

Univerzita Karlova v Praze
Právnická fakulta

Rigorózní práce

Ochrana osobních údajů v pracovněprávních vztazích

Konzultant: Doc. JUDr. Margerita Vysokajová, CSc

Zpracovatel: Mgr. Ludmila Nováková

Březen, 2006

Poděkování

Na tomto místě bych ráda poděkovala Doc. JUDr. Margeritě Vysokajové, CSc.
za konzultace a rady, které mi při zpracování této rigorózní práce poskytla.

Prohlášení

Prohlašuji, že jsem tuto rigorózní práci zpracovala samostatně a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala, způsobem ve vědecké práci obvyklým.

V Praze dne.....*8.5.2006*.....

Ludmila Nováková
Mgr. Ludmila Nováková

Obsah

	Úvod	1
1.	Úprava ochrany osobních údajů na mezinárodní úrovni	3
1.1.	Organizace spojených národů	3
1.2.	Organizace pro ekonomickou spolupráci a rozvoj	4
1.3.	Rada Evropy	5
1.4.	Evropská unie	9
1.4.1	Směrnice Evropského parlamentu a Rady č. 95/46/ES	11
1.4.2	Směrnice Evropského parlamentu a Rady č. 97/66/ES a směrnice č. 200/58/ES	12
1.4.3.	Nařízení Evropského parlamentu a Rady č. 45/2004 a rozhodnutí Evropského parlamentu, Rady a Komise č. 1247/2002/ES	13
1.4.4.	Rozhodnutí týkající se předávání osobních údajů do zahraničí	14
2.	Vývoj právní úpravy ochrany osobních údajů v České republice	16
2.1.	Zákon č. 256/1992 Sb.	17
2.2.	Zákon č. 101/2000 Sb.	18
2.2.1.	Zákon č. 227/2000 Sb.	20
2.2.2.	Zákon č. 177/2001 Sb.	21
2.2.3.	Zákon č. 450/2001 Sb.	23
2.2.4.	Zákon č. 107/2002 Sb.	24
2.2.5.	Zákon č. 309/2002 Sb. a zákon č. 310/2002 Sb.	25
2.2.6	Zákon č. 517/2002 Sb.	26
2.2.7	Zákon č. 439/2004 Sb.	26
2.2.8.	Zákon č. 480/2004 Sb.	28
2.2.9.	Zákon č. 626/2004 Sb.	28
3.	Základní pojmy ochrany osobních údajů a působnost zákona č. 101/2000 Sb.	30
3.1.	Vymezení základních pojmů	30
3.1.1.	Osobní údaj, citlivý osobní údaj, anonymní údaj a zveřejněný osobní údaj	31
3.1.2.	Subjekt údajů	39
3.1.3.	Souhlas subjektu údajů	40
3.1.4.	Zpracování osobních údajů	41
3.1.5.	Správce, zpracovatel a příjemce osobních údajů	43
3.1.6	Evidence a datové soubory	47

3.2.	Působnost zákona 101	47
4.	Práva a povinnosti při zpracování osobních údajů v rámci pracovněprávních vztahů	53
4.1.	Povinnosti zaměstnavatele před zahájením zpracování osobních údajů	54
4.2.	Povinnosti zaměstnavatele v průběhu zpracování osobních údajů	70
4.3.	Povinnosti zaměstnavatele v souvislosti s ukončením zpracování osobních údajů	80
4.4.	Povinnost zaměstnanců při zpracování osobních údajů	83
4.5.	Práva zaměstnanců jako subjektů údajů	86
5.	Některé aktuální otázky spojené se zpracováním osobních údajů v pracovněprávních vztazích	91
5.1.	Předávání osobních údajů zaměstnanců do zahraničí	91
5.2.	Využití rodných čísel v pracovněprávních vztazích	96
5.3.	Kontrola práce zaměstnance a ochrana osobních údajů	101
6.	Úřad pro ochranu osobních údajů	113
6.1.	Kompetence Úřadu pro ochranu osobních údajů podle zákona č. 101/2000 Sb.	115
6.2.	Kompetence Úřadu pro ochranu osobních údajů podle jiných zákonů	120
	Závěr	121
	Literatura	
	Seznam použitých zkratk	
	Resume	
	Přílohy	

Úvod

Ochrana osobních údajů je relativně mladou právní disciplínou – této problematice je obecně věnována větší pozornost přibližně od počátku 90. let, v České republice však spíše až od jejich druhé poloviny. Zato je disciplínou dynamicky se rozvíjející a nabývající na významu v mnoha oblastech života, pracovněprávní vztahy nevyjímaje. Zmíněná aktuálnost a rostoucí důraz kladený na ochranu osobních údajů byly také hlavními důvody volby tématu této práce.

Svou povahou však spadá ochrana osobních údajů do již tradiční oblasti ochrany soukromého života, neboť zajištěním bezpečnosti informací týkajících se konkrétních fyzických osob, tj. osobních údajů, je primárně sledováno zachování soukromí jednotlivce. V době, kdy informace o našem způsobu života jsou ceněným zbožím a jejich zneužití může vyústit ve velmi závažný zásah nejen do soukromí a majetkových poměrů, ale i do základních osobnostních práv dotčené osoby (typicky v případě tzv. krádeže identity), nabývá ochrana osobních dat na významu. Postupující globalizací současné informační společnosti a možnostmi, které nabízejí nové komunikační a počítačové technologie, se rizika, jimž je soukromí každého z nás vystaveno, ještě zvyšují.

Nejlepší ochranou osobních údajů by jistě bylo vyloučení jakéhokoli jejich shromažďování, uchovávání a využívání, což si ovšem lze představit jen stěží. Pro fungování dnešní společnosti je možnost relativně spolehlivé identifikace každého jedince nezbytná a zpracování osobních údajů je proto nedílnou součástí mnoha, ne-li všech, lidských činností. V současné době je (alespoň teoreticky) vyloučeno, aby se občan České republiky nijak nejmenoval, neměl přiděleno rodné číslo nebo nebyl nahlášen k trvalému pobytu a nebyl na základě těchto informací jednoznačně identifikovatelný. Nejrůznějších informací osobního charakteru, které lze nejrůznějšími způsoby využít (a tedy i zneužít), navíc během života neustále přibývá – v souvislosti se školní docházkou, zaměstnáním, rodinným životem apod.

Z nezbytnosti shromažďování a dalšího zpracování osobních dat potom logicky vyplývá potřeba existence pravidel stanovících jednoznačné podmínky nakládání s těmito informacemi tak, aby bylo zajištěno, že nedojde k jejich zneužití. Základním cílem takové úpravy by přitom mělo být dosažení preventivní účinnosti, tj. stavu, kdy by k žádnému zneužití dat a následnému zásahu do soukromí dojít nemělo, neboť již jednou narušené soukromí lze jen stěží obnovit.

V České republice je základní právní normou (lex generalis) upravující pravidla zpracování osobních údajů zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, (dále jen „ZOOÚ“). Tento zákon provádí základní právo na ochranu osobních údajů zakotvené v zákoně č. 2/1993 Sb., o vyhlášení Listiny základních práv a

svobod jako součásti ústavního pořádku České republiky, (dále jen „Listina“) a doplňuje právní úpravu ochrany osobnosti upravenou zákonem č. 40/1964 Sb., občanský zákoník.

Dílčí úprava ochrany osobních údajů (lex specialis) je však obsažena v nejrůznějších právních předpisech veřejnoprávní i soukromoprávní oblasti, z nichž lze jmenovat např. zákon č. 21/1992 Sb., o bankách, zakotvující bankovní tajemství ve vztahu ke zpracovávaným informacím, dále zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, stanovící způsob a rozsah zpracování osobních údajů v souvislosti s předcházením tzv. praní špinavých peněz, dále např. zákon č. 89/1995 Sb., o státní statistické službě, upravující ochranu dat získaných a zpracovaných Českým statistickým úřadem nebo jiným orgánem státní správy při výkonu státní statistické služby, dále zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, upravující pravidla pro vedení Informačního systému evidence obyvatel a pravidla pro nakládání s rodnými čísly, nebo zákon č. 283/1991 Sb., o Policii České republiky, stanovící odlišná pravidla pro zpracování informací policií pro účely trestního řízení a pátrání po osobách. Osobním údajům je poskytována ochrana také na základě zákona č. 140/1961 Sb., trestní zákon, který v § 178 upravuje trestný čin neoprávněného nakládání s osobními údaji.

V neposlední řadě jsou pravidla pro zpracování osobních údajů zakotvena i v zákoně č. 65/1965 Sb., zákoník práce, (dále jen „zákoník práce“), na jehož základě je zaměstnavatel oprávněn či povinen evidovat o svých zaměstnancích určité informace.

Cílem této práce je poskytnout pokud možno ucelený přehled o problematice zpracování osobních údajů právě v rámci pracovněprávních vztahů. V zájmu uceleného pohledu se nelze vyhnout popisu mezinárodní právní úpravy ochrany osobních údajů, z níž česká vychází, a popisu vývoje právní úpravy této problematiky v České republice. Nejvíce prostoru je věnováno rozboru základní terminologie ochrany dat a povinností, které ZOOÚ účastníkům pracovněprávních vztahů ukládá. V závěru práce jsou stručně nastíněny některé aktuální problémy ochrany dat a role českého dozorového orgánu pro tuto oblast – Úřadu pro ochranu osobních údajů (dále také jen „Úřad“).

1. Úprava ochrany osobních údajů na mezinárodní úrovni

Ačkoli snaha chránit si své soukromí provází lidstvo již od dávné historie, právní úprava ochrany osobnosti a soukromí jednotlivce, a tedy implicitně také ochrana osobních údajů jakožto jedna z jejích složek, má své kořeny až v poválečných mírových procesech, kdy se hodnota lidského života a otázka jeho kvality dostaly poprvé do středu zájmu politických špiček i široké veřejnosti.

Právo na ochranu osobnosti a soukromí, které bývá někdy označováno jako právo tzv. čtvrté generace základních práv, tak bylo nejdříve obsahem mezinárodních dokumentů, z nichž poté postupně pronikalo do právních předpisů na národní úrovni. Z hlediska pojetí základních práv jakožto přirozených práv, která má každý již z toho titulu, že je lidským jedincem, mají však tyto národní právní úpravy pouze deklaratorní povahu.¹

1.1. Organizace spojených národů

Historicky prvním z mezinárodních dokumentů upravujících právo na ochranu osobnosti a soukromí byla Všeobecná deklarace lidských práv (dále jen „Deklarace“), která byla vyhlášena dne 10. prosince 1948 na půdě Organizace spojených národů. Čl. 12 Deklarace garantuje práva každého jednotlivce na ochranu před svévolnými zásahy do jeho soukromého života, do rodiny, domova nebo korespondence a před útoky na jeho čest a pověst.² Deklarace poprvé určitým způsobem definovala lidská práva a základní svobody a její význam pro další vývoj úpravy lidských práv na mezinárodní i vnitrostátní úrovni není zanedbatelný, nicméně pro členské státy OSN není Deklarace právně závazná.

V roce 1966 byl k podpisu otevřen další významný dokument OSN – Mezinárodní pakt o občanských a politických právech, který vstoupil v platnost dne 23. března 1976, a který na rozdíl od zmíněné Deklarace pro členské státy právně závazný je.³ Článek 17 tohoto paktu zakotvuje mj. zákaz svévolného zasahování do soukromého života, do rodiny, domova nebo korespondence a současně právo každého na zákonnou ochranu před takovými zásahy. Mezinárodní pakt o občanských a politických právech tak lze považovat za základní kámen dnešních úprav ochrany osobnosti a potažmo ochrany osobních údajů.

¹ Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, a.s., 2004, s. 11.

² Článek 12 Deklarace: „Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“

³ Tento pakt byl přijat Federálním shromážděním ČSSR, ratifikován prezidentem republiky a ve Sbírce zákonů publikován vyhláškou ministra zahraničních věcí č. 120/1976 Sb. ze dne 10. května 1976.

V rámci systému OSN působí již od roku 1946, kdy byla do tohoto systému jako první ze specializovaných mezinárodních organizací začleněna, také Mezinárodní organizace práce (International Labour Organisation, dále jen „MOP“).⁴ Základním cílem MOP je podpora sociální spravedlnosti a mezinárodně uznávaných lidských a pracovních práv, čehož se snaží dosahovat formulováním a prosazováním mezinárodních pracovních standardů stanovících minimální úroveň základních pracovních práv v nejrůznějších oblastech. V souvislosti se zvýšenou pozorností, která je ochraně soukromí a osobních údajů jedinců v poslední době věnována, přijala MOP v roce 1997 Kodex o ochraně osobních údajů zaměstnanců,⁵ v němž specifikuje obecné definice a zásady ochrany osobních údajů ve vztahu k osobním údajům zaměstnanců zpracovávaným zaměstnavateli v rámci pracovněprávních vztahů.⁶

1.2. Organizace pro hospodářskou spolupráci a rozvoj

Přestože současná legislativa v oblasti ochrany osobních údajů ve většině evropských států vychází z dokumentů přijatých Radou Evropy a z právních norem Evropské unie, základní principy právní úpravy byly poprvé vyjádřeny v Pravidlech pro ochranu soukromí a přeshraniční toky osobních údajů,⁷ dokumentu Organizace pro hospodářskou spolupráci a rozvoj (dále jen „OECD“) z roku 1980, která jsou dodnes východiskem pro ochranu osobních údajů v zemích, které nejsou členy Rady Evropy či Evropské unie.

V tomto dokumentu jsou poprvé na mezinárodní úrovni, ač zatím bez větší závaznosti, definovány dnes již běžně užívané pojmy, jako např. „osobní údaj“, „správce osobních údajů“, „předávání osobních údajů“, a dále dnes obecně uznávané zásady, jako zásada omezení shromažďování osobních údajů (Collection Limitation Principle), zásada kvality údajů (Data Quality Principle), zásada stanovení účelu (Purpose Specification Principle), zásada omezeného využití údajů (Use Limitation Principle), zásada bezpečnostních opatření (Security Safeguards Principle), zásada otevřenosti (Openess Principle), zásada účasti subjektu údajů (Individual Participation Principle) nebo zásada zodpovědnosti správce údajů (Accountability Principle). Dále jsou zde zahrnuta i pravidla pro národní a mezinárodní aplikaci uvedených zásad a další doporučené přístupy.

⁴ MOP byla však založena již v roce 1919 v souvislosti s Versailleským mírovým procesem, kde byl mj. přijat i zakládající dokument MOP (Ústava Mezinárodní organizace práce – Constitution of the International Labour Organization).

⁵ Code of Practice on protection of workers' personal data.

⁶ Tento kodex nepřináší nové požadavky na ochranu osobních údajů, pouze aplikuje zásady vyjádřené již dříve v dokumentech Rady Evropy a Evropské unie (viz níže) na pracovněprávní vztahy. Některé požadavky na ochranu osobních údajů zaměstnanců vyjádřené v tomto dokumentu jsou uvedeny v kapitole 5.3.

⁷ Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

1.3. Rada Evropy

Základním dokumentem Rady Evropy v oblasti ochrany lidských práv je Evropská úmluva o ochraně lidských práv a základních svobod (dále jen „Evropská úmluva“),⁸ která byla sjednána v Římě dne 4. listopadu 1950. V čl. 8 Evropské úmluvy je zakotveno právo na respektování soukromého a rodinného života, a to následujícím způsobem:

1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.
2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Citovaný odstavec 1 tedy upravuje identické právo jako již zmíněný čl. 12 Deklarace (ostatně v preambuli Evropské úmluvy je na tento dokument OSN přímo odkazováno) a současně jsou zde, v odstavci 2, taxativně vymezeny podmínky, za nichž je možné deklarované právo na ochranu soukromí omezit.

Dalším výrazným přínosem Evropské úmluvy je, že k zajištění plnění závazků smluvních stran přijatých touto úmluvou byl na základě čl. 19 zřízen Evropský soud pro lidská práva. Čl. 19 tak umožnil výklad a aplikaci Evropské úmluvy nadnárodním, nezávislým soudním orgánem, jehož rozhodnutí jsou významným korektivem legislativy i judikatury všech členských zemí Rady Evropy (některá zásadní rozhodnutí v oblasti ochrany osobních údajů a soukromí zaměstnanců jsou zmíněna v kapitole 5.3).

Evropská úmluva je ve smyslu čl. 10 zákona č. 1/1993 Sb., Ústava České republiky, (dále jen „Ústava“), jako vyhlášená mezinárodní smlouva, k jejíž ratifikaci dal Parlament souhlas a již je Česká republika vázána, součástí našeho právního řádu a má přednost před vnitrostátním právem.

Rychlý vývoj technologií umožňujících sběr, zpracování i přenos obrovského množství údajů či vytváření velkých databází, mající svůj počátek přibližně v 60. letech minulého století, vedl však ke zjištění, že pro účinnou ochranu osobních údajů, a tedy soukromí osob, bude zapotřebí podrobnějších a specifických právních předpisů. Čím jsou totiž informační a komunikační technologie výkonnější, tím větší je riziko zásahu do soukromí osob, jichž se

⁸ Pro Českou a Slovenskou Federativní republiku vstoupila Úmluva v platnost dne 18. března 1992 a vyhlášena byla sdělením Federálního ministerstva zahraničních věcí ČSFR č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8 a dalších protokolů na tuto úmluvu navazujících.

zpracovávané údaje týkají, a tím precizněji je tedy nutno přistupovat k úpravě ochrany takto zpracovávaných údajů.

