



# VĚSTNÍK

ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

## 2003

Částka 29

23. prosince 2003

Cena 58 Kč

### OBSAH

Úvod ..... 2090

#### I. Registrace

Abecední seznam zaregistrovaných subjektů v období  
od 23. 10. 2003 do 10. 12. 2003 ..... 2091

Přehled povolených zpracování osobních údajů zaregistrovaných  
Úřadem v období od 23. 10. 2003 do 10. 12. 2003 ..... 2094

Přehled zrušených registrací ..... 2116

#### II. Sdělení Úřadu

Pracovní dokument o biometrii (předložený WP29 — pracovní skupinou  
pro ochranu osobních údajů podle článku 29 Směrnice 95/46/ES)..... 2117

## ÚVOD

Věstník Úřadu pro ochranu osobních údajů přináší ve své devětadvacáté části přehled povolených zpracování osobních údajů zaregistrovaných v období od 23. října 2003 do 10. prosince 2003 a přehled registrací, které byly v tomto období zrušeny.

V oddílu Sdělení Úřadu je zveřejněn další z dokumentů Pracovní skupiny pro ochranu osobních údajů podle čl. 29 (WP29) Směrnice 95/46/ES, která působí v rámci Evropské komise. Jde o Pracovní dokument o biometrii, který byl přijat dne 1. srpna 2003. Biometrie je obor, který se v posledních letech rychle a úspěšně vyvíjí. Možnosti, které biometrie nabízí, a důsledky, které z jejího dynamického rozvoje vyplývají, je ovšem nutno pozorně sledovat a posuzovat, zvláště v jejich souvislostech se zásadami ochrany osobních údajů a soukromí

# I. REGISTRACE

## Abecední seznam zaregistrovaných subjektů v období od 23. 10. 2003 do 10. 12. 2003

Identifikace	Č. reg.	Identifikace	Č. reg.
AAA AUTO A.S.	00020909	GILLETTE CZECH S.R.O.	00020859
ADJ.CZ, SPOL. S R.O.	00020919	GOLEM OIL, A. S.	00021098
AJA-ÚČTO PRAHA S. R. O.	00020964	GRANTOVÝ FOND VYSOKÉ ŠKOLY EKONOMIE A MANAGEMENTU O.P.S.	00021062
AKVIZIČNÍ A REGISTRAČNÍ S.R.O.	00021085	GREEN-SWAN PHARMACEUTICALS CR, A.S.	00020975
ALTERCAN,S.R.O.	00020983	GREGOR TOMÁŠ	00020847
AMERICAN EXPRESS,SPOL. S R.O.	00011696	GREIFENTHALOVÁ JANA	00021045
AQUASOFT SPOL.S R.O.	00021112	GROSS JAN ING.	00021097
AVACOM S.R.O.	00020895	GŘEŠ ROSTISLAV	00021019
AVNET S.R.O.	00020848	HANÁČKÉ REALITY,S.R.O.	00020853
BARRANDOV STUDIO A.S.	00020999	HANZEL PAVEL	00021065
BARTOSCH ROLF	00021099	HEMALA KAREL	00020897
BENEŠOVÁ JANA	00020966	HEMALOVÁ JAROSLAVA	00020896
BENEŠOVÁ VĚRA ING.	00020968	HLAVNÍ MĚSTO PRAHA	00001029
BLAŽKOVÁ VLASTA PHDR.	00020866	HLUCHÝ MILAN ING.	00021046
BOHÁČOVÁ EVA	00021013	HONKOVÁ JANA	00021036
BOHADLOVÁ RENATA ING.	00021038	HOSKOVEC JAROSLAV ING.	00021032
BÖHM VLADIMÍR	00021027	HRDLIČKA SPOL. S R. O.	00021108
BROKERJET ČESKÉ SPOŘITELNY,A.S.	00020840	HRUBÁ ZDEŇKA	00021081
BUDNIKOV MILAN	00020988	HRUBÝ JOSEF ING.	00021047
C.S. COMMERCE SERVICE, A.S.	00003883	HYKLOVÁ MARIE MGR.	00021057
CAR COMMUNICATION S. R. O.	00012413	CHYSKÝ JAN	00020928
CBT ASTRO 2006 S.R.O.	00021061	ILJUK ANATOLIJ	00021114
CÍSAŘOVSKÝ MICHAL PHDR.	00021103	IPEX A.S.	00021070
COMARR SPOL. S R.O.	00020879	JANEČEK IVO ING.	00021110
CZ.NIC, Z.S.P.O.	00021060	JANKIELOVÁ YVONA ING.	00021022
ČESALOVÁ JANA	00020922	JÁNOŠKA RASTISLAV MUDR.	00021119
ČESKÁ HYPOTEČNÍ FINANCOVÁNÍ BYDLENÍ, S.R.O. DĚLNICKÁ 54	00020860	JAROŠ JAN	00020921
ČESKÉ MUZEUM STŘÍBRA	00020877	JAROUJOVÁ JANA	00021058
ČESKÉ RADIOKOMUNIKACE A.S.	00020937	JEBAVÝ ROMAN	00021043
ČSAD SLANÝ A.S.	00021116	JELENOVÁ HANA	00020959
DANKOVÁ RŮŽENA	00021017	JRC CZECH A.S.	00020886
DELPHARMEA,A.S.	00018647	JUSTIČNÍ AKADEMIE	00020882
DLOUHÝ DAVID	00020899	KADLEČKOVÁ PETRA	00020910
DOLEJŠOVÁ KATEŘINA	00021051	KLEPÁČ JIŘÍ	00020989
DOMOV DŮCHODCŮ	00021029	KLIKOVÁ LENKA	00021055
DOMOV DŮCHODCŮ DOLNÍ CETNO	00021072	KLIMESCHOVÁ ALENA	00020952
DOMOV DŮCHODCŮ MODRÝ KÁMEN	00021084	KMEŤOVÁ JANA PHDR.	00021031
DOSTÁLEK LADISLAV ING.	00021083	KOMAKO FINANCE S.R.O.	00020965
DRATNALOVÁ JAROSLAVA	00020933	KOPECKÝ MIROSLAV	00021066
DRBAL LUBOMÍR	00021076	KORVAS STANISLAV ING.	00020976
DRDA JIŘÍ	00021117	KOSOVÁ JANA	00021033
DUDEK JIŘÍ	00021078	KOŠTÁLOVÁ VĚRA	00020930
DVOŘÁK MAREK	00021075	KOUDELKA ZDENĚK JUDR.	00020963
DVOŘÁKOVÁ KATEŘINA	00021040	KOZÁKOVÁ ALENA	00020996
DVOŘÁKOVÁ MARIE	00021001	KRATOCHVÍL JAN	00020986
DVOŘÁKOVÁ MARIE	00021039	KRČOVÁ DAGMAR	00021100
EGERSDORFOVÁ JANA	00020858	KRNÁVKOVÁ RENATA	00021079
EHRlich PETR	00000083	KROPÁČEK VLASTIMIL	00020979
EQUILIBRIUM S.R.O.	00021105	KŘEŠŤANSKÝ INSTITUT	00020865
EUBE A.S.	00020947	KŘIVÁNEK TOMÁŠ	00021049
EUROPIN GROUP A.S.	00020902	KUBÁT ALEŠ MGR.	00020973
FILIPCOVÁ BOHUSLAVA	00021082	LANDIS+GYR S.R.O.	00020898
FK-ARMATURY TRADE CZ S.R.O.	00020974	LANDSINGEROVÁ BOHUSLAVA	00020969
FRANC ONDŘEJ	00021077	LANDSINGEROVÁ VĚRA	00020841
FUCHS VLADIMÍR ING.	00021069	LAXUS OBČANSKÉ SDRUŽENÍ	00021024
FURIKOVÁ JANA	00020949	LEGNER VLADIMÍR ING.	00021003
GENTEST,S.R.O.	00021048	LEITGEBOVÁ MONIKA	00021020
GERIATRICKÉ CENTRUM TÝNIŠTĚ NAD ORLICÍ	00021056	LEKEŠ MIROSLAV ING.	00020960

