ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Říjen**
2018

Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí

ČSN
ISO/IEC 29134

36 9712

Information Technology – Security techniques – Guidelines for privacy impact assessment

Technologies de l,information – Techniques de sécurité – Lignes directrices pour l,évaluation d,impacts sur la vie privée

Tato norma je českou verzí mezinárodní normy ISO/IEC 29134:2017. 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 29134:2017. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO Pokyn 73:2009 zaveden v TNI 01 0350:2010 (01 0350) Management rizik – Slovník (Pokyn 73)

ISO/IEC 27000:2016 zavedena v ČSN EN ISO/IEC 27000:2017 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

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

Souvisící ČSN

ČSN EN ISO 9000:2016 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN ISO/IEC 16509:2000 (97 9705) Informační technologie – Terminologie roku 2000

ČSN ISO 21500 (01 0345) Návod k managementu projektu

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů

pro opatření bezpečnosti informací

ČSN ISO/IEC 29151 (36 9711) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací

ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti
informací

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

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyny“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména normy řady ISO/IEC 27XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti s řadou norem ISO/IEC 27XXX nepoužívá.

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:

cloud, malware, phishing

Pro účely této normy byl použit překlad anglického termínu „control“ jako „opatření“, „řízení“ nebo „kontrola“ s ohle-
dem na význam v textu normy.

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 – pro posuzování dopadu na soukromí

ISO/IEC 29134 Směrnice

První vydání

2017-06

ICS 35.030

Obsah

Strana

Předmluva..... 5

Úvod..... 6

1..... Předmět normy..... 7

2..... Citované dokumenty..... 7

3..... Termíny a definice..... 7

4..... Zkrácené termíny..... 9

5..... Příprava důvodů pro PIA..... 9

5.1..... Výhody provedení PIA..... 9

5.2..... Cíle podávání zpráv o PIA..... 10

5.3..... Odpovědnost za provedení PIA..... 11

5.4..... Rozsah PIA.....

..... 11

6..... Pokyny k procesu provádění
PIA..... 11

6.1.....
Obecně.....
..... 11

6.2..... Stanovení, zda je PIA nutné (prahová
analýza)..... 12

6.3..... Příprava
PIA.....
..... 12

6.3.1... Vytvoření PIA týmu a poskytnutí
směřování..... 12

6.3.2... Příprava plánu PIA a určení potřebných zdrojů pro provádění
PIA..... 14

6.3.3... Popis toho, co je
hodnoceno.....
..... 14

6.3.4... Zapojení zainteresovaných
stran..... 15

6.4..... Provedení
PIA.....
..... 17

6.4.1... Identifikace toků PII
informací.....
... 17

6.4.2... Analyzovat důsledky případu
použití..... 18

6.4.3... Určení příslušných požadavků na ochranu
soukromí..... 18

6.4.4... Posouzení rizika
soukromí.....
..... 19

6.4.5... Příprava na ošetření rizik
soukromí..... 21

6.5..... Pokračování
PIA.....
..... 25

6.5.1... Příprava zprávy..... 25

6.5.2... Zveřejnění zprávy..... 26

6.5.3... Implementace plánů ošetření rizika soukromí..... 26

6.5.4... Přezkoumání a/nebo audit PIA..... 26

6.5.5... Reflektování změn procesu..... 27

7..... Zpráva PIA..... 27

7.1..... Obecně..... 27

7.2..... Struktura zprávy..... 28

7.3..... Rozsah PIA..... 28

7.3.1... Hodnocený proces..... 28

7.3.2... Kritéria rizika..... 29

7.3.3... Zapojené zdroje a osoby..... 29

7.3.4... Konzultace se zainteresovanými stranami..... 30

7.4..... Požadavky soukromí..... 30

7.5..... Posuzování rizik..... 30

7.5.1... Zdroje rizik..... 30

7.5.2... Hrozby a jejich pravděpodobnost..... 30

7.5.3... Následky a jejich úroveň dopadu..... 30

7.5.4... Hodnocení rizik..... 30

7.5.5... Analýza souladu..... 30

7.6..... Plán ošetření

rizik..... 30

7.7..... Závěr
a rozhodnutí..... 30

7.8..... Shrnutí PIA pro
veřejnost..... 31

Příloha A (informativní) Měřítko kritérií úrovně dopadu
a pravděpodobnosti..... 32

