



VĚSTNÍK

ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

2002

Částka 19

4. září 2002

Cena 70 Kč

OBSAH

Úvod	1558
------------	------

I. Registrace

Abecední seznam zaregistrovaných subjektů v období od 4. 7. 2002 do 22. 8. 2002	1559
---	------

Přehled povolených zpracování osobních údajů zaregistrovaných Úřadem v období od 4. 7. 2002 do 22. 8. 2002	1562
--	------

Přehled registrací zrušených v období od 4. 7. 2002 do 22. 8. 2002	1586
--	------

II. Stanoviska Úřadu

Stanovisko č. 1/2002: Zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče	1587
---	------

III. Sdělení Úřadu

Doporučení č. R (97) 5 Výboru ministrů členským státům o ochraně zdravotních údajů	1589
---	------

Elektronický podpis Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku	1595
Požadavky na kryptografické funkce	1595

Ověření bezpečnosti informačního systému pro certifikační služby z hlediska požadavků § 6 písm. c) vyhlášky č. 366/2001 Sb.	1595
---	------

Usnesení Ústavního soudu	1598
--------------------------------	------

ÚVOD

V devatenácté části Věstníku je publikován přehled povolených zpracování osobních údajů v období od 4. 7. 2002 do 22. 8. 2002 a rovněž přehled zrušených registrací v tomto období. Ve Stanovisku č. 1/2002 se Úřad vyslovuje k problematice zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče. Zabývá se vztahem zákona o ochraně osobních údajů jakožto obecným právním předpisem a zvláštními právními předpisy, z nichž základním je zákon o péči o zdraví lidu. Dále pojednává o právu subjektu údajů na informace vedené o jeho osobě ve zdravotnické dokumentaci a o problematice zpracovávání osobních údajů v souvislosti s prováděním klinického hodnocení a postmarketingového sledování léčiv. V dalším z publikovaných doporučení Rady Evropy – č. R (97) 5, o ochraně zdravotních údajů, se lze seznámit s obecnými zásadami pro zpracování osobních údajů v této oblasti. V části věnované elektronickému podpisu upřesňujeme požadavky Úřadu, které byly publikovány ve Věstníku č. 12/2001, a zveřejňujeme dokument, který je výkladem vyhlášky č. 366/2001 Sb. z hlediska ověřování bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují. Vzhledem k poměrně častým dotazům veřejnosti na vývoj soudního sporu mezi Úřadem pro ochranu osobních údajů a Českým statistickým úřadem, jehož předmětem je stanovení rozsahu údajů shromažďovaných a dále zpracovávaných při sčítání lidu, domů a bytů v roce 2001 a likvidace dvou údajů zpracovávaných nad rámec zákona č.158/1999 Sb., zveřejňujeme usnesení Ústavního soudu v tomto sporu.

I. REGISTRACE

Abecední seznam zaregistrovaných subjektů v období od 4. 7. 2002 do 22. 8. 2002

Identifikace	Č. reg.	Identifikace	Č. reg.
ADAMCOVÁ HELENA	00016724	GERYCHOVÁ ALENA , 14.04.1938	00016831
ALFA FINANCE S.R.O.	00016496	GRAZOVÁ ELIŠKA	00016835
ASKLEPIADÉ, S.R.O.	00016633	GRÉZL JAN	00016733
ASOCIACE PĚT P V ČR	00016709	GRÉZLOVÁ SYLVA	00016734
ASOCIACE RODIČŮ A PŘÁTEL ZDRAVOTNĚ POSTIŽENÝCH DĚTÍ V ČR, KLUB ROSNIČKY	00016550	H 2 PLUS SPOL. S R.O.	00016714
ASOCIACE RODIČŮ A PŘÁTEL ZDRAVOTNĚ POSTIŽENÝCH DĚTÍ V ČR- KLUB HAVLÍČKŮV BROD	00016759	HABARTA PAVEL - POHŘEBNÍ SLUŽBY	00016764
ATEXINGEROVÁ DANA	00016544	HANZLÍK MIROSLAV	00016848
AUTO HOLÝ S.R.O.	00008190	HANZLÍKOVÁ ZLATUŠE ING.	00016847
AUTO SAEL, S.R.O.	00016540	HAROKOVÁ RŮŽENA , 06.02.1936	00016693
AVENTO S.R.O.	00016511	HAVLÍKOVÁ DANA , 28.10.1965	00016777
BAČA JIŘÍ	00016636	HERMANOVÁ JANA , 24.07.1956	00016778
BARVY TEBAS S.R.O.	00016705	HLAVINKOVÁ LENKA	00016852
BAUMAX ČR A.S.	00016804	HOCHMAL LUBOŠ , 07.07.1970	00016770
BECARIO, SDRUŽENÍ MIRKA TOPOLÁNKA PRO ROZVOJ VZDĚLANOSTI	00016771	HOLVER STAR, S.R.O.	00016564
BEDY A.S.	00016505	HONEBNÍ SPOLEČENSTVO HANUŠOVICE	00016849
BENEFICIAL FINANCE A.S.	00016531	HOŠTÁK JAN	00016781
BĚTIKOVÁ JITKA , 25.06.1974	00016801	HOŠTÁKOVÁ VĚRA	00016782
BIMKA JAROSLAV , 27.03.1943	00016798	HRABÁKOVÁ JANA ING., 29.10.1940	00016507
BIRNBAUMOVÁ JARMILA , 19.02.1970	00016517	HRANČÍK MIROSLAV , 20.01.1963	00016837
BLAHUTOVÁ DANA BC.	00016703	HRDLÍČKOVÁ MILENA , 23.08.1977	00016553
BRATRSKÁ ŠKOLA CÍRKEVNÍ ZÁKLADNÍ ŠKOLA	00016528	HUTNICKÁ ZAMĚSTNANECKÁ POJIŠŤOVNA	00004062
BRAVENÝ TOMÁŠ ING.	00016524	CHARVÁTOVÁ JANA	00016726
BŘEZÁK KAREL	00016510	INTEGRA CENTRUM S.R.O.	00016513
BŘEZINA LUBOMÍR , 23.04.1959	00016711	INTERBIS COMMUNICATIONS S.R.O.	00016750
BYTOVÉ DRUŽSTVO MALEŠICKÁ 4-10	00016688	INTERBIS TECHNOLOGIES S.R.O.	00016751
CANDRA MIROSLAV MGR.	00016491	JANELE JAN , 18.10.1956	00016742
COLOSSEUM, A.S.	00016649	KAHÁNEK BOHUSLAV ING.	00016520
COMENIUS, OBČANSKÉ SDRUŽENÍ	00016790	KAHÁNEK IGOR	00016519
CZ.BAT S.R.O.	00016773	KALINOVÁ DANUŠE , 21.02.1967	00016509
ČEČRLOVÁ JANA	00016532	KAŠPAR JIŘÍ ING.	00016784
ČEPRO, A.S.	00016737	KELEMEN S. R. O.	00016588
ČERNÁ DITA	00016562	KOBILÁK ZDENĚK	00016608
ČESKÝ TELECOM, A.S.	00001949	KOMERČNÍ BANKA, A.S.	00007256
ČESKÝ VÝBOR PRO UNICEF	00016669	KOROTVIČKA MIROSLAV , 11.11.1966	00016753
DAPAMED, A.S.	00016830	KORTUS PETR ING., 02.06.1967	00016609
DLOUHÁ IVANA MGR.	00016552	KOSTŘICA JIŘÍ MVDR.	00016869
DLOUHÝ JAROSLAV	00016554	KOTMELOVÁ JANA	00016492
DOLEŽELOVÁ MILADA	00016728	KOTVA NEMOVITOSTI, A.S.	00016504
DROBEČKOVÁ VĚRA , 26.02.1971	00016673	KOUBA JIŘÍ ING.	00016825
DUEL SERVICES EUROPE A.S.	00016699	KOVOPOL RT S.R.O.	00016551
DYS-CENTRUM	00016570	KRÁLOVÁ MAGDALENA ING.	00016589
ED. HAAS CZ S.R.O.	00016729	KRÁLOVÁ MILADA , 08.01.1958	00016695
EKOLAK S. R. O.	00016668	KRAUSOVÁ JIŘINA , 29.06.1964	00016639
ENVINET A.S.	00016876	KROPÁČOVÁ JANA ING., 25.07.1941	00016568
EURORESTA PRAHA S. R. O.	00016631	KUKAČKOVÁ JITKA ING.	00008103
EUROTEL PRAHA, SPOL. S R.O.	00001302	KULÍŠEK JAROSLAV	00016763
FAMKO SPOL.S R.O.	00016696	KULTURNÍ KLUB URČICE	00016756
FANTA JIŘÍ , 11.12.1943	00016741	KUTYPOVÁ JANA	00016787
FERONA, A.S.	00016569	LANGFELLNER ROMAN ING.	00016707
FITMIN A.S.	00016629	LANGROVÁ EVA , 14.03.1954	00016648
FRANFINANCE CZECH REPUBLIC S.R.O.	00016461	LEDECKÁ LUDMILA	00016500
FRANTOVÁ BLANKA , 13.11.1937	00016689	LEGRAND S.R.O.	00016690
FRNKOVÁ SOŇA DIS., 24.01.1978	00016767	LICHTWER CONSULT CZECH S.R.O.	00016861
FRÜHAUF PAVEL	00016708	M.C.TRITON, SPOL. S R.O.	00016691
GASTRO-ŽOFÍN S.R.O.	00016529	MADĚRYČOVÁ ANNA	00016846
GENERAL ELECTRIC INTERNATIONAL, INC.	00016746	MARCUS EVANS (CR) LIMITED-ORGANIZAČNÍ SLOŽKA	00016795
		MARIÁNKOVÁ LUDMILA , 21.03.1955	00016590
		MARKOVÁ MARIE , 29.02.1944	00016527
		MARSH, S.R.O.	00016864

