ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Máj 2025

| STN | **Informačné technológie<br>Bezpečnostné metódy<br>Kódex postupov na ochranu osobných údajov (PII) vo verejných cloudoch, ktoré pôsobia ako sprostredkovatelia PII<br>(ISO/IEC 27018: 2019)** | **STN<br>EN ISO/IEC 27018**<br><br>97 4197 |
|---|---|---|

Information technology
Security techniques
Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Technologies de l'information
Techniques de sécurité
Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Informationstechnik
Sicherheitsverfahren
Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27018: 2020.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27018 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27018: 2020.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27018 has the same status as the official versions.

**Nahradenie predchádzajúcich dokumentov**

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 27018 z novembra 2020 v celom rozsahu.

**140296**

## Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2019 ISO/IEC, ref. č. ISO/IEC 27018: 2019 E.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27018: 2014), ktorého predstavuje menšiu revíziu. Hlavnou zmenou v porovnaní s predchádzajúcim vydaním je oprava redakčnej chyby v prílohe A.

ISO/IEC 27018 vypracovala technická komisia ISO/IEC JTC 1 *Informačné technológie*, subkomisia SC 27 *Bezpečnostné metódy IT*.

### 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 17788 prijatá ako STN ISO/IEC 17788

POZNÁMKA 3. – ISO/IEC 17788 bola zrušená a nahradená ISO/IEC 22123-1 a ISO/IEC 22123-2 prijaté ako STN ISO/IEC 22123-1 Informačné technológie. Cloud computing. Časť 1: Slovník (97 4176) a STN ISO/IEC 22123-2 Informačné technológie. Cloud computing. Časť 2: Koncepty (97 4176).

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

ISO/IEC 27002: 2013 prijatá ako STN EN ISO/IEC 27002: 2019

POZNÁMKA 4. – ISO/IEC 27002: 2013 bola zrušená a nahradená ISO/IEC 27002: 2022 prijatá ako STN ISO/IEC 27002: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022) (97 4172).

### Vypracovanie

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

**Technická komisia:** TK 37 Informačné technológie

**EURÓPSKA NORMA** **EN ISO/IEC 27018**
**EUROPEAN STANDARD**
**NORME EUROPÉENNE**
**EUROPÄISCHE NORM** Máj 2020

ICS 35.030

# Informačné technológie Bezpečnostné metódy Kódex postupov na ochranu osobných údajov (PII) vo verejných cloudoch, ktoré pôsobia ako sprostredkovatelia PII (ISO/IEC 27018: 2019)

Information technology
Security techniques
Code of practice for protection of personally identifiable information
(PII) in public clouds acting as PII processors
(ISO/IEC 27018: 2019)

Technologies de l'information
Techniques de sécurité
Code de bonnes pratiques pour la protection
des informations personnelles identifiables (PII)
dans l'informatique en nuage public agissant
comme processeur de PII (ISO/IEC 27018: 2019)

Informationstechnik
Sicherheitsverfahren
Leitfaden zum Schutz personenbezogener
Daten (PII) in öffentlichen Cloud-Diensten
als Auftragsdatenverarbeitung
(ISO/IEC 27018: 2019)

Túto európsku normu schválil CEN 3. mája 2020.

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

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



Ref. č. EN ISO/IEC 27018: 2020 SK

# Obsah

strana

## Európsky predhovor

Text ISO/IEC 27018: 2019 vypracovala technická komisia ISO/IEC JTC 1 Informačné technológie, medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 27018: 2020 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 najneskôr do novembra 2020 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do novembra 2020.

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 27018: 2019 schválil CEN ako EN ISO/IEC 27018: 2020 bez akýchkoľvek modifikácií.

# Úvod

## 0.1 Pozadie a kontext

Poskytovatelia cloudových služieb, ktorí na základe zmluvy so svojimi zákazníkmi spracúvajú informácie umožňujúce identifikáciu osôb – ďalej osobné údaje – (PII), potrebujú svoje služby prevádzkovať spôsobom, ktorý obom stranám umožní splniť požiadavky platných právnych predpisov a nariadení týkajúcich sa ochrany PII. Požiadavky a spôsob rozdelenia požiadaviek medzi poskytovateľa cloudových služieb a jeho zákazníkov sa líšia podľa právnej jurisdikcie a podľa podmienok zmluvy medzi poskytovateľom cloudových služieb a zákazníkom. Právne predpisy, ktoré upravujú spôsob, akým je povolené spracúvať PII (t. j. zhromažďovať, používať, prenášať a likvidovať, sa niekedy označujú ako právne predpisy o ochrane údajov; PII sa niekedy označujú ako osobné údaje alebo osobné informácie. Povinnosti, ktoré sa vzťahujú na sprostredkovateľa PII sa v jednotlivých jurisdikciách líšia, čo podnikom poskytujúcim služby cloud computingu sťažuje fungovanie na medzinárodnej úrovni.

