ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Marec 2022

STN	**Bezpečnostné metódy Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov Požiadavky a usmernenia (ISO/IEC 27701: 2019)**	**STN EN ISO/IEC 27701** 97 4123

Security techniques
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
Requirements and guidelines

Techniques de sécurité
Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée
Exigences et lignes directrices

Sicherheitstechniken
Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz
Anforderungen und Richtlinien

Táto norma je slovenskou verziou európskej normy EN ISO/IEC 27701: 2021.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
Táto norma má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27701: 2021.
It was translated by Slovak Office of Standards, Metrology and Testing.
It has the same status as the official versions.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza anglickú verziu STN EN ISO/IEC 27701 z augusta 2021.

134335

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2022
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 27000 zavedená v STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenie informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27001: 2013 zavedená v STN EN ISO/IEC 27001: 2019 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2013 vrátane Cor. 1: 2014 a Cor. 2: 2015) (36 9789)

ISO/IEC 27002: 2013 zavedená v STN EN ISO/IEC 27002: 2019 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002: 2013 vrátane Cor. 1: 2014 a Cor. 2: 2015) (36 9784)

ISO/IEC 29100 zavedená v STN EN ISO/IEC 29100 Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov (ISO/IEC 29100) (36 9758)

Vypracovanie normy

Spracovateľ: Ing. Lenka Gondová, Pro Excellence, s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27701

Apríl 2021

ICS 35.030

Bezpečnostné metódy
Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov
Požiadavky a usmernenia
(ISO/IEC 27701: 2019)

Security techniques
Extension to ISO/IEC 27001 and ISO/IEC 27002
for privacy information management
Requirements and guidelines
(ISO/IEC 27701: 2019)

Techniques de sécurité
Extension d'ISO/IEC 27001
et ISO/IEC 27002 au management
de la protection de la vie privée
Exigences et lignes directrices
(ISO/IEC 27701: 2019)

Sicherheitstechniken
Erweiterung zu ISO/IEC 27001 und
ISO/IEC 27002 für das Management
von Informationen zum Datenschutz
Anforderungen und Richtlinien
(ISO/IEC 27701: 2019)

Túto európsku normu schválil CEN 12. apríla 2021.

Členovia CEN sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN
Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CENELEC
Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotéchnique
Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

© 2021 CEN/CENELEC Všetky práva na využívanie v akejkoľvek forme a akýmikoľvek prostriedkami sú vyhradené na celom svete členom CEN a CENELEC.

Ref. č. EN ISO/IEC 27701: 2021 SK

Obsah

strana

Európsky predhovor

Text ISO/IEC 27701: 2019 vypracovala technická komisia medzinárodnej organizácie pre normalizáciu ISO/IEC JTC 1 Informačné technológie a bol prevzatý ako EN ISO/IEC 27701: 2021 technickou komisiou CEN/CLC/JTC 13 Kybernetická bezpečnosť a ochrana údajov, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskoršie do októbra 2021 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskoršie do októbra 2021.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN nezodpovedá za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text medzinárodnej normy ISO/IEC 27701: 2019 bol schválený CEN ako EN ISO/IEC 27701: 2021 bez akýchkoľvek modifikácií.

Úvod

0.1 Všeobecne

Takmer každá organizácia spracúva osobné údaje (PII[1]). Okrem toho sa zvyšuje množstvo a typy spracúvaných PII, ako aj počet situácií, v ktorých musí organizácia spolupracovať s inými organizáciami v súvislosti so spracúvaním PII. Ochrana súkromia v súvislosti so spracúvaním PII je spoločenskou potrebou, ako aj predmetom špecializovaných právnych predpisov a/alebo nariadení na celom svete.

Systém manažérstva informačnej bezpečnosti (ISMS[2]) definovaný v norme ISO/IEC 27001 je navrhnutý tak, aby umožňoval doplnenie špecifických sektorových požiadaviek bez potreby vypracovania nového systému manažérstva. Normy systému manažérstva ISO vrátane špecifických sektorových noriem sú navrhnuté tak, aby ich bolo možné implementovať buď samostatne, alebo ako kombinovaný systém manažérstva.