Identifikace	Č. reg.	Identifikace	Č. reg.
MBG CZECH, A.S.	00016592	OBEC MYSLEJOVICE	00016853
MĚSTO BEČOV NAD TEPLOU	00016719	OBEC OCHOZ	00016826
MĚSTO GOLČŮV JENÍKOV	00016844	OBEC PARTUTOVICE	00016503
MĚSTO KORYČANY	00016749	OBEC PODŮLŠÍ	00016843
MĚSTO KOŽLANY	00016858	OBEC POTŮČKY	00016516
MĚSTO KRALOVICE	00016799	OBEC PŠOV	00016768
MĚSTO ROKYTNICE NAD JIZEROU	00004189	OBEC RAŠKOVICE	00016725
MĚSTO RYCHNOV U JABLONCE NAD NISOU	00016740	OBEC ROHLE	00016522
MĚSTO ŘEVNICE	00016634	OBEC ROZSTÁNÍ	00016760
MĚSTO VARNSDORF MĚSTSKÁ POLICIE	00016548	OBEC RUDÍKOV	00016533
MĚSTO ZÁSMUKY	00016535	OBEC SADOV	00016701
MĚSTSKÁ ČÁST PRAHA - ÚJEZD NAD LESY	00013143	OBEC SAMŠINA	00016713
MĚSTSKÉ KULTURNÍ STŘEDISKO	00016761	OBEC SEDLEC	00016785
MĚSTSKÉ KULTURNÍ STŘEDISKO KONICE	00016755	OBEC SLAVHOSTICE	00016800
MĚSTSKÉ MUZEUM A GALERIE LOMNICE NAD POPELKOU	00016523	OBEC SLAVÍČKY	00016836
MINISTERSTVO OBRANY	00000717	OBEC STANOVICE	00016610
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY		OBEC STAŘEČ	00016525
ČESKÉ REPUBLIKY	00016557	OBEC STŘÍLKY	00016850
MOROVÁ MARTINA	00016834	OBEC SUCHDOL	00016735
MOSCHOVÁ LENKA	00016555	OBEC ŠTĚDRÁ	00016650
MT KLIENT SERVIS S.R.O.	00016494	OBEC TEPLICE NAD BEČVOU	00016530
MUDRÁ RADKA	00016542	OBEC TŘTĚNICE	00016868
NAVRÁTIL MIROSLAV , 18.11.1930	00016591	OBEC UHERČICE	00016565
NAVRÁTILOVÁ MARIE , 02.12.1933	00016829	OBEC UHRČICE	00016637
NAVRÁTILOVÁ RADOSLAVA , 21.05.1950	00016797	OBEC ÚSTÍ	00016534
NORTH AMERICAN PICTURES II S.R.O.	00016857	OBEC ÚTVINA	00016498
NORTH AMERICAN PICTURES S.R.O.	00016856	OBEC VELETOV	00016762
NOVÁK MILOSLAV BC., 20.02.1974	00016739	OBEC VELKÝ BOR	00016720
NOVÁKOVÁ ALENA MGR., 29.08.1954	00016723	OBEC VELKÝ ÚJEZD	00016747
NOVÁKOVÁ JAROSLAVA	00016769	OBEC VÍCEMĚŘICE	00016838
NOVO NORDISK S.R.O.	00008865	OBEC VINTÍŘOV	00016859
OBEC BOHY	00016794	OBEC VOJKOVICE	00016497
OBEC BRODEK U KONICE	00016630	OBEC VŘESOVÁ	00016839
OBEC BRODEK U PROSTĚJOVA	00016871	OBEC VÝROV	00016786
OBEC BŘASY	00016722	OBEC VYSOKÁ LIBYNĚ	00016841
OBEC BUKVICE	00016706	OBVODNÍ SOUD PRO PRAHU 10	00016508
OBEC ČITICE	00016851	OLYMP 2002 A.S.	00016862
OBEC ČEHOVICE	00016872	OPPENBERG SECURITIES,A.S.	00016802
OBEC ČECHY POD KOSÍŘEM	00016867	OTYCHOVÁ VLASTA MGR.	00016514
OBEC ČERNÍKOVICE	00016775	OULEHOVÁ JANA ING., 23.07.1973	00016545
OBEC ČERVENÁ TŘEMEŠNÁ	00016875	PÁCHA JAROSLAV	00016632
OBEC DOLNÍ HRADIŠTĚ	00016765	PALEČEK KAREL ING.	00016558
OBEC DOLNÍ NIVY	00016842	PATREM TRADING LIMITED CZ S.R.O.	00016780
OBEC DOUBRAVA	00016774	PAVELKA MARTIN	00016670
OBEC HEJNÁ	00016866	PAVELKOVÁ JANA	00016671
OBEC HLUŠICE	00010091	PAVELKOVÁ JAROSLAVA , 02.02.1976	00016672
OBEC HORNÍ JELENÍ	00016526	PERGL KAMIL , 12.08.1958	00016549
OBEC HUMBURKY	00016704	PERSONAL AGENCY V.O.S.	00016874
OBEC HUNTÍŘOV	00016828	PLANNING AND DESIGN CONSULTANTS S. R. O.	00016702
OBEC CHLUM U TŘEBONĚ	00016537	PLÍŠEK MILOSLAV	00016827
OBEC CHOTEČ	00016833	PNT BOHEMIA S. R. O.	00016501
OBEC CHYŠE	00016495	PODRABSKÝ RADOMÍR JUDR.	00016694
OBEC JINDŘICHOV	00016715	POPOVÁ AGÁTA	00016561
OBEC JINDŘICHOVICE	00016840	POUROVÁ JANA , 23.04.1961	00016566
OBEC KLENOVICE NA HANÉ	00016738	PRAGONET,A.S.	00016779
OBEC KOČÍN	00016796	PRAGUE INTERNATIONAL MARATHON SPOL. S R.O.	00016855
OBEC KOPIDLO	00016772	PRAŽÁK JAN ING., 19.07.1975	00016712
OBEC KOZOJEDY	00016788	PRINZOVÁ LUCIE , 19.01.1979	00016783
OBEC KRAJKOVÁ	00016873	PROBO TRANS BEROUN SPOL. S R.O.	00016721
OBEC KRALICE NA HANÉ	00016744	PRONIX S. R. O.	00016789
OBEC KRÁSNÉ ÚDOLÍ	00016870	RAMI CZ S.R.O.	00016803
OBEC KRÁSNÓ	00016860	RENAULT ČESKÁ REPUBLIKA,A.S.	00006284
OBEC KVASICE	00016854	REPUBLIKOVÉ CENTRUM VZDĚLÁVÁNÍ S.R.O.	00016640
OBEC LAŠKOV	00016757	RYBECKÁ DAGMAR , 27.03.1951	00016539
OBEC LIBOUČEC	00016731	RYŠAVÝ MIROSLAV ING, 23.07.1945	00016805
OBEC MÍROVÁ	00016499	ŘIČÁNKOVÁ ALENA ING.	00016506
OBEC MORKOVICE - SLÍŽANY	00016502	ŘÍZENÍ LETOVÉHO PROVOZU ČESKÉ REPUBLIKY S.P.	00008467

Identifikace	Č. reg.	Identifikace	Č. reg.
S-CARE S.R.O.	00016791	ŠTĚRBOVÁ MARIE	00016559
SDRUŽENÍ PRAŽSKÝCH PODNIKATELŮ	00016697	TAPTIČ IVAN	00016493
SEDLÁČKOVÁ MIROSLAVA , 03.04.1953	00016754	T-CENTRUM.CZ,A.S.	00016752
SEMANOVÁ TERÉZIA	00016758	TECHNICKÉ SLUŽBY VM S.R.O.	00016538
SERBA KAREL	00016792	TICHÁ LENKA	00016560
SKLOSTROJ TURNOV CZ,S.R.O.	00016776	TRAVEL SPORT SPOL. S R.O.	00016692
SOUKALOVÁ IVETA , 19.03.1970	00016521	TUČEK JIŘÍ	00016845
SPOLEČENSTVÍ K HALTÝŘI 689	00016717	TUROŇ JAROSLAV , 08.02.1951	00016635
SPOLEČENSTVÍ VLASTNÍKŮ JEDNOTEK DOMU Č.P. 690, K.Ú TROJA,V PRAZE 8	00016718	TYCO ELECTRONICS CZECH S.R.O.	00016541
SPOLEČENSTVÍ VLASTNÍKŮ JEDNOTEK VŘESOVÁ 685	00016716	URBAN MICHAL , 25.03.1981	00016628
SPORTOVNĚ STŘELECKÝ KLUB ČD-LOKOMOTIVNÍ DEPO JIHLAVA	00016710	ÚSTECKÝ KRAJ	00001603
STÁTNÍ FOND ŽIVOTNÍHO PROSTŘEDÍ ČR	00005695	VADANA,S.R.O.	00016512
STAVEBNÍ BYTOVÉ DRUŽSTVO AVIA PRAHA	00016865	VAĐURA PAVEL	00016793
STOWASSEROVÁ PETRA	00016543	VETEŠNÍK PAVEL	00016832
SÜSSENBECK JAN , 13.01.1975	00016556	VIK LUBOMÍR , 11.03.1953	00016638
SVOBODA JIŘÍ ING.	00016748	VÍTKOVICE ARÉNA,A.S.	00016730
SYKOTRANS,S.R.O.	00016766	VRLA PETR	00016651
ŠAŠEK STANISLAV	00016518	VYTISKOVÁ EVA , 06.02.1956	00016700
ŠEBESTOVÁ JANA JUDR.	00016515	VÝZKUMNÝ ÚSTAV PRO CHOV SKOTU,S.R.O.	00016563
ŠLAPÁKOVÁ VĚRA	00016736	WIESNEROVÁ ALENA , 16.03.1956	00016571
ŠMÍDEK JAROMÍR	00016745	WINDOR S.R.O.	00016863
ŠOLTA JOSEF	00016727	ZÁKLADNÍ UMĚLECKÁ ŠKOLA,LUHAČOVICE, OKRES ZLÍN	00016732
ŠPIDLA DATA PROCESSING,S.R.O.	00016567	ZELINKA VLADIMÍR ING., 21.05.1951	00016536
ŠTĚPÁNOVÁ PETRA	00013641	ŽÁKOVSKÁ ALENA , 04.08.1953	00016698
		ŽOHOVÁ LENKA	00016743

Přehled registrací zrušených v období od 4. 7. 2002 do 22. 8. 2002

Číslo registrace	Subjekt	Datum zrušení
00000301/001	CMS SPOL. S R. O.	2.8.2002
00000800/001	KRÁL ZDENĚK	16.7.2002
00001302/001	EUROTEL PRAHA, SPOL. S R.O.	22.7.2002
00003099/001	KOPECKÁ JARMILA	29.7.2002

II. STANOVISKA ÚŘADU

STANOVISKO č. 1/2002

Srpen 2002

Zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče

Problematika zpracování osobních údajů v souvislosti se zajišťováním zdravotní péče je v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), upravena v několika směrech. Osobní údaj vypovídající o zdravotním stavu patří mezi citlivé osobní údaje subjektu údajů a jeho zpracování se řídí podmínkami upravenými zejména v § 9 zákona o ochraně osobních údajů. V citovaném ustanovení zákon o ochraně osobních údajů očekává, že ke zpracovávání citlivých osobních údajů správcem nebo zpracovatelem může docházet za podmínky, že **subjekt údajů dal ke zpracování výslovný souhlas**. Souhlas subjektu údajů musí být dán písemně, podepsán subjektem údajů a musí z něho být zřejmé, k jakým údajům je dáván, jakému správci údajů, k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může subjekt údajů kdykoliv odvolat. Správce je povinen předem subjekt údajů o jeho právech poučit. Tento souhlas musí správce uschovat po dobu zpracování osobních údajů, k jejichž zpracování byl souhlas dán, ke zpracovávání citlivého osobního údaje o zdravotním stavu může dále docházet v případě, že **zpracovávání je nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku**, pokud není možno souhlas subjektu údajů získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je subjekt údajů nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas. Významným ustanovením zákona o ochraně osobních údajů je § 9 písm. c), podle něhož lze zpracovávat osobní údaj vypovídající o zdravotním stavu subjektu údajů v případě, že jde o **poskytování zdravotní péče, jakož i jiné posuzování zdravotního stavu podle zvláštního právního předpisu**, zejména pro účely sociálního zabezpečení nebo je **tak stanoveno zvláštním zákonem**.