Poskytovateľ verejnej cloudovej služby je „sprostredkovateľom osobných údajov“, ak spracúva osobné údaje pre zákazníka cloudovej služby a podľa jeho pokynov. Zákazník cloudovej služby, ktorý je v zmluvnom vzťahu so sprostredkovateľom PII vo verejnom cloude, môže byť od fyzickej osoby, „dotknutej osoby PII“, ktorá v cloude spracúva svoje vlastné PII, až po organizáciu, „prevádzkovateľa PII“, ktorá spracúva PII týkajúce sa mnohých dotknutých osôb PII. Zákazník cloudových služieb môže poveriť jedného alebo viacerých používateľov cloudových služieb, ktorí sú s ním spojení, aby využívali služby, ktoré sú mu sprístupnené na základe zmluvy so sprostredkovateľom PII vo verejnom cloude. Je potrebné si uvedomiť, že zákazník cloudovej služby má právomoc nad spracovaním a používaním údajov. Zákazník cloudových služieb, ktorý je zároveň prevádzkovateľom PII, môže podliehať širšiemu súboru povinností upravujúcich ochranu PII ako sprostredkovateľ PII vo verejnom cloude. Zachovanie rozdielu medzi prevádzkovateľom PII a sprostredkovateľom PII spočíva v tom, že sprostredkovateľ PII vo verejnom cloude nemá iné ciele spracúvania údajov ako tie, ktoré stanovil zákazník cloudovej služby v súvislosti s PII, ktoré spracúva, a operácie potrebné na dosiahnutie cieľov zákazníka cloudovej služby.

POZNÁMKA. – Ak sprostredkovateľ PII vo verejnom cloude spracúva údaje o účtoch zákazníkov cloudových služieb, môže na tento účel vystupovať ako prevádzkovateľ PII. Tento dokument sa na takúto činnosť nevzťahuje.

Zámerom tohto dokumentu je v spojení s cieľmi a opatreniami informačnej bezpečnosti uvedenými v norme ISO/IEC 27002 vytvoriť spoločný súbor bezpečnostných kategórií a opatrení, ktoré môže implementovať poskytovateľ služieb verejného cloud computingu, ktorý pôsobí ako sprostredkovateľ PII. Dokument má tieto ciele:

- pomôcť poskytovateľovi verejných cloudových služieb dodržiavať príslušné povinnosti, keď pôsobí ako sprostredkovateľ PII, bez ohľadu na to, či tieto povinnosti spadajú na sprostredkovateľa PII priamo alebo na základe zmluvy;
- umožniť sprostredkovateľovi osobných údajov vo verejnom cloude transparentnosť v príslušných otázkach, aby si zákazníci cloudových služieb mohli vybrať dobre riadené služby spracovania osobných údajov v cloude;
- pomôcť zákazníkovi cloudovej služby a sprostredkovateľovi PII vo verejnom cloude pri uzatváraní zmluvnej dohody;
- poskytnúť zákazníkom cloudových služieb mechanizmus na výkon práv a povinností v oblasti auditu a dodržiavania predpisov v prípadoch, keď individuálne audity zákazníkov cloudových služieb týkajúce sa údajov umiestnených v prostredí virtualizovaných serverov (cloudov) s viacerými stranami môžu byť technicky nepraktické a môžu zvýšiť riziká pre zavedené fyzické a logické opatrenia bezpečnosti siete.

Tento dokument môže pomôcť tým, že poskytne spoločný rámec dodržiavania predpisov pre poskytovateľov verejných cloudových služieb, najmä tých, ktorí pôsobia na nadnárodnom trhu.

### 0.2 Opatrenia ochrany osobných údajov pre verejné cloudové služby

Tento dokument je určený pre organizácie, ktoré ho môžu použiť ako odkaz na výber opatrení ochrany PII v rámci procesu implementácie systému riadenia informačnej bezpečnosti v cloude založeného na norme ISO/IEC 27001, alebo ako usmerňujúci dokument na implementáciu všeobecne uznávaných opatrení ochrany PII pre organizácie, ktoré pôsobia ako sprostredkovatelia PII vo verejnom cloude. Tento dokument vychádza najmä z normy ISO/IEC 27002, pričom zohľadňuje špecifické rizikové prostredie (prostredia) vyplývajúce z týchto požiadaviek na ochranu osobných údajov, ktoré sa môžu vzťahovať na poskytovateľov služieb verejného cloud computingu pôsobiacich ako PII sprostredkovateľov.

