ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Březen 2017**

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

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

Tato norma je českou verzí mezinárodní normy ISO/IEC 27018:2014. 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 27018:2014. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 17788 | Rec. ITU-T Y.3500 zavedena v ČSN ISO/IEC 17788:2017 (36 9865) Informační technologie –
Cloud computing – Přehled a slovník

ISO/IEC 27000:2014 zavedena v ČSN ISO/IEC 27000:2014 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

ISO/IEC 27001:2013 zavedena v ČSN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

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 ISO/IEC 17789 (36 9866) Informační technologie – Cloud computing – Referenční architektura

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

ČSN ISO/IEC 27035 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací

ČSN ISO/IEC 29101 (36 9708) Informační technologie – Bezpečnostní techniky – Rámec architektury soukromí

Vysvětlivky k textu převzaté normy

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

cloud, cloud computing, malware, hardcopy

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 – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

ISO/IEC 27018
První vydání
2014-08-01

ICS 35.030

Obsah

Strana

Předmluva..... 5

0.....
Úvod..... 6

1..... Předmět
normy..... 9

2..... Citované
dokumenty..... 9

3..... Termíny
a definice..... 9

4.....
Přehled..... 10

4.1..... Struktura této
normy..... 10

4.2..... Kategorie
opatření..... 11

5..... Politiky bezpečnosti
informací..... 11

5.1..... Pokyny managementu organizace k bezpečnosti
informací..... 11

6..... Organizace bezpečnosti

informací..... 12

6.1..... Interní organizace..... 12

6.2..... Mobilní zařízení a práce na dálku..... 13

7..... Bezpečnost lidských zdrojů..... 13

7.1..... Před vznikem pracovního poměru..... 13

7.2..... Během pracovního poměru..... 13

7.3..... Ukončení a změna pracovního poměru..... 13

8..... Řízení aktiv..... 13

9..... Řízení přístupu..... 13

9.1..... Požadavky organizace na řízení přístupu..... 13

9.2..... Správa a řízení přístupu uživatelů..... 13

9.3..... Odpovědnosti uživatelů..... 14

9.4..... Řízení přístupu k systémům a aplikacím..... 14

10..... Kryptografie..... 15

10.1.... Kryptografická opatření..... 15

11..... Fyzická bezpečnost a bezpečnost

prostředí..... 15

11.1.... Zabezpečené
oblasti..... 15

11.2....
Zařízení..... 15

12..... Bezpečnost
provozu..... 16

12.1.... Provozní postupy
a odpovědnosti..... 16

12.2.... Ochrana před
malwarem..... 17

12.3....
Zálohování..... 17

12.4.... Zaznamenávání formou logů a monitorování..... 17

12.5.... Řízení a kontrola provozního softwaru..... 18

12.6.... Správa a řízení technických zranitelností..... 18

12.7.... Hlediska auditu informačních systémů..... 18

13..... Bezpečnost komunikací..... 18

13.1.... Správa bezpečnosti sítě..... 18

13.2.... Přenos informací..... 18

14..... Akvizice, vývoj a údržba systému..... 19

15..... Vztahy s dodavateli..... 19

16..... Řízení incidentů bezpečnosti informací..... 19

16.1.... Řízení incidentů bezpečnosti informací a zlepšování..... 19

17..... Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací..... 20

18..... Soulad s požadavky..... 20

18.1.... Soulad se zákonnými a smluvními požadavky..... 20

18.2.... Přezkoumání bezpečnosti informací..... 20

Příloha A (normativní) Soubor rozšířených opatření na ochranu PII zpracovatele PII ve veřejném

cloudu..... 21

Bibliografie..... 28

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 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 oblastech společných zájmů. Práce se zúčastňují také další vládní a 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 významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information.

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpeč-
nostní techniky*.