Zákon o ochraně osobních údajů je tedy obecným právním předpisem, který současně umožňuje, aby zvláštní právní předpis (zákon) upravil zvláštní postupy, práva nebo povinnosti osob zúčastněných na zpracovávání citlivých osobních údajů. Základním z těchto zvláštních předpisů je zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů (dále jen „zákon o péči o zdraví lidu“). V části páté tohoto zvláštního zákona se upravuje „Zpracování osobních údajů souvisejících se zajišťováním zdravotní péče“ (§ 67a až § 67d). Zpracováním osobních údajů podle tohoto

zákona se rozumí zpracování osobních údajů při vedení zdravotnické dokumentace a další nakládání s ní a zpracování osobních údajů v Národním zdravotnickém informačním systému (dále jen „NZIS“). To je velmi důležité ustanovení, které bylo do zákona o péči o zdraví lidu doplněno jeho novelou č. 260/2001 Sb. Do té doby byla povinnost vést dokumentaci zakotvena výslovně (expresis verbis) v zákoně č. 160/1992 Sb., o zdravotní péči v nestátních zdravotnických zařízeních, ve znění pozdějších předpisů (§ 5 odst. 2 písm. d/ zákona) (viz stanovisko ÚOOÚ č. 1/2000). Nyní jsou podle § 67b odst. 1 zákona o péči o zdraví lidu všechna zdravotnická zařízení povinna vést zdravotnickou dokumentaci v rozsahu, který je obsahem § 67b) odst. 2 až 4 zákona o péči o zdraví lidu. Ostatní práva a povinnosti při zpracování osobních údajů souvisejících se zajišťováním zdravotní péče se podle § 67b odst. 9 řídí zvláštním zákonem, kterým je zákon o ochraně osobních údajů.

Pokud jde o **právo subjektu údajů na informace** o zpracovávaných osobních údajích, řídí se podmínky přístupu k zpracovávaným osobním údajům nejen zákonem o ochraně osobních údajů, ale především zákonem o péči o zdraví lidu, a to zejména proto, že podle § 67b odst. 12 má subjekt údajů (pacient) právo na poskytnutí veškerých informací shromážděných ve zdravotnické dokumentaci vedené o jeho osobě a v jiných zápisech, které se vztahují k jeho zdravotnímu stavu; pacient se z informací, které jsou mu sděleny o jeho zdravotním stavu, nesmí dozvědět informace o třetí osobě. Za osoby mladší 18 let nebo osoby zbavené způsobilosti k právním úkonům mají právo na informace podle věty první jejich zákonní zástupci.

Právo subjektu údajů na informace podle zákona o ochraně osobních údajů bývá častým předmětem diskuse v souvislosti s řešením otázek, jejichž obsahem je spor, zda si lékař smí nechat pacientem zaplatit za výpis ze zdravotnické dokumentace. Česká lékařská komora, stejně jako Všeobecná zdravotní pojišťovna v této souvislosti vyjádřily názor, že za tuto činnost lze žádat úhradu pacientem, Svaz pacientů byl naopak názoru opačného a odvolával se přitom na ustanovení § 12 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Podle názoru Úřadu pro ochranu osobních údajů se ani jedna ze stran sporu nezabývala základní otázkou, kterou je nezbytné zodpovědět, a to otázkou, co „výpis ze zdravotnické dokumentace“ jako dokument o zdravotním stavu pacienta vlastně obsahuje a jaká je jeho právní úprava. Z tohoto důvodu je vyjadřovaný vztah ustanovení § 12 zákona

o ochraně osobních údajů, jehož obsahem je povinnost správce (zdravotnického zařízení) jednou za kalendářní rok bezplatně subjektu údajů (pacientovi) na základě písemné žádosti poskytnout informace o osobních údajích o něm zpracovávaných a ustanovení zvláštních právních předpisů obsahujících úpravu výpisu ze zdravotní dokumentace nesprávný a nepřesný.

Úřad pro ochranu osobních údajů se domnívá, že základním východiskem pro posouzení této záležitosti je § 11 zákona o péči o zdraví lidu, jehož obsahem je poskytování zdravotní péče (§ 11), jejíž nedílnou součástí je posudková činnost (§ 21). I když se v zákoně o péči o zdraví lidu pojem „výpis ze zdravotní dokumentace“ nevyskytuje, je existence tohoto dokumentu již obsahem navazujících nebo prováděcích právních předpisů, které se zejména zabývají posuzováním zdravotní způsobilosti (např. zákon č. 218/1999 Sb., branný zákon, zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů, vyhláška ministerstva zdravotnictví č. 127/1996 Sb., vyhláška ministerstva vnitra č. 324/2001 Sb., apod.).

V případě vykazování zdravotní péče podle seznamu zdravotních výkonů s bodovými hodnotami (Metodické opatření MZ č. POJ 2773/5/95) se výpis ze zdravotní dokumentace považuje za administrativní úkon praktického lékaře, popř. registrujícího lékaře, který je prováděn např. pro jiné zdravotnické pracoviště nebo pro nově registrujícího lékaře pro zajištění návaznosti zdravotní péče. Z tohoto výčtu vyplývá, že obsahem výpisu ze zdravotnické dokumentace mohou být i jiné než osobní údaje pacienta nebo údaje o zdravotním stavu pacienta (subjektu údajů).

Bylo by tedy potřeba definovat vztah mezi výpisem ze zdravotnické dokumentace a informacemi o osobních údajích. Podle názoru Úřadu pro ochranu osobních údajů informace o osobních údajích poskytovaná podle § 11 odst. 1, popřípadě podle § 12 odst. 2 zákona o ochraně osobních údajů, neznamená, že jsou subjektu údajů sděleny přímo ony osobní údaje (respektive jejich obsah), ale jde o informaci, jejíž nedílnou součástí je informace o „rozsahu osobních údajů“ (§ 11 odst. 1), popřípadě informace „o osobních údajích o něm zpracovávaných“ (§ 12 odst. 2). Pokud by tedy pacient požadoval takové informace, pak má nárok na jejich obdržení jednou ročně zdarma, protože zvláštní zákony (zákon o péči o zdraví lidu či zákony o veřejném zdravotním pojištění) toto právo nijak neomezuji.

Úřad pro ochranu osobních údajů se rovněž zabýval problematikou zpracovávání osobních údajů v souvislosti s **prováděním klinického hodnocení a postmarketingového sledování léčiv**. Klinické hodnocení humánních léčiv a s tím související zpracování osobních údajů subjektů údajů je prováděno na základě zmocnění, daného příslušnými ustanoveními zákona č. 79/1997 Sb., o léčivech a o změnách a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů a vyhlášky Ministerstva zdravotnictví a Ministerstva zemědělství č. 472/2000 Sb., kterou se stanoví správ-

ná klinická praxe a bližší podmínky klinického hodnocení léčiv. Zadavatel, který zpracovává osobní údaje subjektů hodnocení, může tuto činnost provádět na základě zmocnění citovaných právních předpisů, ale současně musí dodržet všechny své povinnosti správce, které jsou na něj současně kladeny zákonem o ochraně osobních údajů. Zadavatel je tedy v pozici správce osobních údajů, a proto se na něj vztahují všechny povinnosti správce, které vyplývají ze zákona o ochraně osobních údajů. Pokud jde o splnění oznamovací povinnosti zadavatele – správce, vztahuje se na tento postup ustanovení § 18 písm. b) zákona o ochraně osobních údajů, z něhož vyplývá, že oznamovací povinnost správce podle § 16 se nevztahuje na zpracování osobních údajů, jejichž zpracování je správcem uloženo zákonem nebo kterých je třeba k uplatnění práv vyplývajících ze zvláštních zákonů.

V rámci tzv. postmarketingového sledování, v jehož průběhu se hodnotí podávání registrovaného přípravku v rámci běžné lékařské praxe, nejsou již předmětem zpracování osobní údaje, které by mohly přímo či nepřímo identifikovat konkrétní subjekt údajů, nýbrž tzv. anonymní údaje ve smyslu ustanovení § 4 písm. c) zákona o ochraně osobních údajů (anonymním údajem je podle tohoto ustanovení takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů). Pro zpracování těchto údajů se souhlas subjektu údajů nevyžaduje, nezávisle na tom, zda se jedná o osobní údaje ve smyslu § 4 písm. a) nebo § 4 písm. b) zákona o ochraně osobních údajů. Výčet uváděných údajů se však nesmí v žádném případě vázat ke konkrétnímu subjektu údajů, proto nelze souhlasit s tím, aby součástí takovéto databáze byly iniciály subjektu údajů nebo identifikační kód subjektu údajů, jehož prostřednictvím lze identitu subjektu údajů zjistit. Přitom není rozhodující, zda ony klíče ke zjištění identity subjektu údajů budou použity či nikoliv. V takovém případě se pak nejedná o zpracovávání anonymních údajů a správce musí při plnění svých povinností dodržet všechny své povinnosti včetně zpracování osobních údajů se souhlasem subjektu údajů.

V případech, kdy se jedná o zpracovávání informací z tzv. genové sondy, lze konstatovat, že pokud jsou předmětem zpracování „epidemiologické údaje o populaci v určitých oblastech ČR“, půjde zřejmě o určité druhy statistických informací. V tomto případě v zásadě platí ustanovení § 3 odst. 5 zákona o ochraně osobních údajů, z něhož vyplývá, že zpracování osobních údajů pro účely statistické stanoví zvláštní zákony, s přihlédnutím k některým dalším ustanovením zákona o ochraně osobních údajů, např. k § 5 odst. 4 zákona o ochraně osobních údajů, z něhož vyplývá, že bez souhlasu subjektu údajů lze osobní údaje zpracovávat pro účely statistické nebo vědecké. Pro tyto účely zpracování je nutno osobní údaje anonymizovat, jakmile je to možné. Bez souhlasu subjektu údajů však nelze pro účely statistické a vědecké zpracovávat citlivé údaje. Při zpracování osobních údajů pro tyto účely je však nutno zajistit požadovanou úroveň jejich zabezpečení podle § 13 zákona o ochraně osobních údajů.

