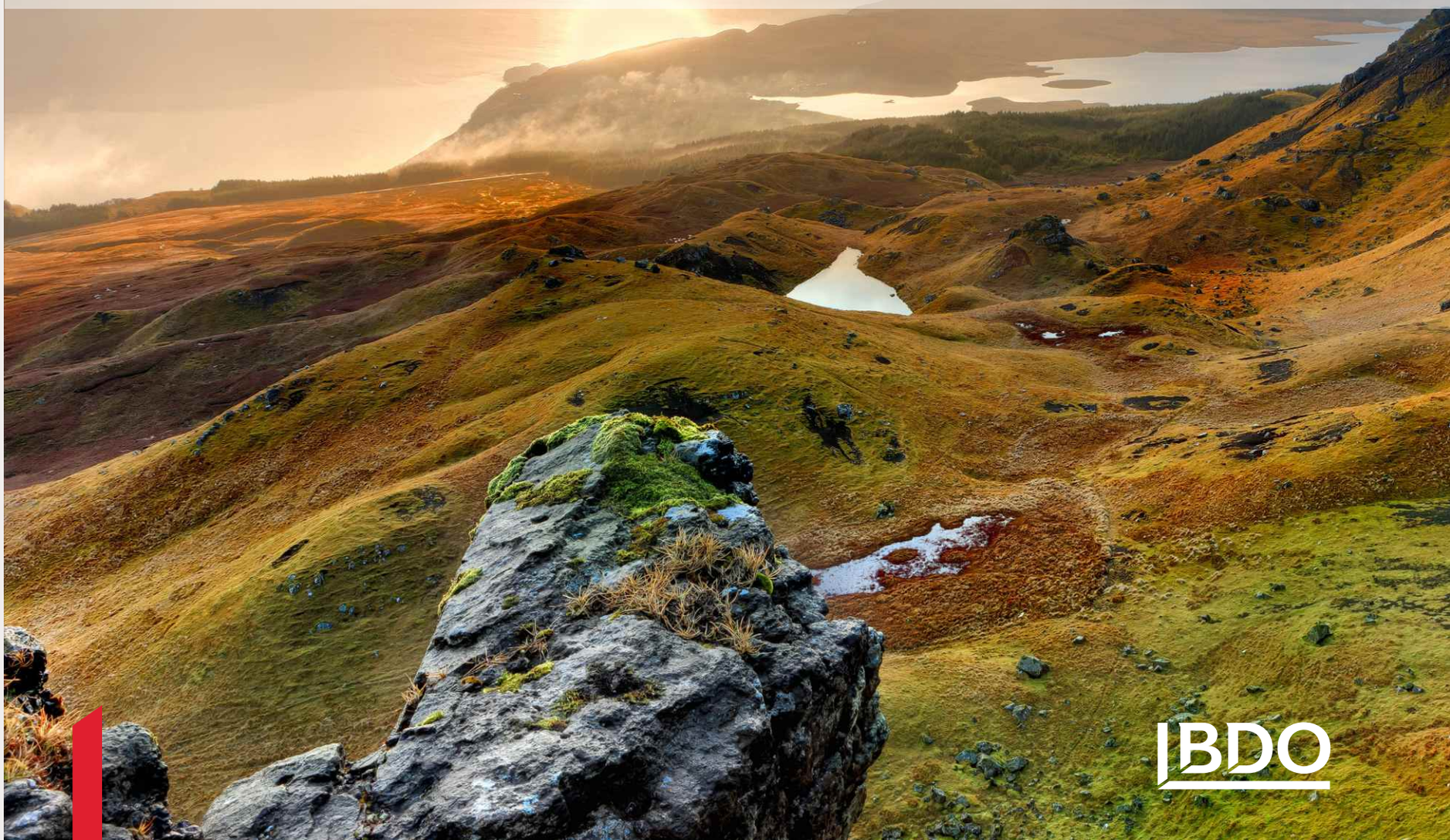
BDO NEWSLETTER

Interní audit



Vážení čtenáři,

dostává se Vám do rukou nový Newsletter BDO určený speciálně pro interní auditory, tentokrát zaměřený na aktuální témata ochrany informací.

Seznámíte se s významnými změnami v ochraně osobních údajů, s novinkami v oblasti kybernetické bezpečnosti a získáte informace o nadcházejících událostech a užitečných publikacích, které byste si rozhodně neměli nechat ujít.

