

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

**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, Rumunská, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédsko, Talianska a Turecko.

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

Obsah

strana

Európsky predhovor	9
Úvod	10
1 Predmet normy	11
2 Normatívne odkazy.....	11
3 Termíny, definície a skratky	11
4 Všeobecne.....	12
4.1 Štruktúra dokumentu	12
4.2 Použitie požiadaviek normy ISO/IEC 27001:2013	12
4.3 Použitie smerníc ISO/IEC 27002:2013.....	13
4.4 Zákazník	14
5 Špecifické požiadavky na PIMS súvisiace s normou ISO/IEC 27001	14
5.1 Všeobecne	14
5.2 Súvislosti organizácie	14
5.2.1 Pochopenie organizácie a jej súvislostí	14
5.2.2 Pochopenie potrieb a očakávaní zainteresovaných strán	14
5.2.3 Určenie predmetu systému manažérstva informačnej bezpečnosti.....	15
5.2.4 Systém manažérstva informačnej bezpečnosti.....	15
5.3 Vodcovstvo	15
5.3.1 Vodcovstvo a záväzok.....	15
5.3.2 Politika	15
5.3.3 Roly, zodpovednosti a právomoci v organizácii	15
5.4 Plánovanie	15
5.4.1 Opatrenia na zvládnutie rizík a príležitostí	15
5.4.2 Ciele informačnej bezpečnosti a plánovanie ich dosiahnutia.....	16
5.5 Podpora	16
5.5.1 Zdroje	16
5.5.2 Kompetentnosť	16
5.5.3 Povedomie.....	16
5.5.4 Komunikácia.....	16
5.5.5 Zdokumentované informácie	16
5.6 Prevádzka.....	17
5.6.1 Plánovanie a riadenie prevádzky	17
5.6.2 Posúdenie rizík informačnej bezpečnosti.....	17
5.6.3 Ošetrovanie rizík informačnej bezpečnosti	17
5.7 Hodnotenie výkonnosti	17
5.7.1 Monitorovanie, meranie, analýza a hodnotenie	17

5.7.2	Interný audit.....	17
5.7.3	Preskúmanie manažmentom	17
5.8	Zlepšovania	17
5.8.1	Nezhoda a nápravné opatrenia	17
5.8.2	Trvalé zlepšovania	17
6	Špecifické usmernenia PIMS týkajúce sa normy ISO/IEC 27002.....	17
6.1	Všeobecne	17
6.2	Politiky informačnej bezpečnosti	18
6.2.1	Smerovanie manažmentu v oblasti informačnej bezpečnosti	18
6.3	Organizácia informačnej bezpečnosti	18
6.3.1	Vnútoraná organizácia	18
6.3.2	Mobilné zariadenia a práca na diaľku	19
6.4	Personálna bezpečnosť	19
6.4.1	Pred nástupom do zamestnania	19
6.4.2	Počas zamestnania	19
6.4.3	Ukončenie a zmena zamestnania	20
6.5	Riadenie aktív	20
6.5.1	Zodpovednosť za aktíva	20
6.5.2	Klasifikácia informácií.....	20
6.5.3	Zaobchádzanie s médiami	20
6.6	Riadenie prístupov	21
6.6.1	Požiadavky na riadenie prístupu	21
6.6.2	Riadenie používateľských prístupov	21
6.6.3	Zodpovednosť používateľov.....	22
6.6.4	Riadenie systémových a aplikačných prístupov	22
6.7	Kryptografia	23
6.7.1	Kryptografické opatrenia	23
6.8	Fyzická bezpečnosť a bezpečnosť prostredia	23
6.8.1	Zabezpečené oblasti	23
6.8.2	Bezpečnosť zariadení	24
6.9	Bezpečnosť prevádzky.....	25
6.9.1	Prevádzkové postupy a zodpovednosť	25
6.9.2	Ochrana pred škodlivým softvérom.....	25
6.9.3	Zálohovanie	25
6.9.4	Zaznamenávanie dát a monitorovanie	26
6.9.5	Riadenie prevádzkového softvéru	26
6.9.6	Riadenie technickej zraniteľnosti.....	27
6.9.7	Audit informačných systémov	27
6.10	Komunikačná bezpečnosť.....	27