Příloha B (informativní) Obecné
hrozby..... 34

Příloha C (informativní) Pokyny pro pochopení použitých
výrazů..... 38

Příloha D (informativní) Ilustrované příklady podporující proces
PIA..... 40

Bibliografie..... 42

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 nelze činit odpovědným 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.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Posuzování dopadů na soukromí (PIA) je nástroj pro posouzení možných dopadů na soukromí procesu, informačního systému, programu, softwarového modulu, zařízení nebo jiné iniciativy, která zpracovává osobně identifikovatelné informace (PII), a, po konzultaci se zainteresovanými stranami, pro přijetí opatření, která jsou nezbytná k ošetření rizik soukromí. Zpráva PIA může obsahovat dokumentaci o opatřeních přijatých k ošetření rizik, například opatřeních vyplývajících z používání systému řízení bezpečnosti informací (ISMS) dle normy ISO/IEC 27001.
PIA je více než nástroj: jedná se o proces, který začíná v nejranějších fázích iniciativy, kdy stále existují příležitosti ovlivňovat její výsledek, a tím zajistit soukromí již ve fázi návrhu. Je to proces, který pokračuje až do zavádění projektu a dokonce i po jeho nasazení.

Iniciativy se podstatně liší v rozsahu a dopadu. Cíle spadající pod nadpis „soukromí“ budou záviset na kultuře, společenských očekáváních a jurisdikci. Cílem tohoto dokumentu je poskytnout škálovatelné pokyny, které lze uplatnit u všech iniciativ. Protože pokyny specifické pro všechny okolnosti nemohou být normativní, pokyny uvedené v tomto dokumentu by měly být interpretovány s ohledem na jednotlivé okolnosti.

Správce PII může mít odpovědnost za provedení PIA a může požádat zpracovatele PII o asistenci při provádění PIA, aby tak jednal jménem správce PII. Zpracovatel nebo dodavatel PII mohou také chtít provést vlastní PIA.

Informace dodavatele týkající se PIA jsou zvláště důležité, pokud jsou digitálně připojená zařízení součástí posuzovaného informačního systému, aplikace nebo procesu. Může být nezbytné, aby dodavatelé takových zařízení poskytovali informace o návrhu týkající se soukromí těm, kdo provádějí PIA. Pokud není poskytovatel digitálních zařízení kvalifikovaný v oblasti PIA a není v této oblasti provozně zajištěný, například:

- drobný prodejce, nebo
- malý a střední podnik (SME) používající digitálně připojená zařízení v průběhu běžných podnikatelských činností,

pak, aby bylo možné provádět minimální aktivitu PIA, může být dodavatel zařízení vyzván, aby poskytl velmi mnoho informací o soukromí a podnikl svoji vlastní PIA s ohledem na očekávaný kontext subjektu PII/SME pro zařízení, které dodává.

PIA je obvykle prováděna organizací, která bere svou odpovědnost vážně a přiměřeně zachází s principy PII. V některých jurisdikcích může být PIA nezbytné ke splnění právních a regulatorních požadavků.

Tento dokument je určen pro použití v případech, kdy dopad na soukromí týkající se subjektů PII zahrnuje zvážení procesů, informačních systémů nebo programů, kde:

- odpovědnost za implementaci a/nebo dodání procesu, informačního systému nebo programu je sdílena
  s jinými organizacemi a mělo by být zajištěno, že každá organizace bude řádně řešit zjištěná rizika;
- organizace provádí řízení rizik soukromí jako součást svého celkového úsilí v oblasti řízení rizik při přípravě na implementaci nebo vylepšení svého ISMS (zavedeného v souladu

s ISO/IEC 27001 nebo rovnocenným systémem řízení); nebo organizace provádí řízení rizik soukromí jako samostatnou funkci;

- organizace (například vláda) podniká iniciativu (například program partnerství veřejného a soukromého sektoru), v němž ještě není známa budoucí organizace správce PII, takže plán ošetření by se nemohl implementovat přímo, a proto by se měl tento plán ošetření stát součástí příslušné legislativy, nařízení nebo smlouvy;

- organizace chce jednat odpovědně vůči subjektům PII.

Opatření, která jsou považována za nezbytná k ošetření rizik zjištěných během procesu analýzy dopadů na soukromí, mohou být odvozena z vícenásobných sad opatření, včetně ISO/IEC 27002 (pro opatření bezpečnosti) a ISO/IEC 29151 (pro opatření ochrany PII) nebo srovnatelných národních norem, nebo mohou být definována osobou odpovědnou za provádění PIA, nezávisle na jakékoli jiné sadě opatření.

1 Předmět normy

Tento dokument poskytuje směrnice pro

- proces posuzování dopadů na soukromí, a
- strukturu a obsah zprávy PIA.

Platí pro všechny typy a velikosti organizací, včetně veřejných společností, soukromých společností, orgánů státní správy a neziskových organizací.

Tento dokument je relevantní pro ty, kdo se podílejí na navrhování nebo realizaci projektů, včetně stran, které provozují systémy zpracování dat a služby, které zpracovávají PII.