Rödl & Partner

COMPLIANCE & ESG NEWS ČESKÁ REPUBLIKA

Vydání:
č. 1/2024

Novinky ze všech oblastí Corporate Compliance, ESG a prevence korporátní odpovědnosti v České republice

www.roedl.cz

2023 právnická firma roku

Právnická firma roku 2012–2023

Rödl & Partner

COMPLIANCE & ESG NEWS ČESKÁ REPUBLIKA

Vydání:
č. 1/2024

Obsah:

Privacy & Data Protection Compliance: Nová metodika pro provozování kamerových systémů

Pavel Koukal
Rödl & Partner Praha

Jak jsme vás již dříve informovali, začátkem února zveřejnil český Úřad pro ochranu osobních údajů novou metodiku na provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů. Jedná se přitom o první výkladový dokument a metodické vodítko českého dozorového úřadu od účinnosti GDPR v roce 2018, které se vztahuje jak na zavádění, tak i na vlastní provozování kamerových systémů. Z nové metodiky přitom vyplývá pro provozovatele kamerových systémů i řada významných požadavků, které v praxi dosud nebyly až na čestné výjimky vůbec zohledňovány.

Nová metodika Úřadu pro ochranu osobních údajů navazuje na Pokyny Evropského sboru pro ochranu osobních údajů (EDPB) č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, které byly vydány v lednu roku 2020. Lze ale obecně konstatovat, že česká metodika je z hlediska požadavků na provozování kamerových systémů do značné míry detailnější i přísnější, než shora uvedené evropské pokyny, a to zejména, pokud jde o odůvodnění účelu a technických požadavků na zabezpečení kamerových záznamů.

Z hlediska svého obsahu se nová metodika skládá ze dvou základních částí, a to jednak z kapitoly věnované výchozím otázkám popisu kamerového systému a dále pak z kapitoly, která se zabývá požadavky na zpracování osobních údajů kamerovým systémem. Z praktického hlediska jsou velmi významné i tři přílohy této metodiky. Těmito přílohami je jednak vzor povinných informací o činnosti zpracování spojených s provozováním kamerového systému a dále pak související vzor záznamu o činnosti zpracování a konečně i vzor balančního testu, jež by měl být podle metodiky povinnou součástí procesu zavádění každého kamerového systému.

Pokud jde o konkrétní požadavky spojené se zavedením a provozováním kamerového systému, tak tyto se týkají v zásadě všech dílčích skupin požadavků na zpracování a ochranu osobních údajů. V tomto směru musí každý provozovatel kamerového systému konkrétně osvědčit a doložit účel a právní základ zpracování osobních údajů, konkrétní plnění povinností ohledně zásady minimalizace zpracování, jakož i nastavenou standardní dobu zpracování údajů z kamerových záznamů a zajištění práv dotčených subjektů údajů, zejména co do plnění informačních povinností provozovatele kamerového systému jako správce osobních údajů.

Podstatná část požadavků na kamerové systémy podle nové metodiky dozorového úřadu se týká zabezpečení kamerových systémů a požadovaných technických a organizačních opatření správce. Metodika přitom v těchto souvislostech rozlišuje tři třídy z hlediska míry porušení práv a zájmů subjektů údajů, a to třídu 1 (malá míra porušení), třídu 2 (střední míra porušení), třídu 3 (vysoká míra porušení) a konečně i třídu 4 (velmi vysoká míra porušení).

V praxi přitom většina provozovatelů kamerových systémů spadá pod třídy 1 a 2 a je proto je prakticky velmi významná tabulka základních technických a organizačních opatření spojených se zabezpečením kamerového systému. V této tabulce jsou uvedena konkrétní opatření, která je třeba přijmout a průběžně provádět, a to jak ve vztahu k ochraně kamer a datového připojení, tak i k ochraně záznamových zařízení a datových nosičů a ochraně dat (kamerových záznamů). Zapomínat nelze ani na ostatní doporučovaná opatření, jako je školení obsluhy nebo zpracování dokumentace.

