přesahují 15 000 obyvatel.[1]

Dále se neslučitelnost funkcí nevztahuje na organizační složky a příspěvkové organizace, u kterých zřizovatel nahradil funkci útvaru interního auditu výkonem veřejnosprávní kontroly podle § 29 odst. 5 zákona o finanční kontrole.

Zákon o finanční kontrole neupravuje sankce za porušení ustanovení upravujících interních audit. Ministerstvo financí není oprávněno ukládat sankce ani nápravné opatření v případě jeho porušení.

Porušení ustanovení obecného nařízení o ochraně osobních údajů upravující povinnost zajistit, aby pověřenec nevykonával úkoly a povinnosti, které by mohli vést ke střetu

[1] Údaj dle Českého statistického úřadu k 1. 1. 2018.

zájmu, lze podle článku 83 obecného nařízení sankcionovat správní pokutou až do výše 10 mil. EUR.