Tento vývoj vedl Radu Evropy k přijetí dvou rezolucí týkajících se ochrany dat při jejich zpracování v rámci automatizovaných databází. První z nich z roku 1973, Rezoluce 73(22),⁹ stanoví principy ochrany údajů pro soukromý sektor a druhá, Rezoluce (74)29,¹⁰ přijatá v roce 1974, definuje obdobné zásady pro sektor veřejný. Již v době přijetí těchto směrnic bylo ovšem zřejmé, zejména s ohledem na nárůst přeshraničního toku údajů a vytváření nadnárodních databází, že národní legislativy nebudou schopny se se všemi nástrahami zpracování osobních údajů vypořádat, a že bude nezbytné přistoupit k detailnějším a efektivnějším úpravám nejen na národní, ale také i na mezinárodní úrovni.¹¹

Zmíněný rozvoj nových technologií a s tím související snaha jednotlivých států lépe upravit ochranu soukromí vedl také k vypracování mnoha právních předpisů upravujících shromažďování a zpracování osobních údajů na úrovni národních legislativ. Světové prvenství patří zákonu na ochranu osobních dat přijatému v roce 1970 v Hessensku (Německo). V průběhu 70. let minulého století byl obdobný zákon přijat v řadě dalších evropských států, konkrétně např. ve Švédsku (1973), v Německu na federální úrovni (1977), v roce 1978 následovaly hned čtyři evropské země – Francie, Dánsko, Norsko a Rakousko a o rok později Lucembursko. Během 80. let byla obdobná právní úprava přijata ve Finsku (1987), Irsku (1988), Nizozemsku (1988) a na Islandě (1989) a poté v průběhu 90. let i v Portugalsku (1991), Španělsku (1992), Belgii (1992), Švýcarsku (1993), Itálii (1996) nebo Řecku (1997).¹²

Prvním uceleným mezinárodním dokumentem upravujícím oblast zpracování osobních údajů se stala Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat (dále jen „Úmluva 108“), která byla Radou Evropy přijata a otevřena k přistoupení dne 28. ledna 1981, a která je – na rozdíl od výše uvedených Pravidel pro ochranu soukromí a přeshraniční toky osobních údajů přijatých OECD – pro přistoupivší státy závazná. Ratifikací Úmluvy 108 se daný stát zavazuje zakotvit principy ochrany osobních údajů ve svém právním řádu.¹³

Úmluva 108 byla, jak vyplývá již z jejího názvu, reakcí Rady Evropy na nárůst zpracování osobních údajů prováděných automatizovaně, tj. za pomoci výpočetní techniky, a byla přijata jednak za účelem harmonizace národních právních předpisů jednotlivých členských států

⁹ Resolution (73)22 on the protection of the privacy of individuals vis à vis electronic data banks in the private sector (Rezoluce o ochraně soukromí jednotlivců ve vztahu k elektronickým databázím v soukromém sektoru).

¹⁰ Resolution (74)29 on the protection of privacy of individuals vis à vis electronic data banks in the public sector (Rezoluce o ochraně soukromí jednotlivců ve vztahu k elektronickým databázím ve veřejném sektoru).

¹¹ Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J. Zákon o ochraně osobních údajů, komentář. Praha: C.H. Beck, 2003, s. 26.

¹² Důvodová zpráva k návrhu ZOOÚ.

¹³ Ze 45 členských států Rady Evropy Úmluvu 108 podepsalo zatím 40 zemí, z toho ji 34 států již i ratifikovalo (<http://www.coe.int>).

Rady Evropy, a jednak za účelem zefektivnění ochrany osobních údajů při jejich automatizovaném zpracování a zaručení odpovídajících práv každému jednotlivci. Úmluva 108 je otevřena k přistoupení i jiným než členským státům Rady Evropy.¹⁴

Česká republika podepsala Úmluvu 108, zejména kvůli neexistenci dozorového úřadu pověřeného poskytováním vzájemné spolupráce mezi smluvními stranami Úmluvy 108, až dne 8. září 2000 a ratifikovala ji dne 9. července 2001.¹⁵ Vzhledem k tomu, že Úmluva 108 je mezinárodní smlouvou ve smyslu čl. 10 Ústavy, je součástí právního řádu ČR a v případě, že stanoví něco jiného než zákon, má před tímto zákonem přednost (fakticky má tedy sílu ústavního zákona).

Úmluva 108 definuje v čl. 2 základní pojmy ochrany osobních údajů jako např. „osobní údaj“, „subjekt údajů“, „správce souboru údajů“, které jsou dnes již ustálenou terminologií v této oblasti.

Podle čl. 3 se Úmluva 108 vztahuje pouze na automatizované soubory dat a automatizované zpracování osobních dat, a to ve veřejném i soukromém sektoru. Členským státům je ovšem současně umožněno rozšířit působnost Úmluvy 108 na jakékoli instituce sdružující fyzické osoby, bez ohledu na jejich právní status, stejně jako na soubory osobních dat, které nejsou zpracovávány automaticky.

Úmluva 108 dále, zejména v hlavě II, stanoví základní zásady pro ochranu zpracovávaných údajů, přičemž tato hlava je uvedena ustanovením ukládajícím smluvním stranám povinnost přijmout potřebná legislativní opatření, aby tyto zásady byly v praxi skutečně provedeny. Obdobně jako v případě základních pojmů, je dnes i obsah těchto základních principů chápán v podstatě jednotně. Jedná se o:

- a) zásada legitimity zpracování [čl. 5 písm. a) – osobní údaje musí být získávány a zpracovávány poctivě a v souladu se zákony];
- b) zásada omezení rozsahu údajů účelem a zásada nezbytnosti údajů [čl. 5 písm. b) – osobních údaje mohou být shromažďovány pouze pro stanovené a oprávněné účely a používány pouze způsobem odpovídajícím těmto účelům];
- c) zásada potřebnosti a přiměřenosti údajů [čl. 5 písm. c) – lze zpracovávat pouze osobní údaje přiměřené stanoveným účelům a v rozsahu odpovídajícím těmto účelům];
- d) zásada kvality údajů [čl. 5 písm. d) – lze zpracovávat pouze přesné a pokud možno aktuální údaje];

¹⁴ Žádný ze států mimo Radu Evropy však doposud této možnosti nevyužil.

¹⁵ Úmluva 108 byla v ČR vyhlášena sdělením o přijetí Úmluvy na ochranu osob s ohledem na automatizované zpracování osobních dat, které bylo vyhlášeno ve Sbírce mezinárodních smluv pod číslem 115/2001 Sb. m. s. dne 15. listopadu 2001.

- e) zásada časového omezení [čl. 5 písm. e) – uchovávat osobní údaje ve formě umožňující zjistit totožnost subjektů údajů je možné pouze po dobu nezbytnou pro dosažení účelů, pro něž byly údaje shromážděny];
- f) zásada bezpečnosti (čl. 7 – je nezbytné přijmout vhodná bezpečnostní opatření na ochranu osobních údajů proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, jakož i proti neoprávněnému přístupu, změnám nebo šíření);
- g) zásada transparentnosti zpracování [čl. 8 písm. a) – každé osobě musí být umožněno zjistit existenci automatizovaného souboru osobních údajů, jeho hlavní účely, jakož i totožnost správce souboru údajů];
- h) zásada práva subjektu údajů na přístup k údajům [čl. 8 písm. b) – každému musí být umožněno získat potvrzení o tom, zda jsou zpracovávány jeho osobní údaje];
- i) zásada práva na opravu či vymazání údajů [čl. 8 písm. c) – povinnost poskytnout každé osobě možnost docílit opravy nebo vymazání údajů zpracovávaných v rozporu se základními zásadami] a
- j) zásada odpovědnosti správce osobních údajů (čl. 10 – povinnost smluvních stran Úmluvy 108 stanovit vhodné postihy a opravné prostředky pro případ porušení ustanovení národních předpisů provádějících uvedené zásady).

Úmluva 108 dále, v čl. 6, přiznává zvláštní režim určitým typům osobních údajů, které jsou zde označeny jako „zvláštní skupiny údajů“, a pro něž je v současné době běžné také označení „citlivé údaje“ (užívané i v českém právním řádu). Jedná se o osobní údaje, při jejichž zpracování je nezbytná zvýšená míra opatrnosti, neboť nesprávné nakládání s nimi může způsobit vážný zásah do soukromí subjektu údajů. Mezi zvláštní kategorie osobních údajů tedy patří zejména údaje vypovídající o rasovém původu, politických názorech, náboženském přesvědčení, zdravotním stavu nebo údaje o odsouzení za trestný čin.

Na základě čl. 18 a násl. Úmluvy 108 byl při Radě Evropy ustaven Poradní výbor pro ochranu dat, kde má každá smluvní strana svého zástupce, a který se podílí na tvorbě stanovisek a dokumentů Rady Evropy v oblasti působnosti Úmluvy 108. Rada Evropy také průběžně monitoruje proces přistupování jednotlivých států k Úmluvě 108 a úroveň ochrany osobních údajů v těchto zemích.

Dne 8. listopadu 2001 byl k Úmluvě 108 přijat Dodatkový protokol o orgánech dozoru a o toku údajů přes hranice¹⁶ reagující na některé otázky, které Úmluva 108 neřešila, a který zakotvuje tzv. zásadu nezávislého dozoru (v čl. 1), tedy povinnost smluvních stran Úmluvy 108 zřídit nezávislý orgán pověřený zabezpečením dodržování vnitrostátních norem naplňujících závazky přijaté v Úmluvě 108. Dodatkový protokol dále upravuje podmínky toku osobních údajů k zahraničnímu příjemci, který není smluvní stranou Úmluvy 108,

¹⁶ Česká republika jej podepsala dne 10. dubna 2002, ratifikovala dne 24. září 2003 a vyhlášen byl sdělením Ministerstva zahraničních věcí č. 29/2005 Sb.m.s.

tj. povinnost smluvní strany vyžádat si v takovém případě záruky bezpečnosti předávaných údajů.

Česká republika zahájila proces přistoupení k Dodatkovému protokolu v podstatě bezprostředně po přijetí Úmluvy 108, k ratifikaci však došlo až dne 24. září 2003, kdy ČR současně využila možnost uvedenou v čl. 3 odst. 2 písm. c) Úmluvy 108 a prohlášením rozšířila její působnost i na neautomatizovaná zpracování.

Zásady stanovené Úmluvou 108 byly dále rozpracovány v řadě doporučení Rady Evropy (Recommendation), která se zabývají ochranou osobních údajů v problémových oblastech, jako je např. zdravotnictví, marketing, činnost veřejné správy nebo nové informační technologie. Doposud bylo vydáno 13 takových doporučení.

S ohledem na to, že k nárůstu automatizovaného zpracování osobních údajů došlo i v zaměstnaneckých vztazích, vydal Výbor ministrů Rady Evropy dne 18. ledna 1989 Doporučení č. R(89)2 o ochraně osobních údajů používaných pro účely zaměstnání.¹⁷ Rada Evropy v tomto dokumentu doporučuje členským státům, aby za účelem minimalizace rizik vyplývajících ze zpracování osobních údajů pro práva a základní svobody zaměstnanců (zejména práva na ochranu soukromí) zajistily důsledné provedení zásad stanovených v Úmluvě 108 ve svých právních předpisech a jejich aplikaci v praxi. Principy zpracování osobních údajů zaměstnanců, uvedené v tomto doporučení, odrážejí zásady stanovené Úmluvou 108 s tím, že jsou zde speciálně adresovány zaměstnavatelům.

1.4. Evropská unie

Hospodářská a sociální integrace členských zemí Evropské unie vyplývající z Maastrichtské smlouvy o Evropské unii z roku 1992 vedla automaticky ke značnému nárůstu přeshraničního toku osobních údajů mezi všemi účastníky společného trhu, tedy jak mezi soukromými, tak i mezi veřejnými subjekty. Výměna dat v tak integrovaném společenství, jakým Evropská unie je, představuje z hlediska bezpečnosti těchto údajů mnohem větší rizika, než je tomu v rámci běžné mezinárodní spolupráce. Zajistit náležitou úroveň ochrany osobních údajů ve společenství čítajícím v součtu více než 370 milionů obyvatel není tedy jednoduchý úkol, a ačkoli je ochraně dat a soukromí věnována na území EU z celosvětového hlediska zřejmě největší pozornost a související právní normy jsou zde obecně velmi přísné, není tento úkol ještě zcela splněn.

Zdrojem evropské legislativy v oblasti ochrany osobních údajů byla výše zmiňovaná Evropská úmluva z roku 1950, na niž se Maastrichtská smlouva ve svém čl. 6 přímo

¹⁷ Text tohoto Doporučení je uveden v Příloze I.

odvolává, a také Úmluva 108, která byla Evropskou unií převzata pro oblast tzv. třetího pilíře, tj. spolupráce na základě dohod o Europolu a Schengenském prostoru.

Na základě Amsterodamské smlouvy z roku 1997 se ochrana osobních dat stala součástí primárního práva EU, neboť podle čl. 286/ex-čl.213b¹⁸ této smlouvy se budou akty Evropské unie týkající se ochrany fyzických osob při zpracování osobních údajů a při volném pohybu těchto údajů přímo uplatňovat vůči institucím založeným touto smlouvou nebo na jejím základě.

Historicky prvním uceleným textem Evropské unie zahrnujícím občanská, politická, ekonomická a sociální práva občanů EU, včetně práva na ochranu jejich osobních údajů, byla Charta základních práv Evropské unie (přijata dne 7. prosince 2000). Tento významný, ač nikoli přímo právně závazný, dokument ve svém čl. 7 stanoví, že všem občanům členských států je zaručeno právo na respektování soukromého a rodinného života a následující čl. 8 zvláště zakotvuje právo na ochranu osobních údajů:

1. Každý má právo na ochranu osobních údajů, které se jej týkají.
2. Tyto údaje musí být zpracovány poctivě, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.
3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

Charta základních práv Evropské unie byla zahrnuta, jako Část II, do návrhu Smlouvy o Ústavě pro Evropu (tzv. „Evropské ústavy“), která byla po dlouhém vyjednávání přijata dne 29. října 2004 v Bruselu. Citovaný čl. 8 Listiny základních práv Evropské unie je zde uveden jako článek II – 68. Zároveň ovšem Evropská ústava zakotvuje obdobné právo ve vlastním textu Ústavy, v Části I, článku I – 51, který zní:

1. Každý má právo na ochranu osobních údajů, které se jej týkají.
2. Evropský zákon nebo rámcový zákon stanoví pravidla o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Dodržování těchto pravidel podléhá kontrole nezávislými orgány.

Ochrana osobních údajů je tak v uvedeném dokumentu věnována pozornost, která svědčí o nemalé důležitosti této problematiky v dnešní Evropě. Zařazení práva na ochranu

¹⁸ Článek 286/ex-čl.213b: „1) Od 1. ledna 1999 se akty Společenství o ochraně fyzických osob při zpracování osobních údajů a při volném pohybu takových údajů uplatní ve vztahu k institucím založeným touto smlouvou nebo na jejím základě.

2) V období před datem uvedeným v odstavci 1 ustaví Rada postupem podle článku 251 nezávislou kontrolní instituci odpovědnou za dohled nad používáním takových aktů Společenství ve vztahu k orgánům a institucím Společenství a vydá případně jiné potřebné předpisy.“

osobních údajů mezi základní práva, jako je právo na svobodu a bezpečnost, právo na informace nebo právo na vyjadřování názorů, znamená, že právě s těmito právy je ochrana údajů neoddělitelně spjata. Na druhé straně však představuje jejich protiklad a demokratické společnosti jsou tak postaveny před nutnost hledat při ochraně těchto práv vyvážený kompromis.¹⁹

Až do roku 1995 byla však situace v Evropské unii taková, že míra ochrany osobních údajů poskytovaná na základě národních norem nebyla ve všech státech stejná, což ve výsledku bránilo volnému toku informací a následně tedy volné soutěži na společném trhu. Rozdílné právní úpravy představovaly pro občany, resp. společnosti, břemeno v podobě nutnosti složité registrace národními orgány dozoru, popř. získávání oprávnění ke zpracování osobních údajů zvláště na území každého státu a obecně v podobě nutnosti přizpůsobit se rozdílným režimům zpracování osobních údajů.

1.4.1. Směrnice Evropského parlamentu a Rady č. 95/46/EC

Sjednocujícím právním předpisem *acquis communautaire* v oblasti ochrany osobních údajů se stala Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (dále jen „Směrnice 95/46“),²⁰ která ukládá členským zemím EU povinnost do 3 let od přijetí této směrnice implementovat její ustanovení prostřednictvím adekvátních legislativních opatření národního práva.²¹

Směrnice 95/46 upřesňuje a rozšiřuje zásady práva na soukromí obsažené v Úmluvě 108, a to zejména o požadavek na technické zabezpečení zpracovávaných údajů a o oznamovací povinnost ohledně zamýšleného zpracování vůči orgánu pověřenému dozorem nad dodržováním pravidel ochrany osobních údajů. V oblasti předávání osobních údajů mimo území EU, do tzv. třetích zemí, vytváří Směrnice 95/46 požadavkem, aby údaje nebyly předány do země, která nezabezpečí jejich adekvátní ochranu (tedy na evropské úrovni), v podstatě tlak na mimoevropské státy, aby přijaly právní úpravu odpovídající zásadám této směrnice.

Směrnice 95/46 se, podle čl. 3, vztahuje pouze na zpracování osobních údajů prováděné zcela nebo alespoň z části automatizovaně nebo na neautomatizované zpracování údajů,

¹⁹ V současné době byla Evropská ústava v některých členských státech (Francii a Nizozemsku) občany odmítnuta a proces jejího schvalování byl pozastaven, nicméně tento fakt na významu práva na ochranu soukromí a osobních údajů nic nemění.

²⁰ Znění Směrnice 95/46 viz Příloha II.