6.10.1	Riadenie bezpečnosti v sieťach	27
6.10.2	Prenos informácií	27
6.11	Akvízia, vývoj a údržba informačných systémov	28
6.11.1	Bezpečnostné požiadavky na informačné systémy	28
6.11.2	Bezpečnosť pri vývoji a pri podporných procesoch	28
6.11.3	Testovacie údaje	29
6.12	Riadenie vzťahov s dodávateľmi	29
6.12.1	Informačná bezpečnosť vo vzťahoch s dodávateľmi	29
6.12.2	Riadenie dodávateľských služieb	30
6.13	Riadenie incidentov informačnej bezpečnosti	30
6.13.1	Riadenie incidentov informačnej bezpečnosti a zlepšovania	30
6.14	Aspekty informačnej bezpečnosti v riadení kontinuity	32
6.14.1	Kontinuita informačnej bezpečnosti	32
6.14.2	Redundancia	32
6.15	Súlady	32
6.15.1	Súlady s právnymi a zmluvnými požiadavkami	32
6.15.2	Preskúmanie informačnej bezpečnosti	33
7	Dodatočné usmernenie ISO/IEC 27002 pre prevádzkovateľov PII	34
7.1	Všeobecne	34
7.2	Podmienky získavania a spracovania	34
7.2.1	Určenie a zdokumentovanie účelu	34
7.2.2	Určenie právneho základu	34
7.2.3	Určenie okolností získania súhlasu	35
7.2.4	Získanie a zaznamenanie súhlasu	35
7.2.5	Posúdenie vplyvu na ochranu osobných údajov	36
7.2.6	Zmluvy so sprostredkovateľmi PII	36
7.2.7	Spoloční PII prevádzkovatelia	36
7.2.8	Záznamy súvisiace so spracovaním osobných údajov	37
7.3	Povinnosti voči dotknutým osobám	37
7.3.1	Určenie a plnenie povinností voči dotknutým osobám	37
7.3.2	Určenie informácií pre dotknuté osoby	38
7.3.3	Poskytovanie informácií dotknutým osobám	38
7.3.4	Poskytnutie mechanizmu na zmenu alebo odvolanie súhlasu	39
7.3.5	Poskytnutie mechanizmu na vznesenie námietky proti spracúvaniu osobných údajov	39
7.3.6	Prístup, oprava a/alebo vymazanie	39
7.3.7	Povinnosti prevádzkovateľov osobných údajov informovať tretie strany	40
7.3.8	Poskytnutie kópie spracovaných PII	40
7.3.9	Vybavovanie žiadostí	40
7.3.10	Automatizované rozhodovanie	41

7.4	Špecificky navrhnutá a štandardná ochrana osobných údajov.....	41
7.4.1	Obmedzenie zberu osobných údajov.....	41
7.4.2	Obmedzenie spracúvania osobných údajov	41
7.4.3	Presnosť a kvalita.....	42
7.4.4	Ciele minimalizácie PII	42
7.4.5	Deidentifikácia a vymazanie PII na konci spracovania	43
7.4.6	Dočasné súbory	43
7.4.7	Uchovávanie.....	43
7.4.8	Likvidácia.....	43
7.4.9	Opatrenia prenosu PII	44
7.5	Zdieľanie, prenos a zverejňovanie osobných údajov	44
7.5.1	Identifikácia základu pre prenos PII medzi jurisdikciami.....	44
7.5.2	Krajiny a medzinárodné organizácie, do ktorých možno preniesť PII.....	44
7.5.3	Záznamy o prenose PII	44
7.5.4	Záznamy o sprístupnení PII tretím stranám	45
8	Dodatočné usmernenie ISO/IEC 27002 pre sprostredkovateľov PII	45
8.1	Všeobecne	45
8.2	Podmienky zberu a spracovania	45
8.2.1	Zmluva so zákazníkom.....	45
8.2.2	Účely organizácie	46
8.2.3	Marketingové a reklamné využitie.....	46
8.2.4	Porušujúce pokyny	46
8.2.5	Povinnosti zákazníka.....	46
8.2.6	Záznamy súvisiace so spracovaním PII.....	47
8.3	Povinnosti voči dotknutým osobám.....	47
8.3.1	Povinnosti voči dotknutým osobám.....	47
8.4	Špecificky navrhnutá a štandardná ochrana osobných údajov.....	47
8.4.1	Dočasné súbory	47
8.4.2	Vrátenie, prenos alebo likvidácia PII	48
8.4.3	Opatrenia prenosu PII	48
8.5	Zdieľanie, prenos a zverejňovanie osobných údajov	48
8.5.1	Základ pre prenos PII medzi jurisdikciami.....	48
8.5.2	Krajiny a medzinárodné organizácie, do ktorých možno preniesť PII.....	49
8.5.3	Záznamy o sprístupnení PII tretím stranám	49
8.5.4	Oznamovanie žiadostí o sprístupnenie PII.....	49
8.5.5	Právne záväzné zverejňovanie PII	49
8.5.6	Zverejnenie subdodávateľov používaných na spracovanie PII.....	50
8.5.7	Zapojenie subdodávateľa do spracovania PII.....	50
8.5.8	Zmena subdodávateľa na spracovanie PII	50

Príloha A (normatívna) – Referenčné ciele riadenia a opatrenia špecifické pre PIMS (prevádzkovatelia PII)	51
Príloha B (normatívna) – Referenčné ciele riadenia a opatrenia špecifické pre PIMS (sprostredkovatelia PII)	55
Príloha C (informatívna) – Mapovanie na ISO/IEC 29100.....	58
Príloha D (informatívna) – Mapovanie na Všeobecné nariadenie o ochrane údajov	61
Príloha E (informatívna) – Mapovanie na ISO/IEC 27018 a ISO/IEC 29151	65
Príloha F (informatívna) – Ako aplikovať ISO/IEC 27701 na ISO/IEC 27001 a ISO/IEC 27002	68
Literatúra	70

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.

Tento 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, Švédsko, Talianska a Turecko.

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 (PII¹). 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 (ISMS²) 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 spracúvania 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 (PIMS³) 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