Organizácia, ktorá zavádza normu ISO/IEC 27001, zvyčajne chráni svoje vlastné informačné aktíva. V kontexte požiadaviek na ochranu PII pre poskytovateľa verejných cloudových služieb, ktorý pôsobí ako sprostredkovateľ PII, však organizácia chráni informačné aktíva, ktoré jej zverili jej zákazníci. Zavedenie opatrení podľa normy ISO/IEC 27002 sprostredkovateľom PII vo verejnom cloude je na tento účel vhodné a potrebné. Tento dokument rozširuje opatrenia podľa normy ISO/IEC 27002 s cieľom zohľadniť distribuovanú povahu rizika a existenciu zmluvného vzťahu medzi zákazníkom cloudovej služby a sprostredkovateľom PII vo verejnom cloude. Tento dokument rozširuje normu ISO/IEC 27002 dvoma spôsobmi:

- pre niektoré z existujúcich opatrení ISO/IEC 27002 sa poskytuje návod k implementácii usmernení uplatniteľných na ochranu osobných údajov vo verejnom cloude; a
- príloha A obsahuje súbor dodatočných opatrení a súvisiacich návodov určených na riešenie požiadaviek na ochranu PII vo verejnom cloude, ktoré nie sú zahrnuté v existujúcom súbore opatrení ISO/IEC 27002.

Väčšina opatrení a návodov v tomto dokumente sa vzťahuje aj na prevádzkovateľa PII. Na prevádzkovateľa PII sa však vo väčšine prípadov vzťahujú ďalšie povinnosti, ktoré tu nie sú uvedené.

### 0.3 Požiadavky na ochranu osobných údajov

Je dôležité, aby organizácia určila svoje požiadavky na ochranu osobných údajov. Existujú tri hlavné zdroje požiadaviek, ktoré sú uvedené nižšie.

a) Právne, zákonné, regulačné a zmluvné požiadavky: Jedným zo zdrojov sú právne, zákonné, regulačné a zmluvné požiadavky a povinnosti, ktoré musí organizácia, jej obchodní partneri, dodávatelia a poskytovatelia služieb splniť, a ich sociokultúrne zodpovednosti a prevádzkové prostredie. Je potrebné poznamenať, že právne predpisy, nariadenia a zmluvné záväzky prijaté sprostredkovateľom PII môžu nariaďovať výber konkrétnych opatrení a môžu si vyžadovať aj osobitné kritériá na vykonávanie týchto opatrení. Tieto požiadavky sa môžu v jednotlivých jurisdikciách líšiť.

b) Riziká: Ďalší zdroj je odvodený od posúdenia rizík pre organizáciu spojených s PII, pričom sa zohľadňuje celková obchodná stratégia a ciele organizácie. Prostredníctvom hodnotenia rizík sa identifikujú hrozby, hodnotí sa zraniteľnosť, pravdepodobnosť výskytu hrozby a odhaduje sa potenciálny dopad. Norma ISO/IEC 27005 poskytuje návod k riadeniu rizík informačnej bezpečnosti vrátane rád týkajúcich sa hodnotenia rizík, akceptovania rizík, komunikácie o rizikách, monitorovania rizík a preskúmania rizík. Norma ISO/IEC 29134 poskytuje návod na posúdenie vplyvu na súkromie.

c) Podnikové politiky: Hoci mnohé aspekty, na ktoré sa vzťahuje firemná politika, vyplývajú z právnych a sociálno-kultúrnych povinností, organizácia sa môže dobrovoľne rozhodnúť ísť aj nad rámec kritérií, ktoré vyplývajú z požiadaviek bodu a).

### 0.4 Výber a implementácia opatrení v prostredí cloud computingu

Opatrenia je možné vybrať z tohto dokumentu (ktorý obsahuje odkazy na opatrenia z normy ISO/IEC 27002, čím sa vytvorí kombinovaný referenčný súbor opatrení pre sektor alebo aplikáciu definovanú rozsahom). V prípade potreby možno vybrať opatrenia aj z iných súborov opatrení alebo podľa potreby navrhnúť nové opatrenia na splnenie špecifických potrieb.

POZNÁMKA. – Služba spracovania PII poskytovaná verejným sprostredkovateľom PII v cloude sa môže považovať skôr za aplikáciu cloud computingu než za samostatný sektor. Napriek tomu sa v tomto dokumente používa termín „špecifický sektor“, keďže ide o konvenčný termín používaný v rámci iných noriem série ISO/IEC 27000.