Identifikace	Č. reg.	Identifikace	Č. reg.
LEONARDO SPOL. S R.O.	00021101	OBEC VELKÝ ÚJEZD	00016747
LETKA TEAM A.S.	00020913	OBEC VĚROVANY	00020901
MACÍČEK PETR	00021002	OBEC VILÉMOV	00021028
MARKOVÁ IVA	00021018	OBERREITER STANISLAV	00020839
MARTIN JANDA CESTOVNÍ AGENTURA	00020935	ODBORNÉ UČILIŠTĚ A PRAKTICKÁ ŠKOLA, BRNO,	
MARTINKOVÁ JANA	00020995	LOMENÁ 44	00021090
MED-FPS.R.O.	00020951	ODSTRČILÍK VLADIMÍR	00020929
MĚSTO TŘEBÍČ	00004572	OPATHERM A.S.	00020863
MĚSTSKÉ INŽENÝRSKÉ SÍŤ STUDÉNKA A.S.	00020862	P.E.S. CONSULTING, S.R.O.	00021107
MICHEL DANIEL	00021106	PACÁKOVÁ EVA	00020911
MIKOVÁ JIŘINA	00020994	PANOCHA VÍTĚZSLAV ING.	00021030
MINAŘÍKOVÁ JANA	00021000	PATKOVÁ LEA	00021042
MOTYČKOVÁ ZDENKA	00021054	PAVLUKOVÁ EVA ING. - DEVONA	00020971
MOULISOVÁ RŮŽENA	00021005	PECKO JULIUS	00020945
NÁCHOD.NET S.R.O.	00020997	PELNÁŘ PETR RSDR.	00020854
NAVRÁTIL PETR	00020907	PELNÁŘOVÁ ANNA	00020855
NĚMCOVÁ LUDMILA	00020957	PETRÁŠ ŠTEFAN	00020880
NEWFANCES,S.R.O.	00020843	PETŘÁŠOVÁ HELENA	00021115
NOKIA CZECH REPUBLIC S.R.O.	00011375	PHARCY S.R.O.	00021089
NOVOTNÁ JAROMÍRA	00020894	PINKASOVÁ JAROSLAVA ING.	00020876
NOVOTNÝ JIŘÍ ING.	00020926	PODANÉ RUCE-PROJEKT OSA FRÝDEK-MÍSTEK	00021026
NOVOTNÝ LADISLAV	00021004	PODSKLANOVÁ IVA	00021015
OBČANSKÉ SDRUŽENÍ BAOBAB	00020842	POLÁNKA JAN ING.	00021102
OBČANSKÉ SDRUŽENÍ DŮM TŘÍ PŘÁNÍ	00021059	PORTLAND TRUST DEVELOPMENTS IV.S.R.O.	00020238
OBČANSKÉ SDRUŽENÍ GREEN DOORS /ZELENÉ DVEŘE/	00020849	POSPÍŠIL JOSEF	00021093
OBEC BĚLKOVICE-LAŠTANY	00020850	POSTUPA JAROSLAV	00020923
OBEC BÍLÁ LHOTA	00021009	PROCHÁZKA MIROSLAV	00021080
OBEC BLATEC	00020982	PRŮSCHL VLASTISLAV	00020961
OBEC BLAŽIM	00020856	PRŮŠA LIBOR MVDR.	00020915
OBEC BOHUŇOVICE	00020912	RADOMSKÝ JAN ING.	00020864
OBEC BOUZOV	00020885	RAIFFEISEN BANK A.S.	00004250
OBEC BYSTROČICE	00021011	RK CENTA S.R.O.	00020939
OBEC BYSTROVANY	00020861	ROYAL SEAL, S.R.O.	00021035
OBEC DASKABÁT	00000985	RŮŽIČKOVÁ EVA	00021007
OBEC DOLANY	00012714	SADLOVSKÁ JANA	00020875
OBEC DOLOPLAZY	00020925	SHROMÁŽDIL FRANTIŠEK ING.	00021074
OBEC DUB NAD MORAVOU	00020955	SCHERING S.R.O.-ČLEN KONCERNU	00020924
OBEC DUBČANY	00021012	SIKOROVÁ IRENA	00021092
OBEC GRYGOV	00021109	SIMPLY YOU, S.R.O.	00020845
OBEC HAŇOVICE	00021010	SIPLEX S.R.O.	00020938
OBEC HLUBOČKY	00009256	SKANSKA CZ REGION BRNO S.R.O.	00020990
OBEC HLUŠOVICE	00020851	SLÁMOVÁ DANA	00021025
OBEC HNĚVOTÍN	00021071	SMOLÍK MIROSLAV	00020887
OBEC HORKA NAD MORAVOU	00020953	SOBOTOVÁ HANA ING.	00020978
OBEC CHARVÁTY	00020884	SOCIÁLNÍ SLUŽBY VSETÍN PŘÍSPĚVKOVÁ ORGANIZACE	00021118
OBEC CHODOVÁ PLANÁ	00019402	SOFROŇOVÁ HELENA	00020846
OBEC KOŽUŠANY-TÁŽALY	00020904	SPOLEČENSTVÍ VLASTNÍKŮ ČP. 289 - 291 V PŘÍBRAMI V	00020900
OBEC KRČMAŇ	00020905	STATUTÁRNÍ MĚSTO BRNO	00005956
OBEC KŘELOV-BŘUCHOTÍN	00021087	STRAKA VLASTIMIL	00020914
OBEC LUTÍN	00017958	ŠEPS EMANUEL	00020883
OBEC MAJETÍN	00020903	ŠIMČISKOVÁ ANNA	00020992
OBEC MEDLOV	00021037	ŠIMÍČKOVÁ MARCELA	00020944
OBEC MRSKLESY	00020972	ŠÍPKOVÁ MIROSLAVA	00021008
OBEC MRTNÍK	00021073	ŠÍPOVÁ LENKA	00020948
OBEC NOVÁ HRADEČNÁ	00020852	ŠKODA RADOVAN	00020954
OBEC PŘÁSLAVICE	00020991	ŠKŮREK JOSEF	00020927
OBEC SAMOTÍŠKY	00020906	ŠNAJDAROVÁ IVANA	00021091
OBEC SKRBEŇ	00020962	ŠPIČKA PAVEL	00020993
OBEC STARÉ SEDLIŠTĚ	00021023	ŠTĚPÁN JAROSLAV DIS.	00020946
OBEC SUCHONICE	00020984	ŠTĚPÁNOVÁ JIŘINA	00021006
OBEC ŠTARNOV	00020956	ŠTIKAROVÁ JANA PHDR.MGR.	00020867
OBEC ŠTĚPÁNOV	00018821	TELENSKÁ HELENA -TERMINAL	00021034
OBEC TĚŠETICE	00020857	TICKETPRO, A.S.	00020874
OBEC TOVĚŘ	00021014	TIDSEO S.R.O.	00020998
OBEC TRŠICE	00020981	TOČÍK STANISLAV	00021016
OBEC ÚJEZD	00020908	TONOVÁ HANA	00020987
OBEC VELKÝ TÝNEC	00020917	TOŠENOVSKÝ VLASTIMIL PHDR.	00020931

