Minimum ochrany osobních údajů pro auditory

„Rozlišení role pověřence a interního auditora a jejich vzájemný vztah je zásadní otázkou, kterou musí správce (zpracovatel) ve své plné a výlučné kompetenci řešit. Tento článek poskytuje přehled nejčastějších problémů a upozorňuje na kritéria, k nimž je nutno při zřízení role pověřence, vedle často již v organizaci existující funkce auditora, přihlédnout. Současně upozorňuje na některé nevhodné zjednodušující přístupy k funkci pověřence, které mohou vést ke znehodnocení mechanizmů ochrany osobních údajů v organizaci, neboť klíčovou osobou a garantem opatření ochrany údajů pro správce musí být v prvé řadě vlastní pověřenec.“

JUDr. Soňa Matochová, Ph.D.
vedoucí oddělení analytického
úřad pro ochranu osobních údajů

Již v průběhu přípravy na účinnost obecného nařízení o ochraně osobních údajů[1] se začalo spontánně objevovat srovnávání funkce auditora a pověřence pro ochranu osobních údajů, případně interního auditu a auditu ochrany osobních údajů. Názory na tato témata nebyly jednotné a teprve v průběhu času začala být problematika chápána v hlubších souvislostech. Do jisté míry kontroverzním tématem se stala především slučitelnost funkce auditora a pověřence, přičemž praxe za situace neustálenosti autoritativního názoru směřovala k nastavování ad hoc řešení podle konkrétních podmínek. Zároveň bylo zřejmé, že existuje větší počet otázek týkajících se vzájemného vztahu ochrany osobních údajů a auditu. Lze uvést jejich příklady:

- Existují nějaké společné rysy ochrany osobních údajů a auditu (interního auditu)? Případně jaké jsou rozdíly mezi těmito oblastmi?
- Jakou roli by měli hrát auditoři (interní auditoři) při zajišťování souladu s ochranou osobních údajů?
- Do jaké míry je potřebné, aby se auditoři orientovali v problematice ochrany osobních údajů?
- Může interní auditor vykonávat funkci pověřence ochrany osobních údajů?
- Jaká je role Úřadu pro ochranu osobních údajů, ústředních orgánů státní správy a profesních komor auditorů při hledání odpovědí na otázky vztahu interního auditu a ochrany osobních údajů?

Při odpovědi na vznesené otázky je potřebné vyjít z širších východisek platných pro oblast ochrany osobních údajů a audit obecně. Úvodem

1 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

je třeba říct, že právě ono hledání správných odpovědi je v logice obecného nařízení, které velmi často nenabízí jednu předem danou správnou odpověď, ale spíše předpokládá systematický přístup vycházející z relevantní právní úpravy, shromáždění rozhodných skutečností a argumentů pro posouzení a poté nalezení nejvhodnějšího řešení. V každém případě je při posuzování nastolených otázek nutné vyjít z účelu, systematiky, institutů a principů právní úpravy ochrany osobních údajů na jedné straně, a z účelu, úkolů a metodik auditu či interního auditu na druhé straně.

Je vhodné začít tím, že ochrana osobních údajů upravená obecným nařízením představuje zásadní komplexní právní úpravu, jejímž účelem je zajištění ochrany osobních údajů v dané oblasti, sektoru či organizaci prostřednictvím aplikace a implementace institutů a principů obecného nařízení. Naopak audit (z lat. *auditus*, slyšení) obecně znamená úřední přezkoumání a zhodnocení dokumentů, zejména účtů, nezávislou osobou. Účelem je zjistit, zda doklady podávají platné a spolehlivé informace, a zhodnotit kvalitu vnitřní kontroly firmy. Obvykle se audit zabývá jen vzorky a jeho výsledek neznamená naprostou jistotu, nýbrž jen rozumnou pravděpodobnost konečného hodnocení. Pokud jde o interní audit ve smyslu zákona o finanční kontrole,[2] je definován jako nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesů v organizaci. Pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení správy organizace.