Požiadavky a usmernenia na ochranu osobných údajov sa líšia v závislosti od súvislostí organizácie, najmä ak existujú vnútroštátne právne predpisy a/alebo nariadenia. Norma ISO/IEC 27001 vyžaduje, aby sa tieto súvislosti chápali a zohľadnili. Tento dokument obsahuje mapovanie na:

– rámec a zásady ochrany súkromia, definované v norme ISO/IEC 29100,

– ISO/IEC 27018,

– ISO/IEC 29151, a

– všeobecné nariadenie EÚ na ochranu osobných údajov.

Môže byť potrebné vykladať tieto normy a nariadenia s ohľadom na miestne právne predpisy a/alebo nariadenia.

Tento dokument môžu používať PII prevádzkovatelia (vrátane tých, ktorí sú spoločnými PII prevádzkovateľmi) a PII sprostredkovatelia (vrátane tých, ktorí využívajú subdodávateľov PII sprostredkovateľov, a tých, ktorí spracúvajú PII ako subdodávatelia sprostredkovateľov PII).

Organizácia, ktorá spĺňa požiadavky uvedené v tomto dokumente, vytvorí dokumentáciu preukazujúcu spôsob spracovávania PII. Takéto dôkazy sa môžu použiť na uľahčenie dohôd s obchodnými partnermi, ak je spracúvanie PII vzájomne relevantné. Môže to pomôcť aj vo vzťahoch s inými zainteresovanými stranami. Použitie tohto dokumentu v spojení s normou ISO/IEC 27001 môže v prípade potreby poskytnúť nezávislé overenie týchto dôkazov.

Tento dokument bol pôvodne vypracovaný ako ISO/IEC 27552.

0.2 Kompatibilita s inými normami systému manažérstva

V tomto dokumente sa uplatňuje rámec vyvinutý organizáciou ISO na zlepšenie súladu medzi jej normami systému manažérstva.

Tento dokument umožňuje organizácii zosúladiť alebo integrovať svoj Systém riadenia informácií o ochrane osobných údajov (PIMS[3]) s požiadavkami iných noriem systému manažérstva.

[1] Personally Identifiable Information (PII) – Osobné údaje.

[2] The Information Security Management System (ISMS) – Systém manažérstva informačnej bezpečnosti.

[3] Privacy Information Management System (PIMS) – Systém riadenia informácií o ochrane osobných údajov.

1 Predmet normy

Tento dokument špecifikuje požiadavky a poskytuje návod na vytvorenie, implementáciu, udržiavanie a neustále zlepšovanie Systému riadenia informácií o ochrane osobných údajov (PIMS) vo forme rozšírenia noriem ISO/IEC 27001 a ISO/IEC 27002 na účely riadenia ochrany osobných údajov v súvislostiach organizácie.

Tento dokument špecifikuje požiadavky súvisiace s PIMS a poskytuje usmernenia pre prevádzkovateľov a sprostredkovateľov PII, ktorí nesú zodpovednosť za spracovanie PII.

Tento dokument sa vzťahuje na všetky typy a veľkosti organizácií vrátane verejných a súkromných spoločností, vládnych subjektov a neziskových organizácií, ktoré sú prevádzkovateľmi PII a/alebo sprostredkovateľmi PII spracúvajúcimi PII v rámci ISMS.

2 Normatívne odkazy

Nasledujúce dokumenty, celé alebo ich časti sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

ISO/IEC 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary.* [Informačné technológie. Bezpečnostné metódy. Systémy riadenie informačnej bezpečnosti. Prehľad a slovník.]

ISO/IEC 27001: 2013 *Information technology – Security techniques – Information security management systems – Requirements.* [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.]

ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security controls.* [*Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.*]

ISO/IEC 29100 *Information technology – Security techniques – Privacy framework.* [Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov.]

koniec náhľadu – text ďalej pokračuje v platenej verzii STN