Identifikace	Č. reg.	Identifikace	Č. reg.
TRIUMFA S.R.O.	00021064	VYHLÍDALOVÁ LENKA ING.	00020942
TYFLOCENTRUM ZLÍN O.P.S.	00021113	VYSOČINA KRAJ	00001602
UNIE PODNIKOVÝCH PRÁVNÍKŮ ČESKÉ REPUBLIKY	00021111	WADIA S.R.O.	00020940
UNILEVER ČR SPOL. S R.O.	00001188	WALMARK A. S.	00001182
ÚSKOBA JAROSLAV	00021096	XPERT S.R.O.	00020920
VALIŠ BOHUŠ	00021044	ZAHRADNÍ ČTVRŤ A.S.	00020941
VALOUŠEK PETR	00020980	ZÁMEČNÍK MARTIN	00020970
VAŇUROVÁ HANA MGR.	00020916	ZDAŘIL PETR	00020881
VENER-VEND, S.R.O.	00020918	ZELENKOVÁ MARKÉTA	00021041
VESELKA LUKÁŠ	00021021	ZEMAN JIŘÍ	00020932
VESELÝ TOMÁŠ	00021052	ZEMANOVÁ JANA	00020967
VLACHOVÁ PAVLÍNA	00021050	ŽENÍŠEK IVAN ING.	00021104
VODÁCKÉ A TURISTICKÉ CENTRUM HONZA S.R.O.	00020934	ŽIVNOSTENSKÁ BANKA A.S.	00001647
VOLČAS, S.R.O.	00021068		

**Přehled zrušených registrací**

<b>Číslo registrace</b>	<b>Subjekt</b>	<b>Datum zrušení</b>
00001254/001	ČESKÝ ZAHRÁDKÁŘSKÝ SVAZ ZO J.Ř.MENDELA	27.7.2002
00001465/002	OKRESNÍ ÚŘAD PŘÍBRAM	27.11.2002
00001835/001	TEINVEST A. S.	22.10.2003
00002096/001	MAREK TOMÁŠ MUDR.	17.10.2003
00005781/001	DOBRUŠSKÉ STROJÍRNY, A.S.	22.7.2002
00008600/001	I&C ENERGO S.R.O.	23.7.2002
00017405/001	DAMIN HOTELSERVICES SPOL. S R.O.	29.10.2003

## II. SDĚLENÍ ÚŘADU

*Tento překlad Úřadu pro ochranu osobních údajů má pouze neoficiální, informativní charakter.*

### PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ PODLE ČLÁNKU 29

## Pracovní dokument o biometrii

Přijato dne 1. srpna 2003

**Pracovní skupina byla zřízena podle článku 29 Směrnice 95/46/ES.  
Je to nezávislý evropský poradní orgán pro ochranu dat a soukromí.  
Její úkoly jsou stanoveny v článku 30 Směrnice 95/46/ES a v článku 14 Směrnice 97/66/ES.**

Sekretariát poskytuje Evropská Komise, Generální ředitelství pro vnitřní trh,  
Ředitelství E „Služby, duševní a průmyslové vlastnictví,  
médiu a ochrana dat“ - B-1049 Brussels - Belgium – úřadovna: C100-6/136  
**Internetová adresa: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)**

#### PRACOVNÍ SKUPINA PRO OCHRANU JEDNOTLIVCŮ V SOUVIS- LOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená Směrnicí 95/46/ES Evropského parlamentu a Rady  
ze dne 24. října 1995<sup>1)</sup>,

s ohledem na články 29 a 30 odstavec 1 písmeno a) a odsta-  
vec 3 uvedené Směrnice,

s ohledem na svůj jednací řád a zejména na články 12 a 14  
jednacího řádu,

**přijala tento pracovní dokument:**

#### 1. ÚVOD

Rychlý rozvoj biometrických technologií a jejich rostoucí  
uplatňování v posledních letech vyžadují pečlivé zkoumání  
z perspektivy ochrany dat<sup>2)</sup>. Široké a nekontrolované pou-  
žívání biometrie vede k obavám v souvislosti s ochranou  
základních práv a svobod jednotlivců. Tento druh dat má  
zvláštní povahu, protože se vztahuje k charakteristikám cho-  
vání a fyziologie jednotlivce a umožňuje jeho jednoznačnou  
identifikaci<sup>3)</sup>.

Zpracování biometrických dat se nyní často používá při  
automatizovaných postupech autentizace/verifikace a identi-  
fikace, zvláště pro kontrolu vstupu jak do fyzicky existují-  
cích, tak virtuálních oblastí (t.j. přístup k určitým elektronic-  
kým systémům nebo službám).

Dříve se používání biometrie omezovalo především na  
oblast testování DNA a otisků prstů. Shromažďování otisků  
prstů se používalo zvláště pro účely prosazování práva (např.  
vyšetřování trestného činu). Jestliže společnost podporuje  
rozvoj databází otisků prstů nebo jiných biometrických data-  
bází pro další běžné aplikace, může to vést ke zvýšení rizika  
možného opětovného použití třetími stranami jako základ  
pro porovnávání a výzkum v rámci jejich vlastních účelů,  
aniž by cílem byl původně sledovaný záměr; těmito třetími  
stranami mohou být i orgány prosazování práva.