²¹ Směrnice 95/46 byla jedním z předpisů, které bylo nezbytné implementovat do českého právního řádu ještě před vstupem do EU, což v ČR vedlo k přijetí ZOOÚ.

pokud jsou tyto údaje součástí souboru uspořádaného podle určitého kritéria, čímž je umožněn snadný přístup k těmto údajům.

Definice základních pojmů, uvedené v čl. 2, stejně jako jednotlivé základní zásady, jsou v současné době mnohdy téměř doslovně promítnuty do českého právního řádu prostřednictvím ZOOÚ²² a není tedy třeba se jim na tomto místě zvláště věnovat.

Na základě čl. 29 Směrnice 95/46 byla zřízena Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů (dále jen „Pracovní skupina 29“), jejímiž členy jsou zástupci jednotlivých dozorových orgánů, kteří se pravidelně scházejí k řešení aktuálních otázek týkajících se harmonizace národních právních předpisů provádějících Směrnici 95/46 nebo vyplývajících z aplikace těchto norem. Tato skupina dále hodnotí celkovou úroveň ochrany osobních údajů v EU i ve třetích zemích a o svých závěrech podává stanoviska či doporučení Evropské komisi. Výsledkem činnosti Pracovní skupiny 29 jsou mj. i stanoviska či rozborů týkající se aktuálních otázek ochrany osobních údajů v nejrůznějších oblastech.²³

1.4.2. Směrnice Evropského parlamentu a Rady č. 97/66/ES a směrnice č. 2002/58/ES

Směrnici 95/46 brzy doplnila speciální norma – Směrnice č. 97/66/ES Evropského parlamentu a Rady z 15. prosince 1997 týkající se zpracování osobních údajů a ochrany soukromí v sektoru telekomunikací, která přizpůsobila některé požadavky Směrnice 95/46 oblasti telekomunikací.²⁴

Vývoj v této oblasti byl však natolik rychlý, že uvedenou směrnici již po pěti letech nahradila nová Směrnice č. 2002/58/EC Evropského parlamentu a rady ze dne 10. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronické komunikace (dále jen „Směrnice 2002/58“), zohledňující především nástup digitálních technologií do telekomunikačních sítí, které vzhledem ke své vyspělosti přináší zvýšená rizika pro bezpečnost zpracovávaných dat. Směrnice 2002/58 dále upravuje podmínky poskytování různých služeb jako je identifikace volajícího a podmínky zveřejňování osobních údajů uživatelů telekomunikačních služeb v tištěných či elektronických seznamech.

Na základě Směrnice 2002/58 jsou členské státy povinny přijmout vnitrostátní právní předpisy zajišťující důvěrnost komunikace prostřednictvím veřejné telekomunikační sítě,

²² Soulad ZOOÚ se Směrnici 95/46 byl precizován zákonem č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, který nabyl účinnosti dne 26. července 2004.

²³ Některá z těchto stanovisek budou zmíněna v následujících kapitolách (zejména v kapitole 5).

²⁴ V České republice byla tato směrnice provedena zákonem č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů.

zejména pak vyloučit odposlouchávání, nahrávání, ukládání, nebo jiné druhy sledování komunikace, bez souhlasu příslušných uživatelů, s výjimkou případů, kdy takovéto omezení představuje nezbytné opatření k – zjednodušeně řečeno – ochraně veřejného zájmu.

Česká republika implementovala uvedenou směrnici hned dvěma zvláštními zákony, a to částečně zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), a zákonem č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Některé otázky, týkající se zpracování osobních údajů v oblasti telekomunikačních sítí, potom upravuje ZOOÚ jakožto *lex generalis*.

1.4.3. Nařízení Evropského parlamentu a Rady č. 45/2001 a rozhodnutí Evropského parlamentu, Rady a Komise č. 1247/2002/ES

Významnou právní normou Evropské unie je také Nařízení Evropského Parlamentu a Rady č. 45/2001 z 18. prosince 2000 o ochraně jednotlivců s ohledem na zpracování osobních údajů institucemi a orgány Společenství a o volném pohybu takovýchto údajů. Jedná se v podstatě o „úklid před vlastním prahem“, neboť zásady stanovené Směrnicí 95/46 a Směrnicí 2002/58 je nutno vztáhnout i na činnost samotných orgánů EU, kde také dochází ke zpracování osobních údajů.

Uvedené nařízení tedy stanoví všem orgánům a institucím zřízeným Smlouvami o založení Evropských společenství nebo na jejich základě identické povinnosti jako stanoví národní předpisy přijaté k provedení Směrnice 95/46 a Směrnice 2002/58 ve vztahu k subjektům mimo institucionální strukturu EU.

Na základě tohoto nařízení byla také při každém orgánu Evropské unie vytvořena funkce tzv. inspektora ochrany údajů, jehož úkolem je dohlížet na plnění evropských pravidel ochrany dat daným orgánem či institucí (tímto institutem se inspirovaly i některé národní právní normy, které nařizují určitým subjektům zpracovávajícím osobní údaje ustanovit obdobného „ombudsmana pro osobní údaje“²⁵).

V roce 2004 zahájil svou činnost, na základě Rozhodnutí Evropského parlamentu, Rady a Komise č. 1247/2002/ES ze dne 1. července 2002 o úpravě a obecných podmínkách výkonu funkce evropského inspektora ochrany údajů, také úřad Evropského inspektora ochrany údajů (neboli Evropského ochránce dat), který je nezávislým kontrolním orgánem pověřeným dohlížet na dodržování předpisů o ochraně dat ve všech institucích Evropské

²⁵ Například německý federální zákon na ochranu osobních údajů (Bundesdatenschutzgesetz, BGBl. I, S.2954) zakotvuje ve svém § 36 institut tzv. pověřence pro ochranu osobních údajů (Beauftragter für den Datenschutz) a ukládá všem subjektům, které zpracovávají osobní údaje automatizovaně zříditi funkci takového pověřence

unie, a který tak plní vůči těmto institucím obdobnou roli jako národní dozorové orgány vůči subjektům zpracovávajícím osobní údaje na území daného státu.²⁶

1.4.4. Rozhodnutí týkající se předávání osobních údajů do zahraničí

Jak bylo uvedeno již výše Směrnice 95/46 se zabývá i podmínkami pro předávání osobních údajů zpracovávaných na území Evropské unie do třetích zemí. Obecně platí, že osobní údaje obyvatel EU mohou být předány mimo území EU pouze, pokud legislativní prostřední v cílové zemi zaručuje adekvátní ochranu osobním údajům, tedy ochranu na úrovni vyžadované Směrnicí 95/46.

Pokud je právní úprava některého nečlenského státu posouzena jako adekvátní, mj. na základě stanovisek Pracovní skupiny 29, může Evropská komise vydat rozhodnutí konstatující, že úroveň ochrany osobních údajů v dané zemi odpovídá standardům Evropské unie, a tedy že předávání osobních údajů do této země není třeba podřizovat povolovacímu režimu dozorového orgánu. Tento režim platí v současné době při transferu osobních údajů do Kanady (ovšem pouze pokud příjemce údajů podléhá působnosti kanadského zákona o ochraně osobních informací a elektronických dokumentech), do Švýcarska, do Argentiny, na Guernsey a na Ostrov Man.

V případě předávání osobních údajů do Spojených států amerických bylo, vzhledem k odlišnému přístupu k této otázce, zapotřebí přijmout odlišné řešení. Problematika adekvátní ochrany osobních údajů v USA (z hlediska EU) je v současné době ostatně velmi aktuální otázkou, Evropská komise vede v této otázce s USA neustálé rozhovory, v nichž se obě strany snaží najít kompromis v rozporu mezi právem na ochranu soukromí (na nějž klade důraz EU) a ochranou veřejného zájmu (zdůrazňovanou ze strany USA).

K určitému kompromisu, ačkoli nedokonalému a poměrně nepraktickému, došlo na základě Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států amerických (2000/520/ES). Tímto rozhodnutím přiznává Evropská komise odpovídající úroveň ochrany osobních údajů těm subjektům, které spadají do kompetence Federální obchodní komise a Departmentu dopravy USA, ovšem pouze za předpokladu, že přistoupily k tzv. zásadám bezpečného přístavu (Safe Harbour), které jsou v rozhodnutí Komise specifikovány, a které odrážejí požadavky Směrnice 95/46.

Oblast předávání osobních údajů osob cestujících letecky do USA, což denně představuje obrovské množství údajů, upravila Evropská komise zvlášť – Rozhodnutím

²⁶ Evropský ochránce dat je jmenován na dobu 5 let, v současné době tedy v této funkci stále působí první jmenovaný ochránce – Peter Hustinx z Nizozemí, jehož zástupcem je Španěl Joaquín Bayo Delgado.

Komise ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cizince a ochranu hranic (2004/535/ES).²⁷

Posledním, ovšem zřejmě nejvíce využívaným, nástrojem s jehož využitím mohou zejména obchodní partneři ze třetích zemí přímo zajistit požadovanou úroveň ochrany osobních údajů, jsou standardní smluvní doložky, jejichž vzory jsou přílohou rozhodnutí Evropské komise. V současné době existují tyto smluvní doložky ve třech různých verzích, z nichž je nutno zvolit tu, která odpovídá postavení v jakém vůči sobě předávající a přijímající subjekt vystupují.²⁸

Uvedené instituty slouží k tomu, aby v důsledku vyžadované vysoké úrovně ochrany osobních údajů v EU nebyl poškozen mezinárodní obchod, neboť předávání nejruznějších dat je v současné době imanentní součástí téměř jakéhokoli podnikání. Rozhodnutí Evropské komise jsou pro členské státy závazná, čímž je zaručeno, že členské státy budou případy, na které se tato rozhodnutí vztahují, posuzovat obdobně jako by se jednalo o předávání osobních údajů v rámci EU a nebudou je tedy podřizovat přísným povolovacím řízením.

Některým otázkám spojeným s předáváním osobních údajů zaměstnanců do třetích zemí bude věnována zvláštní kapitola (viz kapitola 5.1.).

²⁷ V tomto případě se ukázalo, že rozporná stanoviska nezastávají pouze USA a EU, ale i jednotlivé orgány EU – spor mezi Komisí a Evropským parlamentem týkající se předávání údajů osob cestujících letecky do USA skončil až u Evropského soudního dvora.

²⁸ 1) Rozhodnutí Komise ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/46/ES (2001/497/ES).

2) Rozhodnutí Komise ze dne 1. dubna 2005 doplňující rozhodnutí 2001/497/ES s ohledem na zavedení alternativních smluvních doložek pro předávání osobních údajů do třetích zemí.

3) Rozhodnutí Komise ze dne 27. prosince 2001 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům ve třetích zemích podle směrnice 95/46/ES (2002/16/ES).

2. Vývoj právní úpravy ochrany osobních údajů v České republice

Právní úprava ochrany osobních údajů v České republice má své ústavní základy v ustanovení čl. 10 Listiny, jenž zní:

1. Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.
2. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
3. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Citovaný článek tedy zakotvuje čtyři okruhy práv, které spolu velmi úzce souvisí a často se prolínají. Jedná se o právo na ochranu důstojnosti, právo na ochranu dobré pověsti, právo na ochranu soukromí a právo na ochranu osobních údajů. Tato práva jsou předpokladem pro rozvoj každého člověka a pro jeho uplatnění ve společnosti, a je nutno chránit je obdobně jako jeho samotnou existenci. Čl. 10 Listiny tedy navazuje na ústavní ochranu života člověka, zakotvením jeho ochrany také jako intelektuálního jedince, individualizovaného jménem a majícího vlastní soukromý, popř. rodinný život. Čl. 10 Listiny dále rozvíjí, jako speciální ustanovení, čl. 7 Listiny obecně zaručující nedotknutelnost soukromí osob, a zohledňuje fakt, že každý jedinec během svého života vystupuje v mnoha vztazích a mnoha rolích a svou činností vytváří určité hodnoty.²⁹

Na právní úpravu obsaženou v Listině navazuje zejména institut ochrany osobnosti obsažený v § 11 a 12 zákona č. 40/1964 Sb., občanský zákoník, (dále jen „občanský zákoník“) na jejichž základě je poskytována ochrana především hodnotám osobní povahy, tj. např. písemnostem, podobiznám, obrazovým snímkům nebo zvukovým záznamům.

Základy procesní ochrany práv stanovených v Listině jsou potom zakotveny v ustanovení čl. 36 Listiny, na který navazuje ustanovení § 13 občanského zákoníku konkretizující oprávnění osoby, která se domnívá, že došlo k zásahu do jejích osobnostních práv, domáhat se upuštění od neoprávněných zásahů, odstranění následků či přiměřeného zadostiučinění.

Dalším právní oblastí navazující na čl. 10 Listiny je právě ochrana osobních údajů, v současné době upravená ZOOÚ.

V souladu s čl. 4 Listiny je možné práva zaručená v čl. 10 Listiny omezit pouze na základě zákona, a to při současném šetření podstaty a smyslu těchto práv. Z tohoto principu vyplývá jedno ze základních pravidel zpracování osobních údajů – totiž, že o nakládání s

²⁹ Klíma, K. Ústavní právo. Praha: Bohemia Iuris Kapitál a.s., 1997, s. 198

osobními údaji je primárně oprávněna rozhodovat pouze osoba, již se týkají, a její souhlas může být nahrazen pouze zákonným zmocněním.

2.1. Zákon č. 256/1992 Sb.

ZOOÚ ovšem není první právní normou upravující práva a povinnosti v oblasti ochrany osobních údajů v České republice. Uvedenému zákonu předcházela zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, jenž nabyl účinnosti dne 1. června 1992.

Tento zákon vyházel z Úmluvy 108 a jeho působnost se tedy omezovala pouze na nakládání s osobními údaji zpracovávanými prostřednictvím informačního systému, kterým se dle § 4 zákona č. 256/1992 Sb. rozuměl funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Zákon č. 256/1992 Sb. dále upravoval odpovědnost provozovatelů těchto informačních systémů a dalších osob účastnících se zpracování osobních údajů a stanovil omezující podmínky pro nakládání s osobními údaji. Obecně lze ustanovení zákona č. 256/1992 Sb. rozdělit na:

- ustanovení vymezující základní pojmy;
- ustanovení zakotvující povinnosti provozovatele informačního systému, jímž je podle § 11 tohoto zákona osoba (fyzická nebo právnická), která zabezpečuje zpracování informací a vystupuje navenek jako nositel práv a povinností spojených s provozováním informačního systému;
- ustanovení týkající se povinností zprostředkovatele, tedy ve smyslu § 13 zákona č. 256/1992 Sb. osoby zjišťující, shromažďující, zpracovávající nebo poskytující informace pro jinou osobu;
- ustanovení ukládající povinnosti fyzickým osobám, které přichází do styku se zpracovávanými údaji a
- ustanovení upravující způsob vymáhání stanovených povinností.

Podle § 24 tohoto zákona se předpokládalo vydání zvláštního zákona, kterým by byl zřízen státní orgán příslušný k výkonu kontroly v oblasti plnění povinností stanovených zákonem č. 256/1992 Sb. Takový zákon však nikdy vydán nebyl a zejména následkem tohoto nedostatku, a s tím spojené absenci efektivních sankcí za porušení stanovených povinností, byl význam zákona č. 256/1992 Sb. během osmi let jeho platnosti velmi malý.³⁰

Vzhledem k tomu, že dozorový orgán, který by dohlížel na plnění povinností uložených uvedeným zákonem č. 256/1992 Sb. a případně je vymáhal, nebyl zřízen, musel se každý, kdo se cítil poškozen na svých právech následkem neoprávněného nebo nezákonného

³⁰ Mates, P. Ochrana osobních údajů v českém právním řádu. Bulletin advokacie, 2000, č. 9, s. 32.

zpracování svých osobních údajů, obrátit na soud. Uvedený zákon tak bylo možno chápat pouze jako určitý doplněk institutu ochrany osobnosti upraveného občanským zákoníkem.³¹

Právní úprava ochrany osobních údajů v České republice, provedená zákonem č. 256/1992 Sb., tak zaostávala za vývojem práva EU, přičemž zmíněná absence specializovaného kontrolního orgánu a nemožnost účinného vymáhání povinností stanovených tímto zákonem byla sice zřejmě největší, nikoli ale jedinou slabinou právní úpravy této problematiky. Oblast působnosti zákona č. 256/1992 Sb. omezená pouze na provozování automatizovaných informačních systémů byla totiž z hlediska Směrnice 95/46 příliš úzká, dále nebyla např. v dostatečném rozsahu zakotvena informační povinnost vůči osobám, jejichž osobní údaje jsou zpracovávány, oznamovací povinnost vůči dozorovému orgánu byla stanovena jen malému okruhu subjektů a v neposlední řadě chyběla i podrobnější úprava otázky předávání osobních údajů do zahraničí.

Tato situace tak jednak znamenala nekompatibilitu českého právního řádu s legislativou EU v oblasti ochrany osobních údajů, jejíž transponování bylo jednou z podmínek přijetí České republiky do Evropské unie, a jednak bránila přistoupení České republiky k Úmluvě 108, což ve svém důsledku znamenalo nemožnost začlenění českých orgánů do Schengenského informačního systému (podmínkou začlenění je mj. právě přistoupení k Úmluvě 108).³²

2.2. Zákon č. 101/2000 Sb.

Řešením výše uvedené situace bylo přijetí nového zákona, jehož východiskem byly, kromě Listiny a stávajícího zákona č. 256/1992 Sb., právě Úmluva 108 a Směrnice 95/46, jakožto zásadní dokumenty mezinárodního práva v oblasti ochrany osobních údajů.

Dne 4. dubna 2000 byl tedy přijat a dne 1. června 2000 nabyl účinnosti³³ zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, (ZOOÚ).

