ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Srpen**
2018

Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací

ČSN
ISO/IEC 29151

36 9711

Information Technology – Security techniques – Code of practice for personally identifiable information protection

Technologies de l,information – Techniques de sécurité – Code de bonne pratique pour la protection des données a caractere personnel

Tato norma je českou verzí mezinárodní normy ISO/IEC 29151:2017. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29151:2017. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27002:2013 zavedena v ČSN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ISO/IEC 29100:2011 zavedena v ČSN ISO/IEC 29100:2015 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

Souvisící ČSN

ČSN EN ISO/IEC 27000:2017 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27005 (36 9797) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27018 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako

zpracovatelé PII

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

firewall, malware

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací

ISO/IEC 29151
První vydání
2017-08

ICS 35.030

Obsah

Strana

Strana

ISO copyright office
CH. de Blandonnet 8 · CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: www.iso.org/iso/foreword.html.

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*, ve spolupráci s ITU-T. Identický text byl vydán jako ITU-T Doporučení X.1058.

Úvod

Počet organizací zpracovávajících osobně identifikovatelné informace (PII) se zvyšuje, stejně jako množství PII, s nimiž se tyto organizace zabývají. Zároveň také narůstá očekávání společnosti ohledně ochrany PII a bezpečnosti dat týkajících se jednotlivců. Řada zemí rozšiřuje své zákony, aby řešila zvýšený počet narušení dat přitahující pozornost.

Vzhledem k narůstajícímu počtu narušení PII budou organizace, které shromažďují nebo zpracovávají PII, stále více potřebovat návod, jak by měly chránit PII, aby se snížilo riziko narušení soukromí a aby se snížil dopad narušení na organizaci a dotčené jednotlivce. Tato specifikace poskytuje takový návod.

Tato specifikace nabízí pokyny pro správce PII v širokém rozsahu bezpečnosti informací a opatření ochrany PII, které se běžně používají v mnoha různých organizacích, které se zabývají ochranou PII. Zbývající části norem ISO/IEC, které jsou zde uvedeny, poskytují pokyny nebo požadavky týkající se dalších aspektů celkového procesu ochrany PII:

– ISO/IEC 27001 specifikuje proces řízení bezpečnosti informací a souvisící požadavky, které mohou být použity jako základ pro ochranu PII.

– ISO/IEC 27002 poskytuje směrnici pro organizační standardy bezpečnosti informací a postupy řízení bezpečnosti informací, včetně výběru, implementace a řízení opatření, přičemž bere v úvahu prostředí rizik bezpečnosti informací organizace.

– ISO/IEC 27009 specifikuje požadavky na použití ISO/IEC 27001 v jakémkoli konkrétním odvětví (oboru, oblasti použití nebo segmentu trhu). Vysvětluje, jak zahrnout požadavky dodatečné k požadavkům ISO/IEC 27001, jak upřesnit jakýkoliv z požadavků ISO/IEC 27001 a jak zahrnout opatření nebo sady opatření nad rámec přílohy A normy ISO/IEC 27001.

– ISO/IEC 27018 poskytuje pokyny organizacím, které působí jako zpracovatelé PII, když nabízejí možnosti zpracování jako cloudové služby.

– ISO/IEC 29134 poskytuje směrnice pro identifikaci, analýzu a posouzení rizik v oblasti soukromí, zatímco ISO/IEC 27001 společně s ISO/IEC 27005 poskytuje metodiku pro identifikaci, analýzu a posouzení rizik
bezpečnosti.

Opatření by měla být vybrána na základě rizik identifikovaných jako výsledek analýzy rizik za účelem vytvoření komplexního a konzistentního systému opatření. Opatření by měla být přizpůsobena kontextu konkrétního zpracování PII.

Tato specifikace obsahuje dvě části: 1) hlavní část sestávající z článků 1 až 18 a 2) normativní přílohu. Tato struktura odráží běžné postupy pro vývoj odvětvově specifických rozšíření normy ISO/IEC 27002.