Na závěr si můžete zpříjemnit čas vyluštěním auditorské křížovky.

Budeme rádi, když nám dáte vědět, jak se Vám nový Newsletter líbí a co byste uvítali v příštím čísle.

Pěkné počtení Vám přeje,

Ondřej Šnejdar
partner BDO zodpovědný za interní audit

Revoluce v právní úpravě ochrany osobních údajů

Významné změny

Evropský parlament přijal nové nařízení, tzv. obecné nařízení o ochraně osobních údajů (General Data Protection Regulation, „GDPR"), které zásadním způsobem změní evropskou legislativu v oblasti ochrany osobních údajů.

Pro všechny subjekty (soukromé i veřejné), které zpracovávají osobní údaje občanů EU, znamená GDPR vznik nových povinností v souvislosti se zvýšením ochrany a práv občanů EU. Nařízení nabude účinnosti 25. 5. 2018 a v České republice nahradí současnou právní úpravu ochrany osobních údajů.

Přísnější pravidla hry

Orgány dohledu budou při prosazování pravidel přísnější a jejich porušení může být tvrdě sankcionováno. Nejvyšší pokuta podle stávající právní úpravy činí 10 000 000 Kč. GDPR tuto částku razantně navyšuje.

V případě závažného pochybení může být orgánem dozoru udělena pokuta do výše až 20 000 000 EUR nebo až 4 % z celkového ročního světového obratu. Udělením pokuty není dotčeno právo subjektů údajů na náhradu škody.

Proto je důležité pochopit rizika v souvislosti s ochranou údajů, kterým organizace čelí.

- Nová práva subjektů údajů, jako např. právo být zapomenut, právo na přenositelnost osobních údajů, právo na bezplatnou první kopii osobních údajů, právo na omezení zpracování osobních údajů.
- Přísnější požadavky na zpracování osobních údajů; všechny operace s osobními údaji musí být evidovány.
- Detailnější požadavky na zajištění organizačních a technických opatření.
- Povinnost zpracovat analýzu dopadu na ochranu osobních údajů.
- Povinnost zajistit pověřence pro ochranu osobních údajů.
- Nové náležitosti smlouvy o zpracování osobních údajů uzavřené mezi správcem a zpracovatelem.
- Širší informační povinnost vůči subjektům údajů.
- Přísnější požadavky na podobu souhlasu a výslovné právo souhlas odvolat.

GDPR významně mění pravidla hry. Tyto změny pro správce a zpracovatele osobních údajů znamenají výzvu zvládnout rizika a chopit se příležitostí, které nová regulace přináší.

Na koho nařízení dopadá?

Nařízení dopadá na každého, kdo zpracovává osobní údaje. Není tedy rozhodující, zda se jedná o fyzickou nebo právnickou osobu, soukromý či veřejný subjekt.

Podle dosavadní právní úpravy podléhali regulaci jen správci a zpracovatelé usazení v Evropské unii. GDPR se vztahuje i na správce nebo zpracovatele, kteří nejsou usazeni v Evropské unii, ale nabízejí zboží nebo služby subjektům údajů v Evropské unii nebo monitorují jejich chování.

Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je zcela nová ujišťovací a poradenská funkce, s jejímž zavedením u vybraných správců a zpracovatelů GDPR počítá. Úkolem pověřence bude sledovat, zda organizace zpracovává osobní údaje v souladu s GDPR a poskytovat poradenství ohledně zpracování. Pověřenec má být nezávislý a nesmí se podílet na operacích zpracování osobních údajů. Organizační nezávislost bude zajištěna jeho přímou podřízeností vrcholovému vedení organizace.

Pověřenec by měl znát jak právní předpisy týkající se ochrany osobních údajů, ale měl by mít i praxi v této oblasti. Měl by znát problematiku řízení bezpečnosti informací. Pověřencem může být

