

ISO 12859 - ITS - Aspekty ochrany dat systémů ITS

Aplikační oblast: [Architektura ITS systémů](#)

Počet stran: 96

Zavedení normy do ČSN: překladem

Rok zpracování extraktu: 2010

Skupina témat: Právní a obchodní aspekty ITS

Téma normy: Architektura systému ITS

Charakteristika tématu: Aspekty ochrany dat systémů ITS v Evropě

Úvod, vysvětlení východisek

Popis architektury, hierarchie, rolí a vztahů objektů

Obecné pokyny pro vývojáře ITS standardů a systémů na aspekty ochrany osobních údajů a souvisejících legislativních požadavků

Popis procesu / funkce / způsobu použití

Popis rozhraní / API / struktury systému

Definice protokolu / algoritmu / výpočtu

Definice reprezentace dat / fyzikálního významu

Definice konstant / rozsahů / omezení

Úvod

Inteligentní dopravní systémy jsou spojeny s pohybem a výměnou dat. Některá z těchto dat mohou poskytovat osobní informace. V moderním světě je v mnoha případech nemožné, ani žádoucí, aby informace byly vždy anonymní, a proto je jejich utajení chráněno předpisy o zabezpečení dat.

Specifická ochrana osobních dat a legislativa jejich utajení obecně je obsažena ve vnitrostátních právních předpisech, a pro různorodost sociálních, kulturních, ekonomických a právních podmínek se může lišit stát od státu. V mnoha konkrétních případech platí národní aspekty utajení a zabezpečení dat, ale globálně platí obecné zásady stanovené EU a APEC.

Utajení je požadována příkazem o ochraně osobních dat Evropské unie, rámcem pro utajení APEC a směrnicí na ochranu utajení při přeshraničních tocích osobních dat OECD z roku 1980. Tato technická zpráva by měla být vodítkem pro vývojáře ITS norem a systémů k utajení osobních dat již na úrovni základní architektury při návrhu všech norem, systémů a implementací ITS.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Užití

Tato technická zpráva by měla být vodítkem pro vývojáře ITS norem a systémů v oblasti utajení osobních dat a splnění souvisejících legislativních požadavků při návrhu či revizích všech jejich výstupů. Tato zpráva není normou a poskytuje spíše obecná doporučení než závazné požadavky. Národní právo má vždy přednost před mezinárodními směrnicemi, a proto by je měl čtenář interpretovat vždy v kontextu národní legislativy. Příkaz o ochraně osobních dat Evropské unie a navazující prostředky jsou povinné v rámci všech členských zemí. Zpráva je navržena tak, aby poskytovala údaje a vysvětlení těm, jež vytváří mezinárodní normy ITS a těm, kteří vytváří specifikace, implementace a instalace

inteligentních dopravních systémů.

1. Předmět normy

Tato technická [zpráva](#) poskytuje vodítko pro vývojáře ITS norem a systémů v oblasti utajení [osobních dat](#) a splnění souvisejících legislativních [požadavků](#) při návrhu či revizích všech jejich výstupů. Tato [zpráva](#) není normou a poskytuje spíše obecná doporučení než závazné [požadavky](#).

Tato technická [zpráva](#) poskytuje pokyny a nevyjadřuje [požadavky](#) na shodu.

2. Související normy

;Příkaz 95/46/EC Evropského parlamentu a Rady z 24 října 1995.

Příkaz 2002/58/EC evropského parlamentu a Rady z 12 července 2002.

Rámec pro utajení (APEC Privacy Framework APEC#205-SO-01.2) www.apec.org.

Pokyny k ochraně, utajení a přeshraniční toky [osobních dat](#) O. E. C. D. C(80)58 (Final), z 1. října 1980

[ISO 24100](#) Inteligentní dopravní systémy, komunikace v rozsáhlém území, základní principy pro ochranu [osobních dat](#) v sondovacích vozidlech využívaných pro informační služby.

ISO 17799 Informační technologie - bezpečnostní postupy - zásady pro management zabezpečení informací.

ISO/IEC 18028 (všechny části), Informační technologie - bezpečnostní postupy - zabezpečení sítě IT.