U řady našich klientů jsme již začali s přípravou implementace požadavků vyplývajících z nové metodiky Úřadu pro ochranu osobních údajů, které by měly být co nejdříve řešeny každým provozovatelem kamerového systému, a to bez ohledu na jeho celkový rozsah anebo počet kamer.

Kontakt pro další informace

JUDr. Pavel Koukal
advokát
Associate Partner
T +420 236 163 710
pavel.koukal@roedl.com

Whistleblowing: Možnosti využití ISO normy pro interní vyšetřování

Pavlína Vondráčková
Rödl & Partner Praha

V souvislosti s povinností zavést vnitřní oznamovací systém podle zákona č. 171/2023 Sb., o ochraně oznamovatelů vznikla i otázka, jakým způsobem postupovat v rámci interního posuzování důvodnosti oznámení o možném protiprávním jednání.

Zákon o ochraně oznamovatelů v tomto směru žádnou bližší právní úpravu neobsahuje, a proto se jako vhodné řešení jeví využití dostupných standardů ISO, které jsou všeobecně známé a mezinárodně respektované. Pro whistleblowing a interní vyšetřování přitom lze využít zejména dvě poměrně nové a aplikovatelné normy ISO, a to jednak ISO 37002:2021 (Whistleblowing management systmes – Guidelines) a dále pak speciální normu použitelnou přímo pro interní vyšetřování, kterou je ISO/TS 37008:2023 (Internal investigations of organizations — Guidance).

Obecně platí, že ISO/TS 37008 je obecnou normou pro všechna interní vyšetřování v rámci organizací a lze ji tak použít nejen v souvislosti s compliance management systémem, ale na jakékoli interní postupy při zjišťování skutečností v souvislosti s údajným nebo předpokládaným protiprávním jednáním, jiným škodlivým jednáním nebo s nedodržováním interních směrnic.

Z hlediska posuzování důvodnosti oznámení v rámci vnitřního oznamovacího systému je přitom zásadní, že norma ISO/TS 37008 obsahuje konkrétní návody pro interní vyšetřování v rámci organizací, včetně návodů na stanovení základních principů a úpravy interních směrnic, vlastního vedení i podpory interního vyšetřování, jakož i na podávání zpráv o výsledcích interního vyšetřování a použití nápravných opatření.

Kontakt pro další informace

JUDr. Pavlína Vondráčková, Ph.D
advokátka
Associate Partner
T +420 236 163 710
pavlina.vondrackova@roedl.com

→ Compliance & ESG News

Antitrust & Competition Compliance: Zveřejněna metodika Úřadu pro ochranu hospodářské soutěže o compliance programech

Pavel Koukal
Rödl & Partner Praha

S účinností od 1. ledna zveřejnil Úřad pro ochranu hospodářské soutěže svou metodiku o zohledňování compliance programů jako polehčující okolnosti při stanovování pokuty za protisoutěžní jednání. Tato nová metodika byla vydána formou takzvaného oznámení Úřadu a stala se tak v tomto směru součástí jeho soft law.

Význam nového přístupu Úřadu vyjádřeného v metodice spočívá v tom, že soutěžitelé (účastníci řízení) mohou v rámci správního řízení požádat Úřad o zvážení, zda posílení jejich compliance programu či nově zaváděný compliance program bude možné kvalifikovat jako polehčující okolnost při ukládání pokuty.

Žádost o zohlednění compliance programu přitom musí obsahovat důvody, proč je compliance program pro daného soutěžitele dostatečně efektivní pro předcházení porušování pravidel hospodářské soutěže, jakož i texty všech částí compliance programu týkajících se problematiky hospodářské soutěže a konečně i popis konkrétních opatření ve vztahu k posílení či zavádění compliance programu.

