



Board-level zodpovednosť za IT a AI riziká

Prednášajúci



Oliver Göndör
CMS Slovensko

Associate / Advokát
Bratislava

T +421 940 637 842

E oliver.gondor@cms-cmno.com

- Associate v tíme M&A a korporátneho práva
- Zameranie na M&A, PE/VC a korporátne právo
- Podpora domácich a medzinárodných klientov v lokálnych aj cezhraničných transakciách, corporate governance a house keeping (automotive, infraštruktúra, výroba, retail, fondy, development)
- Člen commercial regulatory tímu (B2C, streaming, hazard, tabak, ride-sharing, payments, insurance)
- Člen CMS CEE Crypto Group - krypto regulácia, AML, compliance



Agenda

01

Vymedzenie
zodpovednosti

02

Board a rozsah
zodpovednosti

03

Zodpovedám za
výsledok rozhodnutia?

04

Oslobodenie sa spod
zodpovednosti

05

Dokedy zodpovedám a
kto môže zodpovednosť
vymáhať

06

Ako outsourcovať
zodpovednosť?

07

Príklady

08

Key takeaways



Vymedzenie zodpovednosti

Vymedzenie zodpovednosti

Aké druhy zodpovednosti existujú?

Civilná – podľa Obchodného zákonníka

- nie je veľa publikovaných sporov

Trestná

- Porušovanie povinnosti pri správe cudzieho majetku
 - (§ 237 TZ) úmyselné zavinenie a aspoň malá škoda (>700 EUR)
 - (§ 238 TZ) úmyselné zavinenie a aspoň malá škoda (>250.000 EUR)
 - málo uplatňovaná vo vzťahoch spoločnosť a štatutár

Sústredíme sa na civilnú zodpovednosť



Board a rozsah zodpovednosti



Board (of Directors) = Štatutárny orgán (tzv. štatutárna zodpovednosť)

- Konatelia (s.r.o.) / predstavenstvo (a.s.)
 - Vykonávajú riadenie (governance)
- Nie: (i) tzv. officers (CEO/CFO/CISO) manažérske pozície a (ii) prokuristi
 - Vykonávajú denný manažment
 - Pracovnoprávna / zmluvná zodpovednosť (prokuristi obdobný rozsah zodpovednosti)

Štatutárny orgán zodpovedá za škodu spôsobenú pri výkone funkcie

- Objektívna zodpovednosť, nehľadí sa na zavinenie

Board a rozsah zodpovednosti



Osobná zodpovednosť štatutárov celým majetkom voči spoločnosti

- Zodpovednosť sa týka tých konateľov, ktorí konali v rozpore s odbornou starostlivosťou
 - Zásada „jeden za všetkých, všetci za jedného“ ak rozhodovalo viac štatutárov
 - Následný regresný nárok voči ostatným

Directors & Officers Liability Insurance

- Záchranné koleso pri osobnej zodpovednosti
- Riziká: porušenie povinnosti konať s odbornou starostlivosťou
- Bežné krytie (v zahraničí): povinnosť odškodnenia, náklady obhajoby
- Bežné výluky (v zahraničí): úmyselné porušenia, podvody
- Rôzne druhy D&O poistenia, podľa toho kto platí poistné



**Zodpovedám za
výsledok
rozhodnutia?**

Zodpovedám za výsledok rozhodnutia?

Kam mierim touto otázkou?

- Zodpovedám ako štatutár za akúkoľvek škodu, ktorá sa spoločnosti stane?
 - Zodpovedám aj za pokles objednávok/nedosiahnutie tržieb v dôsledku DDoS útoku?
 - Zodpovedám za akúkoľvek pokutu od ÚOOS?
- Mám právo na omyl?

Štatutár má povinnosť

- Konať s **odbornou (náležitou) starostlivosťou** a v **súlade so záujmami spoločnosti** a **súlade so všetkými spoločníkmi**
 - Kumulatívne naplnenie všetkých 3 podmienok
- Neuprednostniť iný záujem pred záujmom spoločnosti
- Nezvýhodňovať ani neznevýhodňovať žiadneho spoločníka



Zodpovedám za výsledok rozhodnutia?



Čo zahŕňa odborná starostlivosť?