Jedním z cílů, který zákonodárce tímto zákonem sledoval, byla větší účast samotných občanů na ochraně jejich vlastních údajů, a to zejména zavedením principu zpracování osobních údajů primárně jen se souhlasem osoby, o jejíž údaje se jedná, a dále zakotvením práva občana na informace o údajích, které jsou o něm zpracovávány.³⁴ Je ovšem dlužno říci, že povědomí občanů České republiky o důležitosti ochrany osobních údajů a o možnostech, které jim legislativa v této oblasti nabízí, stejně jako povědomí o odpovědnosti

³¹ Maštalka, J. Nástin koncepce ochrany osobních dat v našem právním řádu. Průmyslové vlastnictví, 1994, č. 2, s. 48.

³² Důvodová zpráva k návrhu ZOOÚ, obecná část.

³³ S výjimkou ustanovení týkajících se registrací subjektů, které hodlají zpracovávat osobní údaje, jejichž účinnost byla odsunuta až na 1. prosince 2000, neboť se předpokládalo, že k zahájení registrační činnosti bude ze strany Úřadu zapotřebí provést náročnější technická a organizační opatření.

³⁴ Důvodová zpráva k návrhu ZOOÚ, obecná část.

každého jednotlivce za vlastní osobní údaje, je stále (v porovnání se „staršími“ členy EU) velmi nízké. Obyvatelé ČR, pokud se vůbec o problematiku ochrany svých osobních údajů zajímají, místo prevence spoléhají spíše na následné nápravné zásahy Úřadu pro ochranu osobních údajů. Osvětová činnost, která by do značné míry měla být zajištěna právě Úřadem, tak byla doposud zjevně nedostatečná.³⁵

Praktickým důsledkem přijetí ZOOÚ mělo dále být omezení počtu zpracování osobních údajů (tj. nejrůznějších evidencí) a rozsahu shromažďovaných údajů, a to především s ohledem na zakotvení povinnosti zpracovávat pouze údaje v rozsahu nezbytném pro naplnění sledovaného účelu. Zákonodárce předpokládal, že k tomuto omezení by mělo dojít především v oblasti zpracování prováděného orgány státu. Ani téměř po šesti letech od přijetí ZOOÚ však nelze konstatovat, že by se ve státní správě tento efekt projevil.³⁶ Zajímavostí je, že tento svůj záměr zákonodárce zdůvodňuje finanční náročností zpracování nadměrného množství údajů, případně duplicitního zpracování týchž údajů,³⁷ přičemž důvodem omezení množství shromažďovaných a zpracovávaných údajů by (a to zejména v oblasti veřejné správy vybavené nejrůznějšími pravomocemi) měl být především důraz na minimalizaci zásahu do soukromí osob. Ochrana soukromí je totiž primárním cílem, k jehož naplnění jsou legislativní opatření k ochraně osobních údajů přijímána.

Ačkoli ZOOÚ navazoval na zákon č. 256/1992 Sb., přinesl do právní úpravy oblasti ochrany osobních údajů mnoho změn. Základní rozdíly mezi oběma zákony jsou následující:

- rozdílené vymezení působnosti – zákon č. 256/1992 Sb. se týkal toliko zpracování osobních údajů prostřednictvím automatizovaných informačních systémů, ZOOÚ se vztahuje již na veškeré zpracování osobních údajů, automatizované i neautomatizované;
- odlišná terminologie – tam, kde zákon č. 256/1992 Sb. používá termíny „informace“, „provozování informačního systému“ nebo „zpracování informace“, „dotčená osoba“, „provozovatel“ a „zprostředkovatel“, tam užívá ZOOÚ pojmy „osobní údaj“, „zpracování osobních údajů“, „subjekt osobních údajů“, „správce osobních údajů“ a „zpracovatel osobních údajů“, tedy pojmy více odpovídající termínům užívaným ve Směrnici 95/46 a Úmluvě 108. ZOOÚ dále definuje i některé nové termíny, jako např. „citlivý osobní údaj“;
- jiná struktura povinností subjektů zpracovávajících osobní údaje – ZOOÚ přebírá všechny povinnosti stanovené zákonem č. 256/1992 Sb., avšak formuluje je

³⁵ Teprve v roce 2005 byla Úřadem vydána informační brožura určená široké veřejnosti, informující o základních právech občanů v oblasti ochrany osobních údajů a jim odpovídajících povinnostech subjektů, které osobní údaje zpracovávají.

³⁶ Nejrůznější orgány státu patří k pravidelným provinilcům, s nimiž Úřad vede správní řízení pro porušení povinností stanovených ZOOÚ (viz např. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2004, s. 6).

³⁷ Důvodová zpráva k návrhu ZOOÚ, obecná část.

precizněji, případně je i rozšiřuje tak, aby se jejich znění blížilo povinnostem vymezeným Směrnicí 95/46, navíc přináší některé nové povinnosti, např. výslovně zakotvuje jeden z hlavních principů ochrany osobních údajů – povinnost zpracovávat osobní údaje zásadně na základě souhlasu osoby, o jejíž údaje se jedná (jednotlivým povinnostem vyplývajícím ze ZOOÚ je věnována kapitola 4);

- zcela nově byly v ZOOÚ upraveny podmínky, za nichž je možné předávat osobní údaje do zahraničí;
- přímo ZOOÚ byl také zřízen Úřad pro ochranu osobních údajů,³⁸ jakožto nezávislý orgán s pravomocí provádět dozor nad dodržováním povinností stanovených tímto zákonem, a to jak na základě podnětů a stížností občanů, tak i na základě vlastní kontrolní činnosti. Úřadu byla dále svěřena pravomoc projednávat správní delikty a přestupky, jejichž skutkovou podstatou je porušení povinností stanovených ZOOÚ, a v neposlední řadě je jeho úkolem poskytovat odborné konzultace z oblasti své působnosti³⁹ (činnost Úřadu je popsána v kapitole 6).

ZOOÚ byl od svého přijetí již celkem desetkrát změněn, ať již přímo či nepřímo, a zejména vlivem předposlední z těchto novelizací doznal velmi zásadních změn. Současné znění ZOOÚ se tak od původního v mnoha podstatných bodech odlišuje.

2.2.1. Zákon č. 227/2000 Sb.

Ještě v tomtéž roce, kdy byl přijat, byl ZOOÚ poprvé nepřímo novelizován, a to zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), který nabyl účinnosti dne 1. října 2000.

Uvedeným zákonem byla Úřadu pro ochranu osobních údajů, svěřena kompetence udělovat a odnímat akreditace k působení jako akreditovaný poskytovatel certifikačních služeb (tj. ověřovatel identifikačních údajů uživatele elektronického podpisu) a současně pravomoc provádět dozor nad dodržováním povinností stanovených zákonem č. 227/2000 Sb.

V rámci své pravomoci podle § 20 zákona č. 227/2000 Sb. vydal Úřad prováděcí předpis⁴⁰ a zahájil řízení o udělení akreditace s prvním, a donedávna i posledním, subjektem

³⁸ Což lze považovat za šťastnější řešení než odkaz na zvláštní zřizovací zákon, který by nakonec také nemusel spatřit světlo světa, obdobně jako v případě zákona č. 256/1992 Sb.

³⁹ Vzhledem k tomu, že v době vzniku ZOOÚ byla problematika ochrany osobních údajů v ČR v podstatě okrajovou záležitostí (a dodnes do jisté míry zůstává), je zakotvení této působnosti přímo do zákona jistě přínosem, neboť zakládá právo každé fyzické či právnické osoby obrátit se se svým dotazem či žádostí přímo na Úřad, jakožto autoritu v dané oblasti.

⁴⁰ Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

působícím v ČR jako akreditovaný poskytovatel certifikačních služeb v oblasti elektronického podpisu.

2.2.2. Zákon č. 177/2001 Sb.

V následujícím roce prošel ZOOÚ dvěma dalšími změnami, z nichž první přinesl s účinností od 31. května 2001 zákon č. 177/2001 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., a zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů.

Tento zákon zasáhl do poměrně velkého počtu ustanovení ZOOÚ, přičemž dotčené oblasti lze rozdělit takto:

- úprava postavení a kompetencí Úřadu pro ochranu osobních údajů;
- zúžení působnosti ZOOÚ a zavedení výjimek z povinností stanovených tímto zákonem pro dobrovolná seskupení občanů;
- zakotvení podmínek pro zpracování osobních údajů za účelem nabízení obchodu a služeb;
- úprava informační povinnosti správce osobních údajů (tedy toho, kdo údaje zpracovává) vůči subjektu údajů (tomu, jehož údaje jsou zpracovávány) a
- dílčí úpravy např. definice citlivého osobního údaje, institutu souhlasu se zpracováním osobních údajů nebo ustanovení týkající se sankcí.

Úprava působnosti ZOOÚ spočívala v doplnění věty druhé do § 3 odst. 4 ZOOÚ, čímž bylo z působnosti tohoto zákona vyňato nahodilé shromažďování osobních údajů v rozsahu nezbytném pro výkon nezávislého povolání, které není živností ani jiným podnikáním, a které stanoví povinnost mlčenlivosti. Podle příslušné poznámky pod čarou se tímto rozumí, že ZOOÚ se nevztahuje na činnost advokátů, notářů, patentových zástupců, daňových poradců, auditorů, znalců a tlumočnicků. Toto ustanovení vyřešilo spory ohledně otázky, zda se ZOOÚ vztahuje na činnost uvedených skupin, kdy zejména z řad advokátů zaznívaly důrazné argumenty v tom smyslu, že s ohledem na povinnosti uložené advokátům zákonem č. 85/1996 Sb., o advokacii, a dále vzhledem k tomu, že shromažďování či jiné zpracování osobních údajů není předmětem činnosti advokáta, je nemožné ZOOÚ na výkon povolání advokáta aplikovat.⁴¹

Je třeba říci, že výklad působnosti ZOOÚ způsobem, že se vztahuje na i činnost advokátů konkrétně a všech uvedených „svobodných povolání“ obecně,⁴² byl skutečně příliš

⁴¹ Sokol, T. Zákon o ochraně osobních údajů se na advokáta nevztahuje. Bulletin advokacie, 2000, č. 10, s. 23 (v tomto článku autor polemizuje s opačným názorem vyjádřeným v níže citovaném článku).

⁴² Mates, P. Ochrana osobních údajů v českém právním řádu. Bulletin advokacie, 2000, č. 9, s. 32 (uvedený autor ostatně později také přijal odlišný výklad viz Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, a.s., 2004, s. 187).

extenzivní. ZOOÚ je právní normou stanovící povinnosti těm, u nichž je zpracování osobních údajů prostředkem k dosažení určitého cíle, a jeho působnost nelze rozšiřovat na všechny oblasti, kde se osobní údaje pouze vyskytují, což je v dnešní době ostatně téměř každá lidská činnost. Navíc podmínkou pro vynětí činnosti uvedených skupin z působnosti ZOOÚ byla opět nahodilost zpracování osobních údajů, což již obecně stanovila věta první § 3 odst. 4 tohoto zákona.

Významnou změnou, kterou zákon č. 177/2001 Sb. přinesl, byla liberace dobrovolných sdružení a seskupení občanů z některých povinností stanovených ZOOÚ. Záměrem zákonodárce bylo, v souladu se Směrnicí 95/46, ušetřit na jedné straně tato dobrovolná sdružení a na straně druhé i Úřad pro ochranu osobních údajů rozsáhlé administrativní činnosti spojené zejména s plněním oznamovací povinnosti.⁴³ Tento krok lze hodnotit pozitivně, neboť smyslem ZOOÚ skutečně není vytvoření přehledu o všech subjektech, které vedou pouze evidence svých členů, zvláště za cenu, že výsledný efekt nemůže odpovídat vyloženému úsilí a prostředkům.

Vzhledem k uvedenému se tedy nadále oznamovací povinnost vůči Úřadu nevztahuje na činnost politických stran, politických hnutí, občanských sdružení, odborových organizací, církví a náboženských společností, ovšem za podmínky, že zpracovávány jsou pouze osobní údaje jejich členů a jsou využívány jen pro vnitřní potřebu těchto subjektů, tj. pro činnosti v souladu s účelem, pro který byly založeny. Tentýž okruh subjektů byl liberován i z povinnosti zpracovávat osobní údaje pouze na základě souhlasu dotčené osoby, což by (především vzhledem k povinnosti prokázat tento souhlas kdykoli během zpracování údajů) bylo opět spojeno s nadbytečnou administrativou a zatěžováním uvedených sdružení často spravovaných na dobrovolnickém principu.

Nově byla zákonem č. 177/2001 Sb. do ZOOÚ doplněna úprava povinností spojených s využíváním osobních údajů k nabídce obchodu a služeb, zejména se jednalo o stanovení podmínek pro předávání shromážděných osobních údajů mezi jednotlivými subjekty (zásadně na základě informovaného souhlasu subjektu údajů) a zamezení řetězení takových předání. Důvodem této úpravy byla skutečnost, že v oblasti nabídky obchodu a služeb jsou databáze kontaktů na potenciální klienty vysoce ceněny, a tedy vzájemně předávány (resp. prodávány), a s rostoucím počtem příjemců tak současně roste riziko zásahu do soukromí osob v těchto databázích zaregistrovaných.

Úpravy doznala také informační povinnost vůči osobám, jejichž osobní údaje mají být zpracovávány. S cílem zajistit větší ochranu údajů došlo (z hlediska správců osobních údajů) ke zpřísnění této povinnosti: veškeré relevantní informace, tj. v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem je bude zpracovávat a komu

⁴³ Důvodová zpráva k návrhu zákona č. 177/2001 Sb., obecná část.

mohou být zpřístupněny, musel správce osobních údajů poskytnout, a to písemně, ještě před zahájením zamýšleného zpracování. Na druhou stranu byl rozšířen výčet situací, kdy správce informační povinnost plnit nemusí o případ, kdy zpracovává výlučně již zveřejněné údaje nebo má ke zpracování souhlas dotčené osoby.

Pozice Úřadu pro ochranu osobních údajů byla zákonem č. 177/2001 Sb. vyjasněna doplněním § 2 ZOOÚ, jímž se Úřad zřizuje, o bližší vymezení, že se jedná o ústřední správní úřad pro oblast ochrany osobních údajů a pro oblast elektronického podpisu, tedy oblasti upravené v ZOOÚ a v zákoně č. 227/2000 Sb.

Z dalších úprav provedených zákonem 177/2001 Sb. lze zmínit změnu definice citlivého osobního údaje, za které se dále nepovažují informace o členství v politických stranách či hnutích a zaměstnaneckých organizacích. Vzhledem k tomu, že za citlivý osobní údaj se již před touto změnou považovaly také údaje o politických postojích, byla touto novelou pouze odstraněna určitá duplicita, která by mohla při výkladu definice citlivého osobního údaje působit problematicky. Rozsah údajů, které jsou ZOOÚ považovány za citlivé, se tímto nijak nezměnil, neboť údaj o členství v politické straně či hnutí bezpochyby vypovídá o politických postojích dotčené osoby. Údaje o členství v politických stranách navíc nejsou zařazeny mezi citlivé, resp. zvláštní, údaje ani v Úmluvě 108, ani ve Směrnici 95/46.

V případě zaměstnaneckých organizací hovořily pro vypuštění tohoto údaje zcela praktické důvody, neboť organizace tohoto typu se v právním řádu ČR nevyskytuje, a tak jednak vznikal interpretační problém, jaké organizace měl v daném případě zákonodárce na mysli, a jednak neměl tento citlivý osobní údaj žádný obsah.

Ustanovení ZOOÚ upravující souhlas se zpracováním osobních údajů bylo upraveno v tom smyslu, že nadále již nemusí být tento souhlas obligatorně písemný a správce jej nemusí po celou dobu zpracování uchovávat. Nicméně nová formulace této povinnosti, tj. povinnost souhlas po celou dobu zpracování prokázat, znamená v naprosté většině případů i nadále nezbytnost získat souhlas dané osoby v písemné formě.

2.2.3. Zákon č. 450/2001 Sb.

V pořadí třetí změnu ZOOÚ přinesl zákon č. 450/2001 Sb.,⁴⁴ kterým byly změněny některé zákony upravující nakládání s majetkem obcí a krajů. Změna ZOOÚ byla do uvedené normy vložena poněkud nekonceptně, neboť se nakládání s majetkem netýkala.⁴⁵

⁴⁴ Celý název tohoto zákona zní: Zákon č. 450/2001 Sb., kterým se mění zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů, zákon č. 131/2000 Sb. o hlavním městě Praze, ve znění pozdějších předpisů, zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění zákona č. 320/2001 Sb., zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších

Uvedeným zákonem byl, s účinností od 31. prosince 2001, do ZOOÚ vložen nový § 17a, rozšiřující pravomoc Úřadu pro ochranu osobních údajů o možnost zrušit, na základě následného zjištění, že osobní údaje jsou zpracovávány v rozporu se ZOOÚ, již provedenou registrací zpracování osobních údajů. Zrušení registrace dle § 17a je dále možné v případě, kdy již pominul účel, pro který byly údaje zpracovávány, přičemž v tomto případě má ke zrušení dojít buď na základě žádosti dotyčného správce osobních údajů a nebo z podnětu Úřadu.⁴⁶

Zákon č. 450/2001 Sb. dále zasáhl do ustanovení upravujících organizační otázky Úřadu, avšak pouze tím, že odlišil úpravu platových poměrů předsedy Úřadu a inspektorů od řadových zaměstnanců, což ovšem znamenalo toliko nápravu opomenutí zohlednit postavení Úřadu jakožto ústředního správního orgánu také v tomto směru.⁴⁷

2.2.4. Zákon č. 107/2002 Sb.

V roce 2002 byl ZOOÚ dotčen hned čtyřmi novelami. První z nich, zákon č. 107/2002 Sb., kterým se mění zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činnostmi bývalé Státní bezpečnosti, a některé další zákony, byla do ZOOÚ vnesena pouze jedna změna, odrážející ovšem významný posun českého zákonodárství v přístupu k naší minulosti.