Struktura hlavní části této specifikace, včetně názvů kapitol, odráží hlavní část ISO/IEC 27002. Úvod a kapitoly 1 až 4 jsou základem pro používání této specifikace. Názvy kapitol 5 až 18 odpovídají názvům kapitol ISO/IEC 27002, což odráží skutečnost, že tato specifikace vychází z pokynů v ISO/IEC 27002 a přidává nová opatření specifická pro ochranu PII. Mnoho opatření v ISO/IEC 27002 nevyžaduje žádné posílení v kontextu správců PII. V některých případech jsou však třeba dodatečné pokyny k implementaci, a ty jsou uvedeny pod příslušným názvem (a číslem

kapitoly) z ISO/IEC 27002.

Normativní příloha obsahuje rozšířenou sadu opatření specifických pro ochranu PII, která doplňují opatření uvedená v ISO/IEC 27002. Tato nová opatření ochrany PII, a s nimi související pokyny, jsou rozdělena do 12 kategorií odpovídajících politice ochrany soukromí a 11 zásadám ochrany soukromí v ISO/IEC 29100:

- souhlas a volba;
- účel, legitimita a specifikace;
- omezení shromáždění;
- minimalizace dat;
- omezení používání, uchovávání a zveřejňování;
- přesnost a kvalita;
- otevřenost, transparentnost a oznámení;
- individuální účast a přístup;
- odpovědnost;
- bezpečnost informací; a
- soulad s požadavky na soukromí.

Obrázek 1 popisuje vztah mezi touto specifikací a souborem norem ISO/IEC.

Obrázek 1 – Vztah této specifikace a souboru norem ISO/IEC

Tato specifikace obsahuje směrnice založené na ISO/IEC 27002 a upravuje je podle potřeby tak, aby byly řešeny požadavky na ochranu soukromí, které vyplývají ze zpracování PII:

a) V různých oblastech zpracování, jako jsou:

- veřejné cloudové služby,
- aplikace sociálních sítí,
- zařízení připojená k internetu v domácnosti,
- vyhledávání, analýza,
- cílení PII pro reklamní a podobné účely,
- programy pro analýzu dat velkého objemu,
- zpracování zaměstnanosti,
- řízení podnikání v oblasti prodeje a poskytování služeb (plánování podnikových zdrojů, řízení vztahů se zákazníky);

b) V různých místech, jako jsou:

- osobní platforma zpracování poskytovaná jednotlivci (například chytré karty, chytré telefony a jejich aplikace, inteligentní měřiče, nositelná zařízení),
- sítě pro přenos a shromažďování dat (například když jsou údaje o poloze mobilního telefonu provozně vytvářeny síťovým zpracováním, což může být v některých jurisdikcích považováno za PII),
- v rámci vlastní infrastruktury zpracování organizace,
- na zpracovatelské platformě třetí strany;

c) Pro charakteristiky shromažďování, jako je:

- jednorázové shromáždění dat (například při registraci ke službě),
- průběžné shromažďování dat (například časté sledování parametrů zdravotního stavu pomocí snímačů na těle jednotlivce nebo v jeho těle, vícenásobné shromažďování dat pomocí bezkontaktních platebních karet za účelem platby, systémy shromažďování dat z inteligentních měřičů atd.).

POZNÁMKA Průběžné shromažďování dat může obsahovat nebo přinášet behaviorální, lokalizační a další typy PII. V takových případech je třeba zvážit použití opatření na ochranu PII, které umožňují řídit přístup a shromažďování na základě souhlasu a které umožňují subjektu PII vykonávat

odpovídající kontrolu nad tímto přístupem a shromažďováním.

1 Předmět normy

Toto doporučení | mezinárodní norma stanovuje cíle opatření, opatření a směrnice pro implementaci opatření, aby splňovaly požadavky stanovené během posouzení rizik a dopadu souvisících s ochranou osobně identifikovatelných informací (PII).

Toto doporučení | mezinárodní norma specifikuje směrnice založené na ISO/IEC 27002, přičemž bere v úvahu požadavky na zpracování PII, které mohou být použitelné v kontextu prostředí rizik bezpečnosti informací organizace.

Toto doporučení | mezinárodní norma platí pro všechny typy a velikosti organizací působících jako správci PII (podle definice v ISO/IEC 29100), včetně veřejných a soukromých společností, vládních subjektů a neziskových organizací, které zpracovávají PII.