

STN	Informačné technológie Bezpečnostné metódy Návod na posudzovanie vplyvu na súkromie (ISO/IEC 29134: 2023)	STN EN ISO/IEC 29134 97 4161
------------	--	--

Information technology

Security techniques

Guidelines for privacy impact assessment

Technologies de l'information

Techniques de sécurité

Lignes directrices pour l'étude d'impacts sur la vie privée

Informationstechnik

Sicherheitsverfahren

Leitlinien für die Datenschutz-Folgenabschätzung

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 29134: 2026. Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky. STN EN ISO/IEC 29134 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 29134: 2026. It was translated by Slovak Office of Standards, Metrology and Testing. STN EN ISO/IEC 29134 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 29134 zo septembra 2020 v celom rozsahu.



142958

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2026

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2023 ISO/IEC, ref. č. ISO/IEC 29134: 2023 E.

Pri preklade tejto normy bolo potrebné prijať niektoré jazykové úpravy, pretože slovenčina a angličtina majú určité špecifické vlastnosti a nie vždy je možné urobiť doslovný preklad, aby mala európska norma rovnaký význam v oboch jazykoch.

Anglický výraz „privacy“ sa v preklade tejto normy uvádza ako „súkromie“ alebo „ochrana osobných údajov“ v závislosti od kontextu.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 29134: 2017), ktoré bolo technicky revidované.

Hlavné zmeny sú tieto:

- boli vykonané menšie redakčné zmeny.

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 Guide 73: 2009 dosiaľ neprijatý

ISO/IEC 27000: 2018 prijatá ako STN EN ISO/IEC 27000: 2023 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018) (97 4170)

ISO/IEC 29100: 2011 prijatá ako STN EN ISO/IEC 29100: 2020 Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov (ISO/IEC 29100: 2011, vrátane zmeny A1: 2018) (36 9758)

Vypracovanie

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

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Návod na posudzovanie vplyvu na súkromie
(ISO/IEC 29134: 2023)

Information technology
 Security techniques
 Guidelines for privacy impact assessment
 (ISO/IEC 29134: 2023)

Technologies de l'information
 Techniques de sécurité
 Lignes directrices pour l'étude d'impacts
 sur la vie privée
 (ISO/IEC 29134: 2023)

Informationstechnik
 Sicherheitsverfahren
 Leitlinien für die Datenschutz-Folgenab-
 schätzung
 (ISO/IEC 29134: 2023)

Túto európsku normu schválil CEN 24. mája 2026.

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, Maltu, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, 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	6
Úvod	7
1 Predmet	9
2 Normatívne odkazy	9
3 Termíny a definície	9
4 Skratky	11
5 Príprava podkladov pre PIA	11
5.1 Výhody vykonávania PIA	11
5.2 Ciele podávania správ PIA	12
5.3 Zodpovednosť za vykonanie PIA	13
5.4 Rozsah PIA	14
6 Usmernenie k postupu vykonávania PIA	14
6.1 Všeobecne	14
6.2 Určenie, či je potrebné vykonať PIA (prahová analýza)	15
6.3 Príprava PIA	15
6.3.1 Zriadenie tímu PIA a jeho usmernenie	15
6.3.2 Pripravenie plánu PIA a určenie zdrojov potrebných na vykonanie PIA	17
6.3.3 Opis toho, čo sa posudzuje	18
6.3.4 Zapojenie zainteresovaných strán	19
6.4 Vykonanie PIA	21
6.4.1 Identifikácia informačných tokov PII	21
6.4.2 Analýza dôsledkov prípadu použitia	22
6.4.3 Určenie príslušných požiadaviek na ochranu osobných údajov	23
6.4.4 Posúdenie rizík súkromia	23
6.4.5 Príprava na ošetrovanie rizík súkromia	26
6.5 Sledovanie PIA	31
6.5.1 Príprava správy	31
6.5.2 Publikácia	32
6.5.3 Implementácia plánov ošetrovania rizík súkromia	32
6.5.4 Preskúmanie a/alebo audit PIA	33
6.5.5 Zohľadnenie zmien v procese	33