- Získanie a vyhodnotenie všetkých relevantných informácií k predmetu rozhodnutia
- Zabezpečenie poradenstvo interných/externých odborníkov
- Samoštúdium
- Použitie AI (LLM modelu)
- Dokumentácia procesu rozhodovania (nielen výsledku)

Ak bola odborná starostlivosť naplnená, štatutár nezodpovedá za škodu, ktorú spôsobil

- Podnikateľské riziko nesie spoločnosť
- Právo na omyl (postupovali sme správne, ale nevyšlo to)



Oslobodenie sa spod zodpovednosti

Oslobodenie sa spod zodpovednosti

- Nechcel som nestačí!
 - Nestačí preukázať len neúmyselné porušenie povinnosti
- Liberačný dôvod
 - Preukázať konanie s odbornou starostlivosťou (v dobrej viere a v záujme spoločnosti)
 - Preukazujem ako som sa rozhodoval (aké informácie som mal, čo všetko som pri rozhodovaní použil)
 - Výkon uznesenia VZH, ktoré bolo v súlade so zákonom, spoločenskou zmluvou



Oslobodenie sa spod zodpovednosti

- Business Judgement Rule - doktrína „riadneho obchodného úsudku“
 - Nie je explicitne kodifikovaná – rozpoznaná súdnymi rozhodnutiami
 - Konateľ nezodpovedá za škodu iba vtedy, ak konal s odbornou starostlivosťou a súčasne v dobrej viere, že koná v záujme spoločnosti
 - Povinnosť konať s **odbornou (náležitou) starostlivosťou** a v **súlade so záujmami spoločnosti** a **súlade so všetkými spoločníkmi**
 - Štatuár musí zistiť/ poznať záujmy spoločnosti (vynaložiť primerané úsilie ich zistiť) a až následne posúdiť svoje kroky s odbornou starostlivosťou
 - Dôkazné bremeno preukázať odbornú starostlivosť a dobrú vieru nesie konateľ



Oslobodenie sa spod zodpovednosti

- Preukazovanie odbornej starostlivosti
 - Predpoklady zodpovednosti za škodu
 - Obrátené dôkazné bremeno
 - Čo je to?
 - Platí pri všetkých predpokladoch zodpovednosti za škodu?
 - Dôkazné bremeno člena štatutárneho orgánu sa týka len konania o odbornou starostlivosťou
 - Ak štatutár **neunesie** dôkazné bremeno – **prehráva** spor ak sú naplnené ostatné predpoklady zodpovednosti za škodu (škoda a príčinná súvislosť)



Oslobodenie sa spod zodpovednosti

- Dohody vylučujúce zodpovednosť: Zakázané; aj vo vzťahu k stanovám či spoločenskej zmluve
- Waiver: 3 roky od vzniku škody a schválenie valným zhromaždením bez protestov minoritov nad 10%
- Absolutorium: nemá účinky na zodpovednosť
- D&O Insurance platené spoločnosťou nie je výslovne zákonom zakázané





**Dokedy
zodpovedám a kto
môže zodpovednosť
vymáhať**

Dokedy zodpovedám a kto môže vymáhať

Subjektívna lehota 4 roky v rámci 10-ročnej objektívnej lehoty

- 4 roky: odo dňa, keď sa spoločnosť dozvedela o škode a o zodpovednom
- Najneskôr do 10 rokov od porušenia povinnosti

Kto môže vymáhať škodu

- Spoločnosť (ostatní/noví konatelia),
- Spoločníci
- Veritelia
- Dozorná rada v a.s.





Ako outsourcovat' zodpovednosť?

Ako outsourcovat' zodpovednosť

Limity slovenského jazyka: responsibility vs. liability

- Responsibility – delegovanie úloh (zodpovednosti) je možné
- Liability – právna zodpovednosť je neprenosná

Zmluvné dojedania o preplatení škody či pokút voči dodávateľom

- Ak regulátora udelí pokutu napriek zavedeniu všetkých odporúčaní dataprotection / cyber security auditu





Príklady

Zodpovednosť a ochrana osobných údajov

- Spoločnosť **MedAPP** spúšťa zdravotnícku appku, ktorá spracúva diagnózy, lieky, symptómy a biometrické údaje pacientov. **DPO pred spustením upozorní**, že ide o citlivé zdravotné údaje a systém je vysokorizikový, takže pred uvedením je povinné **riadne DPIA a bezpečnostný audit**.
- **Konateľ tlačí na rýchle spustenie pilotu.**
- **Po 6 mesiacoch odhalí googlením problém jeden z používateľov.** Aplikácia je releasnutá bez DPIA, bez preverenia subdodávateľa a s nevyhodnotenými dátovými tokmi – ktoré nestihli byť odhalené počas vývoja.
- **Problém:** časť zdravotných údajov (diagnózy, dávkovanie liekov a symptómové záznamy) sa omylom odosiela na verejný server tretích strán – záznamy sa dajú dohľadať cez google.
- Únik sa okamžite dostane do médií. Appka bola vypnutá až po troch dňoch od nahlásenia úniku dát.
- Po včasnom nahlásení úniku dát na ÚOOÚ, nasleduje expresná kontrola ÚOOÚ. Úrad žiada DPIA, risk assessment.
- Pokuta od ÚOOÚ je vo výške 100.000 EUR; a právnici upozorňujú na potenciálne žaloby na ochranu osobnosti od užívateľov appky.