Úvod

0.1 Základ a kontext

Poskytovatelé cloudových služeb, kteří zpracovávají osobně identifikovatelné informace (PII) na základě smlouvy se svými zákazníky musí zpracovávat své služby způsobem umožňujícím oběma stranám splnit požadavky použitelné legislativy a předpisů pokrývajících ochranu PII. Požadavky a způsob, jakým jsou požadavky rozděleny mezi poskytovatele cloudových služeb a jeho zákazníky, se mění v závislosti na právní jurisdikci, a podle podmínek smluvního vztahu mezi poskytovatelem cloudových služeb a zákazníkem. Legislativa, která určuje, jak mohou být PII zpracovávány (tj. shromažďovány, používány, přenášeny a likvidovány) je někdy zmiňována jako legislativa na ochranu dat; PII se někdy nazývají osobní data nebo osobní informace. Povinnosti zpracovatele PII týkající se zpracovatele PII se liší v jednotlivých jurisdikcích, což je výzvou pro organizace poskytující služby cloud computingu, aby fungovaly nadnárodně.

Poskytovatel veřejných cloudových služeb je „zpracovatel PII“, když zpracovává PII pro a v souladu s pokyny zákazníka cloudových služeb. Zákazníkem cloudových služeb, který má smluvní vztah se zpracovatelem PII ve veřejném cloudu, může být fyzická osoba, „subjekt PII“, zpracovávající jeho vlastní PII v cloudu, nebo organizace, „dohlížitel PII“, zpracovávající PII týkající se mnoha subjektů PII. Zákazník cloudových služeb by mohl autorizovat jednoho nebo více uživatelů cloudových služeb s nimi spojených, aby používal služby, které jsou pro ně dostupné na základě smlouvy se zpracovatelem PII veřejných služeb. Zákazník cloudových služeb je oprávněn zpracovávat a používat data. Zákazníka cloudových služeb, který je také dohlížitel PII, by se mohl týkat širší soubor povinností určujících ochranu PII, než zpracovatele PII ve veřejném cloudu. Udržování odlišností mezi dohlížitelem PII a zpracovatelem PII spoléhá na zpracovatele PII ve veřejném cloudu, který nemá jiné cíle zpracování dat, než cíle nastavené zákazníkem cloudových služeb vzhledem k PII, která zpracovává, a operacím nutným pro dosažení cílů zákazníka cloudových služeb.

POZNÁMKA Jestliže zpracovatel PII ve veřejném cloudu zpracovává účetní data zákazníka cloudových služeb, mohl by pro tento účel vystupovat jako dohlížitel PII. Tato mezinárodní norma tuto činnost nepokrývá.

Záměrem této mezinárodní normy, je-li používána společně s cíli bezpečnosti informací a opatřeními uvedenými v ISO/IEC 27002, je vytvářet obecnou sadu bezpečnostních kategorií a opatření, které mohou být implementovány poskytovatelem veřejných služeb cloud computingu vystupujícího v roli zpracovatele PII. Tato norma má následující cíle.

- Pomoci poskytovateli služeb veřejného cloudu vyhovět aplikovatelným povinnostem, když vystupuje jako zpracovatel PII, ať už takové povinnosti připadnou zpracovateli PII přímo nebo smluvně.

- Umožnit zpracovateli PII ve veřejném cloudu být transparentním v příslušných záležitostech, aby zákazníci cloudových služeb mohli vybrat dobře spravované služby zpracování PII založených na cloudu.

- Pomoci zákazníkovi cloudových služeb a zpracovateli PII ve veřejném cloudu při uzavírání smluvních ujednání.

- Poskytnout zákazníkům cloudových služeb mechanismus pro provádění auditu a vyhovění právům a povinnostem v případech, kdy audity jednotlivého zákazníka cloudových služeb dat hostovaných v (cloud) prostředí virtualizovaného serveru pro více stran by mohly být technicky

neproveditelné a mohly by zvyšovat rizika pro zavedená fyzická a logická opatření síťové bezpečnosti.

Tato mezinárodní norma nenahrazuje aplikovatelnou legislativu a předpisy, ale může pomoci poskytovatelům veřejných cloudových služeb, zejména těch, které jsou provozovány na nadnárodním trhu, poskytnutím rámce obecné shody.

0.2 Opatření na ochranu PII pro veřejné služby cloud computingu

Tato mezinárodní norma je navržena, aby ji organizace mohly používat jako odkaz na výběr opatření na ochranu PII v procesu implementování systému řízení bezpečnosti informací cloud computingu na základě ISO/IEC 27001, nebo jako pokyny k implementaci obecně akceptovaných opatření na ochranu PII pro organizace vystupující jako zpracovatelé PII ve veřejném cloudu. Tato mezinárodní norma je především založena na ISO/IEC 27002, přičemž zohledňuje specifická riziková prostředí, vyplývající z těch požadavků na ochranu PII, které se mohou aplikovat na poskytovatele veřejných služeb cloud computingu vystupující jako zpracovatelé PII.