III. SDĚLENÍ ÚŘADU

RADA EVROPY VÝBOR MINISTRŮ

DOPORUČENÍ č. R (97) 5

VÝBORU MINISTRŮ ČLENSKÝM STÁTŮM O OCHRANĚ ZDRAVOTNÍCH ÚDAJŮ

*(Schváleno Výborem ministrů dne 13. února 1997
na 584. zasedání zástupců ministrů)*

Výbor ministrů podle podmínek stanovených v článku 15.b Statutu Rady Evropy,

maje na zřeteli, že cílem Rady Evropy je dosažení větší jednoty svých členů:

Připomněl všeobecné zásady o ochraně osobních údajů uvedené v Úmluvě o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat (série evropských dohod – ETS, č. 108) a zejména její článek 6, který stanoví, že osobní údaje týkající se zdraví nesmějí být předmětem automatizovaného zpracování, pokud domácí právní řád nestanoví vhodné záruky;

Vědom si skutečnosti, že informační systémy ve zvýšené míře využívají automatické zpracování zdravotních údajů nejen pro lékařskou péči, lékařský výzkum, řízení nemocnic a veřejné zdravotnictví, ale také mimo sektor zdravotnictví;

Přesvědčen o důležitosti kvality, integrity a dostupnosti zdravotních údajů pro zdraví subjektu těchto údajů a jeho rodinných příslušníků;

Vědom si, že pokrok lékařské vědy záleží ve velké míře na dostupnosti zdravotních údajů o jednotlivých osobách;

Přesvědčen, že je žádoucí upravit shromažďování a zpracování zdravotních údajů, aby se zaručila důvěrnost a bezpečnost osobních údajů týkajících se zdraví osob a aby se zajistilo, že tyto údaje budou používány při zachování práv a základních svobod člověka a zejména jeho práva na soukromí;

Vědom si skutečnosti, že pokrok v lékařské vědě a vývoj informačních technologií od roku 1981 si vynutil novelizovat různá ustanovení Doporučení č. R (81) 1 o předpisech pro automatizované zdravotnické databanky,

doporučil, aby vlády členských států:

- učinily kroky zajišťující, aby zásady obsažené v příloze k tomuto Doporučení se promítly do jejich domácího právního řádu a praxe;
- zajistily široký oběh zásad obsažených v příloze k tomuto Doporučení mezi osobami, které se osobně podílejí na shromažďování a zpracování zdravotních údajů;

Rozhodl, že toto Doporučení nahradí Doporučení č. R (81) 1 o předpisech pro automatizované zdravotnické databanky.

1. Definice

Pro účely tohoto Doporučení:

- výraz „osobní údaje“ pokrývá všechny informace vztahující se k určenému nebo určitelnému jednotlivci nebo identifikovatelné osobě. Jednotlivec nebude považován za určitelného, pokud identifikace vyžaduje nepřiměřeně mnoho času a práce. V případech, kdy jednotlivec není určitelný, považují se údaje za anonymní.
- výraz „zdravotní údaje“ se vztahuje na osobní údaje týkající se zdraví jedince. Vztahuje se také na údaje, které mají zřejmou a úzkou vazbu ke zdraví, jakož i na genetické údaje.
- výraz „genetické údaje“ se vztahuje na všechny údaje jakéhokoli typu o dědičných charakteristikách jedince nebo o dědičném typu takových charakteristik v rámci příbuzenské skupiny jedinců.

Vztahuje se také na všechny údaje o přenosu jakýchkoliv genetických informací (o genech) u jedince nebo v genetické linii, vztahující se k jakémukoli aspektu zdraví nebo nemoci, ať již je či není přítomna jako identifikovatelná charakteristika.

Genetická linie je řada, sestávající z genetických podobností, které jsou výsledkem rozmnožování a jsou sdíleny dvěma či více jedinci.

2. Rozsah

- 2.1 Toto Doporučení se vztahuje na shromažďování a automatické zpracování zdravotních údajů, pokud domácí právní řád, ve specifickém kontextu mimo sektor zdravotnictví, nestanoví jiné vhodné záruky.

- 2.2. Členský stát může rozšířit zásady stanovené v tomto Doporučení na zdravotní údaje, které nejsou předmětem automatizovaného zpracování.

3. Respektování soukromí

- 3.1 Během shromažďování a zpracování zdravotních údajů musí být zaručeno respektování práv a základních svobod a zejména práva na soukromí.
- 3.2. Zdravotní údaje smějí být shromažďovány a zpracovávány jen v souladu s příslušnými zárukami, které musí stanovit domácí právní řád.

V zásadě by zdravotní údaje měli shromažďovat a nakládat s nimi jen zdravotničtí pracovníci nebo osoby či orgány pracující pro zdravotnické pracovníky. Na osoby a orgány zabývající se shromažďováním a zpracováním údajů pro zdravotnické pracovníky, by se měla vztahovat stejná pravidla týkající se mlčenlivosti, která platí pro zdravotnické pracovníky, nebo pravidla srovnatelná.

Správci osobních údajů (záznamů), kteří nejsou zdravotnickými pracovníky lékařské péče, by měli sbírat a zpracovávat zdravotní údaje buď při zachování srovnatelných pravidel týkajících se mlčenlivosti, kterými jsou vázáni zdravotničtí pracovníci lékařské péče, nebo stejně účinných záruk stanovených domácím právním řádem.

4. Shromažďování a zpracování zdravotních údajů

- 4.1. Zdravotní údaje smějí být shromažďovány řádně a v rámci zákonných předpisů a pouze pro specifikované účely.
- 4.2. Zdravotní údaje budou v zásadě získávány od subjektu údajů. Z jiných zdrojů mohou být získány pouze v souladu se zásadami 4, 6 a 7 tohoto Doporučení a jen je-li to nutné k dosažení účelu zpracování nebo jestliže subjekt údajů není schopen tyto údaje poskytnout.
- 4.3. Zdravotní údaje smějí být shromažďovány a zpracovávány:
- a. pokud to zákon stanoví pro:
 - i. účely veřejného zdraví; nebo
 - ii. s výhradou zásady 4.8. zabránění reálnému nebezpečí nebo potlačení specifického trestného činu; nebo
 - iii. jiný důležitý veřejný zájem; nebo
 - b. umožní-li to zákon

- i. pro preventivní lékařské účely nebo pro diagnostické nebo léčebné účely, pokud jde o subjekt údajů nebo o příbuzné v genetické řadě; nebo
- ii. pro záchranu životních zájmů subjektu údajů nebo třetí osoby; nebo
- iii. pro naplnění specifických smluvních povinností; nebo
- iv. pro nastolení, uplatnění nebo ochranu právního nároku; nebo

- c. jestliže subjekt údajů nebo jeho právní zástupce či úřad nebo osoba či orgán ustavené zákonem udělily souhlas pro jeden či více účelů a domácí právní řád nestanoví jinak.

- 4.4. Jestliže byly zdravotní údaje shromažďovány pro účely preventivního lékařství nebo pro diagnostické či léčebné účely s ohledem na subjekt údajů nebo jeho příbuzné v genetické posloupnosti, mohou být tyto údaje zpracovávány pro řízení lékařské služby, prováděné v zájmu pacienta, a to v případech, kdy řízení provádějí zdravotničtí pracovníci, kteří údaje shromáždili, nebo kdy údaje jsou přenášeny v souladu s principy 7.2. a 7.3.

Nenarozené děti

- 4.5. Zdravotní údaje týkající se nenarozených dětí by měly být považovány za osobní údaje a požívat ochranu srovnatelnou s ochranou zdravotních údajů nezletilých.
- 4.6. Pokud domácí právní řád nestanoví jinak, může ten, kdo má rodičovskou odpovědnost, jednat jako osoba mající právní zmocnění za nenarozené dítě, budoucí subjekt údajů.

Genetické údaje

- 4.7. Genetické údaje shromažďované a zpracovávané pro prevenci, diagnostiku nebo léčbu subjektu údajů nebo pro vědecký výzkum by měly být používány jenom pro tyto účely nebo tak, aby jejich zpracování umožňovalo subjektu údajů svobodně a informovaně se v této věci rozhodnout.
- 4.8. Zpracování genetických údajů pro účely soudu nebo pátrání v trestní věci by mělo podléhat specifickým právním předpisům zajišťujícím náležité záruky.

Údaje by měly být užívány pouze tak, aby se předešlo reálnému nebezpečí nebo potlačil určitý trestný čin. V žádném případě by neměly být používány ke zjištění jiných charakteristik, které mohou mít genetickou souvislost.

4.9. Pro jiné účely, než jsou účely uvedené v zásadách 4.7 a 4.8, by mělo být shromažďování a zpracování genetických údajů povoleno v zásadě jen ze zdravotních důvodů, a zvláště aby se zabránilo jakémukoli závažnému poškození zdraví subjektu údajů nebo třetích stran.

Shromažďování a zpracování genetických údajů pro účely předvídání nemoci však může být povoleno v případě převažujícího zájmu a s poskytnutím náležitých záruk definovaných domácím právním řádem.

5. Informování subjektu údajů

5.1 Subjekt údajů musí být informován o následujících věcech:

- a. o existenci záznamu obsahujícího jeho zdravotní údaje a o typu údajů, které byly shromážděny nebo mají být shromážděny;
- b. o účelu nebo účelech, pro které se zpracovávají nebo budou zpracovávat;
- c. tam, kde to přichází v úvahu, o osobách nebo orgánech, pro které jsou nebo budou shromažďovány;
- d. o osobách nebo orgánech, jimž smějí být sděleny a pro jaké účely;
- e. o možnosti subjektu údajů, pokud taková možnost je, odmítnout souhlas, odvolat daný souhlas a o důsledcích takového odvolání;
- f. o správci osobních údajů nebo jeho představitelích, přichází-li to v úvahu, a o podmínkách, za kterých je možný výkon práva přístupu k údajům a jejich oprav.

5.2. Subjekt údajů by měl být informován nejpozději v okamžiku shromažďování údajů. Pokud lékařské údaje nejsou získány od subjektu údajů, je třeba ho vyrozumět co nejdříve a poskytnout mu vhodným způsobem informace uvedené v zásadě 5.1, pokud to není zjevně nepřiměřené nebo neproveditelné, nebo pokud již subjekt údajů tyto informace nedostal.

5.3. Informace pro subjekt údajů musejí být přiměřené a přizpůsobené okolnostem. Především by každému subjektu údajů měly být tyto informace sděleny individuálně.

5.4. Dříve, než se provede genetická analýza, měl by být subjekt údajů informován o cílech analýzy a o možnos-

tech neočekávaných zjištění.

Osoby nezpůsobilé k právním úkonům

5.5. Je-li subjektem údajů osoba nezpůsobilá k právním úkonům, neschopná svobodného rozhodování a domácí právní řád nedovoluje subjektu údajů, aby jednal vlastním jménem, musí být informace podána osobě, která je ze zákona oprávněna jednat v zájmu subjektu údajů.

Jestliže osoba nezpůsobilá k právním úkonům je schopna porozumět, měla by být informována před shromažďováním nebo zpracováním jejích údajů.

Výjimky

5.6. Výjimky ze zásad 5.1, 5.2 a 5.3 mohou být učiněny v těchto případech:

- a. Informování subjektu údajů smí být omezeno, jestliže omezení je stanoveno zákonem a představuje nezbytné opatření v demokratické společnosti:
 - i. k zabránění reálnému nebezpečí nebo potlačení trestného činu;
 - ii. při ochraně veřejného zdraví;
 - iii. k ochraně subjektu údajů a k ochraně práv a svobod druhých;
- b. V případech bezprostředního ohrožení života mohou být údaje, které se považují za nezbytné pro léčení, shromažďovány před podáním informace subjektu údajů.

6. Souhlas

6.1. V případech, kdy se vyžaduje, aby subjekt údajů dal svůj souhlas, by tento souhlas měl být svobodný, výslovný a informovaný.