Jak je již z názvu zákona č. 107/2002 Sb. zřejmé, jeho hlavním záměrem byla novelizace zákona č. 140/1996 Sb., a to konkrétně rozšíření oprávnění k přístupu do svazků bývalé Státní bezpečnosti a dalších bezpečnostních složek. Před uvedenou novelou měli občané ČR právo k přístupu pouze ke svým osobním složkám a k těm písemnostem, které obsahovaly jejich osobní údaje. Se zdůvodněním, že společenský zájem na odhalení a zpřístupnění materiálů dokládajících činnost konkrétních osob při vytváření a udržování zločinného a zavrženíhodného komunistického režimu je vyšší než zájem na ochraně údajů (někdy i kvazi údajů) týkajících se příslušníků bezpečnostních složek a jejich tajných

předpisů, a zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

⁴⁵ Tato situace vznikla tak, že Rozpočtový výbor Poslanecké sněmovny Parlamentu ČR, kterému byl přikázán v té době již téměř půl roku starý poslanecký návrh novel zákonů o rozpočtech obcí, krajů a hlavním městě Praze, doplnil právě do tohoto návrhu body vztahující se k ZOOÚ.

⁴⁶ Druhá z uvedených možností, tedy iniciativa Úřad, je ovšem představitelná pouze v případě, kdy bylo zpracování již v původním oznámení časově vymezeno, jinak si lze jen těžko představit, na základě jakých podkladů by Úřad přezkoumával, zda deklarovaný účel stále trvá (o administrativní a technické náročnosti takové činnosti nemluvě).

⁴⁷ Nadále se tedy platové poměry předsedy a inspektorů Úřadu řídí zákonem č. 236/1995 Sb. o platu a dalších náležitostech spojených s výkonem funkce představitelů státní moci a některých státních orgánů a soudců, zatímco platy řadových zaměstnanců jsou upraveny zákonem č. 143/1992 Sb., o platu a odměně za pracovní pohotovost v rozpočtových a některých dalších organizacích a orgánech.

spolupracovníků,⁴⁸ byly tedy žadatelům zpřístupněny i další svazky, které se jich týkají, ačkoli současně obsahují údaje o třetích osobách.

S ohledem na tuto změnu bylo nezbytné zahrnout zpracování osobních údajů, k němuž při zpřístupňování svazků Státní bezpečnosti a dalších složek dochází, do oblastí, na něž se ZOOÚ nevztahuje, což se stalo, s účinností od 20. března 2002, prostřednictvím nově vloženého § 3 odst. 6 písm. f).

2.2.5. Zákon č. 309/2002 Sb. a zákon č. 310/2002 Sb.

Zákonem č. 309/2002 Sb., o změně zákonů souvisejících s přijetím zákona o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon), bylo opět pouze zasaženo do ustanovení upravujících platové poměry zaměstnanců Úřadu pro ochranu osobních údajů. S účinností od 1. ledna 2004 jsou platové poměry a otázky cestovních náhrad řadových zaměstnanců Úřadu (tedy nikoli předsedy a inspektorů) upraveny právě novým služebním zákonem, tj. zákonem č. 218/2002 Sb., o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon), který v částech týkajících se platových poměrů nabyl účinnosti již 8. května 2002.

ZOOÚ byl dotčen také bezprostředně následujícím zákonem č. 310/2002 Sb., který se týkal změny zákona o ochraně utajovaných skutečností a některých dalších zákonů, a jehož celý název je delší než změna, kterou ZOOÚ přinesl.⁴⁹ Citovaný zákon reaguje zejména na praktické problémy spojené s nemožností nezávislého přezkoumání rozhodnutí Národního bezpečnostního úřadu týkajících se udělení či neudělení bezpečnostní prověrky a zřizuje za tímto účelem tzv. Kolegium na úseku utajovaných skutečností, působící při Nejvyšším státním zastupitelství. Touto změnou byl tedy rozšířen rozsah činností NBÚ, na něž se ZOOÚ nevztahuje, o zpracování osobních údajů souvisejících s ověřováním bezpečnostní způsobilosti fyzických osob. Účinnosti v tomto bodě nabyl zákon č. 310/2002 Sb. dne 12. července 2002.

⁴⁸ Důvodová zpráva k návrhu zákona č. 107/2002 Sb.

⁴⁹ Název tohoto zákona zní: zákon č. 31/2002 Sb., kterým se mění zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 18/1997 Sb., o mírovém využití jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů, zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů, a zákona č. 42/1992 Sb., o úpravě majetkových vztahů a vypořádání majetkových nároků v družstvech, ve znění pozdějších předpisů.

2.2.6. Zákon č. 517/2002 Sb.

Poslední změnou ZOOÚ provedenou v roce 2002 (s účinností od 1. ledna 2003) bylo zúžení kompetencí Úřadu pro ochranu osobních údajů, a to o pravomoci vyplývajících ze zákona č. 227/2000 Sb. (zákon o elektronickém podpisu). Tuto změnu přinesl zákon č. 517/2002 Sb., kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony, jenž ve své části deváté ruší pravomoci Úřadu v oblasti elektronického podpisu, včetně pravomoci vydávat prováděcí právní předpisy k zákonu č. 227/2000 Sb.

Tato úprava byla součástí rozsáhlejších změn provedených zákonem č. 517/2002 Sb. souvisejících se vznikem nového Ministerstva informatiky, na které přešly veškeré kompetence v oblasti informačních a komunikačních technologií, telekomunikací, poštovních služeb a také elektronického podpisu, které dříve spadaly částečně do působnosti Úřadu pro veřejné informační systémy a částečně Ministerstva dopravy a spojů.

2.2.7. Zákon č. 439/2004 Sb.

K doposud nejrozsáhlejší novelizaci ZOOÚ došlo na základě zákona č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Ačkoli úroveň ochrany osobních údajů v České republice a míra kompatibility ZOOÚ s předpisy Evropské unie byla ze strany orgánů EU hodnocena pozitivně,⁵⁰ k dosažení úplné shody s *acquis* bylo nezbytné ZOOÚ ještě upravit. Zákon č. 439/2004 Sb. je proto také často označován jako „euronovela“ ZOOÚ.

Hlavním cílem zákona č. 439/2004 Sb. tedy bylo docílení lepší harmonizace ZOOÚ s předpisy EU (tj. zejména se Směrnicí 95/46) a současně byl prostřednictvím této novely učiněn pokus vyřešit některé aplikační problémy, které v období od přijetí ZOOÚ vyplynuly z praxe Úřadu pro ochranu osobních údajů.

Základní okruhy změn, které zákon č. 439/2004 Sb. přinesl, lze vymezit následujícím způsobem:

- deklarace vztahu ZOOÚ k právu EU a k mezinárodním smlouvám (tj. ke Směrnici 95/46 a Úmluvě 108);
- zpřesnění některých definic, tak aby terminologie užívaná ZOOÚ více odpovídala Směrnici 95/46 (např. pojmu osobní údaj, citlivý osobní údaj nebo souhlas subjektu údajů);

⁵⁰ Peer Review Hodnotící zpráva o ochraně osobních údajů. Věstník Úřadu pro ochranu osobních údajů, 2002, č. 20, s. 1639.

- zavedení některých nových pojmů;
- změna koncepce stanovení výjimek z působnosti ZOOÚ (původní způsob vymezení výjimek pro některé subjekty byl změněn na výčet úkolů, při jejichž zajištění se tento zákon nepoužije);
- nová úprava práva subjektu údajů (osoby, jejíž osobní údaje jsou předmětem zpracování) na přístup k informacím a s tím související úprava některých práv a povinností toho, kdo s údaji nakládá (správce či zpracovatel osobních údajů);
- nové vymezení práva subjektu údajů na nápravu stavu a jemu odpovídajících povinností na straně správce osobních údajů (zejména byla vypuštěna zcela nekoncepční pravomoc Úřadu rozhodovat i o přiznání peněžité náhrady za nemajetkovou újmu⁵¹);
- změna v přístupu Úřadu k povolování předání osobních údajů do členských zemí EU a do států, které jsou smluvní stranou Úmluvy 108 (ZOOÚ nově stanoví zákaz omezování volného pohybu osobních údajů při předání do těchto zemí);
- zpřesnění některých kompetencí Úřadu (v oblasti vedení registru zpracování osobních údajů a v oblasti spolupráce s orgány EU a mezinárodních organizací) a
- novelizace úpravy sankcí za správní delikty a přestupky vyplývající z porušení ZOOÚ tak, aby odpovídala nové koncepci správního trestání (tj. přesné vymezení jednotlivých skutkových podstat).

Ačkoli změny provedené zákonem č. 439/2004 Sb. byly deklarovány jako pouhé úpravy směrem k větším kompatibilitě se Směrnicí 95/46,⁵² ve skutečnosti došlo v mnoha institutech upravených ZOOÚ k podstatným změnám. Některé nejasnosti či rozpory ovšem v ZOOÚ i po této novelizaci zůstaly a některé další zákon č. 439/2004 Sb. naopak ještě přinesl.⁵³

ZOOÚ byl po této novelizaci změněn ještě dvakrát, avšak následující novely nepřinesly již zásadní změny a ZOOÚ, fakticky ve znění zákona č. 439/2004 Sb., je tedy platný dodnes. S ohledem na to, že jednotlivé povinnosti správců osobních údajů (konkrétně zaměstnavatelů) jsou rozebrány v kapitole 4, není tedy třeba se na tomto místě detailně seznamovat se změnami úpravy ochrany osobních údajů provedenými touto novelou. Rozbor úprav, které tato novela přinesla, a jejich dopadu na subjekty zpracovávající osobní údaje i na činnost Úřadu pro ochranu osobních údajů je ostatně tématem dostatečně širokým pro samostatnou práci.

⁵¹ Vzhledem k tomu, že procesním předpisem, podle kterého měl Úřad v takovém případě postupovat, je zákon č. 71/1967 Sb., o správním řízení (správní řád), byly osoby, které se domáhaly náhrady nemajetkové újmy podle ZOOÚ, v porovnání s těmi, kteří uplatňovali obdobné právo podle § 13 občanského zákoníku, neodůvodněně znevýhodněny (účastník správního řízení je z hlediska svých práv v horším postavení než účastník řízení podle zákona č. 99/1963 Sb., občanský soudní řád), navíc soudy mají s rozhodováním o náhradách tohoto typu – na rozdíl od Úřadu – mnohem větší zkušenosti.

⁵² Důvodová zpráva k návrhu zákona č. 439/2004 Sb., obecná část.

⁵³ Zřejmě nejvýraznějším nedostatkem ZOOÚ ve znění zákona č. 439/2004 Sb. je opominutí některých povinností ve výčtu skutkových podstat správních deliktů a tedy faktická imperfektnost některých norem.

2.2.8. Zákon č. 480/2004 Sb.

Předposlední změnu ZOOÚ přinesl zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), který nabyl účinnosti dne 7. září 2004, a který transponuje do českého právního řádu Směrnici Evropského parlamentu a Rady 2000/31/ES, ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu).

Citovaným zákonem byla Úřadu pro ochranu osobních údajů svěřena nová kompetence, a to konkrétně výkon dozoru nad dodržováním povinností stanovených zákonem č. 480/2004 Sb. v oblasti šíření obchodních sdělení. Úřad je tedy na základě uvedeného zákona příslušný kontrolovat plnění některých povinností stanovených zákonem č. 480/2004 Sb. a vést správní řízení s těmi, kteří využili elektronické prostředky k šíření nevyžádaných obchodních sdělení, případně nesplnili některý z požadavků na obsah a formu obchodního sdělení.

Tato kompetence byla Úřadu svěřena s odůvodněním, že šíření obchodních sdělení je často součástí komplexnějších marketingových aktivit, při nichž dochází ke zpracování osobních údajů, a proto je vhodné, aby tato problematika spadala do jeho působnosti.⁵⁴

Nebývalý nárůst těchto tzv. SPAMů v poslední době je celosvětovým problémem, k jehož řešení je dle evropských orgánů nezbytné na území Evropské unie přijmout specializované předpisy zakotvující zákaz takového zneužívání elektronických prostředků a represivní opatření (právní normy obdobné zákonu č. 480/2004 Sb. je na základě uvedené směrnice povinen přijmout každý členský stát EU).

2.2.9. Zákon č. 626/2004 Sb.

Zatím poslední novelizací ZOOÚ byla v podstatě „kosmetická“ úprava provedená zákonem č. 626/2004 Sb., o změně některých zákonů v návaznosti na realizaci reformy veřejných financí v oblasti odměňování. Tímto zákonem byla z § 30 odst. 4 a 5 ZOOÚ vypuštěna slova „další plat“, což neznamená nic jiného než zrušení nároku předsedy a inspektorů Úřadu na tzv. třináctý a čtrnáctý plat. Platové poměry zaměstnanců Úřadu byly obdobným způsobem upraveny změnou zákona č. 143/1992 Sb., o platu a odměně za pracovní pohotovost v rozpočtových a některých dalších organizacích a orgánech, kterým se podle ZOOÚ řídí.

⁵⁴ Důvodová zpráva k návrhu zákon ač. 480/2004 Sb., zvláštní část, komentář k § 10.

V současné době je již připravována další, v pořadí již jedenáctá, změna ZOOÚ, která by měla odstranit přetrvávající nedostatky a sporné otázky, které některá ustanovení ZOOÚ stále vyvolávají (z nichž některé budou zmíněny v následujících kapitolách).⁵⁵

⁵⁵ Podle legislativního plánu prací vlády České republiky by měl být návrh této novely předložen vládě v listopadu tohoto roku a účinnosti by měl nabýt v květnu roku 2007.

3. Základní pojmy ochrany osobních údajů a působnost zákona č. 101/2000 Sb.

Jak bylo uvedeno již v předchozí kapitole je v současné době úprava ochrany osobních údajů v České republice obsažena v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů („ZOOÚ“).

Cílem ZOOÚ je zajistit ochranu osobních údajů při jejich zpracování na území České republiky a při jejich předávání do jiných zemí, a tak naplnit Listinou zaručené právo na ochranu před neoprávněným zasahováním do soukromí. Za tímto účelem tedy ZOOÚ upravuje práva a povinnosti při zpracování osobních údajů a jejich předávání do jiných států, a to v souladu s právem EU a mezinárodními smlouvami, kterými je ČR vázána (tj. zejména Úmluvou 108 a Směrnicí 95/46).⁵⁶ Ustanovením § 2 ZOOÚ byl zřízen Úřad pro ochranu osobních údajů, jakožto specializovaný ústřední správní úřad⁵⁷ pro oblast ochrany osobních údajů v rozsahu stanoveném ZOOÚ a některými dalšími zákony (viz kapitola 6.). Kompetence, činnosti a vnitřní organizace Úřadu jsou specifikovány v hlavě IV až VI ZOOÚ a také v hlavě VII, kde jsou stanoveny sankce za přestupky a jiné správní delikty, jejichž skutkovou podstatou je porušení povinností stanovených tímto zákonem.

Povinnosti spojené se zpracováním osobních údajů jsou upraveny v hlavě II ZOOÚ a dále v hlavě III ZOOÚ, kde jsou zvláště upraveny povinnosti spojené s předáváním osobních údajů do zahraničí. Dříve, než budou rozebrány jednotlivé povinnosti, je však nezbytné vyložit základní pojmy, které ZOOÚ definuje, a dále vymezit oblast působnosti tohoto zákona, tedy situace, na které se pravidla zde uvedená vztahují. Působnost ZOOÚ a vymezení pojmů je obsahem hlavy I tohoto zákona.

3.1. Vymezení základních pojmů

ZOOÚ definuje základní pojmy užívané v oblasti ochrany osobních údajů ve svém § 4, a to v souladu s terminologií zavedenou Úmluvou 108 a Směrnicí 95/46. Zejména po novelizaci ZOOÚ zákonem č. 439/2004 Sb. odpovídají některé definice § 4 ZOOÚ uvedeným mezinárodním vzorům téměř doslovně.

⁵⁶ § 1 ZOOÚ – předmět úpravy.

⁵⁷ Toto označení představuje určitý výkladový problém, neboť instituce v obdobném postavení jako ZOOÚ jsou definovány buď jako orgán státní správy ČR (Úřad pro ochranu hospodářské soutěže) nebo jako ústřední orgán státní správy (Nejvyššího kontrolního úřadu). V daném případě se nejedná o úmysl vyjádřit, že ZOOÚ má jiné postavení, ale „pouze“ o nekonzistentnost zákonodárce v užívání termínů.

3.1.1. Osobní údaj, citlivý osobní údaj, anonymní údaj a zveřejněný osobní údaj

Pojem osobní údaj je samozřejmě základním termínem právní úpravy ochrany osobních údajů. V ZOOÚ je jeho definice uvedena v § 4 písm. a), který stanoví, že pro účely tohoto zákona se osobním údajem rozumí „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů.“ Určitost či určitelnost subjektu údajů je dle citovaného ustanovení dána, jestliže „lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“

Inspirací pro znění této definice byl jak článek 2 písm. a) Směrnice 95/46, vymezující pojem „personal data“, tak i článek 2 písm. a) Úmluvy 108 s obdobným obsahem. Současné znění § 4 písm. a) ZOOÚ je v podstatě kombinací definic uvedených v těchto dokumentech. Citované ustanovení ZOOÚ bylo výrazně upraveno novelizací provedenou zákonem č. 439/2004 Sb., a to tak, že byla odstraněna určitá definice kruhem („osobním údajem je jakýkoli údaj“), dále byl doplněn demonstrativní výčet informací, které obvykle vedou ke zjištění identity osoby, a bylo vypuštěno negativní vymezení pojmu osobní údaj. Až do této novelizace se za osobní údaj totiž nepovažovala taková informace, kterou sice bylo možné vztáhnout k určité fyzické osobě, ale bylo k tomu zapotřebí nepřiměřeného množství času, úsilí nebo materiálních prostředků. S ohledem na neustálý rozvoj informačních technologií, kdy zjištění identity osoby již nevyžaduje nijak výjimečné úsilí či vynaložení nepřiměřených materiálních prostředků, byla tato část vypuštěna.

