

STN	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Návod na vymazanie osobných údajov (ISO/IEC 27555: 2021)	STN EN ISO/IEC 27555 97 4215
------------	---	--

Information security, cybersecurity and privacy protection
Guidelines on personally identifiable information deletion

Sécurité de l'information, cybersécurité et protection de la vie privée
Lignes directrices relatives à la suppression des données à caractère personnel

Informationssicherheit, Cybersicherheit und Datenschutz
Richtlinien zur Löschung persönlich identifizierbarer Informationen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27555: 2025.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27555 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27555: 2025.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27555 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 27555 z augusta 2025
v celom rozsahu.

142995

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, © 2021 ISO/IEC, ref. č. ISO/IEC 27555: 2021 E.

Táto STN obsahuje jednu národnú poznámku.

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 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

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Návod na vymazanie osobných údajov
(ISO/IEC 27555: 2021)

Information security, cybersecurity and privacy protection
 Guidelines on personally identifiable information deletion
 (ISO/IEC 27555: 2021)

Sécurité de l'information, cybersécurité
 et protection de la vie privée
 Lignes directrices relatives à la suppression
 des données à caractère personnel
 (ISO/IEC 27555: 2021)

Informationssicherheit, Cybersicherheit
 und Datenschutz
 Richtlinien zur Löschung persönlich
 identifizierbarer Informationen
 (ISO/IEC 27555: 2021)

Túto európsku normu schválil CEN 7. marca 2025.

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, Švédsko, 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

Obsah

strana

Európsky predhovor	6
Úvod	7
1 Predmet	7
2 Normatívne odkazy	8
3 Termíny a definície	8
4 Symboly a skratky	9
5 Rámec pre vymazanie	10
5.1 Všeobecne	10
5.2 Obmedzenia	10
5.3 Skupiny osobných údajov	10
5.4 Doba uchovávaní a pravidelná lehota na vymazanie	11
5.4.1 Doba uchovávaní	11
5.4.2 Pravidelná lehota na vymazanie	11
5.4.3 Priradenie skupín PII	12
5.5 Archívy a záložné kópie	13
5.6 Štandardná lehota na vymazávanie, počiatočné body, pravidlá vymazávaní a triedy vymazávaní	13
5.7 Osobitné situácie	13
5.8 Dokumentácia politik a postupov	14
6 Skupiny osobných údajov	14
6.1 Všeobecne	14
6.2 Identifikácia	16
6.3 Dokumentácia	16
7 Špecifikácia období vymazania	17
7.1 Štandardné a pravidelné lehoty na vymazanie	17
7.2 Špecifikácie bežnej lehoty na vymazanie	17
7.3 Identifikácia štandardnej lehoty na vymazanie	18
7.4 Špecifikácie lehôt na vymazanie pre osobitné situácie	19
7.4.1 Všeobecne	19
7.4.2 Úprava dátových objektov	19
7.4.3 Potreba predĺžiť obdobie aktívneho používania	19
7.4.4 Pozastavenie vymazania	20
7.4.5 Záložné kópie	20

8	Triedy vymazania	21
8.1	Abstraktné východiskové body – abstraktné pravidlá vymazania	21
8.2	Matica tried vymazania	21
8.3	Priradenie tried vymazania a definícia pravidiel vymazania	23
9	Požiadavky na implementáciu	23
9.1	Všeobecne	23
9.2	Podmienky pre východiskové body mimo IT systémov	25
9.3	Požiadavky na implementáciu pre aspekty týkajúce sa celej organizácie	25
9.3.1	Všeobecne	25
9.3.2	Zálohovanie	26
9.3.3	Logy	26
9.3.4	Prenosové systémy	26
9.3.5	Oprava, vyrad'ovanie a likvidácia systémov a komponentov	26
9.3.6	Každodenný pracovný život	27
9.4	Požiadavky na implementáciu pre jednotlivé IT systémy	27
9.5	Vymazanie v bežných manuálnych procesoch	28
9.6	Požiadavky na implementáciu pre sprostredkovateľa PII	28
9.7	Opatrenie na vymazanie v osobitných prípadoch	28
9.7.1	Správa výnimiek	28
9.7.2	Ďalšie súbory PII	29
10	Zodpovednosti	30
10.1	Všeobecne	30
10.2	Dokumentácia	31
10.3	Implementácia	31
	Literatúra	32

Európsky predhovor

Text ISO/IEC 27555: 2021 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie* medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27555: 2025 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 septembra 2025 a národné normy, ktoré sú s ňou v rozpore sa musia zrušiť najneskoršie do septembra 2025.

