Ochrana osobních údajů - aktuální problémy v EU a v ČR

Karel Neuwirt

MU FI, Brno 18. 10. 2005

Ochrana soukromí a ochrana dat jsou ústavními právy

Ústava pro Evropu:

Každý má právo na svobodu a osobní bezpečnost (čl.II-66)
Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace (čl. II-67)
Každý má právo na ochranu osobních údajů, které se jej týkají (čl. II-68 odst.1)

Charta základních práv Evropské unie:

Každý má právo na respektování jeho soukromého a rodinného života, obydlí a korespondence (čl. 7)

Úmluva o ochraně lidských práv a základních svobod:

Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence (čl. 8)

Ústavy členských států EU a všech demokratických států

Legislativa - Evropa

- Úmluva o ochraně lidských práv a základních svobod (Řím, 1950)
- Úmluva o ochraně jednotlivců s ohledem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981)
- Směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Evropský parlament a Rada, 95/46/EC, 1995)

Evropské orgány

- Rada Evropy –
  Consultative Committee (T-PD)
  Project Group on Data Protection (CJ-PD)
- Evropská komise –
  Article 29 Working Party, Commission 31
- Dozorové úřady členských států EU
  (DP Commissioners)

11. září 2001

- Milník v historii ochrany soukromí
- Bezpečnostní opatření proti terorismu vers. Ochrana soukromí – jak hledat rovnováhu?
- 2002 – 2004 Apokalypsa soukromí?
- Boj s terorismem nesmí být bojem proti lidským právům, soukromí a lidské důstojnosti
- Od “reaktivních” po “pro-aktivní” opatření

Důsledky 11. září

- Rostoucí zájem o bezpečnostní technologie
- Rostoucí zájem o monitorování občanů
- Nové kompetence pro zpravodajské služby
- Prostředky pro bezpečné cestování
- Nové identifikační doklady
- .....
- Integrovaná řešení pro bezpečnější svět

Identita vers. anonymita

Ochrana soukromí
Právní ochrana soukromí – ochrana lidské důstojnosti

Ochrana soukromí

-ochrana osobních informací
-ochrana proti krádeži / zneužití identity,
-informační bezpečnost je integrální součástí ochrany soukromí

Moderní technologie

- Zvyšují ochranu soukromí (Privacy Enhancing)
- Zasahují do soukromí (Privacy Intrusive)
- Nová rizika pro soukromí:

  Internet, video-surveillance

  telekomunikace, mobilní telefony

  čipové karty, RFID

  DNA, biometrika,

  E-cestovní doklady

Identifikační systémy

-které jsou založeny na PIN, čipové kartě apod., pouze identifikují tyto PINy a karty, nikoliv vlastní osoby

- které identifikují jednotlivce bez jeho přímého vlivu

Digitální – e-Identity

- e-identity v digitální společnosti
- Zásadní problém v rozlišení mezi identifikací a verifikací musí být řešen
- Identifikace – pohled ochrany dat
  - pohled bezpečnosti

Identifikační technologie

- Čipové karty
- RFID
- Biometrics
- Monitorovací (sledovací) technologie
  - -pro identifikaci a verifikaci
  - -pro anonymní schéma
  - -pro multi-aplikace

- Bezpečná autorizace – pouze oprávněný uživatel má přístup k datům nebo s nimi provádět vymezené úkony
- Důvěrnost - data jsou chráněna vůči neoprávněnému uživateli
- Integrita dat – data jsou chráněna proti neoprávněné změně
- Dostupnost dat – data jsou přístupná autorizované osobě

Biometrická authentizace

… automatizovaná identifikace nebo verifikace identity jednotlivce, založená na fyziologických charakteristikách nebo na chování jednotlivců. Takové authentizace je dosaženo používáním počítačových technologií při neinvazivních způsobech porovnání obrazů – z reálného života jednotlivce a obrazu již dříve získaného a zaznamenaného ...

Dokumenty o biometrice

- Working document on biometrics, WP80, 2003 (WP 29)
- Opinion No 7/2004 on the inclusion of biometric elements …. on visas (VIS), WP96, 2004 (WP29)
- Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data, Rada Evropy, 2005
- Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents

Biometrická data a ochrana dat:

- Aplikace všech standardních principů stanovených Úmluvou č.108 a Směrnicí 95/46/EC
- Účely (statistika, věda, výzkum, …)
- Definice (co jsou opravdu biometrická data – původní obraz, digitální vzor ?)
- Verifikace vers. Identifikace
- Právo subjektu údajů na informace

Biometrické otisky prstů

- v cestovních dokladech
- ve vízech (VIS EU)
- v Schengenském systému SIS II (má dvě části: centrální databázi Schengenského IS, 1-2 přístupové body v každém státě EU)

???