Zodpovednosť a ochrana osobných údajov



Čo musí konateľ preukázať, aby spustenie appky bez preverenej bezpečnostnej architektúry a dostatočného GDPR compliance, z ktorej vznikol únik údajov bol konaním s odbornou starostlivosťou?

Mal k dispozícii všetky relevantné informácie a vyhodnotil ich, najmä že:

- Poznal povahu spracúvaných údajov (citlivé zdravotné údaje)
- Poznal riziká plynúce z architektúry systému, dátových tokov a subdodávateľov
- Architektúra softvéru bola pred launchom otestovaná, dátové toky boli Zmapované, bezpečnostné testy prebehli

Ako posúdil odporúčania DPO, prečo a na základe čoho mal prijať rozhodnutie, že DPIA nie je potrebná napriek odporúčaniam DPO

Bolo v záujme spoločnosti preferovať rýchlosť launchu pred bezpečnosťou:

- Čo odôvodnilo rýchly launch pred bezpečnosťou

Zodpovednosť za cyber bezpečnosť

- Spoločnosť **Elektro šop s.r.o.** prevádzkujúca e-shop s elektronikou a spotrebným tovarom.
- Počas **Black Friday** dôjde k mimoriadne masívnemu **DDoS útoku**, ktorý úplne **vyradí e-shop na 13 hodín od 9:00 do 22:00**.
- Spoločnosť kvôli výpadku nesplní plánované tržby a nedokáže predať naskladnený tovar v nasledujúcom období.
- Konateľ však v priebehu roka nechal implementovať infraštruktúru a opatrenia odporúčané externým „CISO“ na základe bezpečnostného auditu.
- Audit identifikoval tri možné úrovne ochrany. Konateľ nechal implementovať strednú úroveň.
- DDoS útok bol však sofistikovanejší, väčší a technicky odlišný od všetkých predchádzajúcich útokov — rozsah a intenzita výrazne prekročili historické vzory aj závery auditu.



Zodpovednosť za cyber bezpečnosť



Čo by musel konateľ preukázať, aby neniesol zodpovednosť

Mal k dispozícii všetky relevantné informácie a vyhodnotil ich, najmä že:

- Externý CISO, audit, risk analýza
 - Bol vhodne vybraný; CISO mal skúsenosti, robil na podobných projektoch
- Implementoval primerané opatrenia – úroveň ochrany bežnú pre e-commerce sektor (nie sú požiadavky ako pre banky)
- Rozhodnutie bolo racionálne vzhľadom na predvídateľné riziká
 - Historické dáta neukazovali na extrémne masívne útoky

Dobrá viera v záujem spoločnosti

- stredný stupeň bezpečnosti

AI & IT riziká

Dátové riziká (úniky, nesprávne spracovanie, GDPR)

- Únik osobných alebo citlivých údajov, nelegitímne spracovanie, slabý vendor

Mitigácia

- Preveriť poskytovateľov (technicky + zmluvne)
- Schváliť len nástroje, ktoré majú jasný režim nakladania s dátami
- Nastaviť kontrolu dátových tokov
- Dokumentovať kroky



AI & IT riziká



AI riziká: output / bias & diskriminácia

- Riziká: AI vygeneruje chybný text, škodlivú odpoveď, zavádzajúcu informáciu / AI odporúčania sú neférové, diskriminačné

Mitigácia z pohľadu odbornej starostlivosti

- Interné pravidlo „human in the loop“ povinná kontrola všetkých AI výstupov
- Limity použitia (čo sa môže / nesmie generovať, aké údaje sa môžu vkladať „do AI“)
- Preveriť tréningové dáta (aspoň v rozsahu, ktorý umožní vendor)
- Zaviesť pravidlá pre HR/CRM AI
- Robiť pravidelné kontroly výstupov na bias
- Dokumentovať kroky



Key takeaways

Key takeaways

Základom je odborná (náležitá) starostlivosť a jej dokumentácia

- Dokumentujte ako ste sa rozhodovali a prečo ste rozhodli

Je štatutár zodpovedný za rozhodnutie, z ktorého došlo k nepriaznivému následku (škode)?