Úřad na základě žádosti uzná compliance program jako polehčující okolnost pouze při kumulativním splnění stanovených podmínek. Těmito podmínkami je jednak efektivnost posilovaného či zaváděného compliance programu, jakož i úspěšné využití Leniency programu anebo narovnání v daném správním řízení před Úřadem a zároveň, že v případě již zavedeného compliance programu nedocházelo k protisoutěžnímu jednání s vědomím statutárních orgánů či vyššího managementu daného soutěžitele.

Kontakt pro další informace

JUDr. Pavel Koukal
advokát
Associate Partner
T +420 236 163 710
pavel.koukal@roedl.com

→ Compliance & ESG News

Data Security & IT Compliance: Kybernetická bezpečnost a smluvní vztahy

Lenka Hanková
Rödl & Partner Praha

Ani svět IT se neobejde bez smluv a s narůstající složitostí IT infrastruktury, systémů a jednotlivých procesů společně s riziky a potenciální zranitelností této oblasti je právě kvalitně a jasně nastavená smluvní dokumentace základem pro dobrou spolupráci mezi stranami, a to i v případě problémů. V praxi se lze velmi často ale bohužel setkat s opakem. Jednoduché smlouvy psané IT jazykem, kterému málokterý soudce bude rozumět, volně přeložené vzory smluv ze zahraničí či jen nedostatek právnického oka nad celou koncepcí smlouvy, pak může stát obě strany při vyjednávání cenný čas, ale i nemalé peníze, pokud se jedna ze stran s předloženou smlouvou nespokojí.

Pokud se na smluvní stranu vztahuje regulace kybernetické bezpečnosti, legislativa klade na obsah IT smluv ještě navíc zvláštní požadavky. Již aktuálně platný zákon č. 181/2014 Sb., o kybernetické bezpečnosti, resp. jeho doprovodná vyhláška o kybernetické bezpečnosti stanoví povinným osobám, jaký obsah mají mít smlouvy s významnými dodavateli (tj. provozovateli informačního nebo komunikačního systému, jakož i s každým, kdo

s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti takového systému). Obdobně k tomu přistupuje i připravovaný nový zákon o kybernetické bezpečnosti a dvě z jeho vyhlášek aktuálně čekající na projednání vládou. Pokud se osoba identifikuje jako poskytovatel regulované služby, a tedy takzvaně „spadne" pod tuto novou legislativu (ať již v režimu vyšších či nižších povinností), čeká ji i kontrola všech smluvních vztahů se všemi svými dodavateli, zejména těmi významnými. Významného dodavatele pak nový zákon definuje jako dodavatele, který s poskytovatelem regulované služby vstupuje do závazkového vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti.

Smlouva s významným dodavatelem by podle návrhu nové vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností měla obsahovat zejména ustanovení o bezpečnosti informací, o oprávnění užívat data, o autorství a licencích, o kontrole a auditu, dále povinnost řešit smluvní vztahy v dalšími dodavateli v dodavatelském řetězci, zavést povinnost k dodržování bezpečnostních politik, řešit i řízení změn, soulad s právními předpisy, nastavit celý proces informování povinné osoby o kybernetických bezpečnostních incidentech, způsobu řízení rizik, změny vlastnictví a dalších skutečnostech. Dále by takové smlouvy měly podrobně řešit proces při ukončení smlouvy (exit), jak zajistit kontinuitu činností, předávání dat a jejich likvidaci. Důležitou součástí by měly být i sankce za porušení povinností a právo jednostranně ukončit smlouvu při významné změně kontroly nad dodavatelem nebo jeho zásadními aktivy. Pro poskytovatele regulované služby v režimu nižších povinností pak bude povinný obsah zahrnovat jen část z uvedených náležitostí. Obecně pro všechny dodavatele je pak poskytovatel povinen stanovit pravidla, která zohledňují požadavky systému řízení bezpečnosti informací, a seznámit je s nimi. Je zřejmé, že tyto smluvní povinnosti či jejich část se pak postupně budou „přelévat" i do celého dodavatelského řetězce. Pokud si nejste jisti, zda se uvedené povinnosti na vás budou vztahovat, rádi vám společně s konzultační společností Cybrela s.r.o. pomůžeme nastavit procesy i dokumentaci dle chystané legislativy. V souvislosti s novou kyberneticko-bezpečnostní legislativou pak pořádáme s manažerkou kybernetické bezpečnosti Mgr. Kateřinou Hůtovou dva praktické webináře, na které se můžete zaregistrovat na adrese: www.roedl.cz/cs/cz/Events.aspx.