Úvodem je také důležité upozornit na to, že nelze zaměňovat pojem osobní údaj podle ZOOÚ a projev osobní povahy podle § 11 a násl. občanského zákoníku. Jedná se o dva samostatné právní instituty, přičemž projev osobní povahy může za určitých okolností obsahovat osobní údaje. Často tak dochází k prolínání těchto pojmů, což je, vzhledem k tomu, že právo na ochranu osobních údajů je složkou práva na ochranu osobnosti, logické.⁵⁸

Pojem osobní údaj je ZOOÚ definován poměrně stručně – omezuje se na určení vztahu určité informace k tomu, o kom vypovídá. Jedná se tedy o informaci vztahující se k fyzické osobě, která je buď již určena (je známa její identita) anebo určena být může, a to jednak přímo na základě těchto nebo jiných dostupných informací a jednak nepřímo, kombinací informací z různých zdrojů. Vzhledem k uvedenému je charakter některých informací jako osobních údajů relativní, proto je v určité situaci osobním údajem např. i zákaznické číslo, které je pro většinu osob údajem anonymním, ale pro příslušného obchodníka je údajem

⁵⁸ Úřad pro ochranu osobních údajů. Stanovisko k problémům z praxe č. 1/2000 – k pojmu osobní údaj (www.uoou.cz).

osobním, protože může ze svých záznamů snadno zjistit, která konkrétní fyzická osoba se pod tímto údajem skrývá.

Dle uvedené definice se tedy osobním údajem stane jakákoli informace, pokud jsou současně splněny dvě podmínky:

- 1) tuto informaci lze vztáhnout k fyzické osobě a
- 2) tato fyzická osoba je určitým subjektem identifikována („určena“) nebo identifikovatelná („určitelná“).

Osobní údaje lze různými způsoby třídít, např. na údaje identifikační, kontaktní, popisné, transakční (provozní) nebo citlivé.⁵⁹ Významnou kategorií jsou tzv. identifikační osobní údaje, které jak již tento termín sám napovídá, přímo identifikují osobu, ke které se vztahují. Disponuje-li tedy někdo identifikačními osobními údaji (především se jedná o jméno a příjmení, případně adresu bydliště, datum narození nebo rodné číslo), jsou v podstatě veškeré další informace, které o takto určené osobě má, osobními údaji ve smyslu ZOOÚ, neboť je lze vztáhnout ke konkrétní, určené osobě.

Znakem osobního údaje je, že vypovídá o fyzické osobě, kterou nelze zaměnit s jinou osobou. Nejedná se tak pouze zmíněné identifikátory, které určují konkrétní osobu přímo, ale jde o jakoukoli informaci ve vztahu ke konkrétní fyzické osobě, tedy např. i výše mzdy vyplacená za měsíc nebo diagnóza.

„Určenost“ fyzické osoby je stav, kdy správce osobních údajů přímo disponuje identifikačními údaji fyzické osoby, a jde tedy vždy o objektivní hledisko. Posouzení toho, zda je identita osoby, které se předmětné informace týkají známa či ne (tj. zda je tato osoba jednoznačně určena), by nemělo činit žádné potíže. Osoba může být takto identifikována buď pomocí jednoho přesného identifikátoru (např. rodné číslo nebo již zmíněné zákaznické číslo, ale např. také jako „starosta obce X“) nebo pomocí více údajů, které v kombinaci jednoznačnou identifikaci umožní. Obecně postačí k jednoznačnému odlišení určité osoby kombinace jména, příjmení a adresy bydliště. Pro odlišení několika členů jedné rodiny stejného jména, kteří bydlí na téže adrese, potom postačí připojit datum narození, popř. pouze ročník nebo třeba jen označení „mladší“ či „starší“. Minimální kombinaci údajů, které již vedou k identifikaci, je nutno posuzovat vždy individuálně, vzhledem ke konkrétním souvislostem. Označení osoby jako „pan Novák z Prahy“ zřejmě nebude dostatečné pro přesnou identifikaci dotyčné osoby, ale to pouze za předpokladu, že v Praze nežije pouze jediný pan Novák. Z uvedeného vyplývá, že rozsah údajů potřebných k přesné identifikaci fyzické osoby se odvíjí od situace, v jaké se tato osoba nachází.

„Určitelnost“ osoby má naopak charakter subjektivní, kdy lze fyzickou osobu jednoznačně odlišit buď již na základě osobních údajů, které jsou již k dispozici, anebo údajů, k nimž lze

⁵⁹ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 23.

získat přístup. Při posuzování, zda je fyzická osoba „určitelná“, je nutno přihlížet ke všem možnostem, které konkrétní správce osobních údajů v daném případě má.⁶⁰ V případě, kdy tento správce disponuje identifikačními údaji, nelze již považovat žádný jiný soubor údajů za anonymní, a to ani v případě, že sám identifikátory neobsahuje (za předpokladu, že dotyčný správce má alespoň teoretickou možnost údaje s identifikátory propojit a tak je přiřadit konkrétní osobě). V úvahu je také nutno vzít možnost správce získat potřebné identifikátory z veřejně přístupných zdrojů. Není přitom rozhodující, zda má v úmyslu některé uvedených z možností využít či nikoliv. Pro posouzení určitelnosti fyzické osoby je tedy podstatné, že správce osobních údajů může identifikaci osob provést buď na základě údajů, které již získal, nebo údajů které získat může.

Údajů, které mohou přispět k naší identifikaci, tj. osobních údajů, během života neustále přibývá. Bezprostředně po narození jsme identifikováni jménem, příjmením, adresou trvalého bydliště, datem a místem narození a rodným číslem.⁶¹ Kromě data a místa narození jsou však tyto údaje v čase proměnné (dnes včetně pohlaví) a v souvislosti s naší životní historií se postupně přidávají další, jako např. průběh studia, zaměstnání, zdravotní stav, rodinné poměry apod.

Zvláštní kategorií osobních údajů jsou citlivé osobní údaje, které jsou v ustanovení § 4 písm. b) ZOOÚ vymezeny takto:

„Pro účely tohoto zákona se rozumí citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.“

Ačkoli v mezinárodních dokumentech se místo pojmu citlivý údaj, který zvolil český zákonodárce, používá pojem zvláštní kategorie údajů (článek 8 Směrnice 95/46 a článek 6 Úmluvy 108 užívají shodně termín „special categories of data“), rozsah informací, které mají požívat vyšší ochrany je v uvedených dokumentech i v ZOOÚ v podstatě identický.

V porovnání se Směrnicí 95/46 je však v ZOOÚ poněkud odlišný přístup ke zpracování citlivých údajů. ZOOÚ totiž primárně zpracování takových údajů umožňuje, pouze stanoví přísnější podmínky, kdy zejména požaduje výslovný souhlas dotčené osoby anebo sledování důležitého cíle (§ 9 ZOOÚ). Naopak Směrnice 95/46 obecně zpracování citlivých osobních údajů zakazuje, ale za určitých okolností (s výslovným souhlasem dotčené osoby nebo za účelem zajištění důležitých zájmů) tento zákaz neplatí. Ačkoli výsledný efekt je v podstatě tentýž, lze konstatovat, že ZOOÚ je v přístupu ke zpracování citlivých osobních údajů

⁶⁰ Toto interpretační pravidlo vychází z bodu 26 úvodních ustanovení Směrnice 95/46.

⁶¹ Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J. Zákon o ochraně osobních údajů, komentář. Praha: C.H. Beck, 2003, s. 50.

mírnější, nicméně požadavky Směrnice 95 naplňuje. Režim, který ZOOÚ uplatňuje na všechny kategorie citlivých osobních údajů, stanoví Směrnice 95/46 pouze pro informace týkající se trestné činnosti nebo přestupků.

Přísnější podmínky pro zpracování citlivých osobních údajů jsou zavedeny proto, že nevhodným využitím či přímo zneužitím těchto informací může dojít k mnohem výraznějšímu zásahu do soukromí osob, případně k jejich diskriminaci, ať již v soukromém životě, při jednání se státními orgány nebo třeba na pracovišti.

V ZOOÚ uvedený výčet citlivých osobních údajů je výčtem taxativním. Pro přehlednost lze jednotlivé zde vyjmenované kategorie rozdělit do čtyř tématických skupin:

- 1) informace vypovídající o původu,
- 2) informace týkající se postojů a názorů,
- 3) informace o způsobu života a
- 4) biometrické a genetické údaje.

Do první skupiny spadají údaje vypovídající o národnostním, rasovém nebo etnickém původu, u nichž je důvod zařazení do tohoto ustanovení ZOOÚ evidentní. Posuzování osob (ač skryté) na základě např. jejich rasového původu je stále aktuální otázkou, a je tedy nezbytné pokoušet se i prostřednictvím ZOOÚ zamezit jakékoli diskriminaci osob na základě informací o jejich původu.

Údaje vypovídající o postojích a názorech, tedy informace o politických postojích, o členství v odborových organizacích, o náboženství a o filozofickém přesvědčení, mohou taktéž vést k diskriminaci osoby, které se týkají. Poněkud vágní pojem „filozofický postoj“, byl do této definice zahrnut zřejmě proto, aby se vyloučily spekulace o tom, zda se citlivým údajem rozumí např. pouze informace o sympatiích ke státům uznaným církvím, ale k neregistrovaným náboženským společnostem již nikoli apod. Cílem této části § 4 písm. b) ZOOÚ je chránit veškeré životní postoje a názory, bez ohledu na to, jakým způsobem jsou vyjadřovány. Spadají sem tedy jak údaje vyplývající z písemných či ústních projevů, z fotografií pořízených např. na nejrůznějších demonstracích nebo shromážděních, z účasti či neúčasti na určitém hlasování nebo veřejné anketě či petici atd.

Poněkud specifickou kategorií je údaj vypovídající o členství v odborové organizaci. Tato informace jistě vypovídá o určitém postoji zaměstnance, minimálně o jeho vůli aktivně se podílet na obhajobě práv a oprávněných zájmů zaměstnanců na daném pracovišti. Na druhou stranu práva a zájmy, které zaměstnanec jako člen odborů hájí, pro něj mohou mít doslova existenční význam a jeho členství nelze tedy vždy považovat za pouhé vyjádření názoru nebo přesvědčení jako je tomu např. u členů politických stran. Nevhodné či neoprávněné využití informace o členství by mohlo mít pro daného zaměstnance vážné následky (zejména v podobě diskriminace ze strany zaměstnavatele, jehož zájmy jsou často

v rozporu s požadavky odborových organizací), a proto je tedy vhodné tyto údaje označit za citlivé a podřídít je přísnějšímu režimu.

V pracovněprávních vztazích bývá nejčastěji otázka zpracování citlivého osobního údaje vypovídajícího o členství zaměstnance v odborech posuzována v souvislosti s platbami členských příspěvků formou srážky ze mzdy či platu (blíže viz kapitola 4).⁶²

Další skupinou citlivých osobních údajů jsou údaje, které zjednodušeně řečeno vypovídají o způsobu života jednotlivce. Co se týče informací o trestné činnosti, byl před účinností zákona č. 439/2004 Sb. (tj. novely ZOOÚ) za citlivý údaj považován jakýkoli údaj, který vypovídal o trestné činnosti konkrétní osoby. Uvedenou novelou došlo ke zúžení této oblasti pouze na údaje o odsouzení za trestný čin, což směřovalo k dosažení většího souladu se Směrnicí 95/46 i Úmluvou 108 a současně k nahrazení poněkud vágní formulaci „údaje o trestné činnosti“ jednoznačným pojmem. Náležitá úroveň ochrany osobních údajů v průběhu trestního řízení je garantována zejména zákonem č. 283/1991 Sb., o Policii České republiky, a zákonem č. 141/1961 Sb., o trestním řízení soudním (trestní řád), takže v této oblasti by neměly z hlediska ochrany osobních údajů vznikat problémy.⁶³ ZOOÚ tak poskytuje ochranu především údajům obsaženým v rozhodnutí soudu, k nimž má – vzhledem k zásadě veřejnosti projednávání trestních věcí – přístup v podstatě neomezený okruh osob.

Citlivým osobním údajem vypovídajícím o životním stylu osob jsou dále údaje o sexuálním životě. Obsah pojmu sexuální život by měl být vykládán co nejextenzivněji, tedy nikoli jako pouhý údaj o sexuální orientaci, ale veškeré informace o konkrétním chování či o partnerech.

Je nepopíratelné, že nevhodně využití informace jak o trestných činech, tak i o sexuálním životě, jsou schopny přivodit velmi závažný zásah do soukromí dotčené osoby a poškodit tuto osobu v mnoha soukromoprávních i veřejnoprávních vztazích, a proto je nezbytné, aby tyto údaje byly zpracovávány zásadně na základě zákona nebo s výslovným souhlasem osoby, které se týkají. V každém případě musí být při jejich případném zpracování postupováno vždy způsobem odpovídajícím riziku, které právu na ochranu soukromí hrozí.

Zřejmě nejčastěji jsou v praxi vystaveny určitému riziku nebo neadekvátnímu zacházení citlivé osobní údaje o zdravotním stavu. Tyto údaje mohou částečně také vypovídat o určitých životních postojích, např. v případě kuřáka nebo osoby, která podstoupila plastickou operaci, ale zároveň také o skutečnostech, které jsou vůlí neovlivnitelné, dané buď

⁶² K této problematice se vyjádřil Úřad pro ochranu osobních údajů ve svém stanovisku č. 2/2001 – zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací, a dále ve stanovisku č. 5/2004 – uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky od daně z příjmu (www.uouu.cz).

⁶³ Mates, P., Bartík, V. Nová úprava ochrany osobních údajů. Právní rádce č. 9/2004, s. 42.

geneticky, nebo prostou náhodou. Schopnost těchto údajů vážně zasáhnout do sféry osobního a soukromého života jedince, v případě jejich necitlivého nebo neoprávněného zpracování (např. zveřejnění) je zřejmá.

Citlivým osobním údajem není pouze informace o existenci určité nemoci, stanovená diagnóza, předepsaná forma léčby apod., ale i údaj o absenci onemocnění, tedy i pouhé obecné konstatování, že zdravotní stav je dobrý (na rozdíl od toho údaj o trestní bezúhonnosti nelze považovat za údaj vypovídající o odsouzení za trestný čin, tedy za údaj citlivý⁶⁴).

O zdravotním stavu může často vypovídat již jen údaj o hospitalizaci v obecně známém zařízení (typicky léčebna v Praze Bohnicích) nebo u známého specialisty, přičemž se ale nemusí nutně jednat o zařízení či specialistu známé široké veřejnosti, postačí, aby touto znalostí disponoval jen omezený okruh osob (např. osoby léčené ze závislosti na návykových látkách mají jistě větší přehled o takto specializovaných léčebnách než zbytek populace).

Velmi dynamicky se rozvíjející oblastí citlivých osobních údajů, která do jisté míry souvisí s údaji o zdravotním stavu, jsou tzv. biometrické a genetické údaje.

Biometrický údaj není ZOOÚ definován a při jeho výkladu je nutno vycházet z obecného významu, který tento pojem má, tedy měřitelný fyzický znak umožňující zjištění nebo ověření identity osoby.⁶⁵ Biometrika je tedy jednoznačná identifikace osob na základě jedinečných fyziologických znaků člověka.

Vodítkem, co si pod pojmem biometrický údaj představit, může být také ustanovení § 42e zákona č. 283/1991 Sb., o Policii České republiky, které policistovi umožňuje za účelem identifikace osoby snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy. Jedná se tedy především o otisky prstů či dlaně, obraz oční sítnice nebo duhovky, případně i rozbor tváře či hlasového projevu.

Pořízené záznamy, tj. otisk prstu nebo fotografie, jsou pouze nosiči těchto údajů (nelze tedy říct, že „fotografie, je citlivým osobním údajem“).⁶⁶

Vzhledem k technologickému pokroku v této oblasti není v současné době využití biometrických údajů pouze v rukou vybraných státních orgánů – zmíněné otisky prstů či obraz oční duhovky jsou stále častěji využívány i v soukromém sektoru, zejména jako součást bezpečnostních opatření např. při kontrole osob vstupujících do budov.

⁶⁴ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 67.

⁶⁵ Slovník Association for Biometrics (www.biometrie.cz).

⁶⁶ Je však nutno podotknout, že běžné fotografie nosičem biometrických údajů (alespoň v současné době) nejsou, protože z nich tyto údaje nelze získat a případně následně využít. Naopak fotografie, které jsou již dnes vyžadovány např. při zhotovení občanského průkazu (viz § 5 vyhlášky č. 42/2004 Sb., kterou se provádí zákon o občanských průkazech a zákon o cestovních dokladech), nebo které budou v budoucnu povinnou součástí cestovního pasu, tento požadavek již splňují. Běžné fotografie mohou ovšem být nosičem jak „obyčejných“ osobních údajů, tak i citlivých osobních údajů, především vypovídajících o rase, národnosti nebo etnickém původu.