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

Tento dokument bol vypracovaný na základe žiadosti o normalizáciu, ktorú Európska komisia adresovala organizáciám CEN a CENELEC. Stály výbor štátov EZVO následne schvaľuje tieto žiadosti pre svoje členské štáty.

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

Oznámenie o schválení

Text ISO/IEC 27555: 2021 schválil CEN-CENELEC ako EN ISO/IEC 27555: 2025 bez akýchkoľvek modifikácií.

Úvod

Mnohé funkčné procesy a IT aplikácie používajú osobne identifikovateľné informácie (PII)^{*)}, ktoré podliehajú rôznym ustanoveniam týkajúcim sa súkromia. Organizácie preto musia zabezpečiť, aby PII neboli uchovávané dlhšie, ako je potrebné a aby boli v primeranom čase vymazané. To môže vyžadovať, aby organizácie plnili práva dotknutých osôb, ako je napr. právo na vymazanie (byť zabudnutý). ISO/IEC 29100 definuje zásady „minimalizácie údajov“ a „obmedzenia používania, uchovávanía a zverejňovania“ PII, ktoré možno vynútiť pomocou vymazania ako bezpečnostného opatrenia.

Vymazanie osobných údajov vyžaduje súbor starostlivo navrhnutých, jasných a ľahko zrozumiteľných pravidiel vymazania, ktoré zahŕňajú primerané doby uchovávanía, ktoré spĺňajú požiadavky viacerých zainteresovaných strán. Tieto pravidlá by mali byť tiež v zhode s požiadavkami vyplývajúcimi z kódexov postupov a iných noriem. Mechanizmy musia byť správne implementované a primeraným spôsobom prevádzkované. S cieľom zabezpečiť vymazanie osobných údajov v súlade so zákonom musí prevádzkovateľ osobných údajov vypracovať politiky a postupy vymazania, ktoré obsahujú súbor pravidiel a zodpovedností za príslušné procesy. Šance na úspech pri vypracovaní a implementácii týchto politík a procesov sa môžu zvýšiť, ak prevádzkovateľ osobných údajov použije pri ich navrhovaní a implementácii uznávaný prístup.

Tento dokument poskytuje rámec pre vypracovanie a zavedenie politík a postupov na vymazanie PII, ktoré môže organizácia implementovať. Tento rámec umožňuje konzistentné vymazanie PII v celej organizácii.

1 Predmet

Tento dokument obsahuje návod na vypracovanie a zavedenie politík a postupov na vymazanie osobných údajov (PII) v organizáciách, pričom špecifikuje:

- harmonizovanú terminológiu pre vymazanie PII;
- prístup k efektívnemu definovaniu pravidiel vymazávania;
- opis požadovanej dokumentácie;
- širokú definíciu úloh, zodpovedností a procesov.

Tento dokument je určený na použitie v organizáciách, kde sa uchovávajú alebo spracúvajú osobné údaje.

Tento dokument sa nezaobrá:

- konkrétnymi právnymi ustanoveniami, ako sú stanovené v národných právnych predpisoch alebo špecifikované v zmluvách;
- konkrétnymi pravidlami vymazávania pre určité skupiny osobných údajov, ktoré sú definované prevádzkovateľmi osobných údajov na účely spracovania osobných údajov;
- mechanizmami vymazávania;
- spoľahlivosťou, bezpečnosťou a vhodnosťou mechanizmov vymazávania;
- špecifickými technikami na anonymizáciu údajov.

^{*)} NÁRODNÁ POZNÁMKA 1. – Zaužívaný preklad osobné údaje, skratka „PII“, ďalej len „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/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