Zvláštní obavu související s biometrickými daty vyvolává  
skutečnost, že veřejnost může rostoucím používáním těchto  
dat znečitlivět vůči vlivům jejich zpracování na každodenní  
život. Například používání biometrie ve školních knihov-

nách může u dětí snížit povědomí o rizicích z hlediska  
ochrany dat, která na ně mohou mít dopad v jejich dalším  
životě.

Účelem tohoto dokumentu je přispět k účinnému a homo-  
gennímu uplatňování vnitrostátních právních předpisů  
o ochraně dat, přijatých v souladu se Směrnicí 95/46/ES, na  
biometrické systémy. Tento dokument je zaměřen především  
na biometrické aplikace pro účely autentizace a verifikace.  
Záměrem Pracovní skupiny je vytvořit jednotná evropská  
pravidla, zejména pro výrobce biometrických systémů a pro  
uživatele těchto technologií.

#### 2. POPIS BIOMETRICKÝCH SYSTÉMŮ

Biometrické systémy jsou aplikace biometrických techno-  
logií, které umožňují automatickou identifikaci a/nebo  
autentizaci / verifikaci určité osoby<sup>4)</sup>. Aplikace pro autenti-  
zaci/verifikaci se často používají pro různé úkoly ve zcela  
odlišných oblastech a v odpovědnosti celé řady různých sub-  
jektů.

1) Úřední věstník č. L 281 ze dne 23. 11. 1995, s. 31, dostupný  
na: [http://europa.eu.int/comm/internal\\_market/privacy/law\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law_en.htm)

2) Po 11. září 2001 byla biometrie často prezentována jako dobrý pro-  
středek pro zlepšení veřejné bezpečnosti. V Evropské unii se vedou  
diskuse o zavedení biometrie do osobních průkazů (ID karet), pasů,  
cestovních dokladů a víz. USA budou brzy vyžadovat biometrické  
identifikátory u cizinců při vstupu do země nebo jejím opuštění.  
Úmluva ILO č. 108 byla upravena v roce 2003 za účelem zavedení  
povinné biometrie u námořníků. Rovněž se vedou diskuse na jiných  
mezinárodních fórech jako G8, OECD atd.

3) Avšak jednoznačná identifikace závisí na různých faktorech včetně  
velikosti databáze a typu použité biometrie.

4) Rozdíl mezi autentizací (verifikací) a identifikací je důležitý.  
Autentizace dává odpověď na otázku: Jsem ta osoba, za kterou  
se vydávám? Systém ověří totožnost osoby zpracováním biome-  
trických dat vztahujících se k osobě, která se ptá a učiní rozhod-  
nutí ano/ne (porovnání 1:1). Identifikace odpovídá na otázku:  
Kdo jsem? Systém rozpoznává jednotlivce, který se ptá, a to tak,  
že ho odliší od ostatních osob, jejichž biometrická data jsou rov-  
něž uchovávána. V takovém případě systém vybere jedno z n  
možných rozhodnutí a odpoví, že osoba, která se ptá, je X.

Každý druh biometrie, ať už pro autentizaci/verifikaci nebo identifikaci, se zakládá ve větší či menší míře na příslušném biometrickém prvku, který je:

- **univerzální:** biometrický prvek existuje u všech osob<sup>5)</sup>;
- **jedinečný:** biometrický prvek musí každou osobu odlišovat;
- **a stálý:** každá osoba si v průběhu času biometrický prvek trvale uchovává.

Lze rozlišovat mezi dvěma hlavními kategoriemi biometrických postupů, podle toho, zda používají stabilní data nebo dynamická data charakterizující chování<sup>6)</sup>.

V prvním případě jde o postupy založené na fyzických a fyziologických aspektech, které měří fyziologické vlastnosti osoby a zahrnují: verifikaci otisku prstu, analýzu obrazu prstu, rozpoznávání duhovky, analýzu sítnice, rozpoznávání obličeje, geometrii ruky, rozpoznávání tvaru ucha, detekci pachu těla, rozpoznávání hlasu, analýzu vzorku DNA<sup>7)</sup> a analýzu potních pórů, atd.

V druhém případě existují postupy založené na **rysech chování**, které měří chování osoby a zahrnují verifikaci vlastnoručního podpisu, analýzu stisku tlačítek, analýzu způsobu chůze, atd.

Vezmeme-li v úvahu rychlý technický vývoj a zvýšenou obavu o bezpečnost, pracuje mnoho biometrických systémů tak, že kombinují různé biometrické znaky uživatele s jinými technologiemi identifikace nebo autentizace. Některé systémy například kombinují rozpoznávání obličeje a zaznamenávání hlasu. Pro provedení autentizace lze použít společně tři rozdílné metody – metodu založenou na něčem, co jednotlivce zná (heslo, PIN, atd.), metodu založenou na něčem, co jednotlivce vlastní (rozlišovací známka, klíč CAD, čipová karta, atd.) a metodu založenou na něčem, co jednotlivce je (biometrický rys). Například u jednoho počítače lze vložit čipovou kartu, napsat heslo a provést otisk prstu.

Shromažďování biometrických vzorků, takzvaných biometrických dat (např. obraz otisku prstu, obraz duhovky nebo sítnice, záznam hlasu), se provádí během fáze nazývané „zápis“ za použití senzoru specifického pro každý typ biometrického znaku. Biometrický systém vybírá z biometrických dat rysy specifické pro jednotlivce, aby pak vytvořil biometrickou „šablonu“. Tato šablona je strukturovanou redukcí biometrického obrazu: zaznamenané biometrické měření jednotlivce. Je to právě tato šablona, prezentovaná v digitalizované formě, která se uchovává a nikoli biometrický prvek samotný. Navíc biometrická data mohou být zpracovávána jako hrubá data (obraz) v závislosti na fungování použitého biometrického systému<sup>8)</sup>.

Fáze zápisu hraje klíčovou úlohu, protože jen během ní jsou současně přítomny hrubé údaje, výběrové a ochranné algoritmy (kryptografie, hašování atd.) a šablony. V tomto ohledu je třeba zdůraznit, že pokud hrubá data odhalují informaci, kterou lze považovat za citlivou ve smyslu článku 8 Směrnice 95/46/ES, pak proces zápisu takového údaje by měl být v souladu s tímto ustanovením (viz níže uvedený bod 3.7).

Další otázka, která je také důležitá z hlediska ochrany dat, je forma uchovávání šablon uživatelů. Ta závisí na typu aplikace, pro kterou se bude biometrické zařízení používat a na

velikosti šablon samotných. Šablony mohou být uchovávány jedním z následujících způsobů:

- a) v paměti biometrického zařízení;
- b) v centrální databázi;
- c) na plastových kartách, optických kartách nebo čipových kartách. Tento způsob uchovávání údajů umožňuje uživateli nosit své šablony při sobě jako identifikační prostředek.