Kontakt pro další informace

Mgr. Lenka Hanková
advokátka
Senior Associate
Head of IP/IT Practice Group
T +420 236 163 710
lenka.hankova@roedl.com

ESG: EFRAG – podpora pro ESG reporting

Radim Botek
Rödl & Partner Praha

Přestože od vydání nových ESRS standardů uplynul teprve půlrok, objevila se za tu dobu v oblasti reportingu udržitelnosti řada užitečných novinek.

ESRS Standardy – Evropské standardy pro podávání zpráv o udržitelnosti. Jedná se o soubor pravidel, které mají za cíl sjednotit způsob, jakým společnosti v Evropské unii vykazují svůj dopad na životní prostředí, sociální oblast a správu společnosti (ESG), a to v souladu se Směrnicí o podávání zpráv o udržitelnosti podniků (CSRD).

S vědomím závažnosti výzvy, kterou ESRS a nová úprava ESG reportingu každopádně je a bude, přichází EFRAG téměř každý měsíc s nějakým novým dokumentem s cílem usnadnit orientaci a porozumění celému systému předpisů upravujících Zprávy o udržitelnosti a jejich aplikaci do praxe.

EFRAG – je Evropská poradní skupina pro finanční výkaznictví (EFRAG – European Financial Reporting Advisory Group). Je nezávislým orgánem, který byl založen v roce 2001 s cílem poskytovat Evropské komisi odborné znalosti v oblasti účetnictví a podávání zpráv o udržitelnosti. Ovlivňuje, jak se mezinárodní standardy účetního výkaznictví (IFRS) uplatňují v Evropě. Od roku 2022 rozvíjí standardy pro podnikové výkaznictví.

Pojďme si představit, jak tyto základní novinky z kuchyně EFRAG přicházely v čase:

1. V prosinci 2023 byla vydána sada prvních implementačních příruček k ESRS standardům. Jedná se o návrh nezávazných pokynů, které by měly být vždy používány v kontextu s ESRS. A je pochopitelné, že jako první přišla na řadu klíčová témata, jako jsou stanovení dvojí materiality nebo požadavky na hodnotový řetězec.

Konkrétně se jedná o tyto:

- Draft EFRAG IG 1: Materiality Assessment implementation guidance (MAIG)
  Takzvaný MAIG detailně popisuje požadavky týkající se posouzení dvojí významnosti, včetně navržených postupů a grafického znázornění možných kroků celého procesu vyhodnocení. Tento proces bude zcela zásadní pro správné vymezení a zároveň i zúžení otázek udržitelnosti, které nakonec budou sledovány, vyhodnocovány a zveřejněny. Obsahuje také často kladené otázky, které poskytují návod k uchopení dvojí významnosti z praktického hlediska. Jednou z takových otázek, která bude důležitá i pro nás auditory, je například ta, zda může být významnost aplikovaná pro účely sestavení zprávy o udržitelnosti stejná jako významnost stanovená pro účetní závěrku.