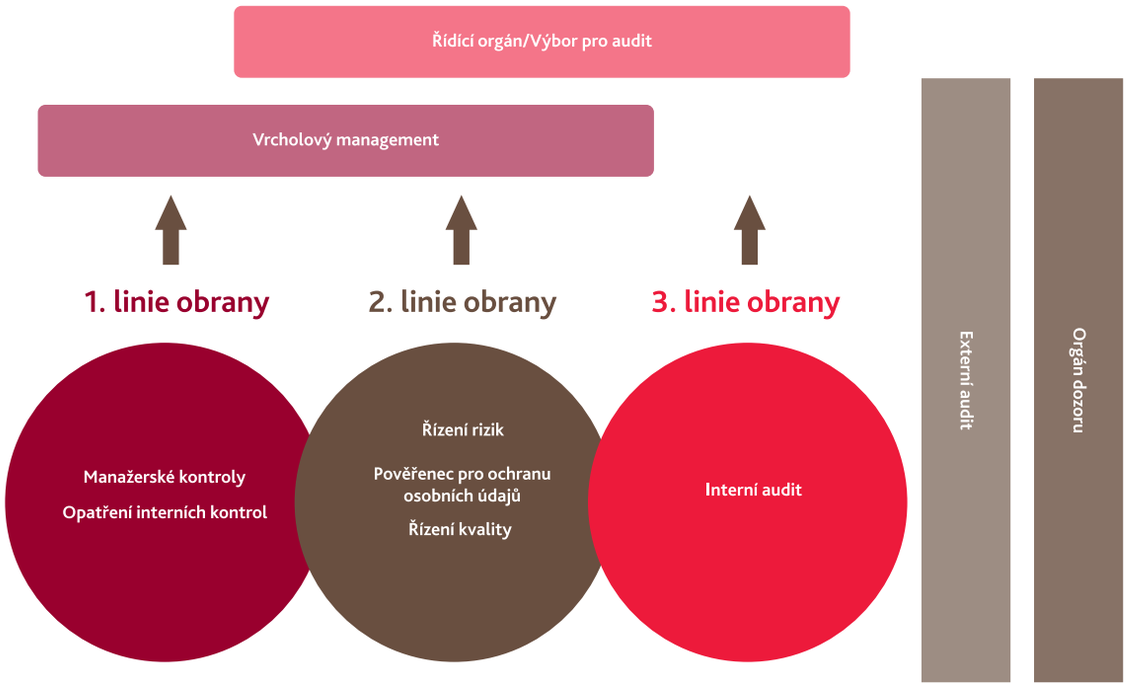
Revoluce v právní úpravě ochrany osobních údajů

zaměstnanec správce nebo zpracovatele, nebo může být zajištěn externě.

Z pohledu modelu tří linií obrany patří pověřenec do druhé linie.

GDPR a interní audit

Interní audit by měl v souladu se standardy 2110, 2120.A1 a 2130.A1 řídicím a kontrolním orgánům organizace podávat ujištění i o zvládání rizik v oblasti ochrany osobních údajů a ohledně fungování funkce pověřence.



Funkce interního auditu by měla také navázat úzkou spolupráci s funkcemi druhé linie obrany, včetně pověřence pro ochranu osobních údajů.

Zajímá Vás více?

Uskuteční-li organizace potřebné změny v dostatečném předstihu ještě před nabytím účinnosti obecného nařízení, ušetří za mimořádná a nákladná opatření, která by po nabytí účinnosti musela přijmout k rychlému zajištění souladu s GDPR. Podniknutí kroků k dosažení souladu je také signálem partnerům a veřejnosti, že organizace respektuje jejich soukromí a odpovědnost za jejich osobní údaje nebere na lehkou váhu.

Bližší informace můžete získat v naší brožuře zabývající se GDPR problematikou.

Přijďte na jeden z našich seminářů, které se konají ve dnech 24. 5., 7. 6. a 21. 6. 2017. Registrovat se můžete zde.

Poslední možnost připravit se na registr smluv

Od 1. 7. 2017 vstoupí v účinnost poslední ustanovení zákona č. 340/2015 Sb., o registru smluv, která stanoví sankce pro případ, že by smlouva nebyla uveřejněna. Taková smlouva nenabude účinnosti, a tedy nebude pro strany závazná. Pokud smlouva nebude uveřejněna ani dodatečně, a to nejpozději do tří měsíců ode dne, kdy byla uzavřena, bude se na ni hledět jako na zrušenou od počátku.

Zajímá Vás jak nastavit procesy související s uveřejňováním v registru smluv a jak auditovat tyto procesy? Přijďte na náš seminář „Audit zvládání rizik procesů uveřejňování do registru smluv", který pořádáme společně s Českým institutem interních auditorů a který se uskuteční 19. 5. od 9:00 v sídle ČIIA. Registrujte se na www.interniaudit.cz.

Otazníky nad výjimkami pro registr smluv

Parlament České republiky projednává novelu zákona o registru smluv, která měla zúžit rozsah subjektů povinných řídit se tímto zákonem.

