



ia

interní auditor

ČTVRTLETNÍK ČESKÉHO INSTITUTU INTERNÍCH AUDITORŮ

ROČNÍK 25, ČÍSLO 3|2021 (101)

3|2021

Audit ochrany oznamovatelů

Vláda dne 1. února 2021 schválila návrh zákona o ochraně oznamovatelů protiprávních jednání (whistleblowerů). Návrh nyní projednává Parlament. Zákon počítá s nezávislým prošetřením podezření na protiprávní jednání nejpozději do třiceti dnů od oznámení. Při nedodržení povinností hrozí až milionové pokuty. Změny se dotknou nejen státní správy, ale také tisíců firem, z nichž některé už zřizují takzvané etické linky, které budou k oznamování protiprávních jednání sloužit.



Mgr. Stanislav Klika
Director, Risk Advisory Services
BDO Audit s.r.o.
Stanislav.Klika@bdo.cz

Návrh zákona, který má být národní úpravou směrnice Evropské unie, musí nabýt platnosti nejpozději do 17. prosince letošního roku. Zákon má poskytnout právní ochranu lidem, kteří informují o poškození veřejného zájmu, o němž se dozví v zaměstnání nebo v souvislosti s ním. Spáchané či plánované nepravosti se mohou týkat veřejných zakázek, finančních služeb, praní peněz, ale třeba i ochrany životního prostředí.

Nová právní úprava přináší řadu povinností. Připravil jsem pro vás proto přehled těch nejdůležitějších. Níže naleznete také užitečná doporučení, která vám pomohou v rámci přípravy auditu ochrany oznamovatelů nebo

kteřá můžete využít v rámci případné poradenské zakázky.

Koho se nové povinnosti týkají?

Nové povinnosti se nedotknou jen státních organizací či velkých nadnárodních koncernů. Vnitřní oznamovací systém budou muset zřídit všechny firmy a organizace s 25 a více zaměstnanci. A dále také veřejní zadavatelé, s výjimkou obcí do 5000 obyvatel. Nová povinnost se tak dotkne většiny firem a organizací.

Co je vnitřní oznamovací systém či etická linka?

Podnikům i dalším subjektům přibude povinnost zavést takzvaný vnitřní oznamovací systém, resp. tzv. etickou linku. Etickou linku si lze představit jako různé kanály a postupy pro přijímání, evidenci a šetření oznámení o porušení závazných pravidel.

Smyslem etické linky je umožnit oznamovatelům využít interní kanál namísto předání informací externím kontrolním orgánům. Firma tak může včas zjistit podvodné chování, překazít je a zabránit dalším škodám, včetně poškození reputace nebo uložení sankce.

Na základě obdržených oznámení by měla firma realizovat nápravná opatření, které zabrání obdobným nežádoucím jevům v budoucnu. Systém musí utajit totožnost oznamovatelů a ochránit je před odvetnými opatřeními.

„Vnitřní oznamovací systém budou muset zřídit všechny firmy a organizace s 25 a více zaměstnanci.“

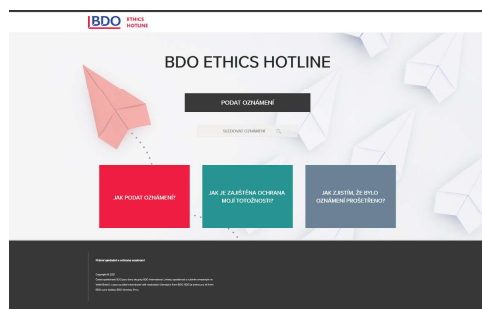
Kdo může oznámení podat?

Okruh oznamovatelů – tedy osob chráněných zákonem – je velmi široký. Kromě zaměstnanců to mohou být i uchazeči o zaměstnání, stážisté, členové představenstva či dozorčí rady. Oznamovat mohou ale i dodavatelé nebo zájemci o zakázku.

Je proto důležité, aby možnost podat oznámení byla snadno dostupná všem uvedeným subjektům. Efektivním řešením je např. zabezpečený internetový formulář na stránkách společnosti.

Jak lze oznámení podat a do kdy musí být vyřízeno?

Oznámení musí být možné podat písemně, telefonicky i osobně. Oznamovatel získá právo znát závěry šetření do třiceti dnů od oznámení. V odůvodněných případech lze tuto lhůtu prodloužit.



Chod vnitřního oznamovacího systému dokážou usnadnit internetové aplikace. Dnešní technologie umožňují rychlé a jednoduché zavedení takzvané etické linky, která slouží pro podání oznámení a zároveň plní funkci helpdesku či komunikační platformy. Aplikace pomůže hlídat lhůty, ať už bylo oznámení podáno prostřednictvím aplikace, nebo např. telefonicky, a do aplikace následně zaevidováno administrátorem. Tato určitá centralizace také přispívá k ochraně osobních údajů oznamovatelů. Těm zase nástroj umožní upozornit na problémy a rizika ve firmě prostřednictvím zabezpečeného formuláře. Užitek tak získají jak oznamovatelé, tak samotné firmy tím, že budou mít svoje rizika více pod kontrolou.

