ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA December 2025

STN	**Systém riadenia informácií o súkromí podľa normy ISO/IEC 27701 Spresnenia v európskom kontexte**	**STN EN 17926** 97 4177

Privacy Information Management System per ISO/IEC 27701
Refinements in European context

Système de management de la protection de la vie privée conformément à l'EN ISO/IEC 27701
Affinements relatifs au contexte européen

Datenschutz-Informationsmanagementsystem per ISO/IEC 27701
Konkretisierungen im europäischen Kontext

Táto slovenská technická norma je slovenskou verziou európskej normy EN 17926: 2023.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN 17926 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN 17926: 2023.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN 17926 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN 17926 z apríla 2024 v celom rozsahu.

141368

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z CEN/CENELEC, © 2023 CEN/CENELEC, ref. č. EN 17926: 2023 E.

Táto norma obsahuje 3 národné poznámky.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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 a TNI možno získať na webovom sídle www.unms.sk.

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

EN ISO/IEC 27001: 2017 prijatá ako STN EN ISO/IEC 27001: 2019

POZNÁMKA 3. – EN ISO/IEC 27001: 2017 bola zrušená a nahradená EN ISO/IEC 27001: 2023 prijatá ako STN EN ISO/IEC 27001: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2022) (97 4171).

Vypracovanie

Spracovateľ: SynCo, s.r.o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA **EN 17926**
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM November 2023

ICS 35.030

Systém riadenia informácií o súkromí podľa normy ISO/IEC 27701 Spresnenia v európskom kontexte

Privacy Information Management System per ISO/IEC 27701
Refinements in European context

Système de management de la protection de la vie privée conformément à l'EN ISO/IEC 27701
Affinements relatifs au contexte européen

Datenschutz-Informationsmanagementsystem per ISO/IEC 27701
Konkretisierungen im europäischen Kontext

Túto európsku normu schválil CEN 13. apríla 2023.

Členovia CEN a CENELEC 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 a CENELEC.

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

Členmi CEN a CENELEC 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 Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

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

Ref. č. EN 17926: 2023 SK

Obsah

strana

Európsky predhovor

Tento dokument (EN 17926: 2023) vypracovala technická komisia CEN/CLC/JTC 13 *Kybernetická bezpečnosť a ochrana údajov*, ktorej sekretariát je v DIN.

Tejto európskej norme sa najneskôr do mája 2024 udelí štatút národnej normy, a to buď uverejnením identického textu, alebo schválením, a národné normy, ktoré sú s ňou v rozpore, sa zrušia najneskôr do mája 2024.

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

Akákoľvek spätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov je na webovej sídle CEN.

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.

Úvod

Norma ISO/IEC 27701 špecifikuje požiadavky a poskytuje návod na vytvorenie, zavedenie, udržiavanie a neustále zlepšovanie systému riadenia informácií o súkromí (PIMS), ktorý možno zaviesť v akejkoľvek jurisdikcii. Keďže ide o systém riadenia určený na medzinárodné použitie, jeho požiadavky sú všeobecné a usmernenie si môžu organizácie prispôsobiť podľa svojho kontextu a platných povinností.

Hoci norma ISO/IEC 27701 bola napísaná so zámerom, aby bola použiteľná v akejkoľvek jurisdikcii vrátane všeobecného nariadenia EÚ o ochrane údajov (GDPR) (príloha D normy ISO/IEC 27701 obsahuje mapovanie medzi ustanoveniami normy a GDPR), je zodpovednosťou organizácie určiť, ako implementovať požiadavky a opatrenia normy ISO/IEC 27701 v kontexte GDPR.

Tento dokument poskytuje spresnenia normy ISO/IEC 27701 pri uplatňovaní opatrení a usmernenia v norme ISO/IEC 27701 špecifické pre GDPR, ak je to potrebné. Tento dokument sa vzťahuje na rovnaké subjekty ako norma ISO/IEC 27701: 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 (systému riadenia informačnej bezpečnosti). Je určený na to, aby ho organizácie používali v kontexte GDPR na účely preukázania súladu s ich povinnosťami. Norma ISO/IEC 27701 v kombinácii s vylepšeniami tohto dokumentu predstavuje súbor požiadaviek, ktorý je špecifickejšie navrhnutý a vhodnejší pre kontext GDPR ako všeobecné požiadavky zo samotnej normy ISO/IEC 27701.

