16. 12. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Význam compliance pro malé a střední podniky aneb co přinesla nová metodika Nejvyššího státního zastupitelství

Požadavky na compliance management systém právnické osoby ve světě nové metodiky Nejvyššího státního zastupitelství

Dne 10. listopadu 2020 byla na tiskové konferenci představena nová metodika Nejvyššího státního zastupitelství (dále jen „NSZ“) pro orgány činné v trestním řízení, která se zabývá exkulpací právnické osoby z trestného činu spáchaného jejími zaměstnanci a dalšími osobami ve smyslu § 8 odst. 5 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů (dále jen „TOPO“).

Hlavním důvodem vydání této třetí verze metodiky je potřeba zdokonalení postupů při vyhodnocování přijatých opatření, neboť není tajemstvím, že jak kriminalisté, tak státní zástupci v některých případech tápou v tom, jak vyložit pojem „vynaložení veškerého úsilí, které lze po právnické osobě spravedlivě požadovat“ v § 8 odst. 5 TOPO, resp. kam jej umístit na ose ohraničené na jedné straně názorem, že stačí závadné jednání zakázat ve vnitřním předpise, a na straně druhé názorem, že pokud přijatá opatření nezamezila závadnému jednání, nebyla dostatečná, a právnická osoba tedy dostatečné úsilí nevyvinula (i s tímto názorem státních zástupců se bylo možné setkat, zejména zkraje účinnosti zákona č. 183/2016 Sb., který do TOPO exkulpaci v ust. § 8 odst. 5 vnesl).

Metodika NSZ i v této verzi staví na významu compliance funkce v právnické osobě a místo přímé odpovědi na otázku, jakou intenzitu preventivních opatření lze považovat za dostatečnou, nabízí návod na hodnocení vyspělosti compliance kultury obecně a efektivitu compliance programu dané právnické osoby konkrétně. Nejedná se o fundamentálně nový přístup, NSZ rozvíjí standardy zavedené především v bankovním sektoru (ale i v dalších odvětvích, zejména u společností s vlastníkem v USA, Německu nebo dalších zemích s vyspělou compliance kulturou), a obdobně jako jiné sofistikovanější rámce pro řízení rizik ve velkých, obvykle mezinárodních skupinách, nabízí nejen orgánům činným v trestním řízení, ale i právě vlastníkům a statutárním orgánům společností návod, jak poznat kvalitu kontrolního prostředí, případně jak tuto kvalitu zvýšit a průběžně udržovat na vysoké úrovni, resp. ve stádiu dostatečné vyspělosti svědčící, slovy zákona, o vynaložení spravedlivě vyžadovatelného úsilí.

Metodika tak pracuje s tzv. Demingovým, nebo téže PDCA[2] cyklem (s komplexnější podobou tohoto průběžného monitorovacího cyklu se lze setkat i v mezinárodně uznávaných standardech pro řízení rizik ISO a COSO[3]), tedy s kontinuálně probíhajícím a neustále se opakujícím cyklem činností i) identifikace a vyhodnocení rizik relevantních pro danou společnost, ii) přijetí mitigačních opatření, iii) nastavení kontrolního prostředí a iv) vyhodnocení kontrolního prostředí prostřednictvím průběžného monitoringu, které opět volně přechází v identifikaci stávajících i nových rizik, čímž se cyklus uzavírá. Tento cyklus není samoúčelný, vede k tomu, že, zjednodušeně řečeno, dané kontrolní (compliance) prostředí plní tři základní funkce:

- Program je přizpůsoben dané společnosti; každá společnost čelí jiné skladbě rizik, např. rizika výrobního závodu budou z velké části jiná (nikoliv menší či jednodušší, ale jiné podstaty), než rizika finanční instituce, a přijatá opatření tak reagují na skutečná rizika, jimž čelí daná společnost - společnost tedy zná svoje procesy a ví, kde hrozí riziko protiprávního jednání;

- Přijatá opatření jsou skutečně účinná a pomáhají včas odhalit případné projevy nežádoucího jednání - společnost tedy efektivně brání relevantním rizikům; a

- Program je dostatečně robustní, aby dokázal reagovat na rizika nová, a to ať již třeba s ohledem na nové legislativní požadavky, nebo na jiné vnější či vnitřní vlivy a jejich změny (např. nové typy či techniky podvodů, změna odběratelských či dodavatelských vztahů atd.) – společnost tedy aktivně hodnotí dostatečnost svého kontrolního prostředí na stávající i nová rizika.