- Draft EFRAG IG 2: Value Chain implementation guidance (VCIG)
  Takzvaný VCIG má usnadnit uživatelům porozumění a správnou implementaci problematiky hodnotového řetězce (value chain) při stanovení dvojí významnosti. Podnik musí v rámci otázek udržitelnosti vyhodnotit dopady, rizika a příležitosti (IRO) nejen z hlediska své vlastní činnosti, ale i přímých i nepřímých a předcházejících i navazujících obchodních vztahů. VCIG například popisuje rozdíl mezi dodavatelským a hodnotovým řetězcem. Je přirozeně významně propojen s výše uvedeným MAIG, na který se v mnoha částech odkazuje. Také VCIG obsahuje často kladené otázky včetně shrnutí důsledků pro zveřejňování. Jako první je zde například diskutována otázka „Kde hodnotový řetězec začíná a kde končí“.

- Draft EFRAG IG 3: Detailed ESRS datapoints implementation guidance and accompanying explanatory note
  Tento soubor ve formátu Excel uvádí úplný seznam podrobných požadavků obsažených v Požadavcích na Zveřejnění a souvisejících Požadavcích na Uplatňování definovaných jednotlivými ESRS standardy. Soubor obsahuje doplňující informace (sloupce) užitečné pro navigaci a filtrování obsahu.

Všechny zúčastněné strany měly možnost poskytnout zpětnou vazbu k návrhu implementačních příruček do 2. února 2024. V dohledné době se tak již můžeme těšit na jejich finální znění.

2. V lednu 2024 byla spuštěna také veřejná konzultace k pracovnímu návrhu dvou nových ESRS standardů pro malé a střední podniky (SME). A to samostatně pro kotované (ESRS LSME ED) a nekotované (ESRS VSME ED) účetní jednotky. Na tyto společnosti se nevztahuje povinnost sestavení a zveřejnění Zpráv o udržitelnosti, nicméně i ony čelí výzvám ESG reportingu například ze strany obchodních partnerů či bank čím dál častěji.

V rámci ESRS LSME/VSME by mělo být dosaženo maximální míry zjednodušení při zajištění úrovně ESG výkaznictví, které bude schopno splnit potřeby investorů a ostatních zainteresovaných stran. ESRS pro SME by tak měly usnadnit podnikům přechod k udržitelnějšímu podnikání, zajistit přístup k financování a snížit zátěž spojenou s vyřizováním individuálních požadavků na údaje o udržitelnosti. V neposlední řadě by standardy měly zajistit dostupnost standardizovaných informací i jejich následného ověření pro všechny zúčastněné strany.

Konzultace by měla být ukončena do 21. května 2024.

3. Koncem roku 2023 byla opět na stránkách EFRAG spuštěna platforma pro podávání dotazů k problematice ESRS standardů. ESRS Q&A Platform si klade za cíl shromažďovat a odpovídat na technické otázky v oblasti ESRS standardů, které nebyly vyřešeny ani po dosavadní důkladné analýze všech zainteresovaných stran.

Do 7. března bylo zaevidováno přes 340 otázek z celkem 31 zemí. Asi není překvapením, že suverénně nejvíce dotazů bylo ze společností se sídlem v Německu a že ČR se svým jediným dotazem tak nějak zapadá do celkového povědomí ohledně ESG reportingu u nás. V únoru a březnu 2024 pak byly publikovány sady otázek včetně komentářů ze strany EFRAG.

Všechny výše komentované informace lze samozřejmě najít na stránkách EFRAG: https://efrag.org.

V rámci našeho pravidelného měsíčního newsletteru vám budeme přinášet další články zaměřené na jednotlivá témata i jednotlivé ESRS standardy. V nich se vám postupně mimo jiné pokusíme přiblížit pojmy jako jsou právě dvojí významnost, hodnotový řetězec, dopady, zúčastněné strany, datový bod, co vlastně znamená zkratka IRO, apod.