V podstatě není nezbytné pro účely autentizace/verifikace uchovávat referenční data v databázi; postačuje uchovávat osobní údaje decentralizovaně. Naopak identifikace může být provedena pouze při uchování příslušných údajů v centralizované databázi, protože systém, aby ověřil totožnost subjektu údajů, musí porovnat jeho/její šablony nebo hrubá data (obraz) se šablonami nebo hrubými daty všech osob, jejichž data jsou již centrálně uchovávána.

Další bod, který je z hlediska ochrany dat rozhodující, je skutečnost, že některé biometrické systémy jsou založeny na informacích jako například otisky prstů nebo vzorky DNA, které mohou být shromažďovány bez vědomí subjektu údajů, jelikož tento subjekt může nevědomě zanechat stopy. Při použití biometrických algoritmů na otisk prstu nalezený na sklenici by někdo mohl být schopen<sup>9)</sup> porovnáním dvou šablon zjistit, zda osoba je v souboru v databázi obsahující biometrická data, a pokud ano, kdo to je. To se rovněž týká ostatních biometrických systémů, jako například systémů založených na analýze stisku kláves nebo dálkovém rozpoznávání obličeje, v závislosti na specifických rysech použité technologie<sup>10)</sup>. Problematickým aspektem na jedné straně je, že toto shromažďování dat a jejich zpracování lze provádět bez vědomí subjektu údajů a na straně druhé, že bez ohledu na jejich aktuální spolehlivost se tyto biometrické technologie hodí k všeobecnému používání vzhledem k nízké úrovni jejich „invazivnosti“. Proto se ukazuje jako nezbytné stanovit pro ně zvláštní záruky.

### 3. POUŽITÍ ZÁSAD SMĚRNICE 95/46/ES

#### 3.1. Použití Směrnice 95/46/ES

Článek 2 a) Směrnice 95/46/ES definuje „osobní údaje“ jako „veškeré informace týkající se identifikované nebo

- 5) *V tomto ohledu nejsou všechny biometrické prvky rovnocenné a míra odlišení jedné osoby od jiné je velmi rozdílná podle typu použité biometrie. Nejlépe rozlišitelnými biometrickými prvky se zdají být DNA, sítnice a otisk prstu.*
- 6) *Některé postupy mohou být založeny jak na fyziologii tak na charakteristikách chování.*
- 7) *Ačkoli použití DNA pro biometrickou identifikaci vyvolává specifické problémy, tento dokument se jimi nezabývá. Lze uvést, že vytvoření profilu DNA v reálném čase jako autentizačního nástroje se zdá být v současné době nemožné.*
- 8) *Tento dokument se vztahuje především na biometrické systémy založené na šablonách a může být rovněž použit na hrubá data. Avšak specifická hrubých dat může vést k přizpůsobení požadavků na ochranu dat.*
- 9) *To však znamená mít alespoň určité prostředky, jako je schopnost sejmout otisk prstu ze sklenice bez jeho poškození, technické zařízení na zpracování dat z otisků prstů, přístup k algoritmu tvůrce databáze a/nebo k databázi otisků prstů.*
- 10) *Viz bod 3 o použití Směrnice 95/46/ES a zejména bod 3.3., o povinnosti informovat subjekt údajů.*

identifikovatelné fyzické osoby (...); identifikovatelná osoba je ta, která může být identifikována přímo nebo nepřímo, především na základě identifikačního čísla nebo jednoho či více prvků specifických pro její fyzickou, fyziologickou, mentální (...) identitu“. Bod 26 preambule připojuje následující výklad: „pro určení, zda je osoba identifikovatelná, je třeba přihlídnout ke všem prostředkům, které mohou být rozumně použity buď správcem nebo jakoukoli jinou osobou pro identifikaci dané osoby“.

V souladu s touto definicí jsou hodnoty naměřené při biometrické identifikaci nebo jejich digitální převod do formy šablony ve většině případů osobní údaje<sup>11)</sup>. Zdá se, že biometrická data mohou být vždy považována za „údaje týkající se fyzické osoby“ protože jde o data, která poskytují ve své podstatě informace o dané osobě. V souvislosti s biometrickou identifikací je osoba všeobecně identifikovatelná, jelikož biometrická data jsou používána pro identifikaci nebo autentizaci/verifikaci alespoň v tom smyslu, že subjekt údajů je odlišený od kohokoli jiného<sup>12)</sup>.

Podle článku 3, odst. 1 Směrnice 95/46/ES se zásady ochrany údajů použijí na zpracování osobních údajů zcela nebo částečně automatizovaná a na jiná než automatizovaná zpracování osobních údajů, které jsou nebo se mají stát součástí uspořádaného systému. Směrnice se nepoužije, pokud jsou data zpracovávána fyzickou osobou výlučně v rámci osobní nebo domácí činnosti. Mnoho biometrických aplikací v domácím užívání bude spadat do této kategorie.

Mimo těchto specifických výjimek může být zpracování biometrických dat považováno za zákonné jenom tehdy, jestliže jsou všechny příslušné postupy – počínaje zápisem – prováděny v souladu s ustanoveními Směrnice 95/46/ES.

Tento dokument nezahrnuje všechny otázky vyvstávající při aplikaci Směrnice 95/46/ES na biometrická data. Spíše se zabývá pouze těmi nejdůležitějšími z nich, a neposkytuje tak vyčerpávající pohled na důsledky použití Směrnice 95/46/ES.

### 3.2. Zásada účelu a proporcionality

Podle článku 6 Směrnice 95/46/ES musejí být osobní údaje shromažďovány pro stanovené, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Kromě toho musejí být osobní údaje přiměřené, relevantní a míru nepřesahující s ohledem na účely, pro které jsou shromažďovány a dále zpracovávány (zásada účelu).

Dodržování této zásady předpokládá nejprve jasné vymezení účelu, pro který jsou biometrická data shromažďována a zpracovávána. Dále je nezbytné vyhodnotit dodržování zásady proporcionality a dodržování legitimitnosti s přihlédnutím k rizikům pro ochranu základních práv a svobod jednotlivců a především k tomu, zda lze nebo nelze dosáhnout záměru méně obtěžujícím způsobem. Proporcionalita byla hlavním kritériem téměř u všech rozhodnutí týkajících se zpracování biometrických údajů, dosud přijatých orgány pro ochranu dat.<sup>13)</sup>

Pokud jde o kontrolu přístupu (autentizaci/verifikaci), Pracovní skupina je toho názoru, že biometrické systémy týkající se fyzických charakteristik, které nezanechávají stopy (např. tvar ruky, ne však otisky prstů) nebo biometrické systémy

týkající se fyzických charakteristik, které zanechávají stopy, ale neopírají se o ukládání do paměti těch dat, která jsou v držení někoho jiného než dotyčného jednotlivce (jinými slovy, data nejsou ukládána do zařízení pro kontrolu přístupu nebo do centrální databáze) vytvářejí méně rizik pro ochranu základních práv a svobod jednotlivců<sup>14)</sup>. Některé orgány pro ochranu dat schválily toto stanovisko a konstatovaly, že biometrická data by pokud možno neměla být ukládána do databáze, ale pouze na předměty, kterými výlučně disponuje uživatel, jako je mikročipová karta, mobilní telefon, bankovní karta<sup>15)</sup>. Jinými slovy, aplikace autentizace/verifikace, které mohou fungovat bez centrálního uchovávání biometrických dat, by neměly používat nadbytečné identifikační postupy.