ICAO dokumenty

International Civil Aviation Organisation (ICAO)

- Biometrics deployment of machine readable travel documents, ICAO, 2004
- Standards 9303 for MRTD, ICAO

ePassport

- An MRTD (Machine Readable Travel Document) cestovní doklad (pas) se vsazeným bezkontaktním čipem, podle návrhu standardu ICAO
- Bezkontaktní čip podle normy

  ISO/IEC 14443 (proximity 0-10 cm)

RFID passports

Mohou být čteny na vzdálenost, nepotřebují fyzický kontakt pro čtení údajů v nich zapsaných

Experti varují: RFID čip může být čten jakoukoliv čtečkou, nejen tou, která je instalována u pasové kontroly. To znamená, že držitel pasu průběžně vysílá své jméno, národnost, věk, adresu, a vše co je v RFID čipu zapsáno. Každý, kdo má čtečku může číst tyto informace, aniž by o tom držitel pasu věděl či k tomu dal svůj souhlas.

(Bruce Schneier, Int. Herald Tribune, Oct. 04, 2004)

Cestovní dokumenty

Jsou oficiální dokumenty vydané státem nebo kompetentními institucemi, které jsou držitelem používány pro mezinárodní cestování a které obsahují povinné viditelné (pro čtení zrakem) údaje a fotografii držitele

- Cestovní pas
- Víza
- Jiné cestovní dokumenty (např. identifikační identifikační průkaz)

(viz Draft Recommendation on Identity and Travel Documents and Terrorism, TER-S-IT, 2005)

Uchovávání dat

- „Data retention“ telekomunikačních dat – aktuální problém EU
- Iniciativa Francie, U.K., Irska, Švédska – uchovávání telekomunikačních dat pro účely prevence, vyšetřování, odhalování a trestání kriminality vč. Terorismu – odmítnuta Evropským parlamentem.
- 85% telekomunikačních dat pro potřeby policie se týká dat ne starších 6 měsíců
- Návrh na změnu směrnice 2002/58/ES


NEBUĎTE DRZÁ! MÁ-LI NÁŠ ÚŘAD NA OCHRANU OSOBNÍCH ÚDAJŮ OBČANA CHRÁNIT, MUSÍ VĚDĚT, CO CHRÁNÍ.

KRESBA: MIROSLAV KEMEL

karel.neuwirt@centrum.cz

Závěry

Zprávy on aplikaci zásad Úmluvy 108 na shromažďování a zpracování biometrických dat

Rada Evropy, 2005

1

Biometrical data are to be regarded as a specific category of data as they are taken from the human body, remain the same in different systems and are in principle inalterable throughout life. They might be altered, however, for instance through aging, illnesses or surgical interventions

2

Before having recourse to biometrics, the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life

3

Biometrics should not be chosen for the sole sake of convenience. Human dignity might be affected by the use of biometrics. Socio-cultural aspects and possible reluctance towards the instrumental use of the human body, should be taken into account.

4

The biometric data and any associated data generated by the system must be processed for specific, explicit and legitimate purposes and should not be processed further for purposes that are incompatible with these.

5

The data should be adequate, relevant and not excessive in relation to these purposes. A technical system using biometric data should be configured to exclude the possibility to collect more biometric or associated data than is necessary for the purposes of the processing. Where templates are sufficient, the collection or the storage of the picture should be avoided

6

In choosing the system architecture, the controller should balance the advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand. A reasoned choice should be made between storage solely on an individual storage medium, a decentralised database or a central database, bearing in mind the aspects relating to data security.

7

The architecture of a biometric system should not be disproportionate in relation to the purpose of the processing. Therefore, if verification suffices, the controller should not develop an identification solution. Biometric data that are solely used for verification purposes preferably should be stored only on a secured individual storage medium, e.g. a smart card, held by the data subject only

8

The data subject should be informed about the purposes of the system and the identity of the controller unless he or she already knows, and about the personal data that are processed and the persons or the categories of persons to whom they will be disclosed as far as the information is necessary to guarantee the fairness of processing

9

The data subject has a right of access, rectification, blocking and erasure of the data relating to him or her. These rights extend to the biometric data undergoing automatic processing attached to his identity, possibly associated data (such as date and place of use of the system) and to whom they have been communicated

10

The controller should foresee adequate technical and organisational measures that aim to protect biometric and associated data against accidental or deliberate deletion or loss, as well as against illegal access, alteration or communication to unauthorised persons or any other form of illegal processing

11

A procedure of certification and monitoring and control, if appropriate by an independent body, should be promoted, particularly in the case of mass applications, with regard to the quality standards for the software, the hardware and the training of the staff in charge of enrolment and matching. A periodic audit of the system's performance is recommendable

12

If, as a result of a biometric system, a data subject is rejected, the controller should, on his or her request, re-examine the case and should, where necessary, offer appropriate alternative solutions. Procedures should be in place and made known to the data subject in the case of an allegedly false result of the system