6.2. Výsledky jakékoli genetické analýzy by měly být formulovány v mezích cílů lékařské konzultace, diagnostiky nebo léčby, pro které byl dán souhlas.

6.3. V případech, kdy se zamýšlí nakládat se zdravotními údaji vztahujícími se k osobě nezpůsobilé k právním úkonům, která není schopná svobodného rozhodování, a kdy domácí právní řád nedovoluje, aby subjekt údajů jednal vlastním jménem, bude se vyžadovat souhlas osoby právně uznané, aby jednala v zájmu subjektu údajů.

Jestliže v souladu se zásadou 5.5 (viz výše) byla osoba

nezpůsobila k právním úkonům informována o úmyslu shromážďovat a zpracovávat její zdravotní údaje, na její přání se vezme zřetel, pokud domácí právní řád nestanoví jinak.

7. Komunikace

7.1. Zdravotní údaje nesmějí být sdělovány bez splnění podmínek stanovených v této kapitole a v kapitole 12.

7.2. Obzvláště pokud není zaručena vhodná právní ochrana domácím právním řádem, mohou být zdravotní údaje sdělovány pouze osobě, která má povinnost mlčenlivosti stanovenou pro zdravotnické pracovníky nebo srovnatelnou povinnost mlčenlivosti a která splňuje zásady stanovené v tomto Doporučení.

7.3. Zdravotní údaje smějí být sdělovány, jsou-li závažné a:

- a. jestliže sdělení je poskytnuto podle zákona a tvoří nezbytná opatření v demokratické společnosti pro:
 - i. potřeby veřejného zdraví; nebo
 - ii. zabránění reálnému nebezpečí nebo potlačení konkrétního trestného činu
 - iii. jiný důležitý veřejný zájem; nebo
 - iv. ochranu práv a svobod druhých; nebo
- b. jestliže sdělování je dovoleno zákonem pro účel:
 - i. ochrany subjektu údajů nebo příbuzného v genetické linii;
 - ii. zabezpečení životních zájmů subjektu údajů nebo třetí osoby; nebo
 - iii. splnění specifických smluvních povinností; nebo
 - iv. nastolení, uplatnění nebo ochrání právního nároku; nebo
- c. jestliže subjekt údajů nebo jeho právní zástupce nebo úřad, nebo jakákoliv osoba či orgán činící opatření ze zákona, dal souhlas pro jeden nebo více účelů, a jestliže domácí právní řád nestanoví jinak; nebo
- d. pokud subjekt údajů nebo jeho právní zástupce nebo úřad, nebo jakákoliv osoba či orgán činící opatření ze zákona, výslovně nic nenamítal proti jakémukoliv nepovinnému sdělení, jestliže údaje byly shromážďovány v kontextu svobodně zvolené preventivní, diagnostické nebo terapeutické péče a jestliže účel sdělení, obzvláště při zajištění zdravotní péče pacientovi nebo pro řízení zdravotních služeb prováděných v zájmu pacienta, není v rozporu s účelem zpracování, pro který byla

shromážďována.

8. Práva subjektu údajů

Práva přístupu a oprav

8.1. Každé osobě musí být umožněn přístup k jejím zdravotním údajům, buď přímo nebo prostřednictvím zdravotnického pracovníka nebo, pokud to domácí právní řád dovoluje, prostřednictvím osoby jí určené. Informace musí být dostupná ve srozumitelné formě.

8.2. Přístup ke zdravotním údajům může být odmítnut, omezen nebo pozdržen, pouze stanoví-li to zákon a jestliže:

- a. to představuje nutné opatření v demokratické společnosti v zájmu ochrany bezpečnosti státu, bezpečnosti občanů nebo k potlačení trestných činů; nebo
- b. znalost informace může způsobit vážné poškození zdraví subjektu údajů; nebo
- c. informace o subjektu údajů odhaluje také informace o třetích stranách nebo, pokud jde o genetické údaje, tato informace může způsobit vážnou škodu pokrevnímu příbuznému nebo osobě, která má přímou vazbu na tuto genetickou linii; nebo
- d. údaje jsou využívány pro statistické účely nebo pro účely vědeckého výzkumu a prokazatelně určitelné není žádné riziko porušení soukromí subjektu údajů, zvláště pak možnosti použití shromážďovaných údajů k podpoře rozhodování nebo opatření vztahujících se k jakémukoliv jednotlivci.

8.3. Subjekt údajů smí požádat o opravu jeho se týkajícího chybného údaje a v případě odmítnutí musí mít možnost se odvolat.

Neočekávaná zjištění

8.4. Osoba podrobující se genetické analýze by měla být informována o neočekávaných zjištěních, pokud jsou splněny následující podmínky:

- a. domácí právní řád nezakazuje podávání takových informací;
- b. osoba požádala o takové informace;
- c. informace pravděpodobně nezpůsobí vážnou

škodu:

- i. jejímu zdraví; nebo
- ii. jejímu pokrevnímu rodu, členu její rodiny, nebo osobě v přímé genetické linii, pokud domácí právní řád poskytuje přiměřenou ochranu.

Podle písmene a. by osoba měla být rovněž informována, jestliže je tato informace důležitá pro její léčbu či prevenci.

9. Zabezpečení

9.1. Proti náhodnému nebo nezákonnému zničení, náhodné ztrátě, jakož i proti neautorizovanému přístupu, změnám, sdělením a jiným formám zpracování osobních údajů musí být učiněna náležitá technická a organizační opatření k jejich ochraně v souladu s tímto Doporučením.

Taková opatření musejí zajistit náležitou úroveň bezpečnosti s přihlédnutím na jedné straně k technickému stavu způsobu uložení a na druhé straně k citlivému charakteru zdravotních údajů a vyhodnocení potenciálních rizik.

Tato opatření musejí být periodicky prověřována.

9.2 Aby se zajistila důvěrnost, integrita a přesnost zpracovávaných údajů a rovněž ochrana pacientů, musí se přijmout vhodná opatření:

- a. aby se zabránilo v přístupu jakékoliv neautorizované osobě k zařízením používaným pro zpracování osobních údajů (kontrola vstupu do těchto zařízení);
- b. aby se neautorizované osobě zabránilo číst, kopírovat a měnit údaje na médiích (kontrola médií);
- c. aby se zabránilo neautorizovanému vstupu údajů do informačního systému a jakýmkoli neautorizovaným konzultacím, modifikacím nebo výmazům uložených osobních údajů (kontrola paměti);
- d. aby se zabránilo neautorizovaným osobám využívat automatizované systémy pro zpracování údajů pomocí zařízení pro přenos údajů (kontrola využití);
- e. aby se zajistilo, jednak se zřetelem na selektivní přístup k údajům a jednak k zabezpečení zdravotních údajů, že zpracování jako obecné pravidlo je stanoveno tak, že umožní oddělení:
 - identifikačních znaků a údajů vztahujících se

k identifikaci osob,

- administrativních údajů,
 - lékařských údajů,
 - sociálních údajů,
 - genetických údajů (kontrola přístupu);
- f. aby se zaručila možnost ověřit si a zkontrolovat, kterým osobám a kterým orgánům je možno osobní údaje sdělit pomocí zařízení pro přenos údajů (kontrola komunikace);
 - g. aby se zaručilo, že bude možné a posteriori ověřit a zjistit, kdo měl přístup do systému a jaké osobní údaje byly vloženy do informačního systému, kdy a kým (kontrola ukládání údajů);
 - h. aby se zabránilo neautorizovanému čtení, kopírování, změně nebo výmazu osobních údajů během sdělování osobních údajů a transportu médií pro ukládání údajů (kontrola transportu);
 - i. aby se údaje zajistily vytvářením bezpečnostních kopií (kontrola dostupnosti).

9.3 Správci souborů se zdravotními údaji by měli v souladu s domácím právním řádem vypracovat vhodné interní předpisy, které by respektovaly zásady obsažené v tomto Doporučení.

9.4 Tam, kde je to nutné, by měli správci souborů se zdravotními údaji jmenovat nezávislou osobu odpovědnou za bezpečnost informačních systémů a ochranu údajů, která bude kompetentní pro podávání rad o těchto otázkách.

10. Uchovávání

10.1 Všeobecně smějí být zdravotní údaje uchovávány jen po dobu potřebnou k dosažení účelu, pro který byly shromážděny a zpracovány.

10.2 Když v legitimním zájmu veřejného zdraví, lékařské vědy – prováděné osobou pověřenou léčením nebo kontrolním zdravotním orgánem – nebo z historických nebo statistických důvodů, se ukáže nutným uchovávat zdravotní údaje, které již nemají žádné použití pro původní účel, budou provedena technická opatření, aby se zajistilo správné uchovávání a zabezpečení s ohledem na soukromí pacienta.

10.3 Na žádost subjektu údajů musejí být jeho zdravotní údaje vymazány – pokud z nich nebyly udělaný údaje anonymní nebo pokud tomu nebrání důležité a legitimní zájmy, zejména zájmy uvedené v odstavci 10.2 nebo

povinnost uchovávat údaje.

11. Přeshraniční toky

11.1 Zásady tohoto Doporučení se vztahují i na toky zdravotních údajů přes hranice.

11.2 Toky zdravotních údajů do státu, který ratifikoval Úmluvu o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat (ETS 108), a který disponuje právním řádem, který poskytuje alespoň rovnocennou ochranu zdravotních údajů, by neměly podléhat zvláštním podmínkám ohledně ochrany soukromí.

11.3 Tam, kde ochrana zdravotních údajů může být považována za odpovídající zásadě rovnocenné ochrany stanovené v Úmluvě, neměla by být stanovena žádná omezení toků zdravotních údajů do státu, který neratifikoval Úmluvu, který však má zákonná ustanovení, jež jsou v souladu se zásadami této Úmluvy a tohoto Doporučení.

11.4 Pokud domácí právní řád nestanoví jinak, k tokům zdravotních údajů do státu, jehož zákonná ustanovení nejsou v souladu s Úmluvou a tímto Doporučením, by nemělo v zásadě dojít, pokud:

- a. nebyla přijata nutná opatření, včetně smluvních opatření, o respektování zásad Úmluvy a tohoto Doporučení a subjekt údajů má možnost proti předávání údajů podat námitku, nebo
- b. subjekt údajů nedal svůj souhlas.

11.5 Pokud nejde o naléhavý případ nebo o předávání, ke kterému subjekt údajů dal informovaný souhlas, měla by být přijata vhodná opatření zajišťující zvláštní ochranu údajů předávaných z jedné země do druhé, a zejména

- a. osoba odpovědná za předávání by měla adresátovi udat specifikované a legitimní účely, pro které byly údaje původně shromážděny, jakož i osoby nebo orgány, kterým mohou být sděleny;
- b. pokud domácí právní řád nestanoví jinak, adresát by se měl osobě odpovědné za předávání zavázat, že bude respektovat specifikované a legitimní důvody, které přijal, a že nebude sdělovat údaje jiným osobám nebo orgánům než těm, které byly udány osobou odpovědnou za předávání.