Normu ISO/IEC 27701 možno teda považovať za medzinárodný rámec, ktorý možno zdokonaliť pre konkrétny regionálny kontext (v prípade tohto dokumentu GDPR), a dokonca pridať požiadavky vhodné pre danú jurisdikciu/krajinu alebo sektor (mimo rozsahu tohto dokumentu).

Zlepšenia normy ISO/IEC 27701 pre spracovateľské operácie ako súčasť výrobkov, procesov a služieb špecifikované v tomto dokumente sa môžu použiť na posudzovanie zhody, ktoré môže vykonať prvá, druhá alebo tretia strana. Najmä certifikačné orgány môžu použiť tieto požiadavky a spresnenia na posúdenie zhody systému riadenia informácií o súkromí podľa normy ISO/IEC 17021, ako aj operácií spracovania v rámci výrobku, procesu alebo služby podľa normy ISO/IEC 17065. Certifikačné systémy pre produkty zahŕňajúce spracovanie PII môžu odkazovať na tento dokument, ako je opísané v ISO/IEC 17067 pre systémy „typu 6“.

POZNÁMKA. – „výrobok“ sa môže chápať ako „proces“ alebo „služba“ (ISO/IEC 17065, kapitola 1 a príloha B).

Požiadavky uvedené v tomto dokumente môžu byť súčasťou systému, ktorý sa riadi podľa normy ISO/IEC 17065 pre požiadavky na výrobky zahŕňajúce činnosti spracovania PII („požiadavky na výrobky“ podľa normy ISO/IEC 17065, článok 3.8) a podľa normy ISO/IEC 17021 pre požiadavky na systém riadenia (systém ISO/IEC 17067 typu 6).

V článku 42 GDPR sa podporuje vytvorenie mechanizmov certifikácie ochrany údajov. Ustanovenia tohto dokumentu môžu príslušné orgány použiť na špecifikáciu certifikačných mechanizmov ochrany údajov podľa článku 42 GDPR s cieľom posúdiť zhodu spracovateľských operácií v PIMS podľa normy ISO/IEC 17065 vrátane posúdenia systematických prvkov systému riadenia informácií o súkromí, ako to umožňuje kapitola 6 normy ISO/IEC 17067.

1 Predmet

Tento dokument špecifikuje spresnenia pre aplikáciu normy ISO/IEC 27701 v európskom kontexte.

Tento dokument sa vzťahuje na rovnaké subjekty ako norma ISO/IEC 27701: 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 (systému riadenia informačnej bezpečnosti).

Organizácia môže použiť tento dokument na implementáciu všeobecných požiadaviek a opatrení podľa normy ISO/IEC 27701 v závislosti od svojho kontextu a platných povinností.

Certifikačné kritériá založené na týchto spresneniach môžu poskytnúť certifikačný model podľa ISO/IEC 17065 pre operácie spracovania vykonávané v rámci systému riadenia informácií o súkromí podľa ISO/IEC 27701, ktorý možno kombinovať s certifikačnými požiadavkami pre ISO/IEC 27701 podľa ISO/IEC 17021.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 27701: – [1] *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines* [*)]. [Bezpečnostné metódy. Rozšírenie noriem ISO/IEC 27001 a ISO/IEC 27002 o riadenie bezpečnosti osobných údajov. Požiadavky a usmernenia.]

EN ISO/IEC 27001: 2017 *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001: 2013 including Cor 1: 2014 and Cor 2: 2015).* [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2013 vrátane Cor 1: 2014 a Cor 2: 2015).]

3 Termíny a definície

V tomto dokumente nie sú uvedené žiadne termíny a definície.

ISO a IEC udržiavajú terminologické databázy na používanie v normalizácii na nasledujúcich adresách:

- ISO Online browsing platform: dostupné na https://www.iso.org/obp;
- IEC Electropedia: dostupné na https://www.electropedia.org/.

[1] V príprave. V čase uverejnenia v etape prípravy: ISO/IEC DIS 27701: 2023.

[*)] NÁRODNÁ POZNÁMKA 1. – V čase vydania prekladu norma publikovaná v ISO ako ISO/IEC 27701: 2025.