ISO 27001 Informační technologie - bezpečnostní postupy - systémy řízení zabezpečení informací -

[požadavky](#).

ISO 27002 Informační technologie - bezpečnostní postupy - zásady pro management zabezpečení informací.

ISO 27005 Informační technologie - bezpečnostní postupy - řízení rizika zabezpečení informací.

ISO 27006 Informační technologie - bezpečnostní postupy - [požadavky](#) na orgány poskytující audit a osvědčení o systémech řízení zabezpečení informací.

3. Termíny a definice

odpovědnost zodpovědnost za respektování stanovených opatření.

omezení sběru dat [omezení sběru osobních dat](#).

kvalita dat přijatelný standard přesnosti [osobních dat](#).

otevřenost politika [otevřenosti](#) ve vývojových trendech, praktiky a zásady s ohledem na [osobní data](#).

zabezpečení dat prevence nesprávného použití dat v počítačích, právní zabezpečení předcházející nesprávnému použití informací uložených v počítačích, zvláště informací o jednotlivých lidech.

osobní data jsou to data o žijícím jednotlivci, identifikující nebo [identifikovatelná](#), jak je určeno zákony na jejich utajení a právními konvencemi.

kontrolor osobních informací - entita nebo organizace kontrolující sběr, držení a zpracování nebo [využití osobních informací](#)

utajení - kvalita, s jakou je zabráněno zveřejnění nebo zobrazení ostatním

specifikace účelu - účel, pro jaký jsou [osobní data](#) shromažďována

Další termíny a zkratky z oboru ITS jsou obsaženy ve [slovníku ITS terminology](#).

4. Symboly a zkratky

APEC- Organizace Asijsko – Pacifické ekonomické spolupráce

OECD- Organizace pro ekonomickou spolupráci a rozvoj

EU- Evropská unie

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www.ITSterminology.org).

6 Pozadí

V kapitole jsou vysvětlena základní východiska vzniku této technické [zprávy](#). [Zpráva](#) vznikla z [požadavku](#) Rakouska a vyplynula z místních právních studií, týkajících se ochrany [osobních dat](#) v ITS. Jako výchozí materiály jsou zde zmíněny směrnice EU, doporučení OECD a APEC. Jako cesta pro zajištění utajení a ochranu [osobních dat](#) je zde formulován [požadavek](#) na zabezpečení dat. Zvláštní pozornost je při tom nutno věnovat zpracování, přenosu a ukládání informací pro oprávněné uživatele s povoleným přístupem a potenciálním tokům informací s externími entitami. V ITS je často nutná spolupráce různých institucí z různých [domén služeb ITS](#), kde výměna dat má za cíl zlepšování funkčnosti. Záměrem této technické [zprávy](#) je zdůraznit platnost směrnic EU i doporučení OECD a APEC v oblasti ITS. Rozbor východisek vzniku této technické [zprávy](#) je zde proveden na příkladech.

7 Doporučení

Technická [zpráva](#) navrhuje dodržování následujících obecných zásad pro zabezpečení a utajení [osobních dat](#) využívaných v ITS:

- neubližovat
- jednat slušně a podle platných zákonů
- [osobní data](#) využívat pouze k přesně specifikovaným cílům
- legitimní cíle musí být stanoveny již v době sběru dat
- nezpracovávat [osobní data](#) k jiným než stanoveným účelům
- neuvolnit [osobní data](#) bez [souhlasu](#) dotčené osoby mimo definované [výjimky](#)
- rozsah [osobních dat](#) musí být adekvátní danému účelu a nesmí být shromažďováno nic navíc
- data musí být přesná a podle daného účelu aktuální
- [osobní data](#) uchovávat jen po dobu nezbytnou pro daný účel
- přístup k osobním údajům jen minimu osob pro zajištění daného účelu
- pravidla pro nakládání s osobními údaji musí být stanovena jasně a musí být přístupná
- záruka přiměřeného zabezpečení“
- kumulativní interpretace vícenásobných doporučení

Příloha A (informativní)

V příloze je uveden text příkazu 95/46/EC Evropského parlamentu a Rady z 24 října 1995 na ochranu osob s ohledem na zpracování jejich [osobních dat](#) a o volném pohybu těchto dat.