Obvykle organizace implementující ISO/IEC 27001 chrání svoje vlastní informační aktiva. V kontextu požadavků na ochranu PII na poskytovatele veřejných cloudových služeb vystupujících jako zpracovatel PII však organizace chrání informační aktiva, která mu zákaznici svěřili. Implementace opatření z ISO/IEC 27002 zpracovatelem PII ve veřejném cloudu je k tomuto účelu vhodná a je nezbytná. Tato mezinárodní norma rozšiřuje opatření uvedená v ISO/IEC 27002, aby odpovídala distribuované povaze rizika a existenci smluvního vztahu mezi zákazníkem

cloudových služeb a zpracovatelem PII ve veřejném cloudu. Tato mezinárodní norma rozšiřuje ISO/IEC 27002 dvěma způsoby:

– pokyny k implementaci použitelné na ochranu PII ve veřejném cloudu jsou poskytnuty pro některá opatření uvedená v ISO/IEC 27002, a

– příloha A poskytuje sadu dalších opatření a připojené pokyny, které mají řešit požadavky na ochranu PII ve veřejném cloudu, kterými se nezabývá soubor opatření ISO/IEC 27002.

Většina z opatření a pokynů uvedených v této mezinárodní normě se aplikují také na dohlížitele PII. Dohlížitel PII však bude ve většině případů předmětem dalších závazků, které zde nejsou specifikovány.

0.3 Požadavky na ochranu PII

Je nezbytné, aby organizace stanovila své požadavky na ochranu PII. Existují tři hlavní zdroje požadavků, které jsou uvedené dále.

a) Právní, statutární, regulatorní a smluvní požadavky: Jedním zdrojem jsou právní, statutární, regulatorní a smluvní požadavky a závazky, které organizace, její obchodní partneři, dodavatelé (kontrahenti) a poskytovatelé služeb musí plnit, a jejich sociokulturní odpovědnosti a provozní prostředí. Právní, regulační a smluvní závazky zpracovatele PII mohou určovat výběr konkrétních opatření a mohou také vyžadovat specifická kritéria pro implementování takových opatření. Tyto požadavky mohou být v různých jurisdikcích odlišné.

b) Rizika: Další zdroj je odvozen z posouzení rizik hrozících organizaci spojené s PII, s přihlédnutím k celkové podnikatelské strategii a cílům organizace. Posouzení rizik identifikuje hrozby, ohodnotí zranitelnosti a pravděpodobnost výskytu a je odhadnut možný dopad. ISO/IEC 27005 poskytuje pokyny na řízení rizik bezpečnosti informací, zahrnující doporučení ohledně posouzení rizik, akceptace rizik, komunikace rizik, monitorování rizik a přezkoumání rizik. ISO/IEC 29134 poskytuje pokyny pro posouzení dopadu na soukromí.

c) Korporátní politiky: I když mnoho aspektů pokrytých korporátní politikou je odvozeno z právních a sociokulturních závazků, organizace si mohou také dobrovolně zvolit, že přijmou vyšší kritéria než ta, která jsou odvozena z požadavků, uvedených pod bodem a).

0.4 Výběr a implementace opatření v prostředí cloud computingu

Opatření mohou být vybrána z této mezinárodní normy (která zahrnuje odkaz na opatření z ISO/IEC 27002, a vytváří tak spojený odkaz na soubor opatření pro úsek aplikací definovaný rozsahem). Opatření mohou být také na základě požadavku vybrána z jiných souborů opatření, nebo mohou být navržena nová opatření, splňující specifické potřeby, je-li to vhodné.

POZNÁMKA Služba zpracovávající PII poskytnutá zpracovatelem PII ve veřejném cloudu by měla být vzata v úvahu jako aplikace cloud computingu, spíše než jako samostatný obor. Nicméně je v této mezinárodní normě použit termín „specifický podle oborů“, protože je to obvyklý termín používaný v jiných normách řady ISO/IEC 27000.