12. Vědecký výzkum

12.1 Všude, kde je to možné, by měly být zdravotní údaje

používané pro lékařský výzkum anonymní. Profesionální vědecké organizace a veřejné orgány by měly podporovat vývoj technik a procedur zajišťujících anonymitu.

12.2 Jestliže by však takováto anonymita znemožnila uskutečnit výzkumný lékařský projekt a tento projekt se má uskutečnit pro legitimní účely, může být proveden s osobními údaji za podmínky, že:

- a. subjekt údajů dal informovaný souhlas k jednomu nebo více výzkumným účelům, nebo
- b. subjektem údajů je osoba nezpůsobilá k právním úkonům a neschopná svobodného rozhodnutí, a domácí právní řád nedovoluje subjektu jednat vlastním jménem, jeho zákonný zástupce nebo úřad nebo jakákoliv osoba nebo orgán ustavené zákonem, dal souhlas v rámci výzkumného projektu majícího vztah ke zdravotnímu stavu nebo k nemoci subjektu údajů, nebo
- c. zpřístupnění údajů pro účel definovaného lékařského výzkumného projektu týkajícího se důležitého veřejného zájmu bylo schváleno orgánem nebo orgány určenými k tomu domácím právním řádem, avšak pouze jestliže:
 - i. subjekt údajů není výslovně proti zpřístupnění; a
 - ii. přes rozumné úsilí se ukázalo nemožným spojit se se subjektem údajů a vyžádat si jeho souhlas; a
 - iii. zájmy výzkumného projektu schválení opravňují; nebo
- d. výzkumný projekt je stanoven zákonem a představuje nutné opatření pro veřejné zdraví.

12.3 Podléhající doplňkovým opatřením vymezeným domácím právním řádem, zdravotničtí pracovníci oprávnění provádět vlastní lékařský výzkum by měli mít možnost používat zdravotní údaje, kterými disponují, po takovou dobu, o níž byl subjekt údajů informován a jestliže proti této možnosti nevznesl námitky.

12.4 Co se týče jakéhokoliv lékařského výzkumu založeného na osobních údajích, nahodilé problémy, včetně problémů etického a vědeckého charakteru, vzniklé respektováním ustanovení Úmluvy, by měly být posuzovány také ve světle dalších relevantních nástrojů.

12.5 Osobní údaje pro lékařský výzkum nesmějí být publikovány ve formě umožňující identifikovat subjekty údajů, pokud nebyl získán jejich souhlas k publikaci a publikace je

Elektronický podpis

- Vzhledem k tomu, že
- s účinností od 1. 12. 2001 byla ISO 17799 přejata do soustavy českých technických norem,
 - dne 25. května 2002, tj. rok po schválení FIPS 140-2, ukončil NIST testování kryptografických modulů podle FIPS 140-1 a zahájil testování podle FIPS 140-2, mění se znění požadavků Úřadu zveřejněných v kap. I. Věstníku č. 12/2001 následovně:

Úřad zveřejňuje požadavky podle § 2 odst. 7 a § 8 odst. 2 písm. b) vyhlášky č. 366/2001 Sb.

Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku

Při zpracování dokumentů „Celková bezpečnostní politika“ a „Systémová bezpečnostní politika“ se postupuje dle požadavků těchto norem:

ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti,

ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3.

Požadavky na kryptografické funkce

- Výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, musí odpovídat požadavkům na kryptografické moduly dle:
- Standard pro hodnocení bezpečnosti kryptografických modulů vydaný National Institute of Standards and Technology v USA – FIPS PUB 140-1 úroveň 3 nebo FIPS PUB 140-2 úroveň 3.

Původní znění uvedené ve Věstníku Úřadu č. 12/2001 se ruší.

Ověření bezpečnosti informačního systému pro certifikační služby z hlediska požadavků § 6 písm. c) vyhlášky č. 366/2001 Sb.

1. Úvod do problematiky

Podle § 6 písm. c) vyhlášky č. 366/2001 Sb. je jedním z požadavků ověření bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují, doložení:

„písemného posudku, jehož součástí je potvrzení, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti¹⁾, je používání informačního systému pro certifikační služby v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech uvedených v § 2 odst. 1 písm. c) a d). Kontrola bezpečnostní shody musí být prováděna opakovaně, a to vždy nejpozději do 12 měsíců od provedení poslední kontroly bezpečnostní shody“.

Základní požadavky na bezpečnost jsou specifikovány v zákoně č. 227/2000 Sb. a precizovány vyhláškou č. 366/2001 Sb.; v souladu s ustanovením § 2 odst. 7 jsou ve Věstníku Úřadu pro ochranu osobních údajů (dále jen „Věstník“) zveřejňována další upřesnění.

Věstník č. 19/2002 specifikuje, že při zpracování celkové bezpečnostní politiky (dále jen „CBP“) a systémové bezpečnostní politiky (dále jen „SBP“) se postupuje podle norem:

- ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti (dále jen „ČSN 17799“).
- ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT (dále jen „ČSN 13335“) 1 – 3,

2. Komentář a výklad

2.1. Kontrola bezpečnostní shody

Kontrola bezpečnostní shody²⁾ může být použita (ČSN 13335-3, kap. 11.2) ke kontrole shody:

- nových systémů a služeb IT po jejich implementaci (odsouhlasení – ČSN 13335-3, kap. 10.4),
- existujících systémů a služeb IT (monitorování, řešení incidentů – ČSN 13335-3, kap. 11.5),
- existujících systémů a služeb IT, když byly provedeny změny dotýkající se bezpečnosti systému IT (řízení změn – ČSN 13335-3, kap. 11.3).

Cílem kontroly bezpečnostní shody (ČSN 13335-3, kap. 11.2) je získat ujištění, že ochranná opatření

- jsou implementována,
- jsou implementována správně,
- jsou správně používána,
- jsou testována tehdy, je-li to důležité,
- poskytují vhodnou úroveň ochrany (v případě odsouhlasení se jedná o explicitní požadavek na ujištění).

Předmětem kontroly bezpečnostní shody jsou ochranná opatření jak u vlastních informačních technologií, tak i technologií obchodních partnerů, resp. poskytovatelů systémů (ČSN 13335-3, kap. 10.4; ČSN 17799, kap. 12.2.1).

Z hlediska efektivnosti je podstatné (ČSN 13335-2, kap. 16.2), aby ochranná opatření byla a zůstala ve shodě se specifikovanými ochrannými opatřeními (viz bezpečnostní politiky; plán bezpečnosti systému {ČSN 13335-2, kap. 13; ČSN 13335-3, kap. 9.7 }) v průběhu

- akvizice
- vývoje
- provozu
- údržby (včetně ukončení provozu/vyřazení z provozu).

Terminologie a členění životního cyklu vychází ze standardu ISVS³⁾ (dále jen „S_1_5“). Hlavním důvodem jeho užití je sjednocení metodiky a terminologie. Tento standard je veřejně dostupný, integruje v sobě i problematiku bezpečnosti, je zpracován v souladu s ČSN ISO/IEC 12207 a případnému zájemci může poskytnout doplňující informace.

2.1.1. Personál provádějící kontrolu bezpečnostní shody

Kontrolu bezpečnostní shody mohou provádět externí nebo interní pracovníci (ČSN 13335-2, kap. 16.2; ČSN 13335-3, kap. 11.2). V souladu s dokumenty CWA 14172-3:2001 (E)⁴⁾ kap. 3.5 lze doporučit, aby vedle odborné kompetentnosti byla prokázána i nezávislost subjektu provádějícího kontrolu bezpečnostní shody; z ČSN 13335-2 kap. 9.2. lze dovodit odpovědnost statutárního orgánu za specifikaci požadavků na kvalitu a kompetence subjektů provádějících kontrolu bezpečnostní shody.

2.1.2. Realizační výstupy kontroly bezpečnostní shody; posudek, potvrzení

Postupy či forma a obsah realizačních výstupů kontroly bezpečnostní shody nejsou vyhláškou ani zmíněnými normami exaktně specifikovány (interními normami organizace je možné navíc zohlednit i další potřeby, např. prioritu efektivnosti); norma (ČSN 13335-3, kap. 10.4) explicitně předpokládá přizpůsobení konkrétnímu systému IT.

Z hlediska postupů norma uvádí, že se jedná zejména o revize dokumentů, fyzické inspekce a technická hodnocení. Z normou specifikovaných klíčových činností (např. ČSN 13335-3, kap. 10.4 a 11.1; ČSN 17799, kap. 12), určení (ČSN 13335-2, kap. 16.3 a 7.2) a principů integrity lze dovodit, že realizačním výstupem budou minimálně

- zpráva (ve vyhlášce č. 366/2001 Sb. nazývána „posudek“) popisující průběh kontroly bezpečnostní shody, prezentující postupy, požadavky, použité a zjištěné fakta a závěry (zejména ve vztahu k normou explicitně specifikovaným klíčovým problémům - např. ČSN 13335-3, kap. 10.4, 11.2, 11.4), a to vše takovým způsobem, aby jiný čtenář zprávy (předpokládá se, že je obeznámen s obecnými principy bezpečnosti) mohl snadno nalézt informace, jež ho zajímají;

a

- hlášení (ve vyhlášce č. 366/2001 Sb. nazýváno „potvrzení“)
 - shrnující závěry z procesu kontroly bezpečnostní shody
 - a konstatující zejména:
 - zda bezpečnost byla odsouhlasena „plně“, „částečně“, „s omezením“, či odsouhlasena „nebyla“;
 - zda existují doklady o zřeknutí se práva na bezpečnost a zda trvá jejich platnost;

- zda existují jakákoli omezení zpracování;
- za jakých podmínek (změny systému nebo jeho okolí; platnost hodnocení; periodičita) by se měla opakovat kontrola bezpečnostní shody.

Realizační výstupy pak slouží jako podklad k udělení souhlasu (ČSN 13335-2, kap. 14) s uvedením systému nebo služby do provozu (resp. pokračováním v provozu); primárně tento souhlas uděluje management organizace.

2.2. Dokumentace systému

Jedním z atributů dokumentace systému je i lokace v čase, resp. místo a určení v životním cyklu.

Celková bezpečnostní politika („CBP“) a systémová bezpečnostní politika („SBP“) vznikají v počátečních fázích životního cyklu systému.

Certifikační prováděcí směrnice, plán pro zvládání krizových situací a plán obnovy tvoří součást výstupů vývojové etapy; jsou v nich popsány způsoby zajištění cílů z CBP a SBP.

Požadavek § 6 písm. c) vyhlášky č. 366/2001 Sb. explicitně odkazuje na CBP a SBP; z principů kontroly bezpečnostní shody dovodíme významnost výstupů, zejména pak certifikační prováděcí směrnice, plánu pro zvládání krizových situací a plánu obnovy. S vědomím této skutečnosti vyhláška č. 366/2001 Sb. § 2 odst. 1 vyžaduje po poskytovateli certifikačních služeb doložení i těchto dokumentů.

2.2.1. Celková bezpečnostní politika

CBP je dokumentem strategického významu; v organizaci každému známý dokument (ČSN 13335-3, kap. 10.2; ČSN 17799, kap. 3), vytvářející základ pro dosažení a udržení specifikované úrovně bezpečnosti.

