

 | NOVÝ ZÁKON O KRITICKÉ INFRASTRUKTUŘE (ZKI)

Je vaše organizace připravena **splnit požadavky personální bezpečnosti?**

Splňte povinnosti dle **ZKI, nZoKB, DORA, ISO 27001** a dalších!

Ověření spolehlivosti dle ZKI

Prováděcí předpisy: nařízení vlády č. 127/2026 Sb., o základních službách a kritériích významnosti a vyhláška č. 122/2026 Sb. vyhláška o plánu odolnosti, posouzení rizik jsou schváleny a od 1. srpna 2026 se jimi musí řídit. Zákon a prováděcí předpisy vyžadují ověřování interních a externích pracovníků a dodavatelů.

U koho je třeba ověřit spolehlivost?

Interních a externích pracovníků s přímým nebo vzdáleným přístupem do prostor, k informacím či systémů KI.

Všech externích pracovníků?

Dodavatelů a kritických dodavatelů, které je třeba evidovat. Dále se ověření týká dalších článků dodavatelského řetězce.

Co je ověření spolehlivosti?

Minimálně se jedná o ověření totožnosti a trestní bezúhonnosti. U cizinců i zahraniční ekvivalenty, pokud pobývali v cizině déle než 3 měsíce v posledních 3 letech. Další rozsah stanoví subjekt na základě posouzení rizik.

Lhůta pro splnění povinností

Splnění požadavků u stávajících pracovníků a zahájení screeningů kandidátů a dodavatelů je třeba bezodkladně po zařazení na Seznam subjektů KI.

Ověřte svou připravenost

- Identifikovali jste kritické pracovníky a dodavatele?
☐ Ano ☐ Ne ☐ Pracujeme na tom
- Provádíte již screening zaměstnanců a externích pracovníků?
☐ Ano ☐ Ne ☐ Částečně
- Máte zavedenou dokumentovanou politiku ověřování spolehlivosti?
☐ Ano ☐ Ne ☐ Ještě ne
- Jsou záznamy o screeningu a auditní záznamy bezpečně uloženy?
☐ Ano ☐ Ne ☐ Nevím

Pokud jste odpověděli “Ne” nebo “Ještě ne”, je čas jednat.

Za porušení povinností podle ZKI hrozí sankce až 25 milionů Kč nebo 0,3 % obrátu v pokutách!



Jak Scout funguje

Naše kontroly jsou jednoduché, rychlé a automatizované. Umožňují vám mít přehled o zaměstnancích i dodavatelích – a vždy doložit soulad se zákonem.

Klíčové funkcionality:

- Sdílení výsledků s dalšími organizacemi
- Rozšířené uchování dat
- Kontroly v pravidelných intervalech
- Prvotřídní zákaznická podpora
- API integrace do vlastních systémů
- Možnost vlastního brandingů
- Onboarding a školení uživatelů
- Nastavení vlastních kontrol



3 jednoduché kroky



1. Ověřte pracovníky

Zaměstnance i dodavatele s přístupem do prostor a IT systémů kritické infrastruktury.



2. Sdílejte výsledky

Přehled a reporty dostupné v portálu Scout, připravené k auditu i sdílení partnerům.



3. Prokažte shodu

Splňte zákonné povinnosti a zvyšte svou důvěryhodnost u státu i obchodních partnerů.

Potřebujete další podporu v oblasti compliance?

Hrozby pro strategické organizace, kritickou infrastrukturu a národní bezpečnost jsou stále častější, což nutí mnoho organizací naplňovat přísné bezpečnostní požadavky. **Scout** je navržen tak, aby poskytoval řešení v souladu s předpisy pro široké spektrum evropských i globálních požadavků na personální bezpečnost. Rádi s vámi prodiskutujeme jakékoli další otázky.



Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí



265/2025 Sb. nový Zákon o kybernetické bezpečnosti



266/2025 Sb. Zákon o kritické infrastruktuře



Zákon o odolnosti digitálního provozu



Hodnocení bezpečnosti, dostupnosti, integrity zpracování, důvěrnosti a soukromí dat



Ochrana dat a bezpečnost

Scout je držitelem certifikace ISO 27001. Používáme end-to-end šifrování (AES-256, TLS 1.3) a řízení přístupu (RBAC). Vaše data jsou chráněna při přenosu i uložení. Svěřte starosti o personální bezpečnosti profesionálním. **Kontaktujte nás ještě dnes.**