Výběr opatření závisí na organizačních rozhodnutích vycházejících z kritérií pro akceptaci rizik, možnostech ošetření rizik, a obecném přístupu k řízení rizik, použitém organizací a, prostřednictvím smluvních ujednání, jejími zákazníky a dodavateli, a bude také podléhat celé příslušné národní a mezinárodní legislativě a předpisům. Když nejsou vybrána opatření z této mezinárodní normy, je

třeba to zdokumentovat se zdůvodněním jejich vynechání.

Výběr a implementace opatření dále závisí na aktuální roli poskytovatele veřejného cloudu v kontextu celé referenční architektury cloud computingu (viz ISO/IEC 17789). Do poskytování infrastruktury a aplikačních služeb v prostředí cloud computingu může být zapojeno mnoho různých organizací. Za určitých okolností mohou být vybraná opatření jedinečná pro konkrétní kategorii služeb referenční architektury cloud computingu. V jiných případech se mohou při implementování bezpečnostních opatření vyskytnout sdílené role. Je nutné, aby smluvní ujednání jasně specifikovala odpovědnosti týkající se ochrany PII všech organizací zapojených do poskytování nebo používání cloudových služeb, zahrnujících zpracovatele PII ve veřejném cloudu, jeho subdodavatele a zákazníka cloudových služeb.

Opatření v této mezinárodní normě mohou být pokládána za základní principy a mohou být aplikovatelná pro většinu organizací. Podrobněji jsou vysvětlena dále společně s pokyny k implementaci. Implementace může být jednodušší, budou-li požadavky na ochranu PII vzaty v úvahu v návrhu informačního systému, služeb a operací zpracovatele PII ve veřejném cloudu. Takové zvážení je prvkem konceptu často nazývané „Soukromí na základě návrhu“. Bibliografie vyjmenovává příslušné dokumenty, například ISO/IEC 29101.

0.5 Vytváření dalších směrnic

Na tuto mezinárodní normu je možné pohlížet jako na výchozí bod pro vytváření směrnic na ochranu PII. Je možné, že ne všechna opatření a pokyny v tomto souboru postupů budou použitelné. Mohou být také požadována další opatření a směrnice, které nejsou obsaženy v této mezinárodní normě. Při vývoji dokumentů obsahujících další směrnice nebo opatření může být užitečné zařadit, kde je to vhodné, křížové odkazy do kapitol této mezinárodní normy, aby se usnadnila kontrola shody prováděná auditory a obchodními partnery.

0.6 Faktory životního cyklu

PII má přirozený životní cyklus, od vytváření a počátku přes ukládání, zpracování, používání a přenášení k případnému zničení nebo pokažení. Rizika pro PII se mohou v průběhu jejich životního cyklu měnit, ale ochrana PII zůstává v určitém rozsahu ve všech etapách významná.

Požadavky na ochranu PII je nutné zohlednit při řízení existujících a nových informačních systémů po celou dobu jejich životního cyklu.

1 Předmět normy

Tato mezinárodní norma stanoví obecně akceptované kontrolní cíle, opatření a směrnice pro zavedení opatření na ochranu osobně identifikovatelných informací (PII) v souladu s principy soukromí uvedené v ISO/IEC 29100 pro prostředí veřejného cloud computingu.

Tato mezinárodní norma zejména specifikuje směrnice založené na ISO/IEC 27002, přičemž bere v úvahu regulatorní požadavky na ochranu PII, které mohou být použitelné v rámci kontextu prostředí rizik bezpečnosti informací poskytovatele služeb veřejného cloudu.

Tato mezinárodní norma je použitelná pro všechny typy a velikosti organizací, zahrnující veřejné a soukromé společnosti, vládní úřady a neziskové organizace, které poskytují služby pro zpracování informací jako zpracovatelé PII prostřednictvím cloud computingu na základě smlouvy s jinými organizacemi.

Směrnice v této mezinárodní normě mohou mít také význam pro organizace vystupující jako dohlížitelé PII; avšak dohlížitelé PII mohou být předmětem další legislativy, předpisů a závazků na ochranu PII, které nejsou aplikované na zpracovatele PII. Cílem této mezinárodní normy není pokrytí takových dodatečných závazků.