Výber opatrení závisí od organizačných rozhodnutí založených na kritériách akceptácie rizika, možnostiach ošetrenia rizika a všeobecnom prístupe k riadeniu rizík uplatňovanom v organizácii a prostredníctvom zmluvných dohôd aj u jej zákazníkov a dodávateľov. Podlieha tiež príslušným vnútroštátnym a medzinárodným právnym predpisom a nariadeniam. Ak nie sú vybrané opatrenia z tohto dokumentu, je potrebné to zdokumentovať s odôvodnením vynechania.

Okrem toho, výber a implementácia opatrení závisí od skutočnej úlohy poskytovateľa verejného cloudu v kontexte celej referenčnej architektúry cloud computingu (pozri ISO/IEC 17789). Na poskytovaní služieb infraštruktúry a aplikácií v prostredí cloud computingu sa môže podieľať mnoho rôznych organizácií. Za určitých okolností môžu byť vybrané opatrenia jedinečné pre konkrétnu kategóriu služieb referenčnej architektúry cloud computingu. V iných prípadoch môžu existovať spoločné úlohy pri implementácii bezpečnostných opatrení. V zmluvných dohodách je potrebné jasne špecifikovať zodpovednosti za ochranu PII všetkých organizácií zapojených do poskytovania alebo využívania cloudových služieb vrátane sprostredkovateľa PII vo verejnom cloude, jeho subdodávateľov a zákazníka cloudových služieb.

Opatrenia uvedené v tomto dokumente možno považovať za hlavné zásady, ktoré sú použiteľné pre väčšinu organizácií. Podrobnejšie sú vysvetlené nižšie spolu s návodom na implementáciu. Implementácia môže byť jednoduchšia, ak sa požiadavky na ochranu PII zohľadnili pri návrhu informačného systému, služieb a prevádzky sprostredkovateľa PII vo verejnom cloude. Takéto zohľadnenie je prvkom koncepcie, ktorá sa často nazýva „Privacy by Design“ (pozri literatúra [9]).

### 0.5 Vypracovanie ďalších návodov

Tento dokument možno považovať za východiskový bod pre vypracovanie návodov na ochranu osobných údajov. Je možné, že nie všetky opatrenia a návody uvedené v tomto kódexe postupov sú použiteľné. Okrem toho môžu byť potrebné ďalšie opatrenia a návody, ktoré nie sú zahrnuté v tomto dokumente. Keď sa vypracúvajú dokumenty obsahujúce ďalšie návody alebo opatrenia, môže byť užitočné zahrnúť krížové odkazy na ustanovenia v tomto dokumente, ak sú použiteľné, aby sa audítorom a obchodným partnerom uľahčilo riadenie súladu.

### 0.6 Úvahy o životnom cykle

PII má prirodzený životný cyklus od vytvorenia a vzniku cez uchovávanie, spracovanie, používanie a prenos až po konečné zničenie alebo zánik. Riziká pre PII sa môžu počas ich životnosti meniť, ale ochrana PII zostáva do určitej miery dôležitá vo všetkých etapách.

Požiadavky na ochranu osobných údajov je potrebné zohľadniť pri riadení existujúcich a nových informačných systémov počas ich životného cyklu.

# 1 Predmet

V tomto dokumente sa stanovujú všeobecne uznávané ciele opatrení, opatrenia a návody na vykonávanie opatrení na ochranu osobných údajov (PII) v súlade so zásadami ochrany súkromia uvedenými v norme ISO/IEC 29100 pre prostredie verejného cloud computingu.

V tomto dokumente sa špecifikujú najmä návody založené na norme ISO/IEC 27002, pričom sa zohľadňujú regulačné požiadavky na ochranu osobných údajov, ktoré možno uplatniť v kontexte prostredia(prostredí) rizík informačnej bezpečnosti poskytovateľa verejných cloudových služieb.

Tento dokument sa vzťahuje na všetky typy a veľkosti organizácií, vrátane verejných a súkromných spoločností, vládnych subjektov a neziskových organizácií, ktoré poskytujú služby spracovania informácií ako sprostredkovatelia PII prostredníctvom cloud computingu na základe zmluvy s inými organizáciami.

Návody v tomto dokumente môžu byť relevantné aj pre organizácie, ktoré pôsobia ako prevádzkovatelia PII. Na prevádzkovateľov PII sa však môžu vzťahovať ďalšie právne predpisy, nariadenia a povinnosti týkajúce sa ochrany PII, ktoré sa nevzťahujú na sprostredkovateľov PII. Cieľom tohto dokumentu nie je pokryť takéto dodatočné povinnosti.

# 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 odkazov sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 17788 *Information technology – Cloud computing – Overview and vocabulary.* [Informačné technológie. Informatický cloud. Prehľad a slovník.]

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

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.]