Z výše uvedeného je zřejmé, že audit a ochrana osobních údajů představují dvě rozdílné oblasti, které vyžadují ke svému zvládnutí odborníky se zcela rozdílnou kvalifikací a předpoklady. V obou případech se přitom jedná o vysoce specializované odbornosti. I když v současné době neexistuje dostatek odborníků zabývajících se ochranou osobních údajů, jde pouze o přechodnou situaci, jejímž řešením by jistě nebylo svěřit ochranu osobních údajů auditorům. To však nic nemění na tom, že existují i přirozené průniky obou oblastí. U činností souvisejících s prováděním auditu musí být vždy vyřešeny i dílčí otázky ochrany osobních údajů, zatímco vynaložené náklady na ochranu osobních údajů se nevyhnou posouzení auditorem, pokud jde o jejich hospodárné vynakládání. Také sofistikované a rozpracované metody a poznatky interního auditu, které využívají systémové a analytické přístupy a metody, je jistě možné v obecné rovině využít i při auditu osobních údajů.

V kontextu vztahu interního auditu a ochrany osobních údajů bývá často poukazováno na podobnost mezi pověřencem pro ochranu osobních údajů a auditorem. Domnívám se, že tuto podobnost lze spatřovat především v tom, že obě funkce vyžadují vysokou specializovanou odbornou kvalifikaci, nadto v rámci širšího vědomostního základu (zpravidla právnické nebo ekonomické vzdělání). Ovšem zatímco pověřenec pro ochranu osobních údajů musí znát právní úpravu a praxi ochrany osobních údajů a souvisejících oblastí, náležitě se orientovat v IT odbornosti a kybernetické bezpečnosti, interní auditor je odborníkem v jiných oblastech, zaměřuje se i na velmi specifické otázky, což např. ve veřejné správě verifikuje služební zkouška. U obou odborností je společná také nezbytnost stálého odborného růstu, kontinuálního vzdělávání a samostudia. Je přitom v zájmu organizace (statutárního orgánu), aby pro výkon obou funkcí našel ty nejlepší odborníky, protože jen tak zajistí soulad s požadavky interního auditu nebo ochrany osobních údajů. Výslovně je třeba také zdůraznit etické či morální předpoklady pro výkon obou profesí,

„V kontextu vztahu interního auditu a ochrany osobních údajů bývá často poukazováno na podobnost mezi pověřencem pro ochranu osobních údajů a auditorem.“

„Auditor i pověřenec tedy mají své místo v organizaci a předpokládá se jejich spolupráce a sdílení know-how.“

2 Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).

osobnostní integritu a spolehlivost.
Je zřejmé, že rozdílné úkoly vyžadují nejen rozdílné profesní předpoklady, ale i rozdílný způsob myšlení, přístupů k řešení problémů, a dokonce rozdílné osobní vlastnosti. Zatímco interní auditor pracuje víceméně samostatně, případně v rámci útvaru vnitřního auditu, a výsledky své práce odevzdává vedoucímu organizace, u pověřence budou velmi důležité jeho komunikační a negociační schopnosti, včetně schopnosti srozumitelně vysvětlit otázky ochrany osobních údajů ostatním pracovníkům či tazatelům (subjektům údajů), případně přesvědčit vedení organizace o potřebě realizovat vhodné postupy k ochraně osobních údajů. V zásadě lze říct, že problematika ochrany osobních údajů je širší, dotýká se více právních oblastí a není oddělitelná od otázek prosazování základních práv, včetně aplikace principu proporcionality. Navíc, protože jde o problematiku novou a v řadě aspektů dosud výkladově neustálenou, vyžaduje zvýšené úsilí a nasazení zejména v počátečním období účinnosti obecného nařízení.