Dne 19. 4. 2017 Senát Parlamentu České republiky přijal pozměňovací návrhy k projednávané novele. Senát navrhované výjimky pro povinné subjekty, kromě úlevy pro Budějovický budvar, odmítl. Sněmovně se tak vrací text novely, který se razantně neodklání od původní verze zákona o registru smluv.

Senát nesouhlasil se zavedením výjimek pro podnikající povinné subjekty průmyslové nebo obchodní povahy a výjimek pro Kancelář prezidenta republiky, Parlament a některé další orgány.

Novelou ve znění senátních pozměňovacích návrhů se bude znovu zabývat Poslanecká sněmovna nejdříve 16. 5. 2017. Vzhledem k blížícím se volbám nelze odhadnout, zda se ve Sněmovně najde dostatek hlasů nutných pro odmítnutí Senátní verze novely.

Významné rozšíření okruhu působnosti zákona o kybernetické bezpečnosti

Poslanecká sněmovna projednává novelu, která mění zákon o kybernetické bezpečnosti. Touto novelizací vláda reaguje na evropskou směrnici, která má zajistit vysokou úroveň bezpečnosti sítí a informačních systémů v EU. Návrh významně rozšiřuje působnost stávajícího zákona o kybernetické bezpečnosti na provozovatele základních služeb i správce a provozovatele informačních systémů základních služeb, kteří působí ve významných odvětvích infrastruktury, jako jsou energetika nebo doprava. Rozšíření zasáhne rovněž klíčové poskytovatele digitálních služeb, jako jsou například některé e-shopy a internetové vyhledávače.

Nově zahrnuté skupiny adresátů budou muset podniknout odpovídající kroky a přijmout relevantní kontrolní mechanismy eliminující bezpečnostní rizika a oznamovat případné kybernetické incidenty Národnímu bezpečnostnímu úřadu.

Orgány veřejné moci budou muset smluvně upravit pravidla zákaznického auditu

Jednou z novinek je také povinnost správce nebo provozovatele systému nebo komunikačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby, který je orgánem veřejné moci, začlenit podmínku dostupnosti dat do jeho smlouvy s poskytovatelem služeb cloud computingu. Důvodem je nutnost zajistit přístup k informacím a datům z těchto systémů uložených v cloudu. Novela také stanoví náležitosti smlouvy uzavírané mezi orgánem veřejné moci a poskytovatelem služeb cloud computingu. Jednou z nich je i ujednání o pravidlech zákaznického auditu, který bude moci orgán veřejné moci vykonat u poskytovatele nebo takovou službu pro sebe zajistit externě.

„Nově zahrnuté skupiny adresátů budou muset podniknout odpovídající kroky a přijmout relevantní kontrolní mechanismy eliminující bezpečnostní rizika a oznamovat případné kybernetické incidenty Národnímu bezpečnostnímu úřadu."

Institut interních auditorů vydal nový vzorový statut interního auditu

Na stránkách Institutu interních auditorů (www.theiia.org) je k dispozici nový vzor statutu interního auditu. Tento vzor má posloužit jako vodítko k upravení postavení interního auditu v organizaci v souladu s Mezinárodním rámcem pro profesní praxi interního auditu, zejména pak standardem 1000 – Účel, pravomoci a odpovědnosti a standardem 1010 – Přijetí závazných směrnic ve statutu interního auditu.