Malé a střední podniky - podobná rizika, méně zdrojů

Již z popisu základních funkcí compliance programu je zjevné, že se jedná o disciplínu poměrně náročnou na odborné kapacity a že výše uvedené standardy ISO a COSO nelze jednoduše přenést do prostředí českých malých a středních podniků. S tím však metodika NSZ počítá a při hodnocení efektivity compliance programu malých a středních podniků (SME) bude použit též princip proporcionality, tedy bude nezbytné zkoumat, zda a nakolik společnost uzpůsobila svůj compliance program svým kapacitám a komplexnosti svého obchodního modelu.

Na druhou stranu je zapotřebí vzít v potaz, že řada podniků má již nastaveny nějaké základy „compliance programu“ či „compliance management systému“, tedy řízení shody, byť třeba nikoliv v oblasti trestního práva. Výrobní podniky pracují s normami stanovenými např. certifikačními autoritami nebo požadavkem na kvalitu stanovenou zákazníkem – odběratelem. Součástí obchodních vztahů mezi společnostmi pak bývá požadavek na důvěrnost vyměňovaných informací, např. obchodního tajemství, vzorů či cenových informací, s čímž souvisí nejen požadavek na důvěrnost zaměstnanců, ale též na zabezpečení elektronických úložišť a nosičů, na kterých jsou důvěrné informace zachyceny. Řada zejména zahraničních odběratelů vyžaduje též potvrzení a někdy i osvědčení souladu se zákonnými normami[4], technickými standardy[5], etickými standardy atd.

Program řízení shody tedy v řadě podniků již funguje a jeho rozšíření do trestněprávní oblasti je tedy logickou cestou, jak společnosti připravit obranný štít pro případ, že by některá z osob, jejichž jednání je společnosti přičitatelné, porušila v rámci podnikatelské činnosti společnosti zákon a dopustila se trestného činu. Pro tento případ již v minulosti řada společností (i z řad SME), právě v reakci na úpravu TOPO, přijala etický kodex nebo jiný vnitřní předpis upravující pravidla jednání zaměstnanců a zástupců společnosti při činnosti společnosti. Etický kodex je a má být základem (nejen) trestněprávní compliance, avšak nelze jej jen „opsat“ nebo si jej koupit jako „compliance balíček“, který jako ochranu před trestním stíháním právnické osoby v minulosti prodávaly i některé advokátní kanceláře, avšak bez toho, aby se alespoň seznámily se specifiky dané společnosti, s jejími riziky, procesy a kontrolním prostředím. Taková „univerzální“ řešení pro všechny však mají tendenci nezohledňovat specifická rizika konkrétní právnické osoby, neobsahují popisy a kontrolní mechanismy, a pokud je už obsahují, jsou obvykle přehnaně komplikované, nezohledňují praxi dané právnické osoby, a tedy vyžadují nadbytečné kapacity. V důsledku toho pak taková „univerzální řešení“ mnohdy nejsou dodržována pro svou složitost a v případě trestního řízení by poskytla medvědí službu; pokud by policejní vyšetřovatel konstatoval existenci vnitřního předpisu a zároveň

jeho systematické nedodržování, lze jen těžko počítat s tím, že by takový vnitřní předpis mohl sloužit jako důvod k exkulpaci (nebo alespoň jako polehčující okolnost).

Risk - based přístup

Jak je uvedeno výše, metodika NSZ předpokládá, že právnická osoba, volící cestu compliance funkce jako opatření pro omezení trestněprávních rizik, nastaví svůj compliance management systém přiměřeně podmínkám svého podnikání, tj. zejména rizikům, kterým čelí, a dostupným zdrojům. Očekává se tedy tzv. risk-based přístup, kdy společnost identifikuje klíčová rizika (tj. závažná rizika podle pravděpodobnosti jejich materializace a očekávatelného dopadu), a implementuje dostatečné kontrolní mechanismy pro zamezení, případně pro včasné odhalení závadného jednání. Uměním je pak takové kontrolní mechanismy napárovat na již prováděné kontroly či na jiné procesy, které mohou po úpravě sloužit právě ke kontrole. Právě takový „streamlining", tedy zefektivnění kontrolních procesů a zaměření se na důležitá rizika, je náročnou disciplínou, bez níž hrozí, že compliance program bude buď neefektivní, nebo excesivně náročný.

Blýská se na regtech

Velké a zejména mezinárodní společnosti obvykle disponují dostatečným aparátem na nastavení a udržování efektivního compliance programu, menší společnosti často alespoň na základní nastavení či ověření kvality compliance programu obvykle potřebují externí pomoc od advokátních kanceláří nebo poradenských společností; zapojení odborného know-how spolu s interní znalostí procesů společnosti při přípravě compliance programu, ať už ve fázi identifikace relevantních rizik, nastavování mitigačních opatření či ověřování jejich účinnosti, bude ještě nějakou dobu preferovaným způsobem, jak zajistit dostatečnou efektivitu compliance funkce.