Forma a stupeň podrobnosti CBP nejsou normami exaktně specifikovány; z požadavků norem (ČSN 13335-3, kap. 7.2; ČSN 17799, kap. 3) lze dovodit, že musejí splňovat zejména předpoklady úplnosti, srozumitelnosti, měřitelnosti, odpovědnosti, vynutitelnosti a vymahatelnosti.

Z hlediska obsahu Úřad pro ochranu osobních údajů (dále jen „Úřad“) doporučuje využít generická návěští kapitol, resp. podkapitol ČSN 13335-3, příloha A a ČSN 17799.

K omezení zneužitelnosti informací obsažených v CBP Úřad doporučuje, aby základní dokument, určený všem zaměstnancům i uživatelům, obsahoval přílohy s problémově orientovaným obsahem a selektivní dostupností; to však nikoli na úkor integrity.

Podstatné je, aby CBP specifikovala bezpečnostní cíle vyplývající z

- charakteru činnosti organizace a jejího poslání,
- požadavků (případně omezení) managementu,
- legislativního prostředí a regulačních závazků,
- bezpečnosti obecně.

Významným cílem, zejména pro poskytovatele certifikačních služeb, je i stanovení požadované míry bezpečnosti a úrovně její zaručitelnosti.

Na základě hrubé analýzy rizik jsou definovány priority a doporučeny prostředky k dosažení cílů, vymezeny zdroje a určena přijatelná zbytková rizika.

S ohledem na to, že nelze vyloučit poskytování některých služeb externími subjekty, považuje Úřad za významné, aby již na této úrovni byly vytvořeny předpoklady pro adekvátní naplnění legislativních požadavků v procesu kontroly bezpečnostní shody.

CBP je chápána jako dokument střednědobé platnosti; revize či vyšší míra podrobnosti CBP může být vyvolána změnami analýzy rizik, manažerskou revizí, výsledky kontroly bezpečnostní shody či vyhodnocením bezpečnostních incidentů.

Dalšími procesy je CBP rozpracována do vyšší míry podrobnosti a konkretizace v odpovídajících systémových bezpečnostních politikách.

2.2.2. Systémová bezpečnostní politika informačního systému

SBP vzniká v počátečních fázích životního cyklu systému a navazují na ni plány systému a dokumentace k testům (ČSN 13335-3, kap. 9.6 a 9.7; S_1_5 - kap. 6.3. a 7.13).

Forma a obsah SBP nejsou normami exaktně specifikovány; účelem SBP je specifikovat či řešit úkoly na vyšší úrovni podrobnosti a s vyšší mírou poznání, než je tomu u CBP. Klíčové statě SBP jsou uvedeny v ČSN 13335-2, kap. 12 a ČSN 13335-3, kap. 9.6.; požadavek na popis vazeb na okolní informační systémy (vyhláška č. 366/2001 § 2 odst. 6 písm. b)) lze naplnit i formou bezpečnostních politik rozhraní.

SBP je schvalována vyšším managementem organizace jako závazný soubor zásad a pravidel; s ohledem na návaznost alokace adekvátních zdrojů (vazba na plán bezpečnosti systému) k implementaci a prosazování bezpečnosti v provozu je nezbytné, aby údaje uvedené v SBP vycházely z úplného výčtu, byly konkrétní a identifikovaly ochranná opatření pro dosažení požadované míry bezpečnosti a úrovně zaručitelnosti (vazba na dokumentaci k testům).

Úřad považuje za podstatné zdůraznit požadavek zohlednit v analýze rizik nejen bezpečnost obecně, ale věnovat odpovídající pozornost specifickým atributům systému, organizace a jejího okolí.

2.2.3. Plán pro zvládání krizových situací a plán obnovy

Řízení kontinuity podnikatelských činností se věnuje kapitola 11 ČSN 17799, zatímco norma ČSN 13335 nevyčleňuje tyto aktivity, ale předpokládá, že se jedná o naplnění cílů CBP a SBP (existenci plánů lze dovodit např. z činností při řešení incidentů - ČSN 13335-2, kap. 16.4 a ČSN 13335-3, kap. 11.5.); cíle, analýza rizik a plán bezpečnosti primárně určují inherentní robustnost systému, z které je odvozen charakter plánu pro zvládání krizových situací a plán obnovy (dále jen „PKSPO“).

Forma a obsah PKSPO nejsou normami exaktně specifikovány; účelem PKSPO je, aby činnost organizace mohla být obnovena v požadovaných lhůtách, resp. byl vytvořen předpoklad k minimalizaci škod. Úřad předpokládá, že generické činnosti uvedené v ČSN 17799, kap. 11 budou rozpracovány do konkrétních podmínek systému; současně je připraven akceptovat, aby forma byla podřízena účelu PKSPO.

Úřad přikládá vysoký význam testování, udržování a přehodnocování PKSPO.

2.2.4. Certifikační prováděcí směrnice

Citované normy ČSN 13335 a ČSN 17799 mají vyšší míru obecnosti a širší aplikovatelnosti. Problematické kryptografických opatření je explicitně věnována kapitola 10.3 ČSN 17799.

Vyhláška č. 366/2001 Sb. v § 2 odst. 4 uvádí, že

„obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.“

Forma a obsah certifikační prováděcí směrnice (dále jen „CPS“) nejsou výše uvedenými normami exaktně specifikovány. Úřad doporučuje, aby pro CPS byla použita struktura uvedená v RFC 2527.

Na bázi RFC 2527 byl Úřadem zpracován dokument, který extrahuje podstatné ve vztahu ke struktuře CPS. Dokument, v jazyce českém, bude na vyžádání zaslán zájemcům elektronickou poštou. Žádosti lze uplatnit na adrese e-mail: info@uouu.cz.

S ohledem na význam CPS a její postavení ve vztahu k CBP, SBP, PKSPO a směrnici systému považuje Úřad za optimální, aby CPS v jednotlivých kapitolách a subkapitolách rekapitulovala relevantní bezpečnostní cíle, zásady a pravidla a následně specifikovala způsoby jejich naplnění, resp. stručnou charakteristiku této realizace, a odkaz na příslušné směrnice, resp. jiné interní normativy.

Použité zkratky

CBP	celková bezpečnostní politika
CPS	certifikační prováděcí směrnice
EESSI	European Electronic Signature Standardization Initiative
ISVS	informační systém veřejné správy
IT	informační technologie
PKSPO	plán pro zvládání krizových situací a plán obnovy
S_1_5	Standard ISVS pro náležitosti životního cyklu informačního systému verze 1.1; Věstník Úřadu pro veřejné informační systémy, ročník 1, částka 5; Praha 2000
SBP	systémová bezpečnostní politika

- 1) ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1 – 3.
- 2) Kontrola bezpečnostní shody je nazývána také bezpečnostní audit nebo bezpečnostní revize (ČSN 13335-2, kap. 16.2)
- 3) Standard ISVS pro náležitosti životního cyklu informačního systému verze 1.1; Věstník Úřadu pro veřejné informační systémy, ročník 1, částka 5; Praha 2000
- 4) EESSI Conformity Assessment Guidance – part 3: Trustworthy Systems Managing Certificates for Electronic Signatures

V odpověď na časté dotazy veřejnosti i médií na vývoj soudního sporu mezi Úřadem pro ochranu osobních údajů a Českým statistickým úřadem, které v poslední době byly vyvolány tiskovou konferencí ČSÚ (konala se 17. 6. 2002), zveřejňuje Úřad pro ochranu osobních údajů Usnesení Ústavního soudu ze dne 16. 1. 2002, k čemuž získal svolení Ústavního soudu.

III. ÚS 672/01

ČESKÁ REPUBLIKA

USNESENÍ

Ústavního soudu

Ústavní soud rozhodl ve věci ústavní stížnosti navrhovatele Českého statistického úřadu, se sídlem v Praze 8, Sokolovská 142, o návrhu na zahájení řízení ve sporu o rozsah kompetencí podle čl. 87 odst. 1 písm. k) Ústavy ve věci stanovení rozsahu údajů shromažďovaných a dále zpracovávaných při sčítání lidu, domů a bytů v roce 2001 a ve věci zničení těchto údajů, mimo ústní jednání dne 16. ledna 2002 soudcem zpravodajem JUDr. Vlastimilem Ševčíkem, **takto:**

Návrh se **odmítá.**

Odůvodnění

Podáním, označeným jako „návrh na zahájení řízení ve sporu o rozsah kompetencí podle čl. 87 odst. 1 písm. k) Ústavy ve věci stanovení rozsahu údajů shromažďovaných a dále zpracovávaných při sčítání lidu, domů a bytů v roce 2001 a ve věci zničení těchto údajů“, a následně doplněným dalším podáním ze dne 19. prosince 2001, se navrhovatel domáhá zahájení řízení, když tvrdí, že jde o kompetenční spor mezi státními orgány, totiž mezi Českým statistickým úřadem a Úřadem pro ochranu osobních údajů [čl. 87 odst. 1 písm. k) Ústavy, § 120 odst. 1, 2 písm. a) zák. č. 182/1993 Sb., ve znění pozdějších předpisů, dále jen zákona] ve věci příslušnosti k přijetí rozhodnutí (opatření) o tom, které údaje mají být zjišťovány (shromažďovány) a dále zpracovávány v rámci sčítání lidu, domů a bytů v roce 2001.

Z obsahu návrhu a odůvodnění jím napadených rozhodnutí vyplývá, že kontrolním protokolem Úřadu pro ochranu osobních údajů ze dne 23. dubna 2001 byla navrhovateli v souladu s § 40 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen zákon o ochraně osobních údajů), uložena likvidace těchto osobních údajů shromažďovaných a zpracovávaných v rámci sčítání lidu, domů a bytů v roce 2001:

1. „počet všech narozených dětí“,
2. „z toho v nynějším nebo v pozdějším manželství“,
3. „uveďte kolik osob zaměstnáváte“.

Proti tomuto opatření podal navrhovatel námitku k předsedovi Úřadu pro ochranu osobních údajů, o níž bylo rozhodnuto takto:

1. položka, označená jako „1.“ v opatření k nápravě „počet všech narozených dětí“, se z opatření k nápravě, uložených kontrolním protokolem ze dne 23. dubna 2001, vypouští,
2. uložena likvidace položek označených v opatření k nápravě uložených kontrolním protokolem jako „2.“ a „3.“ tedy „z toho v nynějším či pozdějším manželství“ a „uveďte kolik osob zaměstnáváte“ se potvrzuje.

Z odůvodnění návrhu dále plyne, že podle navrhovatele Úřad pro ochranu osobních údajů svými zásahy a vydanými rozhodnutími znemožňuje výkon jeho pravomocí podle zákona č. 158/1999 Sb., o sčítání lidu, domů a bytů v roce 2001 (dále jen zákon o sčítání), a to tak, že jimi zasahuje do toho, jaké údaje mají být shromažďovány a zpracovávány v roce 2001 a zda a kdy mají být tyto údaje likvidovány, ačkoliv je k přijímání takových opatření příslušný výlučně navrhovatel. Pokud tedy Úřad pro ochranu osobních údajů uložil navrhovateli provést likvidaci osobních údajů bez toho, aby tak učinil na základě žádosti konkrétního subjektu, překročil svoji kompetenci, jež mu přiznává zákon o ochraně osobních údajů. Navrhovatel dále ve svém podání rozvíjí vztah obou zákonů (zákona o ochraně osobních údajů a zákona o sčítání) a z nich dovozuje nepřislušnost Úřadu pro ochranu osobních údajů vydávat opatření stran údajů, které mají být zjišťovány a zpracovávány v rámci sčítání v roce 2001. Navrhovatel poukázal na to, že pokud by měl vykonat uloženou mu povinnost, musel by zničit všechny sčítací formuláře, čímž by sčítání nemohlo proběhnout, a proto by také došlo ke značným rozpočtovým ztrátám a závěrem navrhl, aby Ústavní soud vydal následující nález:

1. Orgánem příslušným stanovit rozsah shromažďovaných a dále zpracovávaných údajů podle zákona o sčítání je na základě zmocnění k vydání prováděcího právního předpisu uvedeného v § 7 odst. 3 a § 22 tohoto zákona Český statistický úřad.
2. Orgánem příslušným rozhodnout o likvidaci údajů shromažďovaných a dále zpracovávaných podle zákona o sčítání a vyhlášky č. 354/2000 Sb., kterou se stanoví vzory sčítacích tiskopisů pro sčítání v roce 2001 a vzor průkazu sčítacího komisaře a sčítacího revizora, zejména o skartaci nebo jiné likvidaci sčítacích tiskopisů, je Český statistický úřad.
3. Úřad pro ochranu osobních údajů je povinen zdržet se

zásahů do kompetencí Českého statistického úřadu při zpracování údajů pro účely sčítání v roce 2001.

4. Opatření k nápravě, uložené Úřadem pro ochranu osobních údajů Českému statistickému úřadu v kontrolním protokole ze dne 23. dubna 2001, se spolu s rozhodnutím předsedy Úřadu pro ochranu osobních údajů, č.j. 549/01-KP/RP ze dne 28. června 2001, zrušují.

Návrh je nepřipustný.

Předně bylo nutno v dané věci posoudit, zda jde o kompetenční spor ve smyslu dále uvedených ustanovení Ústavy ČR a zákona. Jinými slovy řečeno, zda jde o spor, jež přísluší k rozhodnutí Ústavnímu soudu.

Ústavní soud rozhoduje ve sporech o rozsah kompetencí státních orgánů podle čl. 87 odst. 1 písm. k) Ústavy ČR. Předmětem takového kompetenčního sporu, ve smyslu uvedeného ustanovení Ústavy ČR a § 120 zákona, je otázka příslušnosti vydat rozhodnutí nebo činit opatření nebo jiné zásahy (dále jen rozhodnutí) ve věci uvedené v návrhu na zahájení řízení. Ústavní soud v případě, že jiný orgán, který je účastníkem řízení v kompetenčním sporu, vydal rozhodnutí ve věci uvedené v návrhu a podle Ústavního soudu je k vydání takového rozhodnutí příslušný jiný orgán, příp. jestliže orgán vydal rozhodnutí, kterým svoji kompetenci popřel, a podle zjištění Ústavního soudu je k vydání rozhodnutí ve věci příslušný. Ústavní soud takové rozhodnutí svým nálezem zruší (§ 125 zákona); je tedy zřejmé, že účelem řízení ve sporech o rozsah kompetencí je rozhodnutí v konkrétním sporu, kdy dva orgány uplatňují spornou kompetenci k vydání rozhodnutí (pozitivní kompetenční konflikt) nebo svou příslušnost popírají (negativní kompetenční konflikt), nikoliv však abstraktní výklad Ústavy ČR, příp. jednoduchého práva (k tomu srov. např. Filip/Holländer/Šimíček: Zákon o Ústavním soudu. Komentář. C. H. Beck, 2001, str. 472 a násl.), o který navrhovatel usiluje. Tento závěr vyvodil Ústavní soud z následujících úvah:

Podle § 2 zákona o ochraně osobních údajů jsou Úřadu pro ochranu osobních údajů svěřeny kompetence ústředního správního úřadu pro oblast kontroly osobních údajů v rozsahu stanoveném tímto zákonem. Za tímto účelem provádí tento úřad dozor nad dodržováním povinností stanovených zmíněným zákonem při zpracování osobních údajů. Při výkonu dozoru ve formě kontroly pak postupuje podle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů. Zjistí-li kontrolující při výkonu kontroly, že došlo k porušení povinností stanovených zákonem o ochraně osobních údajů, uloží potřebná opatření tak, aby zjištěné nedostatky byly odstraněny (§ 40 zákona o ochraně osobních údajů).

V dané věci tato situace nastala, a proto kontrolující (Úřad pro ochranu osobních údajů) svým opatřením (kontrolním protokolem ze dne 23. dubna 2001) navrhovateli, v souladu s § 40 odst. 1 zákona o ochraně osobních údajů, uložil likvidaci dotčených údajů.

Naproti tomu kompetence Českého statistického úřadu je stanovena v zákoně o sčítání. Z ust. § 17 tohoto zákona vyplývá, že stěžejním úkolem Českého statistického úřadu je organizačně-technické zabezpečení sčítání a zpracování, resp. zveřejnění údajů takto získaných. Nadto podle § 13 odst. 4 zákona o sčítání, není-li stanoveno jinak, použije se na ochranu údajů o fyzických osobách shromažďovaných při sčítání zákon o ochraně osobních údajů.

Provede-li se komparace kompetencí navrhovatele a Úřadu pro ochranu osobních údajů, jak vpředu byly vloženy, a to ve vztahu k vydaným a návrhem napadeným rozhodnutím Úřadu pro ochranu osobních údajů, je zřejmé, že při vydání rozhodnutí (opatření), jímž byla uložena likvidace údajů, ke kompetenčnímu konfliktu nedošlo a ani dojít nemůže, neboť není splněna základní podmínka kompetenčního konfliktu ve smyslu čl. 87 odst. 1 písm. k) Ústavy ČR a § 120 zákona, totiž že by šlo o spor, kdo by měl vydat rozhodnutí (opatření) podle § 40 zákona o ochraně osobních údajů. Navrhovatel v tomto směru žádné námitky nevznáší a pouze v tomto případě by šlo o pozitivní kompetenční konflikt, k jehož řešení by byl Ústavní soud příslušný. Existenci kompetenčního konfliktu je totiž nutno posuzovat vždy ve vztahu ke konkrétnímu rozhodnutí, resp. ve vztahu orgánu příslušnému k jeho vydání. Navrhovatel ve svém návrhu zaměřuje povinnost skartovat sčítací tiskopisy po skončení zpracování výsledků sčítání (§ 13 odst. 5 zákona o sčítání), tedy povinnost uloženou mu ex lege, s příslušností Úřadu pro ochranu osobních údajů k vydání rozhodnutí (opatření) podle § 40 odst. 1 zákona o ochraně osobních údajů.

Z povahy věci je proto zřejmé, že nemůže dojít ke sporu, kdo vydá rozhodnutí o uložení likvidace osobních údajů (opatření k nápravě) podle § 40 odst. 1 zákona o ochraně osobních údajů, neboť orgánem k tomu oprávněným je vždy Úřad pro ochranu osobních údajů.

Tomuto závěru nasvědčuje ostatně i to, že navrhovatel byl účastníkem správního řízení, zahájeného Úřadem pro ochranu osobních údajů, který mu napadenými rozhodnutími autoritativně uložil povinnost (likvidaci části údajů). Navrhovatel v této souvislosti poukazuje na nesprávný výklad zákona o ochraně osobních údajů a zákona o sčítání Úřadem pro ochranu osobních údajů, jinak řečeno brojí proti rozsahu věcné působnosti Úřadu pro ochranu osobních údajů takové rozhodnutí (opatření), ve vztahu k údajům získaným podle zákona o sčítání, vydat. Situace, že by navrhovatel zahájil řízení podle § 40 zákona o ochraně osobních údajů, však nepřipadá v úvahu, a jak již bylo zmíněno, navrhovatel takovou svoji kompetenci v návrhu ani neuplatňoval. Za tohoto stavu věci je zřejmé, že navrhovatel se svým návrhem domáhá abstraktního výkladu kolizních ustanovení obou zákonů, k čemuž však není Ústavní soud příslušný (k tomu srov. např. rozhodnutí pléna Ústavního soudu ve věci sp. zn. Pl. 58/2000 ze dne 20. března 2001, č. 285/2001 Sb.).

Jinou otázkou ovšem je, zda k návrhu připojená rozhodnutí byla vydána v rámci příslušných právních předpisů, tedy

zda ob stojí z hlediska zákonnosti, jejímž nedílným prvkem je posouzení otázky rozsahu věcné příslušnosti Úřadu pro ochranu osobních údajů ve vztahu k vydaným rozhodnutím. Z tohoto hlediska však nemohla být tato rozhodnutí podrobená přezkumu Ústavním soudem, neboť orgánem k tomu oprávněným je příslušný správní soud. Proti rozhodnutí předsedy Úřadu pro ochranu osobních údajů lze totiž podat správní žalobu (§ 40 odst. 2 zákona o ochraně osobních údajů).

Z takto rozvedených důvodů byl návrh navrhovatele posouzen jako nepřipustný, neboť jde o návrh, k jehož projednání není Ústavní soud příslušný (§ 43 odst. 1 písm. d)

zákona), a jako takový byl odmítnut, jak je ze znělky tohoto usnesení patrné.

Poučení: Proti tomuto usnesení není odvolání přípustné (§ 43 odst. 3 zákona).

V Brně dne 16. ledna 2002

JUDr. Vlastimil Ševčík
soudce Ústavního soudu ČR

Věstník Úřadu pro ochranu osobních údajů

Vydavatel: Úřad pro ochranu osobních údajů

Adresa redakce: Úřad pro ochranu osobních údajů, Havelkova 22, 130 00 Praha 3

Šéfredaktor: Mgr. Ladislav Hejlík, tel.: 02/21008 248, fax: 2271 7682

e-mail: info@uoou.cz

internetová adresa: www.uoou.cz

Administrace: Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: (02) 830 903 52, 830 903 54, fax: (02) 33 55 34 22, www.sevt.cz, e-mail: 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 980 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: (02) 830 903 52, 830 903 54, fax: (02) 33 55 34 22; drobný prodej v prodejnách SEVT, a. s. – Praha 5, Elišky Peškové 14, tel./fax: (02) 57 32 00 49, – Praha 4, Jihlavská 405, tel.: (02) 61 26 43 25 – Brno, Česká 14, tel.: (05) 42 21 39 62 – Ostrava, Nádražní 29, tel.: (069) 612 06 90 – České Budějovice, Česká 3, tel.: (038) 73 19 045 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 zaevídování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamaci je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČO (právnícká osoba) a kmenové číslo předplatitele. **Podávání novinových zásilek** povoleno ŘPP Praha.

ISSN 1213-3442