Proto se Pracovní skupina domnívá, že použití jiných typů aplikací (tj. založených na digitálních šablonách otisků prstů v terminálu nebo v centrální databázi) by mělo být pečlivě posouzeno dříve, než budou takové aplikace nasazeny. Pokud však bude tento typ systému zaváděn, například v případech jako jsou zařízení s vysokým stupněm bezpečnosti<sup>16)</sup>, může to být považováno za zpracování dat přinášející rizika ve smyslu článku 20 Směrnice 95/46/ES a podléhající předchozí kontrole ze strany orgánů pro ochranu dat v souladu s vnitrostátními právními předpisy (viz bod 3.5).

Směrnice 95/46/ES zakazuje další zpracování, které by bylo neslučitelné s účelem, pro který byla data shromažďována. Například jsou-li biometrická data zpracovávána pro účely kontroly přístupu, použití těchto dat k posouzení emocionálního stavu subjektu údajů nebo pro sledování na pracovišti by nebylo slučitelné s původním účelem shromažďování. Musejí být učiněna všechna opatření, aby se předešlo takovému neslučitelnému opětnému použití<sup>17)</sup>. Směrnice 95/46/ES stanovuje výjimky ze zákazu dalšího zpracování dat pro neslučitelné účely, vztahují se však na ně zvláštní podmínky.

11) V případech, kde biometrická data, jako šablona, jsou uchovávána způsobem, kdy správce nebo jakákoli jiná osoba nemohou použít žádné rozumné prostředky pro identifikaci subjektu údajů, neměla by tato data být považována za osobní údaje.

12) Identifikovatelnost osoby rovněž závisí na dostupnosti dalších dat, která - dohromady nebo samostatně - umožňují příslušnou osobu identifikovat. Možnost „přímé identifikace“ pomocí „jednoho nebo více prvků specifických pro její fyzickou identitu“ je výslovně uvedeno v definici osobních údajů v článku 2a Směrnice 95/46/ES.

13) Rozhodnutí například nizozemských, francouzských, německých, italských a řeckých orgánů.

14) Lze rozlišit případ, kdy jsou biometrická data zpracovávána centrálně, od případu, kdy jsou příslušná biometrická data uchovávána na mobilním zařízení a proces porovnávání probíhá na kartě, ale ne na senzoru nebo kdy senzor je dokonce součástí mobilního zařízení.

15) Měly by se vzít v úvahu mechanismy pro řešení problémů vzniklých v důsledku ztráty, odcizení nebo poškození karet a měly by se prosazovat ty, které nevedou k uchovávání biometrických dat. Tam, kde je to možné, by data měla být získána opět přímo od subjektu údajů.

16) Současný stav biometrické technologie je takový, že spolehlivá a čistá řešení identifikace okruhu osob reálného rozsahu v reálném čase dosud ještě neexistují a není pravděpodobné, že nějaká budou k dispozici v dohledné budoucnosti.

17) Jak je uvedeno výše, tento účel musí být jasně stanoven.

Je všeobecně přijímáno, že riziko opětovného použití biometrických dat, získaných z fyzických stop nevědomě zanechaných jednotlivci (například otisků prstů), pro neslučitelné účely je relativně nízké, pokud data nejsou uchovávána v centralizovaných databázích, nýbrž zůstávají u dané osoby a jsou nedostupná třetí straně. Centralizované uchovávání biometrických dat rovněž zvyšuje riziko použití biometrických dat jako klíče k propojení různých databází, což by mohlo vést k vytvoření podrobných profilů zvyklostí jednotlivce jak ve veřejném, tak v soukromém sektoru. Mimoto otázka slučitelného účelu vyvolává otázku interoperability různých systémů používajících biometrii. Nezbytná standardizace interoperability by mohla vést k většímu vzájemnému propojování databází.

Použití biometrie dále vyvolává otázku proporcionality jednotlivých kategorií zpracovávaných dat z hlediska účelu, pro který jsou data zpracovávána. Biometrická data mohou být používána, pouze pokud jsou přiměřená, relevantní a míru nepřesahující. To vyžaduje přísné posouzení nezbytnosti a proporcionality zpracovávaných dat<sup>18)</sup>. Například francouzský CNIL zamítl používání otisků prstů v případě vstupu dětí do školní jídelny,<sup>19)</sup> ale schválil pro stejný účel použití geometrie ruky. Portugalský úřad pro ochranu dat nedávno vydal nepříznivé rozhodnutí ve věci použití biometrického systému (otisku prstu) na jedné univerzitě, kterým se měla kontrolovat výkonnost a dochvilnost zaměstnanců nepatřících mezi vyučující personál<sup>20)</sup>. Německý úřad pro ochranu dat vynesl kladné rozhodnutí k zavedení biometrických charakteristik do identifikačních dokumentů za účelem prevence jejich falzifikace, s podmínkou, že data budou uchovávána v mikročipu karty a ne v databázi pro porovnávání s otisky prstů držitele.

Zvláštní potíž může vyvstat v důsledku toho, že biometrická data často obsahují více informací, než které jsou nezbytné pro funkce identifikace nebo autentizace/verifikace. To je mnohem pravděpodobnější v případě, kdy se jedná o originální obraz (hrubá data), protože šablona může a měla by být technicky konstruována způsobem vylučujícím zpracování dat, která nejsou nezbytná. Nepotřebná data by měla být zlikvidována co možná nejdříve<sup>21)</sup>. Kromě toho některá biometrická data mohou odhalit rasový původ nebo se týkají zdravotního stavu (viz níže bod 3.7.).

A konečně by mělo být zmíněno, že používání biometrických systémů by mělo být koncipováno takovým způsobem, aby mohly být považovány za technologie na podporu ochrany soukromí, mimo jiné proto, že mohou omezit rozsah zpracování jiných osobních údajů, jako jména, adresy, bydliště atd.

### 3.3. Korektní shromažďování a informování subjektu údajů

Zpracování biometrických dat a zejména jejich shromažďování by mělo být prováděno korektně<sup>22)</sup>. Správce by měl informovat subjekt údajů v souladu s články 10 a 11 Směrnice 95/46/ES<sup>23)</sup>. To zahrnuje zejména přesné vymezení účelu a totožnosti správce souboru dat (což bude často osoba provozující biometrický systém nebo používající biometrické postupy).

