Certifikace systému ochrany osobních údajů podle ISO/IEC 27701

Již druhý rokem je pro zájemce k dispozici norma ISO/IEC 27701: 2019 pro řízení ochrany osobních údajů. Cílem normy je rozšířit stávající systém řízení bezpečnosti informací (ISMS) podle ISO/IEC 27001 o další požadavky na zavedení, implementaci, udržování a neustálé zlepšování systému managementu ochrany osobních údajů (Privacy Information Management System – PIMS). Standard nastiňuje rámec požadavků pro správce a zpracovatele personifikovaných informací (Personally Identifiable Information – PII) za účelem snížení rizika narušení práv jednotlivců na soukromí.

ISO/IEC 27701 má být certifikovatelným rozšířením certifikací ISO/IEC 27001. Jinými slovy, organizace, které plánují usilovat o certifikaci ISO/IEC 27701, budou také muset mít certifikaci ISO/IEC 27001.

TÜV NORD tedy může nabídnout svým zákazníkům rozšíření stávající akreditované certifikace systému ISMS i o požadavky ISO/IEC 27701 a nabídnout tak alternativu pro neakreditovanou certifikaci dosud používané BS 10012.

Historie standardu

V pracovní skupině WG 5 společné technické komise ISO/IEC 1/SC 27 „Technologie správy identit a soukromí“ byl v dubnu 2016 z iniciativy francouzských odborníků navržen nový pracovní bod, který se rozvinul do návrhu normy ISO/IEC 27552.

První návrh komise CD ISO/IEC 27552 byl zveřejněn v únoru 2018, druhý pak v srpnu 2018. Návrh mezinárodní normy DIS byl vydán v lednu 2019 a schválen v březnu 2019. Jelikož nebyly nutné žádné technické změny, bylo vydání závěrečného návrhu FDIS již vynecháno.

Společná technická komise ISO/IEC 1/SC 27 dokončila technické práce na ISO/IEC 27552 v dubnu 2019. Před vydáním však byla ISO/IEC 27552 přečíslována na ISO/IEC 27701, a to v souladu s rezolucí technické správní rady ISO č. 39/2019, která stanovila, že každý systém managementu „typu A“ (obsahující požadavky) musí mít číslo zakončené „ 01 ”. Přečíslování bylo dokončeno v červenci 2019. Samotná norma byla zveřejněna 6. srpna 2019.

Zamýšlená aplikace standardu - přínos

Základní ambicí ISO/IEC 27701 je rozšířit stávající systém řízení bezpečnosti informací o řídicí prvky specifické pro ochranu osobních údajů, a tedy vytvořit systém, který umožní efektivní ochranu soukromí v rámci organizace.

Dobře nastavený PIMS má mnoho potenciálních výhod pro správce a zpracovatele PII – za všechny lze zmínit přinejmenším následující tři významné výhody:

První výhodou je bezesporu vytvoření podmínek pro dosažení shody s obecnými požadavky na ochranu osobních údajů. V rámci Evropské unie lze zmínit Obecné nařízení o ochraně osobních údajů (GDPR), mimo EU pak například brazilský zákon o ochraně osobních údajů (LGPD) či kalifornský zákon o ochraně soukromí spotřebitelů (CCPA). Další požadavky na subjekt mohou vznášet i jiné zainteresované strany – zákazníci, akcionáři, zaměstnanecké organizace apod. Organizace, na které se vztahuje více povinností dodržovat zásady ochrany osobních údajů (např. v několika jurisdikcích, ve kterých firmy působí, nebo jejich zaměstnanci žijí), čelí komplikacím, které vyplývají z požadavku na sladění, uspokojení a monitorování všech příslušných požadavků. Systémový přístup tedy snižuje zátěž související s dodržováním těchto předpisů.

Druhým přínosem pro firmy je možnost poskytnutí nezbytných důkazů o splnění příslušných požadavků na ochranu osobních údajů pro zúčastněné strany, jako je vrcholové vedení, vlastníci, odbory nebo státní úřady. Certifikace PIMS tak může potenciálně i pro zvýšení důvěryhodnosti organizace vůči veřejnosti.

V neposlední řadě může být certifikace PIMS cenná při komunikaci o dodržování ochrany osobních údajů se zákazníky a dalšími partnery. Správci PII vyžadují od zpracovatelů PII důkazy o tom, že systém řízení soukromí je ve shodě s příslušnými požadavky na ochranu osobních údajů. Jednotný rámec důkazů založený na mezinárodních standardech může takovouto komunikaci o transparentnosti dodržování předpisů výrazně zjednodušit, zvláště když jsou důkazy validovány akreditovaným auditorem třetí strany.

Prokázání shody v této oblasti je rovněž zásadní pro strategická podnikatelská rozhodnutí, jako jsou fúze, akvizice a scénáře zahrnující dohodu o sdílení dat.

Kontakt: Mgr. Viktor Šaroch, PhD., saroch@tuev-nord.cz, +420 602 664 895