K otázce, zda může být interní auditor zároveň pověřencem, se v nedávné době vyjádřilo také stanovisko ministerstva financí. Z tohoto stanoviska[3] vyplývá, že interní auditor podle zákona o finanční kontrole[4] nemůže být jmenován pověřencem pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů. Naopak pověřenec nemůže být organizačně začleněn do útvaru interního auditu nebo podřízen vedoucímu útvaru interního auditu nebo internímu auditorovi. V odůvodnění se uvádí, že 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[5]. Stanovisko shrnuje, že i když na první pohled může vymezení úkolů pověřence evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze je zaměňovat. S tímto závěrem ministerstva financí lze souhlasit.

Zajímavou otázkou je podrobnější srovnání nezávislosti pověřence a auditora. V obou případech je nezávislost definována přímo právní úpravou, avšak s použitím mírně odlišných slovních formulací. Nezávislost interního auditora je definována jako funkční a organizační, což spočívá v tom, že je přímo podřízen vedoucímu orgánu veřejné správy a je oddělen od řídicích výkonných struktur. Dále je stanoveno, že útvar interního auditu nelze pověřovat úkoly, které jsou v rozporu s nezávislým plněním jemu stanovených úkolů.[6] U pověřence je nezávislost formulována obecněji,[7] a to tak, že nedostává žádné pokyny týkající se jeho úkolů a je přímo podřízen vrcholovým řídicím pracovníkům správce nebo zpracovatele. Za specifické a ojedinělé je v rámci našeho právního řádu třeba považovat ustanovení, podle něhož pověřenec nemůže být propuštěn ani sankcionován v souvislosti s plněním svých úkolů. Účelem tohoto přímo účinného ustanovení obecného nařízení je preventivně chránit pověřence, aby se nemohl stát předmětem postihu např. v situacích, kdy by navrhoval a prosazoval opatření směřující k vyššímu standardu ochrany osobních údajů, se kterými by vedení organizace nesouhlasilo.

Nicméně za důležitější než výše citované odlišné slovní znění obou ustanovení vztahujících se k nezávislosti interního auditora a pověřence je třeba považovat účel činnosti, ke kterému je nezávislost vztažena. Úkolem pověřence je zajištění vysoké úrovně ochrany fyzických osob a odstranění překážek bránících volnému pohybu osobních údajů, zatímco interní audit sleduje cíle v oblasti odpovědnosti za řízení a kontrolu veřejných financí. Z praktického hlediska je tedy zřejmé, že interní auditor je víceméně součástí kontrolních mechanizmů v oblasti ekonomiky organizace, zatímco pověřenec pracuje primárně s osobními údaji a navrhuje vhodné postupy při jejich ochraně. Znamená to, že jak nezávislost pověřence, tak auditora je v jim svěřených oblastech samostatná. Musí tedy vždy navrhovat opatření podle toho, za jakou činnost jsou odpovědni, což bude prakticky znamenat odlišné návrhy postupů v odlišných oblastech.

K činnosti pověřence lze ještě dodat, že se předpokládá, že kolem sebe vytvoří neformální tým osob, které ve své činnosti v rámci organizaci zajišťují některé aspekty ochrany osobních údajů. Takový tým lze považovat za nanejvýš vhodnou platformu ke sdílení zkušeností v oblasti ochrany osobních údajů a formulování projektů, návrhů a doporučení, které povedou k následnému vytváření nové kultury ochrany osobních dat v organizaci. To vlastně také bylo smyslem zavedení institutu pověřence do právní úpravy obecného nařízení.

3 https://www.mfcr.cz/cs/legislativa/metodiky/2018/stanovisko-ministerstva-financi-k-proble-31614
4 Zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole).
5 Ustanovení § 29 odst. 1 zákona o finanční kontrole.
6 Ustanovení § 29 odst. 4 zákona o finanční kontrole.
7 Čl. 38 odst. 3 obecného nařízení.