Systémů, které shromažďují biometrická data bez vědomí subjektů údajů, je nutno se vyvarovat. Některé biometrické systémy, jako dálkové rozpoznávání obličeje, shromažďování otisků prstů nebo tajné nahrávání hlasu, představují v tomto směru větší riziko.

### 3.4. Kritéria pro legitimní zpracování dat

Zpracování biometrických dat musí být založeno na jednom z předpokladů legitimacy stanoveném v článku 7 Směrnice 95/46/ES. Pokud správce souboru dat používá souhlas jako podklad legitimacy, Pracovní skupina zdůrazňuje, že musejí být dodrženy podmínky stanovené v článku 2 Směrnice 95/46/ES (jakýkoli svobodný a informovaný projev vůle, kterým dává subjekt údajů najevo svůj souhlas s tím, aby osobní údaje, které se ho týkají, byly zpracovávány).

### 3.5. Předběžná kontrola - oznamování

Jak již bylo uvedeno dříve, Pracovní skupina podporuje používání biometrických systémů, které neuchovávají stopy v paměti terminálu přístupového zařízení, ani je neukládají do centrální databáze (viz bod 3.2.). Pokud je však záměr takové systémy používat a s přihlédnutím k riziku použití nebo opětovného použití pro odlišné účely, jakož i s přihlédnutím k zvláštním nebezpečím v případě neoprávněného přístupu, Pracovní skupina doporučuje, aby členské státy vzaly v úvahu možnost podrobit je předběžné kontrole orgány pro ochranu dat v souladu s ustanovením článku 20 Směrnice 95/46/ES, protože tento druh zpracování pravděpodobně představuje specifická rizika pro práva a svobody subjektů údajů. Jestliže členské státy hodlají zavést předběžnou kontrolu týkající se zpracování biometrických dat, měly by konzultace s národními orgány pro ochranu dat proběhnout ještě před zavedením takových opatření.

18) *Mimoto, za určitých okolností, musí i nadále zůstat zachována anonymita nebo možnost použití pseudonymů. V této souvislosti je třeba vzít v úvahu mechanismy pro řešení problémů vzniklých v důsledku ztráty, odcizení nebo poškození karet a měly by se prosazovat ty mechanismy, které nevedou k uchovávání biometrických dat. Tam kde je to možné, by data měla být získána opět přímo od subjektu údajů.*

19) *Ukazuje se však, že orgán pro ochranu dat ve Spojeném království přistoupil na používání otisků prstů za podobných okolností tam, kde byla zavedena přiměřená ochranná opatření.*

20) *Portugalský úřad pro ochranu dat zastává názor, že použití takových systémů je neproporcionální a nadbytečné z hlediska účelu zpracování údajů. Systém by uchovával tato data v biometrickém zařízení a základní soubor kontrolovaných by čítal přibližně 140 osob.*

21) *Tuto likvidaci rovněž podporuje článek 6, 1, e) Směrnice 95/46/ES, který vyžaduje uchovávat osobní údaje po dobu ne delší, než je nezbytné pro účely, pro které jsou data zpracovávána.*

22) *Článek 6 (a) Směrnice 95/46/ES.*

23) *Výjimky z povinnosti informovat subjekty údajů podle článků 10 a 11 Směrnice 95/46/ES by se měly zakládat na legislativních opatřeních a současně by měly vytvářet opatření nezbytné pro omezení rozsahu informační povinnosti při zabezpečení zájmů uvedených v článku 13 Směrnice 95/46/ES (veřejná bezpečnost, prevence, vyšetřování, odhalování a stíhání trestných činů, atd.).*

### 3.6. Bezpečnostní opatření

Správce musí v souladu s ustanoveními článku 17 Směrnice 95/46/ES přijmout veškerá vhodná technická a organizační bezpečnostní opatření na ochranu osobních údajů proti náhodnému nebo nezákonnému zničení nebo náhodné ztrátě, změně, neoprávněnému prozrazení nebo přístupu, zejména pokud zpracování zahrnuje předávání biometrických dat po síti. Bezpečnostní opatření musejí být učiněna, jestliže jsou biometrická data zpracovávána (uchovávání, předávání, výběr charakteristik a porovnávání, atd.) a zejména, když správce předává takové údaje prostřednictvím Internetu. Kromě kontroly přístupu a ochrany, která skutečně znemožní rekonstruovat původní data ze šablon, by bezpečnostní opatření mohla zahrnovat například kódování šablony a ochranu kódovacích klíčů.

V této souvislosti by měly být vzaty v úvahu některé nové technologie. Zajímavým vývojovým krokem je možnost použití biometrických dat jako kódovacích klíčů. To by *a priori* vytvářelo menší riziko pro subjekt údajů, protože dekódování může být provedeno pouze na základě nového sběru biometrických dat od subjektu údajů samotného, a tak se lze vyhnout vytváření databází obsahujících šablony biometrických dat, u kterých existuje možnost jejich opětovného použití pro nesouvisející účely.

Nezbytná bezpečnostní opatření by měla být zavedena od počátku zpracování, a zvláště pak během fáze „zápisu“, kde jsou biometrická data převáděna na šablony nebo obrazy. Je třeba pochopit, že jakákoli ztráta rysů integrity, důvěrnosti a dostupnosti v souvislosti s určitými databázemi, by zjevně neblaze ovlivnila všechny budoucí aplikace založené na informacích obsažených v takových databázích, a zároveň by způsobila nenapravitelnou škodu subjektům údajů. Kdyby například otisky prstů oprávněného jednotlivce byly přiřazeny k totožnosti jednotlivce neoprávněného, mohl by posledně jmenovaný mít přístup k službám dostupným vlastníkovvi otisku prstu, aniž by k tomu byl oprávněn. To by mohlo vést ke krádeži identity, což by, bez ohledu na to, zda bude nebo nebude odhalena, učinilo otisky prstů jednotlivce nespolehlivými pro budoucí použití a tím by omezilo jeho svobodu.

Chyby, které se vyskytnou v biometrických systémech mohou mít vážné důsledky pro jednotlivce a zejména chybné odmítnutí oprávněných osob a chybné přijetí neoprávněných osob může způsobit vážné problémy na mnoha různých úrovních. *A priori* by použití biometrických dat mělo snížit riziko takových chyb. Avšak rovněž by mohlo vyvolat zdání, že identifikace nebo autentizace/verifikace subjektu údajů je vždy správná. Subjekt údajů může shledat jako obtížné nebo dokonce nemožné prokázat opak. Systém může například mylně identifikovat subjekt údajů jako někoho, komu by nemělo být povoleno použít letadlo nebo vstoupit do určité země, a ten by pak měl velmi omezené prostředky, jak čelit problému s takovým, proti němu namířeným „nesporným“ důkazem. Pro tyto případy by mělo být znovu zdůrazněno, že jakékoli rozhodnutí, které má právní dopad na jednotlivce, by mělo být učiněno až po potvrzení výsledku automatizovaného zpracování v souladu s článkem 15 Směrnice 95/46/ES.