Jak lze novou povinnost využít pro zlepšení řízení podnikových rizik?

Podvodníci používají stále sofistikovanější metody, jak někoho napálit. Ať už jde o krádeže, nebo zpronevěry firemního majetku, neoprávněné slevy pro dodavatele, nebo získávání neoprávněného prospěchu od dodavatelů, podvodníci mohou připravit firmy o spoustu peněz i dobrou pověst. Riziko podvodu nebo

jiného nežádoucího jednání byste tedy rozhodně neměli podceňovat.

Preventivní mechanismy nemusí v konkrétních případech podvodům zabránit. Proto je důležité, abyste zavedli postupy, které umožní podvody odhalovat. Postupů, kterými lze podvody odhalit, je více. Doporučuji, abyste je vhodně kombinovali tak, aby vybalancovaly přínosy a vynaložené náklady.

Jedním z nákladově efektivních nástrojů detekce podvodů a nežádoucího jednání je zavedení vnitřního oznamovacího systému. Podle globální studie ACFE¹ je až 43 % podvodů odhaleno na základě oznámení ze strany zaměstnanců nebo zákazníků. Pro zajímavost interní audit podle této studie odhalil jen 15 % případů!

„Auditoři mohou podpořit organizaci při zavedení nebo zlepšení vnitřního oznamovacího systému.“

Zavedením etické linky tak firma získá účinný prostředek pro příjem informací o možných rizicích, nebo dokonce podvodech, a budete tak na ně schopna včas reagovat.

Jaké jsou další přínosy funkční ochrany oznamovatelů?

Společnost BDO každý rok zpracovává mezinárodní průzkum týkající se rizik, které hýbou světem. Nad těmito riziky se zamýšlejí vrcholoví představitelé firem ze všech koutů světa. Letošní Global Risk Landscape byl ve znamení zvládnání krize spojené s covid-19.

Tím hlavním poselstvím letošního průzkumu je, že společnosti, které se nebojí riskovat, si během pandemie vedly mnohem lépe. Riskovat v pandemii? To se ale

snadno řekne a hůř udělá. Co měly společného ty firmy, které se do většího rizika pustily a úspěšně jej zvládly?

Mezi faktory úspěchu patřila především schopnost nazírat věci z jiného úhlu pohledu, otevřenost a flexibilita v procesech a také péče o lidi – o zaměstnance, partnery i širší veřejnost. Získaná loajalita totiž pomáhá přestát nejrůznější krize.

Ochrana oznamovatelů patří mezi důležité mechanismy zodpovědného podnikání. Nabízí stakeholderům možnost bezpečně a jednoduše komunikovat, co je trápí. Pomáhá tak vytvářet důvěru ve vzájemných vztazích, čímž podporuje dlouhodobou spolupráci.

Jaká rizika jsou spojena s ochranou oznamovatelů?

Za nedodržení povinností vyplývajících ze zákona o ochraně oznamovatelů mají hrozit vysoké pokuty – až milion korun nebo 5 % z čistého obrátu za poslední ukončené účetní období.

Oznamovatel se bude moci obrátit i přímo na Ministerstvo spravedlnosti. Také z tohoto důvodu je v zájmu firem, aby jejich vnitřní oznamovací systém byl důvěryhodný a jednoduchý. Protože jinak ho oznamovatelé nejspíš nevyužijí a obrátí se rovnou na ministerstvo.

Vysoké pokuty a hrozba externích kontrol však nejsou jediným negativním dopadem nedodržení stanovených povinností. Jak bylo naznačeno výše, čím dál důležitější je dodržování principů společenské odpovědnosti firem a dobré vztahy s klíčovými partnery a veřejností. Porušování povinností spočívajících v ochraně oznamovatelů může odradit dosavadní i potenciální partnery od spolupráce a poškodit reputaci společnosti.

Tipy pro interní auditory

Auditoři mohou podpořit organizaci při zavedení nebo zlepšení vnitřního oznamovacího systému. Ověření procesů ochrany oznamovatelů (dosavadních nebo nově

¹ Report to the Nations: 2020 Global study on occupational fraud and abuse

zavedených) je možné pro zjednodušení strukturovat například následovně:

- postupy a nástroje pro příjem, správu a šetření oznámení,
- bezpečnost informací,
- transparentnost a zvyšování povědomí,
- personální zajištění vnitřního oznamovacího systému.

Postupy a nástroje

Pro firmy a organizace bude klíčové, aby stihly zavést vnitřní oznamovací systém do konce března příštího roku. Nejpozději od 1. dubna 2022 budou muset disponovat funkčním a bezpečným systémem pro přijímání oznámení.