Genetickými údaji se rozumí informace získané rozbořením DNA, přičemž je známo, že touto analýzou je možné získat skutečně velké množství údajů, které navíc nevypovídají pouze o osobě, o jejíž DNA se jedná, ale také o třetích osobách, tj. předcích či potomcích této osoby. Vzhledem k tomu, že s genetickými údaji se tradičně zachází jako s údaji citlivými, které je nutno náležitě chránit, neměly by být v této oblasti s aplikací podmínek stanovených ZOOÚ spojeny významnější problémy.

Otázkou je, zda by nebylo vhodnější pojem biometrický údaj pro potřeby ZOOÚ přímo definovat, a to způsobem, který by vyjasnil, spadají-li pod režim tohoto zákona veškeré měřitelné údaje o člověku (tedy i výška či váha) nebo jen údaje, které jsou zpracovávány digitálně, anebo i psychologické charakteristiky jedince, které mohou při neoprávněném či nevhodném zpracování taktéž způsobit významný zásah do soukromí, které ale nejsou měřitelné v pravém slova smyslu (ačkoli mnohdy jsou vyjádřitelné v objektivních hodnotách, typicky hodnota tzv. IQ⁶⁷).

Vzhledem k tomu, že motivací k zařazení biometrických údajů mezi údaje citlivé byl technologický vývoj umožňující jejich digitální zpracování, bylo by zřejmě nejvhodnější podrobit režimu zpracování citlivých osobních údajů podle ZOOÚ jen určité zpracování biometrických údajů, zejména právě automatizované.⁶⁸

Jak biometrické, tak i genetické údaje mají obrovský informační potenciál a v budoucnu se s jejich zpracováním budeme setkávat zřejmě stále častěji. Lze předpokládat, že již v blízké budoucnosti bude možné získávat osobní údaje touto cestou mnohem snáze a také je mnohem snáze vyhodnocovat a dále využívat, s čímž bude zřejmě spojeno také zvýšené riziko zneužití těchto údajů. Zařazení biometrických a genetických údajů do kategorie údajů citlivých je tak logickou reakcí na dosavadní rozvoj moderních technologií a současně přípravou na předpokládaný další vývoj.

Určitým protipólem osobního údaje je údaj anonymní, definovaný v § 4 písm. c) ZOOÚ jako „takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.“ Takový údaj tedy nelze spojit s konkrétní fyzickou osobou, neboť neobsahuje žádnou charakteristiku nebo jedinečný znak této osoby.

Pojmově čistým anonymním údajem je pouze ten, který již při shromažďování není vztážitelný k žádné osobě (např. informace získané v rámci různých anonymních anket či průzkumů). Zpracování údajů, které nejsou osobními údaji, ale logicky vůbec režimu ZOOÚ

⁶⁷ Výsledky psychologických testů, tj. právě např. hodnota IQ, je však obvykle nutno posuzovat jako údaje vypovídající o zdravotním stavu, tedy opět jako citlivé osobní údaje.

⁶⁸ Matoušová, M. Pohled praxe na novelu zákona o ochraně osobních údajů. Právní rádce č. 11/2004, s. 71. Zde lze podotknout, že v mnohých členských státech EU nejsou biometrické údaje posuzovány automaticky jako citlivé, ale jejich citlivost je odvozována ze způsobu zpracování. Obecně zřejmě není důvod označovat za citlivý osobní údaj např. i velikost chodidla, tak jak to vyplývá ze ZOOÚ.

nepodléhá (dle § 3 ZOOÚ vymezujícím působnost tohoto zákona). Osobní údaje lze ovšem anonymizovat až dodatečně, a to buď částečně, nebo absolutně.⁶⁹ Částečnou anonymizací osobního údaje se rozumí stav, kdy správce osobních údajů oddělí ze shromážděných dat identifikační údaje a dále zpracovává pouze tu část dat, kterou již nelze vztáhnout ke konkrétním osobám. Správce má však nadále možnost zpracovávaná data fyzickým osobám zpětně přiřadit, nicméně z hlediska třetích osob, které s osobními údaji přímo nakládají nebo kterým mohou být zpracovávané údaje z různých důvodů zpřístupněny, se jedná o údaje anonymní (příkladem může být běžný postup při vyhodnocování výsledků testů či zkoušek nebo statistických průzkumů). Absolutní anonymizací údajů je logicky stav, kdy by již ani správce osobních údajů nebyl schopen předmětné informace vztáhnout ke konkrétní osobě.

Definice anonymního údaje se nevyskytuje ani v Úmluvě 108, ani ve Směrnici 95/46. Do ZOOÚ byla vložena zřejmě proto, že v dalších ustanoveních tohoto zákona se pracuje s pojmem „anonymizování osobních údajů“, a to v souvislosti se zpracováním osobních údajů pro účely statistické a vědecké, kdy ZOOÚ požaduje anonymizaci zpracovávaných údajů, jakmile to bude možné [§ 5 odst. 1 písm. e) ZOOÚ].

ZOOÚ dále zvlášť definuje zveřejněný osobní údaj, kterým je podle § 4 písm. l) ZOOÚ „osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.“

Opět se jedná o termín, který mezinárodní dokumenty, jimiž se ZOOÚ inspiroval, nezmiňují. Český zákonodárce však považoval za důvodné tento pojem vymežit, a to pravděpodobně vzhledem ke znění jedné z výjimek z povinnosti zpracovávat osobní údaje zásadně se souhlasem subjektů údajů, jedná-li se právě o zpracování oprávněně zveřejněných osobních údajů [§ 5 odst. 2 písm. d) ZOOÚ].

ZOOÚ jmenuje prostředky, jejichž prostřednictvím ke zveřejnění údajů obvykle dochází, pouze příkladem. Taxativní výčet zde logicky není možný již jen s ohledem na neustálý technologický vývoj v této oblasti. Veřejným seznamem podle § 4 písm. l) ZOOÚ je typicky obchodní rejstřík, katastr nemovitostí nebo také běžný telefonní seznam. Z hlediska uvedené definice zveřejněného údaje přitom není rozhodující, zda byl údaj publikován oprávněně či nikoli.⁷⁰

Zveřejňování osobních údajů představuje jeden z nejzávažnějších problémů ochrany osobních údajů. Jednou zveřejněný údaj je nadále jen velmi obtížné chránit a zásah do soukromí osoby je tak do jisté míry již nevratný. Typickým příkladem je zveřejňování jmen dlužníků, ať již soukromými subjekty nebo např. obcemi, což může dotčenou osobu vážně poškodit v mnoha dalších soukromoprávních i veřejnoprávních vztazích. Bez ohledu na to,

⁶⁹ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 34.

⁷⁰ Tato okolnost je však již podstatná při posuzování jednání toho, kdo tuto informaci zveřejnil, a dále při případném dalším využití takového údaje, neboť jak je již uvedeno výše, lze zveřejněné údaje dále zpracovávat bez souhlasu osoby, které se týkají, pouze pokud byly zveřejněny oprávněně.

jak moc si příslušní hříšníci tuto nechtěnou popularitu „zasloužili“, se obvykle jedná o neoprávněný zásah do soukromí těchto osob, a tedy o porušení některého ustanovení ZOOÚ.

Oprávněně zveřejněnými údaji jsou ty, k jejichž zveřejnění dává správci osobních údajů svolení buď sám subjekt údajů, nebo jej k tomu zmocňuje zákon, např. zveřejnění osobních údajů výherců nejrůznějších soutěží nebo zveřejňování informací o osobách v souvislosti s vedením trestního řízení podle zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Podmínky zpřístupnění osobních údajů konkrétních osob vždy by měly být předem smluvně vymezeny nebo dány příslušným zákonem.

V otázce zveřejňování osobních údajů je ZOOÚ prakticky neustále v jistém konfliktu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, který sleduje v podstatě opačný cíl, tedy zpřístupnění maximálního objemu informací o činnosti státních orgánů, orgánů územní samosprávy a veřejných institucí hospodařících s veřejnými prostředky co nejširšímu okruhu subjektů. Tento konflikt je však do značné míry pouze zdánlivý, neboť z ustanovení § 2 odst. 3 zákona 106/1999 Sb. jednoznačně vyplývá, že tento zákon se nevztahuje na poskytování osobních údajů a informací podle zvláštního právního předpisu, kterým je míněn mj. právě ZOOÚ. Z uvedeného vyplývá, že žadatel podle zákona č. 106/1999 Sb. má právo obdržet určité informace o činnosti subjektu vykonávajícího státní správu, ale nikoli osobní údaje těch, kterých se výkon této činnosti týká. Příslušný úřad či orgán tak musí obsah informace před poskytnutím náležitě posoudit a zvolit vhodnou míru anonymizace osobních údajů.

3.1.2. Subjekt údajů

Subjektem údajů se podle § 4 písm. d) ZOOÚ rozumí „fyzická osoba, k níž se osobní údaje vztahují“. Tento výraz, na rozdíl od pojmu „dotčená osoba“ užívaného předchozím zákonem č. 256/1992 Sb., i jeho obsah plně odpovídá termínu „the data subject“ a jeho definicím obsaženým v Úmluvě 108 i Směrnici 95/46.

Ačkoli uvedená definice se zdá být jednoznačná, vznikla v souvislosti s jejím výkladem jedna zásadní otázka, a to, zda se ZOOÚ vztahuje i na zpracování osobních údajů zemřelých osob.

Úmyslem zákonodárce při formulování definice subjektu údajů v ZOOÚ bylo zdůrazněním vztahu osobních údajů k určitému subjektu, umožnit aplikaci ZOOÚ např. i na údaje týkající se nenarozených dětí.⁷¹ Analogicky by se tedy měl ZOOÚ vztahovat i na osobní údaje zemřelých.

⁷¹ Důvodová zpráva k návrhu ZOOÚ, zvláštní část, komentář k § 4 písm. d).

Těžko si lze představit, že po dobu života fyzické osoby požívají její osobní údaje ochrany podle ZOOÚ, ale okamžikem její smrti je možné s těmito údaji nakládat zcela volně. Není důvod, aby nebylo možné i po smrti osoby požadovat po správci osobních údajů plnění povinností podle ZOOÚ, zvláště povinnosti uchovávat osobní údaje pouze po dobu nezbytnou k dosažení účelu jejich zpracování, kdy může být právě smrt subjektu údajů důvodem, pro ukončení zpracování jeho osobních údajů.⁷² Pouze tam, kde má subjekt údajů na základě ZOOÚ, jakožto účastník právního vztahu, určitá práva (např. právo obdržet určité informace nebo požadovat nápravu vadného stavu), dochází po jeho smrti k zániku těchto práv, neboť ZOOÚ přechod práv neupravuje. Tím samozřejmě není vyloučena možnost příbuzných dotčené osoby domáhat se práva na ochranu osobnosti podle § 15 občanského zákoníku.

Existují však i názory, že ZOOÚ má jednoznačně na mysli žijící fyzickou osobu a na zpracování osobních údajů zemřelých osob se tedy nevztahuje.⁷³ Avšak výše uvedená definice osobního údaje stanoví pouze podmínku vztažitelnosti určité informace ke konkrétní fyzické osobě, což je zcela jistě možné i po smrti této osoby. Není tedy důvodu zbavovat osobní údaje zemřelých osob ochrany podle ZOOÚ.

3.1.3. Souhlas subjektu údajů

Definice souhlasu subjektu údajů, kterým je podle § 4 písm. n) ZOOÚ „svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“, byla do ZOOÚ vložena až zákonem č. 439/2004 Sb. s tím, že se tak ZOOÚ ještě více přiblíží Směrnici 95/46, kde je v článku 2 písm. h) vymezen pojem „the data subject's consent“. Vzhledem k určitým výkladovým problémům, které předchozí znění definice souhlasu (resp. obou předchozích znění) vyvolávalo, bylo také zapotřebí jasně stanovit, že souhlas podle ZOOÚ je jednostranným právním úkonem, nikoli dohodou subjektu údajů se správcem osobních údajů nebo nějakým zvláštním právním institutem.

Původní znění ZOOÚ sice definici souhlasu neobsahovalo, ale v ustanovení o povinnosti správce zpracovávat osobní údaje zásadně na základě souhlasu byly stanoveny jeho formální a obsahové náležitosti, a to obligatorní písemnost a absolutní odvolatelnost (tj. souhlas mohl být „kdykoli odvolán“). Nejenže byl souhlas tedy vysoce formalizovaným úkonem, ale správce osobních údajů nemohl vykonávat svoji činnost, aniž by nebyl v neustálé nejistotě, zda a případně kdy, se subjekt údajů rozhodne souhlas odvolat. Poměrně záhy (zákonem č. 177/2001 Sb.) byl však tento absolutní požadavek písemné formy a odvolatelnosti souhlasu změněn na relativní (subjekt údajů mohl tedy souhlas sice kdykoli

⁷² Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 210.

⁷³ Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, a.s., 2004, s. 190.

odvolat, pokud se však nedohodl se správcem osobních údajů jinak). Teprve zákon č. 439/2004 přinesl – vložením nové definice souhlasu subjektu údajů – důraz na svobodu a informovanost souhlasu, jako projevu vůle subjektu údajů. Obsahem souhlasu je v souladu s úpravou podle Směrnice 95/46 svobodné, zřejmé a vědomé vyslovení podmínek, za kterých má dojít ke zpracování osobních údajů, což logicky není možné bez dostatečného povědomí o tom, k čemu je souhlas poskytován.

Co se týče formy souhlasu, ta je dnes ponechána na rozhodnutí konkrétního správce. Je však pravděpodobné, že i nadále bude převažovat forma písemná, již jen z toho důvodu, že správce musí být schopen po celou dobu zpracování souhlas subjektu údajů prokázat.

Původní úprava souhlasu se zpracováním osobních údajů byla odůvodněna potřebou vyšší míry ochrany subjektu údajů v počátečním období po účinnosti ZOOÚ, kdy na jedné straně správci osobních údajů nedokázali stanovit jasné podmínky budoucího zpracování a na straně druhé občané zpřístupňovali své osobní údaje často velmi lehkomyšlně.⁷⁴

Souhlas, jeho platnost nebo možnost odvolání, se řídí obecnou úpravou právních úkonů podle občanského zákoníku, a to včetně všech zde obsažených interpretačních pravidel, jako je např. princip dobré vůle, šetření známého úmyslu jednajícího nebo *in dubio mitius*.

3.1.4. Zpracování osobních údajů

Osobním údajům je ochrana na základě § 3 ZOOÚ poskytována pouze tam, kde jsou „zpracovávány“, definice zpracování osobních údajů, uvedená v § 4 písm. e) ZOOÚ, musí být tedy nastavena natolik obecně, aby tento pojem plně pokrýval co nejširší rozsah způsobů nakládání s osobními údaji.

Zpracováním osobních údajů se tedy rozumí „jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“

Výčet úkonů uvedený v citovaném ustanovení je demonstrativní, ZOOÚ zde vyjmenovává pouze běžné operace s osobními údaji, čímž je ponechán prostor i pro další způsoby či techniky, které v současné době nejsou ještě rozšířeny nebo ani vyvinuty.

Zpracováním osobních údajů je nutno rozumět každou jednotlivou operaci, nikoli pouze celý soubor kroků potřebných k dosažení stanoveného cíle, např. i „pouhé“ shromáždění

⁷⁴ Kučerová, A. Úvaha nad novelou zákona o ochraně osobních údajů. Právní zpravodaj č. 12/2004, s. 9.

osobních údajů je zpracováním ve smyslu ZOOÚ (pod podmínkou existence určitého, předem stanoveného, úmyslu osobní údaje zpracovávat – viz kapitola 3.2).

Znění citované definice zcela odpovídá článku 2 písm. b) Směrnice 95/46 který vymezuje termín „processing of personal data“ jako jakýkoli úkon nebo soubor úkonů s osobními údaji a zároveň demonstrativně jmenuje některé základní způsoby nakládání s osobními údaji, které je nutno hodnotit jako zpracování osobních údajů.

Některé operace s osobními údaji jsou, vzhledem k jejich častému výskytu v praxi nebo proto, že s těmito pojmy ZOOÚ dále pracuje, definovány ZOOÚ samostatně, a to v ustanoveních § 4 písm. f) až i) ZOOÚ.

V § 4 písm. f) ZOOÚ je definováno shromažďováním osobních údajů, a to jako „systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování“.

Shromažďování údajů je logicky prvním krokem každého, kdo má v úmyslu osobní údaje zpracovávat. Jedná se o cílené získávání údajů či informací o fyzických osobách, přičemž není rozhodné, zda se jedná o jednorázový nebo soustavný, pravidelně či nepravidelně se opakující úkon. O shromažďování osobních údajů jako o zpracování podle ZOOÚ je možno hovořit, pokud jsou získané údaje ukládány na nějaký nosič (lhostejno, zda např. na disketu, CD nebo na papír), aby mohly být buď bezprostředně, nebo kdykoli v budoucnu využity k dosažení stanoveného účelu. V případě, kdy jsou osobní údaje takto úmyslně shromažďovány za účelem jejich dalšího využití, je za zpracování podle ZOOÚ možno považovat již shromáždění jediné (první) informace.⁷⁵

Další běžnou operací je uchovávání osobních údajů, kterým podle § 4 písm. g) ZOOÚ je „udržování údajů v takové podobě, která je umožňuje dále zpracovávat“.

Podstatou uchovávání údajů je tedy jejich udržování v takovém stavu, že je kdykoli možno je dále využít nebo s nimi nějakým způsobem nakládat. Na rozdíl od podoby dat, která by měla být v zásadě po celou dobu zpracování k původně stanovenému účelu neměnná, je formu nosiče možno v průběhu uchovávání údajů měnit tak, aby bylo zaručeno jejich bezproblémové budoucí zpracování (např. převedení údajů z listinné do elektronické formy).