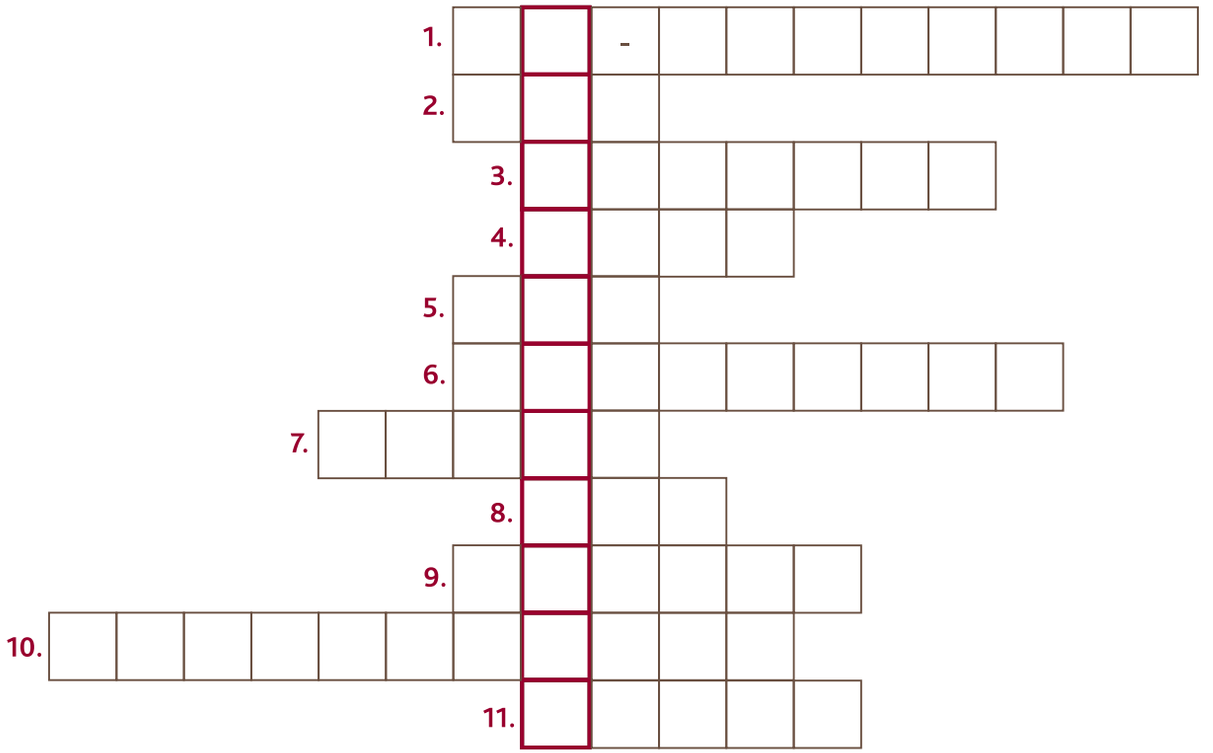
K dispozici je nový GTAG: „Assesing Cybersecurity Risk – Roles of the Three Lines of Defense“

Publikace GTAG (Global Technology Audit Guides) jsou metodiky připravené Institutem interních auditorů, které se zabývají otázkami managamentu, rizik, kontrol a bezpečnosti v souvislosti s informačními technologiemi.

Nová publikace „Assesing Cybersecurity Risk“ se věnuje aktuálnímu tématu kybernetické bezpečnosti. Interní auditoři získají tipy, jak postupovat při posouzení rizik spojených s kybernetickou bezpečností a jak v otázkách kybernetické bezpečnosti spolupracovat s první a druhou linií obrany. Publikace také nastiňuje nová rizika a obvyklé hrozby v oblasti kybernetické bezpečnosti, s kterými se jednotlivé linie obrany v rámci svých pracovních úkolů potýkají.

Křížovka o ceny

Vyluštěte křížovku a zašlete tajenku na monika.markova@bdo.cz a získejte **25% slevu** na jeden z našich GDPR seminářů.



1. Druh out-sourcingu, do kterého jsou zapojeny i lidské zdroje klienta

2. Ústřední správní úřad pro oblast kybernetické bezpečnosti

3. V širším smyslu soudní rozhodnutí, v užším smyslu rozhodnutí vyššího soudu, které má význam pro další rozhodování obdobných věcí

4. Měna Eurozóny

5. Nezávislý orgán, který prověřuje, jak stát hospodaří se státním majetkem a s prostředky získanými ze zahraničí a vyjadřuje se ke státnímu závěrečnému účtu a dohlíží také na plnění státního rozpočtu

6. Soubor principů a závazných požadavků

7. Rámec vytvořený mezinárodní asociací ISACA pro IT management a IT governance

8. Zkratka vnitřního kontrolního systému

9. Nejistota, že dojde k určité události, která by mohla mít negativní vliv na plnění stanovených cílů. Měří se podle možných následků a pravděpodobnosti výskytu.

10. Věda, která se zabývá obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích.

11. Systematický proces objektivního získávání a vyhodnocování informací o ekonomických činnostech a událostech, s cílem zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a sdělit výsledky zainteresovaným zájemcům

Hlavní kontaktní osoby

Ondřej Šnejdar
ondrej.snejdar@bdo.cz

Petr Slavíček
petr.slavicek@bdo.cz

Stanislav Klika
stanislav.klika@bdo.cz

Lukáš Hendrych
lukas.hendrych@bdo.cz