7	Správa PIA	34
7.1	Všeobecne	34
7.2	Štruktúra správy	34
7.3	Rozsah pôsobnosti PIA.....	35
7.3.1	Hodnotený proces	35
7.3.2	Kritériá rizík	36
7.3.3	Zdroje a zapojené osoby	36
7.3.4	Konzultácie so zainteresovanými stranami.....	37
7.4	Požiadavky na ochranu osobných údajov	37
7.5	Posúdenie rizík.....	37
7.5.1	Zdroje rizík.....	37
7.5.2	Hrozby a ich pravdepodobnosť	37
7.5.3	Dôsledky a úroveň ich vplyvu	37
7.5.4	Hodnotenie rizík	37
7.5.5	Analýza súladu.....	37
7.6	Plán ošetrovania rizík.....	38
7.7	Záver a rozhodnutia.....	38
7.8	Sumarizácia PIA pre verejnosť	38
	Príloha A (informatívna) – Kritériá mierky úrovne vplyvu a pravdepodobnosti.....	39
	Príloha B (informatívna) – Všeobecné hrozby	41
	Príloha C (informatívna) – Usmernenie k chápaniu používaných termínov	47
	Príloha D (informatívna) – Znázornené príklady na podporu procesu PIA.....	49
	Literatúra.....	51

Európsky predhovor

Text ISO/IEC 29134: 2023 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 29134: 2026 technickou komisiou CEN-CENELEC/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 novembra 2026 a národné normy, ktoré sú s ňou v rozpore sa musia zrušiť najneskoršie do novembra 2026.

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

Tento dokument nahrádza EN ISO/IEC 29134: 2020.

Akakoľvek spätná väzba a otázky k tomuto dokumentu majú byť adresované národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto orgánov možno nájsť na webovej stránke CEN a CENELEC.

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 Turecka.

Oznámenie o schválení

Text ISO/IEC 29134: 2023 schválil CEN-CENELEC ako EN ISO/IEC 29134: 2026 bez akýchkoľvek modifikácií.

Úvod

Posudzovanie vplyvu na súkromie (PIA) je nástroj na:

- posúdenie potenciálnych vplyvov procesu, informačného systému, programu, softvérového modulu, zariadenia alebo inej iniciatívy, ktorá spracúva osobné údaje (PII) na súkromie;
- prijímanie potrebných opatrení na ošetrovanie rizika súvisiaceho s ochranou osobných údajov po konzultácii so zainteresovanými stranami.

Správa PIA môže obsahovať dokumentáciu o opatreniach prijatých na ošetrovanie rizík, napríklad opatrenia vyplývajúce z používania systému riadenia informačnej bezpečnosti (ISMS) podľa normy ISO/IEC 27001. PIA je viac než len nástroj: je to proces, ktorý sa začína v čo najskorších fázach iniciatívy, keď ešte existujú možnosti ovplyvniť jej výsledok, a tým zabezpečiť ochranu osobných údajov už v štádiu návrhu. Je to proces, ktorý pokračuje až do nasadenia projektu a dokonca aj po ňom.

Iniciatívy sa výrazne líšia rozsahom a vplyvom. Ciele spadajúce pod „ochranu osobných údajov“ budú závisieť od kultúry, spoločenských očakávaní a jurisdikcie. Cieľom tohto dokumentu je poskytnúť škálovateľné usmernenie, ktoré možno uplatniť na všetky iniciatívy. Keďže usmernenie špecifické pre všetky okolnosti nemôže byť normatívne, usmernenie v tomto dokumente by sa malo interpretovať s ohľadom na jednotlivé okolnosti.

Prevádzkovateľ PII môže mať povinnosť vykonať PIA a môže požiadať sprostredkovateľa PII, aby mu pri tom pomohol a konal v mene prevádzkovateľa PII. Sprostredkovateľ PII alebo dodávateľ môže tiež chcieť vykonať vlastnú PIA.