Příkaz je členěn na tyto kapitoly:

- Obecná ustanovení.
- Obecná pravidla a zákonitosti.

- Soudní prostředky, odpovědnost a sankce.
- Přenos osobních dat třetím zemím.
- Prováděcí předpisy.
- Orgán dohledu.
- Uplatnění opatření ve společnosti
- Závěrečná ustanovení

Dále je zde uveden text příkazu 2002/58/EC Evropského parlamentu a Rady, který rozšiřuje předchozí příkaz vzhledem k utajení v elektronických komunikacích. Tento příkaz nemění základní ochranu utajení z příkazu 95/46, ale zabývá se specifickými problémy vztahujícími se k elektronickým komunikacím, zvláště přes veřejné sítě.

Příloha B (informativní)

Příloha uvádí text rámce pro utajení APEC Privacy Framework, který schválili ministři zemí APEC, vědomi si důležitosti efektivní ochrany soukromí za účelem odstranění bariér informačním tokům. Rámeček se skládá z těchto částí:

- Úvod
- Účel a definice
- Principy utajení APEC
- Implementace
 - na národní úrovni
 - na mezinárodní úrovni

Příloha C (informativní)

Příloha uvádí text Pokynů k ochraně, utajení a přeshraničním tokům osobních dat O. E. C. D. z roku 1980. Pokyny obsahují tyto části:

- Obecné definice
- Základní principy národní aplikace
- Základní principy mezinárodní aplikace: volné toky a legitimní omezení
- Národní implementace
- Mezinárodní spolupráce

Příloha D (informativní)

Příloha uvádí příklad národní implementace pokynů APEC. Implementace pokynů se mění podle struktury a praxe v různých režimech. Jako příklad implementace směrnice APEC poskytuje tato příloha ukázkou způsobu realizace v USA.

Příloha E (informativní)

V příloze je uveden příklad principu „kumulativní interpretace“ příkazu EU a směrnice APEC. Právní výklad příkazu i směrnice se může lišit země od země. Pokud porovnáme několik klauzulí ze z příkazu a směrnice zjistíme, že „kumulativní účinek“ obou může být úspěšně využit. Samozřejmě příkaz EU má v zemích EU silnější právní dopad.

Příloha F (informativní)

Příloha uvádí přehled anotací norem ISO souvisejících s bezpečností (včetně norem řady ISO 2700x) a zahrnuje:

- ISO 17799 Informační technologie - bezpečnostní postupy - zásady pro management zabezpečení informací.
- ISO/IEC 18028 (všechny části), Informační technologie - bezpečnostní postupy - zabezpečení sítě IT, a zvláště:
 - ISO/IEC 18028-1 Management bezpečnosti sítě
 - ISO/IEC 18028-5 Zabezpečená komunikace napříč sítěmi s využitím virtuální privátní sítě
- ISO 27001 Informační technologie - bezpečnostní postupy - systémy řízení zabezpečení informací - [požadavky](#).
- ISO 27002 Informační technologie - bezpečnostní postupy - zásady pro management zabezpečení informací.
- ISO CD 27003 Informační technologie – směrnice pro implementaci systému řízení informační bezpečnosti
- ISO FCD 27004 Informační technologie - bezpečnostní postupy – měřítka pro management informační bezpečnosti.
- ISO 27005 Informační technologie - bezpečnostní postupy - řízení rizika zabezpečení informací.
- ISO 27006 Informační technologie - bezpečnostní postupy - [požadavky](#) na orgány poskytující audit a osvědčení o systémech řízeních zabezpečení informací.
- [ISO 24100](#) Inteligentní dopravní systémy, komunikace v rozsáhlém území, základní principy pro ochranu osobních dat v sondovacích vozidlech využívaných pro informační služby.

V závěru této poslední přílohy je uveden seznam informačních zdrojů – bibliografie.

Související termíny

- [bezpečnostní ochrana](#)
- [specifikace účelu](#)
- [soukromí](#)
- [otevřenost](#)
- [omezení sběru \(dat\)](#)
- [omezení použití](#)
- [ochrana dat](#)
- [odpovědnost](#)
- [kvalita dat](#)
- [individuální přístup](#)
- [správce osobních údajů](#)