Auditor i pověřenec tedy mají své místo v organizaci a předpokládá se jejich spolupráce a sdílení know-how. Sloučení obou činností nebude přicházet v úvahu již proto, že auditor a pověřenec jsou odborníky „na něco jiného," a není tedy ani vhodné. Nejde však o dogma a vždy je třeba posoudit konkrétní situaci. Je třeba rozlišovat činnost interního auditora podle zákona o finanční kontrole a auditora, jehož postavení není upraveno tímto způsobem. Nadto je okruh interních auditorů podle zákona o finanční kontrole omezen jen na určený okruh subjektů ve veřejné správě, zatímco pověřence musí mít všechny veřejné subjekty. Pokud se tedy praxe v počátečním období účinnosti obecného nařízení snažila nalézt ekonomicky úsporná řešení ve spojení obou odpovědností u jedné osoby, je to třeba považovat za přechodné řešení. Navíc obecné řešení umožňuje pružná řešení, pokud jde o pověřence, takže správci (zpracovateli) nic nebrání, aby pověřence zaměstnával na částečný úvazek nebo externě.

„U obou odborností je společná také nezbytnost stálého odborného růstu, kontinuálního vzdělávání a samostudia."

Závěrem je na místě učinit zmínku o roli státních orgánů a profesních komor v procesu implementace obecného nařízení. Zatímco, ve shodě s kompetenčním zákonem, ústřední orgány státní správy mají své místo při metodickém vedení subjektů v jim svěřených oblastech, kam patří i právně nezávazná doporučení vhodných postupů v oblasti ochrany osobních údajů, Úřad pro ochranu osobních údajů je nezávislým dozorovým úřadem, který se v rámci své působnosti podílí na vzdělávání a poskytuje obecné konzultace v oblasti ochrany osobních údajů, nikoliv však konkrétní návody k postupu dotčených subjektů. V tomto ohledu je třeba zdůraznit plnou odpovědnost správce (zpracovatele), který jediný zná veškeré konkrétní okolnosti a požadavky týkající se jeho činnosti, a podle nich musí nastavit pravidla ochrany osobních údajů. Výslovně je také v kontextu otázek řešených v tomto článku zdůraznit významnou a dosud plně v praxi neuchopenou roli profesních komor při výkladu otázek ochrany osobních údajů nastolených obecným nařízením v oblasti jejich zájmu.

Výše uvedená vysvětlení týkající se otázek ochrany osobních údajů a auditu (interního auditu) umožňují učinit následující závěry:

- Zatímco praxe ochrany osobních údajů představuje implementaci principů ochrany osobních údajů, jejímž cílem je dosáhnout náležité ochrany soukromí a osobních údajů, audit obecně je především činností metodickou, která směřuje k optimálnímu nastavení procesů v organizaci.
- Jak ochrana osobních údajů, tak interní audit, představují vysoce odborné činnosti předpokládající, že je budou vykonávat specializovaní odborníci, kteří se budou průběžně vzdělávat a zvyšovat svou kvalifikaci.
- Jak pro funkci pověřence, tak auditora je podstatné, aby splňovali morální a etické předpoklady vážící se k jejich činnosti.
- U obou funkcí jsou samostatně formulovány požadavky na nezávislost, kterou je nezbytné vnímat především v rámci účelů jim svěřených odlišných činností.
- Střet zájmů musí být vždy posuzován v konkrétním případě vzhledem k okolnostem a celkovému nastavení činností správce (zpracovatele) prostřednictvím právní úpravy i interních předpisů.
- Lze souhlasit se stanoviskem ministerstva financí, které dospělo k závěru, že i když na první pohled může vymezení úkolů pověřence evokovat podobnost s úkoly, které jsou svěřeny internímu auditorovi, nelze obě činnosti zaměňovat.
- V praxi se předpokládá spolupráce obou profesí, takže interní auditor by měl být součástí širšího zázemí ochrany dat v organizaci a přispívat ke zvyšování kultury zacházení s osobními údaji.
- V každém případě je konkrétní řešení otázek ochrany osobních údajů vždy plně a výlučně odpovědností správce (zpracovatele).