ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Duben**
2021

Terminologie a klasifikace technik odstranění identifikace dat zvyšujících soukromí

ČSN
ISO/IEC 20889

36 9039

Privacy enhancing data de-identification terminology and classification of techniques

Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée

Tato norma je českou verzí mezinárodní normy ISO/IEC 20889:2018. 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 20889:2018. 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 27000 zavedena v ČSN EN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

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

Souvisící ČSN

ČSN ISO/IEC 9797-2 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 2: Mechanismy používající dedikovanou hašovací funkci

ČSN ISO/IEC 10118-4 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 4: Hašovací funkce používající modulární aritmetiku

ČSN EN ISO 25237 (98 2020) Zdravotnická informatika – Pseudonymizace

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

ČSN EN ISO/IEC 27038 (36 9847) Informační technologie – Bezpečnostní techniky – Specifikace pro

digitální zpracování dokumentů

ČSN EN ISO/IEC 29100 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

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

ČSN EN ISO/IEC 29134 (36 9712) Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí

ČSN ISO 31000 (01 0351) Management rizik – Směrnice

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Upozornění na národní poznámky

Do normy byly doplněny národní poznámky upozorňující na nesprávné odkazy na Bibliografii.

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

Terminologie a klasifikace technik odstranění identifikace dat zvyšujících soukromí

ISO/IEC 20889
První vydání
2018-11

ICS 35.030

Obsah

Strana

Strana

Strana

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 jednotliví 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.

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. 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) nebo v seznamu patentových prohlášení obdržených IEC (viz http://patents.iec.ch).

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 www.iso.org/iso/foreword.html.

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

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směrovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

Úvod

Je prokázáno, že hlavní výhody lze odvodit ze zpracování elektronicky uložených dat, včetně takzvaných „dat velkého objemu“. Pokud však tato data zahrnují osobně identifikovatelné informace (PII), jak tomu často je, zpracování těchto dat musí být v souladu s platnými principy ochrany osobních údajů. Vhodné použití technik odstranění identifikace je důležitou součástí opatření umožňujících využití výhod zpracování dat při zachování souladu s příslušnými principy soukromí podle ISO/IEC 29100.

Okamžitý význam má tento dokument pro ochranu osobních údajů fyzických osob (tj. subjektů PII), ale pojem „subjekt dat“, definovaný a používaný v tomto dokumentu, je širší než „subjekt PII“ a zahrnuje například organizace a počítače.

Tento dokument se zaměřuje na běžně používané techniky pro odstranění identifikace strukturovaných souborů dat a také na soubory dat obsahující informace o subjektech dat, které lze logicky reprezentovat ve formě tabulky. Tyto techniky jsou použitelné zejména na soubory dat, které lze konvertovat do formy tabulky (např. data uchovávaná v databázích typu klíč-hodnota). Je možné, že techniky popsané v tomto dokumentu neplatí pro složitější soubory dat, např. soubory obsahující volný text, obrázky, zvuk nebo video.

Použití technik odstranění identifikace představuje osvědčený postup ke zmírnění rizika opětovné identifikace, ale ne vždy však zaručuje požadovaný výsledek. Tento dokument zavádí pojem formálního modelu měření soukromí jako přístupu k aplikaci technik odstranění identifikace dat.

POZNÁMKA 1 Příloha C objasňuje, jak jsou vybrané techniky odstranění identifikace popsané v tomto dokumentu využitelné pro odstranění identifikace ve volném textu.

POZNÁMKA 2 Uplatnění technik odstranění identifikace může představovat možnost ošetření rizik soukromí vyplývající z posouzení dopadu na soukromí, jak je popsáno v ISO/IEC 29134[32].

Výběr technik odstranění identifikace musí efektivně řešit rizika opětovné identifikace v daném provozním kontextu. Je proto potřeba klasifikovat známé techniky odstranění identifikace pomocí standardizované terminologie a popsat jejich vlastnosti, včetně základních technologií a použitelnosti každé techniky ke snížení rizika opětovné identifikace. To je hlavním cílem tohoto dokumentu. Vztah mezi terminologií použitou v tomto dokumentu a souvisící terminologií používanou jinde (např. pojem anonymizace) je popsán v příloze B. Avšak specifikace podrobných postupů pro výběr a konfiguraci technik odstranění identifikace, včetně posouzení užitečnosti dat a celkového rizika útoku založeného na opětovné identifikaci, je mimo rozsah tohoto dokumentu.

POZNÁMKA 3 Autentizace, poskytování průkazných informací a prokazování identity jsou také mimo rozsah tohoto dokumentu.

Techniky odstranění identifikace jsou obvykle doprovázeny technickými a jinými organizačními opatřeními ke zvýšení jejich efektivnosti. Tam, kde je to vhodné, je také popsáno použití těchto opatření.

Tento dokument poskytuje přehled základních konceptů souvisících s odstraněním identifikace dat a zavádí standardní terminologii a popis činnosti a vlastností celé řady technik odstranění identifikace. Neurčuje však, jak by tyto techniky měly být řízeny a spravovány v konkrétním případě použití. Očekává se, že budou vypracovány rámcové normy specifické pro jednotlivá odvětví, které takové pokyny poskytnou.

1 Předmět normy

Tento dokument poskytuje popis technik odstranění identifikace dat zvyšujících soukromí, sloužící k popisu a návrhu opatření v oblasti odstranění identifikace v souladu s principy soukromí podle ISO/IEC 29100.

Tento dokument zejména specifikuje terminologii, klasifikaci technik odstranění identifikace podle jejich charakteristik a jejich použitelnost pro snížení rizika opětovné identifikace.

Tento dokument je použitelný pro organizace všech typů a velikostí, včetně veřejných a soukromých společností, vládních subjektů a neziskových organizací, vystupujících jako správci PII nebo zpracovatelé PII jednající jménem správce, implementující procesy odstranění identifikace dat za účelem zvýšení soukromí.