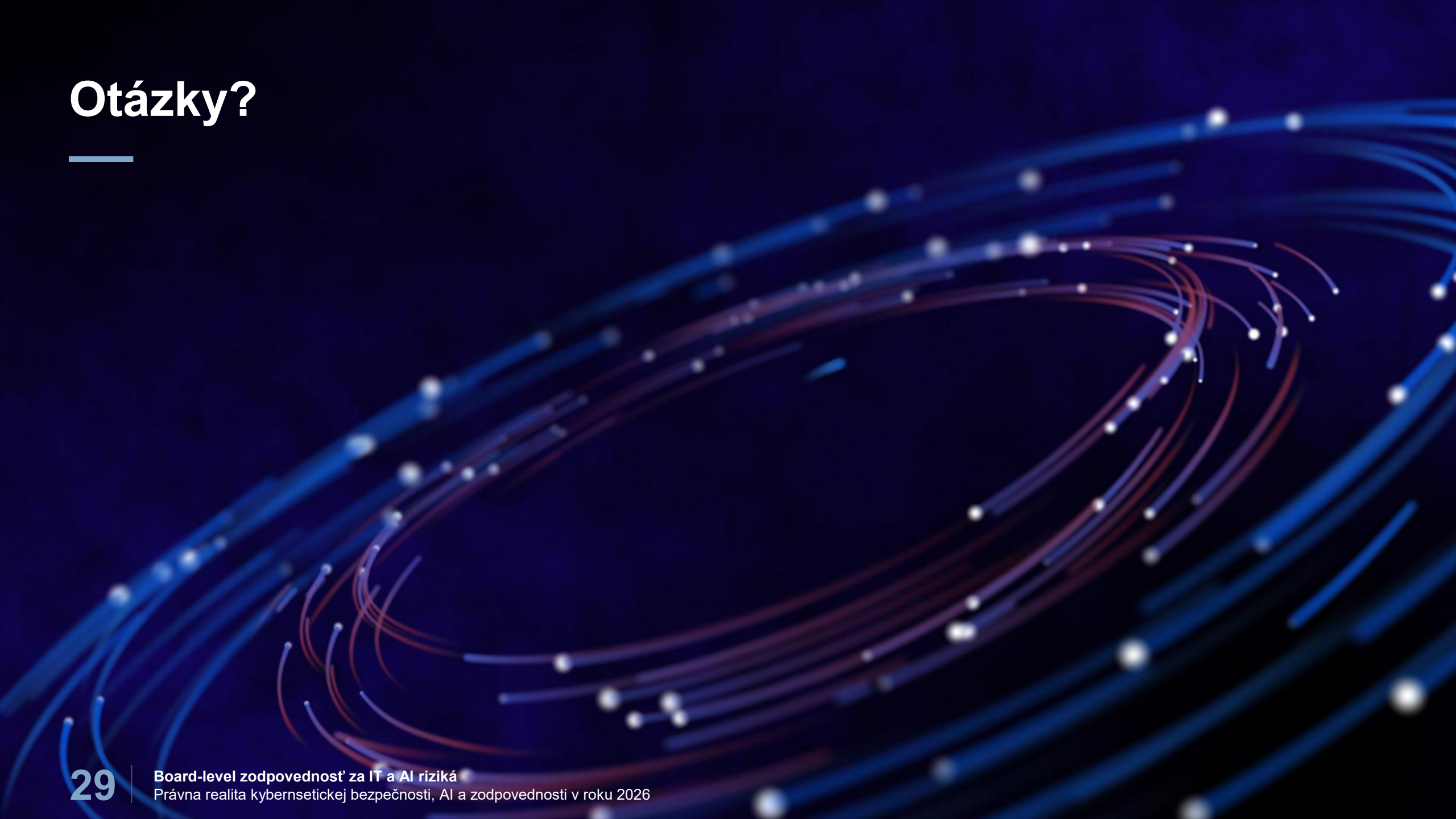
- Áno, ak pri rozhodovaní nepostupoval s odbornou starostlivosťou.
- Zodpovedá štatutár za správne rozhodnutie, alebo za správny proces rozhodovania?
 - Správny proces rozhodovania

Pozor na outsourcing

- Liability nie je prenosná, neviete sa jej vzdať, neviete ju vylúčiť, ale je poistiteľná



Otázky?



—

Ďakujem za pozornosť.



Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.

cms-lawnow.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS is an international organisation of independent law firms ("CMS Member Firms"). CMS LTF Limited (CMS LTF) is a company limited by guarantee incorporated in England & Wales (no. 15367752) whose registered office is at Cannon Place, 78 Cannon Street, London EC4N 6AF United Kingdom. CMS LTF coordinates the CMS Member Firms. CMS LTF provides no client services. Such services are solely provided by CMS LTF's CMS Member Firms in their respective jurisdictions. CMS LTF and each of its CMS Member Firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS LTF and each CMS Member Firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the CMS Member Firms or their offices; details can be found under "legal information" in the footer of cms.law.

CMS Locations

Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bengaluru, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Chennai, Cologne, Dubai, Dublin, Duesseldorf, Ebene, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Gurugram, Hamburg, Hong Kong, Hyderabad, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Mumbai, Munich, Muscat, Nairobi, New Delhi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Silicon Valley, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Sydney, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

Further information can be found at **cms.law**

Prague - 15357192.2