Kontakt pro další informace

Ing. Radim Botek
auditor
Associate Partner
T +420 236 163 311
radim.botek@roedl.com

ESG: Německý zákon o náležité péči v dodavatelských řetězcích již ve druhém roce své účinnosti

Pavel Koukal
Rödl & Partner Praha

V agendách ESG aktuálně představuje náležitá péče v oblasti udržitelnosti podniků, vedle vykazování nefinančních informací a reportingu, druhý hlavní směr jejího rozvoje.
Pokud jde o legislativní základ náležité péče na úrovni Evropské unie, v tomto směru dosud nebyl ukončen příslušný legislativní proces v rámci společné pravomoci Evropského parlamentu a Rady (EU) a stále se tak čeká na přijetí klíčové směrnice o náležité péči podniků v oblasti udržitelnosti (Corporate Sustainability Due Diligence Directive, CSDDD, respektive CS3D).
Na tomto místě je třeba upozornit, že některé členské státy EU ještě před schválením CSDDD vydaly vlastní právní předpisy týkající se náležité péče v oblasti udržitelnosti podniků. Z našeho pohledu je přitom i pro obchodní společnosti v České republice významné, že od 1. ledna vstoupil již do druhého roku své účinnosti německý zákon o náležité péči v dodavatelských řetězcích (Lieferkettensorgfaltspflichtengesetz, LkSG), který ještě před přijetím společné evropské úpravy názorně ukazuje, jak budou koncipovány konkrétní povinnosti vybraných podniků v oblasti náležité péče.
Působnost zákona se původně týkala „pouze“ zhruba 900 německých podniků (podnikatelských seskupení), ale s účinností od 1. ledna 2024 se kritérium minimálního počtu zaměstnanců snížilo na 1 000 zaměstnanců, což vedlo k tomu, že povinnosti náležité péče podle LkSG se rozšířily na nejméně 4 800 podniků. Tím se výrazně navýšil i počet českých obchodních společností, na které mohou povinnosti podle LkSG dopadat nepřímo, a to buď z toho důvodu, že jsou jako dceřiné společnosti členy nadnárodní podnikatelské skupiny se sídlem ve Spolkové republice Německo, anebo z toho důvodu, že jsou součástí takového dodavatelského řetězce v postavení přímého anebo nepřímého dodavatele.
Hlavním nástrojem je v tomto směru povinnost náležité péče (Sorgfaltspflicht, angl. due diligence), kterou se v zásadě rozumí nefinanční prověrka všech aktivit povinných subjektů. V tomto směru je klíčové, že sama povinnost náležité péče zahrnuje celou řadu dílčích povinností, a to zejména povinností spočívajících ve vytvoření systému rizik, stanovení vnitropodnikové příslušnosti a odpovědnosti, provádění pravidelných analýz rizik, zavedení preventivních opatření ve vlastní podnikatelské činnosti a vůči přímým dodavatelům, přijímání opatření k nápravě, zřízení postupu pro podání stížností, uplatňování povinností náležité péče ve vztahu k rizikům u nepřímých dodavatelů a vedení příslušné dokumentace. Nedílnou součástí těchto dílčích povinností náležité péče je i podávání pravidelných zpráv o plnění náležité péče.

Kontakt pro další informace

JUDr. Pavel Koukal
advokát
Associate Partner
T +420 236 163 710
pavel.koukal@roedl.com

→ Compliance & ESG News

Odborné akce z oblastí Governance-Risk-Compliance

I letos pro vás chystáme řadu odborných akcí z jednotlivých oblastí Governance-Risk-Compliance. Sledujte nás i nadále: Akce | Rödl & Partner (roedl.cz)

Impresum

COMPLIANCE & ESG NEWS ČESKÁ REPUBLIKA
VYDÁNÍ Č. 1/2024

Rödl & Partner

Vydavatel:
Rödl & Partner Consulting & Valuation, s.r.o.
Platnéřská 191/2, 110 00 Praha 1
IČO: 25724231
Reg. Městský soud v Praze, C 64494

T +420 236 163 111
www.roedl.cz

Redakce:
Jana Švédová
Pavel Koukal

Layout:
Rödl & Partner