Nakonec by mělo být zmíněno, že použití biometrie by

mohlo zdokonalit kontrolní postupy například v případě přístupu k osobním údajům týkajících se třetích stran, například v případě krádeže nebo zneužití (autorizační postupy).

### 3.7. Citlivé údaje

Některá biometrická data by mohla být pokládána za citlivá ve smyslu článku 8 Směrnice 95/46/ES, a to zejména data vypovídající o rasovém nebo etnickém původu nebo data o zdravotním stavu. Například u biometrických systémů založených na rozpoznávání obličeje mohou být zpracovávána data vypovídající o rasovém nebo etnickém původu. V takových případech se kromě obecně závazných zásad Směrnice použijí zvláštní ochranná opatření podle článku 8.

To neznamená, že každé zpracování biometrických dat bude nezbytně zahrnovat citlivé údaje. Zda zpracování obsahuje citlivé údaje, je otázkou posouzení v závislosti na použité specifické biometrické charakteristice a biometrické aplikaci samotné. Je mnohem pravděpodobnější, že tomu tak bude v případě, kdy se zpracovávají biometrická data ve formě obrazů, jelikož ze šablony v zásadě nemůže být provedena rekonstrukce hrubých dat.

### 3.8. Jednoznačný identifikátor

Biometrická data jsou jedinečná a většina z nich vytváří unikátní šablonu (nebo obraz). Při širokém používání, zejména týkají-li se značné části populace, lze biometrická data považovat za identifikátor obecně použitelný ve smyslu Směrnice 95/46/ES. Pak by bylo možno použít článek 8, odst. 7 Směrnice 95/46/ES a členské státy by musely stanovit podmínky pro jejich zpracování.

Kde jsou biometrická data určena k použití jako klíč k propojování databází obsahujících osobní údaje<sup>24)</sup>, mohou zvláště závažné problémy nastat vždy, když subjekt údajů nemá žádnou možnost vznést námitku proti zpracování biometrických dat. To může obvykle nastat ve vztazích mezi občany a veřejnými orgány.

V tomto směru by bylo žádoucí, aby šablony a jejich digitální vyjádření byly zpracovávány matematickými operacemi (kódování, algoritmy nebo hašovací funkce), za použití různých parametrů pro každý používaný biometrický produkt, aby se zabránilo kombinaci osobních údajů z několika databází cestou porovnávání šablon nebo digitálních vyjádření.

### 3.9. Etické kodexy a použití technologie na podporu soukromí

Pracovní skupina vyzývá výrobce, aby vytvářeli biometrické systémy, které usnadní provádět doporučení obsažená v tomto pracovním dokumentu, a pokud budou vyvíjeny evropské nebo mezinárodní standardy, měly by být vypracovávány ve spolupráci s orgány pro ochranu dat v zájmu podpory biometrických systémů koncipovaných způsobem „přátelským“ k ochraně dat, minimalizujícím sociální rizika a předcházejícím zneužití biometrických dat. Pracovní skupina v této souvislosti zdůrazňuje význam technologií na podporu soukromí (Privacy Enhancing Technologies, PET) s cílem minimalizovat shromažďování dat a zabránit nezákonnému zpracování.

24) Viz také výše bod 3.2 o kompatibilním opětovném použití.

Dále Pracovní skupina podtrhuje význam etických kodexů, které mají přispívat k náležitému provádění zásad ochrany dat s přihlédnutím ke zvláštním rysům různých sektorů v souladu s článkem 27 Směrnice 95/46/ES. Etické kodexy ze Společenství je možné předkládat Pracovní skupině, která mimo jiné rozhodne, zda jsou předložené návrhy v souladu s ustanoveními vnitrostátních právních předpisů o ochraně dat, přijatých podle Směrnice 95/46/ES.

#### **ZÁVĚRY**

Pracovní skupina zastává názor, že většina biometrických dat je spojena se zpracováním osobních údajů. Je proto nezbytné při vývoji biometrických systémů plně dodržovat zásady ochrany dat stanovené Směrnicí 95/46/ES s přihlédnutím ke zvláštní povaze biometrie, mimo jiné k možnosti shromažďovat biometrická data bez vědomí subjektu údajů a ke skutečnosti, že je lze téměř s jistotou přiřadit k jednotlivci.

Dodržování zásady proporcionality, která tvoří jádro ochrany zajištěné Směrnicí 95/46/ES, vede, zvláště v souvislosti s autentizací/verifikací, k jasnému upřednostnění biometrických aplikací, které nezpracovávají data získaná

z tělesných stop nevědomě zanechaných jednotlivci nebo u kterých nejsou data uchovávána v centralizovaném systému. To umožňuje subjektu údajů lépe provádět kontrolu zpracovávaných osobních údajů, které se ho týkají.

Pracovní skupina má v úmyslu přezkoumat tento pracovní dokument s ohledem na zkušenosti orgánů pro ochranu dat a na výsledky technologického vývoje souvisejícího s biometrickými aplikacemi. Jelikož biometrická data jsou již v současné době zaváděna k širokému využití v řadě různých oblastí, bude nezbytné neprodleně provést další práce, zvláště v souvislosti se zaměstnáním, vízy a přistěhovalectvím a bezpečností cestování.

Ačkoli odpovědnost za vývoj biometrických systémů vyhovujících požadavkům na ochranu dat spočívá na výrobcích, byl by ve všech směrech prospěšný pracovní dialog zejména na základě návrhu etického kodexu mezi všemi zainteresovanými stranami včetně orgánů pro ochranu dat.

V Bruselu dne 1. srpna 2003  
Za Pracovní skupinu  
*předseda*  
Stefano RODOTÀ



---

## Věstník Úřadu pro ochranu osobních údajů

**Vydavatel:** Úřad pro ochranu osobních údajů

**Adresa redakce:** Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7

**Šéfredaktor:** Bohumír Lukaj, tel.: 234 665 484, fax: 234 665 505

e-mail: [info@uoou.cz](mailto:info@uoou.cz)

internetová adresa: [www.uoou.cz](http://www.uoou.cz)

**Administrace:** Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, [www.sevt.cz](http://www.sevt.cz), e-mail: [sevt@sevt.cz](mailto:sevt@sevt.cz). – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 700 Kč – Vychází podle potřeby – **Tiskne:** BESTia s. r. o., Na pískách 140, Praha 6.

**Distribuce:** Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 5, Elišky Peškové 14, tel./fax: 257 320 049, – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962 – Ostrava, Nádražní 29, tel.: 596 120 690 – České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. **Distribuční podmínky předplatného:** Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnícká osoba) a kmenové číslo předplatitele. **Podávání novinových zásilek** povoleno ŘPP Praha.

ISSN 1213-3442