Informácie z PIA dodávateľa sú dôležité najmä vtedy, keď sú digitálne pripojené zariadenia súčasťou hodnoteného informačného systému, aplikácie alebo procesu. Môže byť potrebné, aby dodávateľia takýchto zariadení poskytli osobám vykonávajúcim PIA informácie o návrhu relevantné z hľadiska ochrany osobných údajov. Je možné, že dodávateľ digitálnych zariadení nemá dostatok kvalifikácie a zdrojov na PIA, napríklad:

- malý maloobchodný predajca; alebo
- malý a stredný podnik (SME), ktorý v rámci svojej bežnej obchodnej činnosti používa digitálne pripojené zariadenia.

Za týchto okolností môže byť dodávateľ zariadenia vyzvaný, aby poskytol veľké množstvo informácií o ochrane osobných údajov a vykonal vlastnú PIA, s ohľadom na kontext dotknutej osoby/SME, pre zariadenie, ktoré dodáva, s cieľom umožniť mu vykonať minimálnu PIA.

PIA zvyčajne vykonáva organizácia, ktorá berie svoju zodpovednosť vážne a primerane zaobchádza s PII dotknutých osôb. V niektorých jurisdikciách sa môžu uplatňovať právne a regulačné požiadavky týkajúce sa PIA.

Tento dokument je určený na použitie v prípadoch, keď vplyv na súkromie dotknutých osôb zahŕňa posúdenie procesov, informačných systémov alebo programov, kde:

- zodpovednosť za implementáciu a/alebo realizáciu procesu, informačného systému alebo programu je zdieľaná s inými organizáciami a malo by sa zabezpečiť, aby každá organizácia riadne riešila identifikované riziká;
- organizácia vykonáva riadenie rizík súkromia ako súčasť svojho celkového úsilia o riadenie rizík pri príprave na implementáciu alebo zlepšenie svojho ISMS (vytvoreného v súlade s normou ISO/IEC 27001 alebo ekvivalentným systémom riadenia); alebo organizácia vykonáva riadenie rizík súkromia ako samostatnú funkciu;

- organizácia (napr. štátna správa) vyvíja iniciatívu (napr. program verejno-súkromného partnerstva), v rámci ktorej ešte nie je známa budúca organizácia, ktorá je prevádzkovateľom PII, v dôsledku čoho nie je možné priamo implementovať plán ošetrovania, a preto sa predpokladá, že tento plán ošetrovania sa namiesto toho stane súčasťou príslušných právnych predpisov, nariadení alebo zmluvy;
- organizácia chce konať zodpovedne voči dotknutým osobám.

Opatrenia, ktoré sa považujú za potrebné na riešenie rizík identifikovaných počas procesu analýzy vplyvu na súkromie, môžu byť odvodené z viacerých súborov opatrení vrátane noriem ISO/IEC 27002 (pre bezpečnostné opatrenia) a ISO/IEC 29151 (pre opatrenia ochrany osobných údajov) alebo porovnateľných vnútroštátnych noriem, alebo ich môže definovať osoba zodpovedná za vykonanie PIA nezávisle od akéhokoľvek iného súboru opatrení.

1 Predmet

Tento dokument obsahuje návod na:

- proces posudzovania vplyvu na súkromie; a
- štruktúru a obsah správy PIA.

Je použiteľný pre všetky typy a veľkosti organizácií vrátane verejných spoločností, súkromných spoločností, vládnych subjektov a neziskových organizácií.

Tento dokument je dôležitý pre osoby zapojené do navrhovania alebo realizácie projektov vrátane strán prevádzkujúcich systémy a služby spracovania údajov, ktoré spracúvajú osobné údaje.

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 Guide 73: 2009 *Risk management – Vocabulary*. [Manažérstvo rizík. Slovník.]

ISO/IEC 27000: 2018 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.]

ISO/IEC 29100: 2011 *Information technology – Security techniques – Privacy framework*. [Informačné technológie. Bezpečnostné metódy. Rámec ochrany osobných údajov.]

koniec náhľadu – text ďalej pokračuje v platenej verzii STN