Protože však compliance program začíná být čím dál více nezbytnou funkcí v rámci korporátního nastavení též malých a středních podniků[6], které mnohdy nemají rozpočet na komplexní právní a procesní poradenství ohledně compliance management systému, vznikl pod kuratelou Národního centra kompetence pro Kyberbezpečnost[7] projekt Masarykovy univerzity pro nabídnutí technického řešení compliance programu pro malé a střední podniky, jehož se PRK Partners účastní. Cílem je nabídnout malým a středním podnikatelům automatizované nástroje pro řešení otázek souvisejících se zajištěním souladu s regulatorními, právními či technickými normami a minimalizaci kybernetických hrozeb (tzv. compliance přístup) s orientací také na kybernetickou bezpečnost a kyberkriminalitu, a to vzhledem k tomu, že stále více aktivit se přesouvá z reálného světa do virtuálního prostoru, což je v současné době ještě umocněno aktuální situací vyvolanou COVID-19. V konečném důsledku tak projekt usiluje o navržení škálovatelných nástrojů pro řízení compliance rizik v digitalizovaném světě, tedy ze kterých si každý malý a střední podnik vybere a upraví ty nástroje, pomocí kterých bude řídit pouze ta rizika, kterým skutečně čelí.

Projekt je aktuálně v analytické fázi, kdy projektový tým zjišťuje potřeby a rizika, kterým SME čelí. Data jsou sbírána prostřednictvím edukativního dotazníku; zájemci tak mají možnost se na jednu stranu seznámit s okruhy běžných rizik, kterým malé a střední podniky čelí, a zároveň poskytnout zpětnou vazbu nad závažností takových rizik pro svou společnost. Dotazník je k dispozici na adrese zde.

Mgr. Martin Frolík
JUDr. Juraj Szabó, Ph.D.

Martin Frolík *je právník specializovaný na řízení compliance, regulatorních, právních a ostatních nefinančních rizik s dlouholetou praxí ve finančním sektoru. Působí v advokátní kanceláři PRK*

Partners, se specializací na navrhování, revidování a implementaci komplexních compliance programů v rámci obchodních společností. Za PRK Partners se účastní projektu Compliance program pro malé a střední podniky Národního centra kompetence pro Kyberbezpečnost[1], který si klade za cíl ve střednědobém horizontu přijít s technologickým řešením regulatorních požadavků (regtech) kladených na malé a střední podniky v oblasti compliance, ochrany informací a kyberbezpečnosti. Projektový tým tvoří přední experti Masarykovy univerzity a dalších partnerských společností na otázky compliance a kyberbezpečnosti.

***Juraj Szabó** je právníkem s dlouholetou zkušeností s řízením právní a compliance agendy ve velkých nadnárodních skupinách v bankovnictví a energetice. Implementoval komplexní compliance program ve skupině ČEZ. V současné době působí na Nejvyšším státním zastupitelství ČR jako expert na hodnocení compliance programů a je spoluautorem aktuální verze metodiky NSZ. Je též předsedou Rozhodčího soudu při HK ČR a AK ČR a rovněž se aktivně účastní projektu Compliance program pro malé a střední podniky.*

---

[1] Dílčí projekt Compliance program pro malé a střední podniky realizovaný v rámci projektu Národní centrum kompetence pro Kyberbezpečnost je řešen s finanční podporou TA ČR

[2] Zkratka ze slov Plan, Do, Check, Act, např. k dispozici >>> zde.

[3] Např. cyklus průběžného řízení rizik podle metodiky COSO -k dispozici >>> zde, nebo ISO standard pro řízení compliance rizik 19600:2014 k dispozici >>> zde, resp. chystaná nová verze tohoto standardu pod číalwm 37301 k dispozici >>> zde.

[4] Např. UK Antibribery / Antislavery law

[5] Např. ISO 27001 ohledně informační bezpečnosti,

[6] A to nejen s ohledem na aktuálně diskutovanou politiku, ale i chystanou legislativu; např. ve smyslu k dispozici >>> zde. bude každý zaměstnavatel s více než 50 zaměstnanci povinen zajistit přijímání a včasné nezávislé prošetřování a vyřizování oznámení možného spáchání trestného činu nebo přestupku nebo porušení jiné zákonné povinnosti stanovené některými právními předpisy (whistleblowing).

[7] Blíže k dispozici >>> zde.

Další články:

- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí

- TOP 5 judikátů z korporátního práva za rok 2025
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách