ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2015**

Informační technologie – Bezpečnostní techniky –
Rámec soukromí

ČSN
ISO/IEC 29100
36 9705

Information technology – Security techniques – Privacy framework

Technologies de l,information – Techniques de sécurité – Cadre privé

Tato norma je českou verzí mezinárodní normy ISO/IEC 29100:2011. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29100:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN a TNI

TNI 01 0350 (01 0350) Management rizik – Slovník (Pokyn 73)

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

Vysvětlivky k textu převzaté normy

Pro účely této normy byl anglický termín „principal“ přeložen jako „subjekt“ a anglický termín „controller“ přeložen jako „dohlížitel“.

Anglický termín „symbol“ se překládá českým slovem „symbol“, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 29100
Rámec soukromí První vydání
2011-12-15

Obsah

Strana

Tabulka A.1 – Přiřazení pojmů ISO/IEC 29100 k pojmům ISO/IEC 27000 24

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vypracování mezinárodních norem prostřednictvím 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 JTC1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 29100 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie,* subkomise SC 27
IT Bezpečnostní techniky.

Úvod

Tato mezinárodní norma poskytuje celkový rámec pro ochranu osobně identifikovatelných informací (PII) v systé-
mech informačních a komunikačních technologií (ICT). Má obecnou povahu a zařazuje organizační, technické a procedurální aspekty do souhrnného rámce soukromí.

Rámec soukromí má za cíl pomoci organizacím definovat jejich požadavky na zabezpečení soukromí

souvisící s PII v rámci ICT prostředí:

- specifikováním obecné terminologie soukromí;
- definováním aktérů a jejich rolí ve zpracování PII;
- popisem požadavků na zabezpečení soukromí; a
- odkazováním na známé principy soukromí.

V některých jurisdikcích by mohly být odkazy této mezinárodní normy na požadavky zabezpečení soukromí chápány jako doplňky k zákonným požadavkům na ochranu PII. Vlivem rostoucího počtu informací a komunikačních technologií, které zpracovávají PII, je důležité mít mezinárodní normy bezpečnosti informací, které poskytují obecné pochopení ochrany PII. Cílem této mezinárodní normy je rozšířit existující bezpečnostní normy přidáním zaměření týkajícího se zpracování PII.

Zvyšující se komerční použití a hodnota PII, sdílení PII napříč právními jurisdikcemi, a rostoucí složitost ICT systémů může učinit pro organizaci obtížné zajistit soukromí a dosáhnout souladu s různými platnými zákony. Strany zúčastněné vzhledem k soukromí mohou zabránit vzniku nejistoty a nedůvěry řádným nakládáním se záležitostmi soukromí a vyhnutím se případům zneužití PII.

Použití této mezinárodní normy:

- je pomocí při návrhu, implementaci, provozu a údržbě ICT systémů, které pracují s PII a chrání PII;
- urychlují inovativní řešení, umožňující ochranu PII v rámci ICT systémů; a
- zlepšují programy organizace na ochranu soukromí využitím doporučených postupů.

Rámec soukromí poskytnutý v této mezinárodní normě může sloužit jako základ pro další podněty k normalizaci soukromí, například pro:

- technické referenční architektury;
- implementaci a použití specifických technologií týkajících se soukromí a celkového řízení soukromí;
- kontroly soukromí u procesů outsourcovaných dat;
- posouzení rizik soukromí; nebo
- konkrétní inženýrské specifikace.

Některé jurisdikce mohou požadovat soulad s jedním nebo více dokumenty, na které je odkaz v ISO/IEC JTC 1/SC 27 WG 5 Stálý dokument 2 (WG 5 SD2) – *Oficiální odkazy na dokumenty týkající*

se soukromí [3] nebo s dalšími použitelnými zákony a předpisy, ale cílem této mezinárodní normy není být globální modelovou politikou, ani legislativním rámcem.

1 Předmět normy

Tato mezinárodní norma poskytuje rámec soukromí, který

- specifikuje obecnou terminologii v oblasti soukromí;
- definuje aktéry a jejich role ve zpracování osobně identifikovatelných informací (PII);
- popisuje úvahy o bezpečnostních opatřeních na zabezpečení soukromí; a
- poskytuje odkazy na známé principy soukromí pro informační technologie.

Tato mezinárodní norma je použitelná pro fyzické osoby a organizace zapojené do specifikování, pořizování, architektonického řešení, návrhu, vývoje, testování, udržování, administrování, provozování systémů informačních a komunikačních technologií nebo služeb, kde jsou pro zpracování PII požadována opatření ohledně soukromí.