„Úkolem číslo jedna bude výběr příslušné osoby (či osob), která dostane na starost přijímání oznámení a jejich nestranné a objektivní prošetřování.“

V této souvislosti budou muset firmy nastavit a zdokumentovat postupy pro přijímání, správu a šetření oznámení. Auditor by měl získat ujištění, že:

- oznámení mohou podat snadno všichni potenciální oznamovatelé,
- jsou sbírány relevantní informace podporující posouzení oznámení,
- oznámení jsou brána vážně, jsou prošetřována a v případě zjištění

nedostatků nebo rizik jsou realizována nápravná opatření,

- oznámení jsou vyřizována včas a jsou dodržovány zákonné i interní lhůty,
- zpracovávají se i anonymní oznámení,
- jsou určeny kanály pro příjem oznámení a jsou stanoveny postupy pro příjem oznámení jednotlivými kanály,
- funkcionality nástrojů a řešení pro příjem a správu oznámení vhodně podporují plnění stanovených povinností a jsou zdokumentovány pro případné externí kontroly,
- jsou nastaveny interní i externí kanály pro předávání informací, včetně plnění informační povinnosti vůči oznamovateli,
- jsou nastaveny kroky v rámci posouzení a šetření oznámení.

Bezpečnost informací

Firmy a organizace musí zajistit, aby totožnost oznamovatele nebyla bez jeho výslovného souhlasu sdělena nikomu jinému než příslušným osobám, které jsou kompetentní přijímat oznámení nebo na ně navazovat v rámci procesu jejich posouzení a prošetřování. To platí i pro jakékoli další informace, z nichž lze přímo či nepřímo odvodit totožnost oznamovatele. Totožnost oznamovatele a veškeré další informace lze poskytnout třetím stranám pouze v případě, že se jedná o povinnost uloženou právním předpisem.

Podobně je nutné chránit také osobní údaje osob dotčených šetřením oznámení a další citlivé firemní informace. Tato

oblast je spojena se zásadami ochrany osobních údajů a informační bezpečnosti. Auditor tak může ověřit, že:

- k údajům v oznámení a dalším informacím je řízen a monitorován přístup (seznamovat se s údaji v oznámení mohou pouze tzv. příslušné osoby),
- existují přiměřená pravidla pro hesla,
- údaje a další informace jsou bezpečně uloženy a archivovány (např. odhlašování el. zařízení v nepřítomnosti, zamykání fyzických dokumentů),
- dokumenty a elektronická zařízení, která je obsahují, jsou bezpečně likvidovány,
- nástroje používané pro příjem a správu oznámení splňují požadavky na bezpečnost informací (např. nastavení a správa uživatelských rolí, loga, minimalizace získávaných osobních údajů a možnosti případné anonymní komunikace, možnost smazat údaje atd.),
- uživatelé jsou řádně proškoleni, a to i pro případ možných bezpečnostních incidentů,
- s třetími stranami jsou uzavřeny písemné smlouvy.

Transparentnost a zvyšování povědomí

Jak bylo uvedeno výše, oznámení může podat značně široký okruh fyzických osob. Tyto osoby musí mít k dispozici jednoduše dostupné a srozumitelné informace ohledně podání a zpracování oznámení. Součástí firemních předpisů tak může být veřejně dostupná politika

ochrany oznamovatelů, kde firma popíše především:

- přístup k ochraně oznamovatelů,
- kdo a jak může oznámení podat,
- čeho se může oznámení týkat,
- jak a v jakém časovém horizontu bude oznámení posouzeno a
- jak bude zajištěna ochrana oznamovatelů a dalších osob.

V této souvislosti je důležité zaměstnancům a dalším partnerům také připomínat hodnoty a pravidla, které firma zastává a prosazuje.

Personální zajištění

Úkolem číslo jedna bude výběr příslušné osoby (či osob), která dostane na starost přijímání oznámení a jejich nestranné a objektivní prošetřování. Nikdo jiný se nebude moci s oznámeními seznamovat. Tato osoba by měla být bezúhonná, důvěryhodná a proškolená v postupech správy a šetření oznámení. Aby měla ochrana oznamovatelů smysl, oznámení nesmí šetřit ti, vůči nimž směřuje. Proto je nutné ve firemních postupech nastavit opatření pro prevenci střetu zájmů.

Vnitřní oznamovací systém může spravovat jak zaměstnanec společnosti, tak externí firma. Jak bylo uvedeno, u zaměstnance je třeba dobře zvážit, komu roli přidělít s ohledem na možný střet zájmů. Toto u externího poskytovatele většinou odpadá. Další výhodou externího zajištění může být nižší riziko prozrazení totožnosti oznamovatelů. ■