Blokováním osobních údajů se podle § 4 písm. h) ZOOÚ rozumí „vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat.“

Blokované osobní údaje nadále existují, ale jsou dočasně znepřístupněny pomocí opatření znemožňujících po určitou dobu jejich zpracování (jakýmkoli způsobem a kterýmkoli subjektem). K blokování údajů může přistoupit z mnoha důvodů sám správce osobních

⁷⁵ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 234.

údajů, např. jako postup pro zajištění či zabezpečení údajů, toto jeho rozhodnutí ale nesmí být v rozporu se zájmy subjektů údajů.

Blokování může také vycházet z opatření uložených Úřadem pro ochranu osobních údajů, a to v případě, kdy bylo správci osobních údajů na základě provedené kontroly uloženo nápravné opatření (podle § 40 odst. 2 ZOOÚ) v podobě likvidace zpracovávaných údajů. Až do provedení uložené likvidace, případně až od vyřešení námitek proti tomuto opatření, musí být dotčené osobní údaje blokovány, tedy nesmí s nimi být jakkoli nakládáno.

Logicky posledním krokem zpracování je likvidace osobních údajů, kterou § 4 písm. i) ZOOÚ definuje jako „fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.“

Způsob likvidace se samozřejmě odvíjí od nosiče, na kterém jsou uchovávány, ale společný je cíl tohoto kroku, kterým je definitivní neexistence a nedostupnost těchto informací. Může se tedy jednat jak o fyzickou likvidaci nosiče nebo o vymazání údajů, za předpokladu, že není možné údaje následně jakkoli obnovit v takové podobě, aby měly charakter osobních údajů podle ZOOÚ. Likvidace osobních údajů podle § 4 písm. i) ZOOÚ je záměrná operace prováděná s osobními údaji z rozhodnutí odpovědného subjektu, zejména proto, že pominul účel zpracování, nebo na základě žádosti subjektu údajů podle § 21 ZOOÚ (tj. v případě, kdy se subjekt domnívá, že zpracování je v rozporu se zákonem nebo jeho právem na ochranu soukromého a osobního života) anebo jako nápravné opatření uložené Úřadem. Náhodné zničení údajů nelze za likvidaci v tomto smyslu považovat⁷⁶ (zde naopak je na místě otázka, zda dotčený správce přijal veškerá bezpečnostní opatření, jak mu ukládá § 13 ZOOÚ – viz níže).

3.1.5. Správce, zpracovatel a příjemce osobních údajů

Klíčovým pojmem ZOOÚ je rovněž termín správce osobních údajů. Tím je podle § 4 písm. j) ZOOÚ „každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj.“

Citovaná definice je opět převzata ze Směrnice 95/46 a v souladu s jejím článkem 2 písm. d), užívajícím pojem „controller“, je za správce osobních údajů podle ZOOÚ nutno považovat každou fyzickou nebo právnickou osobu, státní orgán nebo jakýkoli jiný subjekt, kterému je zpracování osobních údajů buď uloženo právním předpisem, nebo se pro něj rozhodl sám.

Účelem zpracování je cíl, kterého má být právě pomocí zpracování osobních údajů dosaženo a pojmem prostředky se rozumí zejména technická zařízení, jejichž

⁷⁶ Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J. Zákon o ochraně osobních údajů, komentář. Praha: C.H. Beck, 2003, s. 57.

prostřednictvím hodlá správce zpracování provádět, tj. hlavně výpočetní technika, ale také prostředky manuálního zpracování jako např. předtištěný formulář.

Je-li povinnost zpracovávat osobní údaje stanovena zákonem, popř. z něj vyplývá nepřímě, měl by tento zákon současně vymezit i účel zpracování a konkrétní prostředky, které má daný správce využít. Zákonem je zpracování osobních údajů typicky stanoveno v oblasti státní správy nebo pro výkon veřejné moci pověřenými subjekty soukromého práva, tedy správním orgánům, obcím, soudům, profesním komorám nebo zaměstnavatelům apod. Správce pověřený zákonem logicky nesmí své úkoly a kompetence jakkoli rozšiřovat, tedy zpracovávat osobní údaje k jinému než stanovenému účelu nebo jinými než stanovenými prostředky. Nejsou-li konkrétní prostředky zákonem určeny (což ovšem nelze považovat za vhodné řešení), může je správce zvolit sám, přičemž odpovídá za jejich adekvátnost. Účel zákonem stanoveného zpracování osobních údajů, pokud není výslovně vymezen, je možno vyvodit obvykle z předmětu úpravy dané normy.

Zpracování osobních údajů v rámci prosazování státní moci je, s ohledem na čl. 2 odst. 3 Ústavy, možné pouze za účelem a prostředky stanovenými zákonem. Státní orgány a jiné subjekty podílející se na výkonu státní správy tedy nemohou samy stanovit účel, k jehož dosažení budou osobní údaje zpracovávat.⁷⁷

Správce, který se rozhodl dosahovat určitého cíle pomocí zpracování osobních údajů, aniž by to byla jeho zákonná povinnost, je limitován (při určení tohoto cíle a prostředků) pouze tím, že se musí jednat o postup, který není zákonem výslovně zakázán. Správcem osobních údajů je tak každý, kdo např. v rámci výkonu své podnikatelské činnosti, živnosti nebo profese systematicky (v rozsahu nad své zákonné povinnosti) zpracovává osobní údaje svých obchodních partnerů, klientů nebo zaměstnanců, případně i jejich rodinných příslušníků.

Podle věty druhé § 4 písm. j) ZOOÚ může správce, pokud mu to zvláštní zákon nezakazuje, zpracováním osobních údajů pověřit zpracovatele osobních údajů (nebo i více zpracovatelů). Správce tedy může buď provádět celé zpracování, tj. veškeré operace s ním spojené, sám nebo může část, případně i veškeré kroky, zpracování převést na zpracovatele. Avšak i v případě, kdy dojde k přenosu všech činností spojených se zpracováním na zpracovatele, nedochází k úplnému přechodu odpovědnosti za předmětné zpracování. Správce, vzhledem k tomu, že jemu bylo provádění zpracování buď uloženo zákonem, nebo jej stanovil sám, se nemůže zbavit odpovědnosti za plnění povinností se zpracováním osobních údajů spojených. Subjektu údajů je tak garantováno, že se svých práv může domáhat především u správce. Pro subjekt údajů může být totiž obtížné „dopátrat

⁷⁷ Typickým příkladem, kdy je zákonný účel zpracování osobních údajů překračován, je zveřejňování usnesení rady či zastupitelstva obce v plném (neanonymizovaném) znění např. v místním tisku nebo na Internetu, čímž dochází ke zpracování osobních údajů (např. dlužníků obce nebo osob kupujících od obce nemovitost) mimo zákonem stanovený účel a tedy k porušení ZOOÚ.

se“, který z mnoha možných zpracovatelů pověřených správcem svým postupem do jeho práv zasáhl, čímž by byla výrazně snížena jeho možnost domoci se nápravy.

Zpracovatel osobních údajů je definován hned v následujícím ustanovení § 4 písm. k) ZOOÚ a je jím „každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.“

Obdobně jako v případě správce osobních údajů není rozhodné, zda se jedná o fyzickou či právnickou osobu, anebo zda se zpracovatel svou činností podílí na výkonu veřejné moci či na čistě soukromoprávních aktivitách. Zpracovatel provádí veškeré operace s osobními údaji zásadně buď na základě pověření správcem, tj. smluvně, nebo na základě výslovného zákonného zmocnění. Neurčuje tedy ani účel, ani prostředky zpracování a musí se řídit podmínkami stanovenými zákonem nebo správcem, pro kterého zpracování osobních údajů provádí.

Uvedená definice odpovídá ustanovení článku 2 písm. e) Směrnice 95/46, kde je zpracovatel vymezen velmi jednoduše jako ten, kdo zpracovává osobní údaje pro správce („processor“).

ZOOÚ nijak neomezuje počet zpracovatelů, které může správce do zpracování zapojit, správce tedy může jednotlivé kroky zpracování rozdělit mezi libovolný počet zpracovatelů. Jisté omezení lze spatřovat v povinnosti správce osobních údajů nakládat s údaji tak, aby nedošlo k jejich ohrožení, neoprávněnému zpracování nebo ztrátě apod. (§ 13 ZOOÚ).

Zpracovatel je v praxi obvykle pověřen správcem, tedy smluvně. Situace, kdy postavení zpracovatele osobních údajů vyplývá určitému subjektu přímo ze zákona, jsou méně časté.⁷⁸ Náležitosti smlouvy, kterou správce pověřuje zpracovatele, aby pro něj vykonával některé kroky zpracování osobních údajů, jsou upraveny v § 6 ZOOÚ. Pro smlouvu o zpracování osobních údajů se obligatorně vyžaduje písemná forma a je nezbytné v ní vymezit rozsah, účel a dobu zpracování osobních údajů a dále specifikovat záruky zpracovatele týkající se technických a organizačních opatření k zabezpečení ochrany osobních údajů.

Podle § 7 ZOOÚ se na zpracovatele osobních údajů vztahují přiměřeně i některé povinnosti stanovené v § 5 ZOOÚ správcí (kterým je věnována následující kapitola), tedy např. povinnost zpracovávat pouze přesné osobní údaje, shromažďovat pouze údaje odpovídající stanovenému účelu a v přiměřeném rozsahu nebo uchovávat údaje pouze po dobu nezbytnou k naplnění tohoto účelu. Lze spekulovat o tom, na kolik je toto ustanovení vůči zpracovatelům spravedlivé, neboť je na ně v podstatě částečně přenášena odpovědnost za rozhodnutí správce. Česká právní úprava vztahu správce osobních údajů a zpracovatele totiž nepřejala pravidlo zakotvené v článku 17 odst. 3 Směrnice 95/46, že zpracovatel jedná

⁷⁸ Např. činnost obecních a krajských úřadů podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), které jsou v souvislosti se zpracováním údajů z Informačního systému evidence obyvatel výslovně označeny za zpracovatele osobních údajů ve smyslu ZOOÚ.

se“, který z mnoha možných zpracovatelů pověřených správcem svým postupem do jeho práv zasáhl, čímž by byla výrazně snížena jeho možnost domoci se nápravy.

Zpracovatel osobních údajů je definován hned v následujícím ustanovení § 4 písm. k) ZOOÚ a je jím „každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje.“

Obdobně jako v případě správce osobních údajů není rozhodné, zda se jedná o fyzickou či právnickou osobu, anebo zda se zpracovatel svou činností podílí na výkonu veřejné moci či na čistě soukromoprávních aktivitách. Zpracovatel provádí veškeré operace s osobními údaji zásadně buď na základě pověření správcem, tj. smluvně, nebo na základě výslovného zákonného zmocnění. Neurčuje tedy ani účel, ani prostředky zpracování a musí se řídit podmínkami stanovenými zákonem nebo správcem, pro kterého zpracování osobních údajů provádí.

Uvedená definice odpovídá ustanovení článku 2 písm. e) Směrnice 95/46, kde je zpracovatel vymezen velmi jednoduše jako ten, kdo zpracovává osobní údaje pro správce („processor“).

ZOOÚ nijak neomezuje počet zpracovatelů, které může správce do zpracování zapojit, správce tedy může jednotlivé kroky zpracování rozdělit mezi libovolný počet zpracovatelů. Jisté omezení lze spatřovat v povinnosti správce osobních údajů nakládat s údaji tak, aby nedošlo k jejich ohrožení, neoprávněnému zpracování nebo ztrátě apod. (§ 13 ZOOÚ).

Zpracovatel je v praxi obvykle pověřen správcem, tedy smluvně. Situace, kdy postavení zpracovatele osobních údajů vyplývá určitému subjektu přímo ze zákona, jsou méně časté.⁷⁸ Náležitosti smlouvy, kterou správce pověřuje zpracovatele, aby pro něj vykonával některé kroky zpracování osobních údajů, jsou upraveny v § 6 ZOOÚ. Pro smlouvu o zpracování osobních údajů se obligatorně vyžaduje písemná forma a je nezbytné v ní vymezit rozsah, účel a dobu zpracování osobních údajů a dále specifikovat záruky zpracovatele týkající se technických a organizačních opatření k zabezpečení ochrany osobních údajů.

Podle § 7 ZOOÚ se na zpracovatele osobních údajů vztahují přiměřeně i některé povinnosti stanovené v § 5 ZOOÚ správci (kterým je věnována následující kapitola), tedy např. povinnost zpracovávat pouze přesné osobní údaje, shromažďovat pouze údaje odpovídající stanovenému účelu a v přiměřeném rozsahu nebo uchovávat údaje pouze po dobu nezbytnou k naplnění tohoto účelu. Lze spekulovat o tom, na kolik je toto ustanovení vůči zpracovatelům spravedlivé, neboť je na ně v podstatě částečně přenášena odpovědnost za rozhodnutí správce. Česká právní úprava vztahu správce osobních údajů a zpracovatele totiž nepřejala pravidlo zakotvené v článku 17 odst. 3 Směrnice 95/46, že zpracovatel jedná

⁷⁸ Např. činnost obecních a krajských úřadů podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), které jsou v souvislosti se zpracováním údajů z Informačního systému evidence obyvatel výslovně označeny za zpracovatele osobních údajů ve smyslu ZOOÚ.

pouze podle pokynů správce, který je jediným subjektem zodpovědným za celé zpracování. Uvalení povinností, které má podle ZOOÚ správce osobních údajů, v téměř stejném rozsahu i na zpracovatele je teoreticky výhodné z hlediska snazšího prosazování ZOOÚ, nelze však označit za správné.⁷⁹

ZOOÚ ukládá zpracovateli i určité povinnosti, které se na správce nevztahují, např. povinnost neprodleně upozornit správce na porušování povinností stanovených tímto zákonem a takové zpracování ukončit (§ 8 zákona 101).

Ačkoli zpracování osobních údajů fakticky provádí zaměstnanci správce a zpracovatele, případně jiné osoby v obdobném postavení, nejsou tyto osoby z hlediska ZOOÚ zpracovateli osobních údajů, neboť jejich činnost nevyplývá přímo z pověření správce nebo zákonného zmocnění. Na činnost uvedených osob v souvislosti se zpracováním osobních údajů se vztahují ustanovení § 14 a 15 ZOOÚ, kde je jim uložena povinnost postupovat zásadně v souladu s pokyny subjektu, pro který svoji činnost vykonávají, a povinnost mlčenlivosti o zpracovávaných osobních údajích a o bezpečnostních opatřeních přijatých k jejich ochraně.

Zákonem č. 439/2004 Sb., tzv. euronovelou, byla definiční ustanovení ZOOÚ doplněna o vymezení pojmu příjemce, kterým je podle § 4 písm. o) ZOOÚ „každý subjekt, kterému jsou osobní údaje zpřístupněny“, a to s výjimkou subjektů, které zpracovávají osobní údaje za účelem výkonu kontroly, dozoru nebo dohledu při zajišťování veřejného pořádku, vnitřní bezpečnosti, předcházení či odhalování trestné činnosti nebo významných hospodářských či finančních zájmů České republiky [tj. za účelem zajištění úkolů podle § 3 odst. 6 písm. g) ZOOÚ].

Doplněním tohoto termínu bylo transponováno ustanovení článku 2 písm. g) Směrnice 95/46, kde je příjemce („recipient“) vymezen obdobným způsobem. Definice příjemce osobních údajů má význam z hlediska informační povinnosti správce osobních údajů podle § 11 ZOOÚ, kde je správci uloženo informovat subjekt údajů mj. i o tom, komu budou jeho údaje v průběhu zpracování zpřístupněny.

Vynětí subjektů, kterým jsou zpřístupňovány osobní údaje pro výkon veřejné moci, z definice příjemce bylo vedeno záměrem osvobodit zejména správce rozsáhlých datových souborů ve státní správě (např. Informačního systému evidence obyvatel, obchodního rejstříku nebo katastru nemovitostí) od povinnosti informovat o subjektech postupujících v souladu s § 3 odst. 6 písm. g) ZOOÚ jakožto o příjemcích jim zpracovávaných údajů.⁸⁰

⁷⁹ Matoušová, M. Pohled praxe na novelu zákona o ochraně osobních údajů. Právní rádce č. 11/2004, s. 70.

⁸⁰ Důvodová zpráva k návrhu zákona č. 439/2004 Sb., zvláštní část, komentář k bodu 9.

3.1.6. Evidence a datové soubory

Novelizací provedenou zákonem č. 439/2004 Sb. bylo do ZOOÚ dále doplněno ustanovení § 4 písm. m) definující evidenci nebo datový soubor osobních údajů jako „jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií“ (dále jen „datový soubor“).

Podstatným definičním znakem datového souboru je způsob vnitřního uspořádání umožňující zpřístupnění zde obsažených informací za pomoci určitého hlediska. Datovým souborem podle citovaného ustanovení tak jsou např. i osobní složky zaměstnanců, za předpokladu, že jsou uchovávány např. v kartotéce řazené podle abecedního pořádku.

Datový soubor, vzhledem k snadné přístupnosti údajů, jistě představuje vyšší riziko pro osobní údaje, s nimiž pracuje, ale z hlediska potřeb právní úpravy ochrany osobních údajů v ČR není doplnění této definice do ZOOÚ příliš významné. V dalším textu se tento pojmem již nevyskytuje. Tato změna ZOOÚ znamenala v podstatě pouze zvýšení harmonizace české právní úpravy ochrany osobních údajů se Směrnicí 95/46, která v článku 2 písm. c) definuje termín „personal data filing system“.

3.2. Působnost zákona č. 101/2000 Sb.

Oblast působnosti ZOOÚ je, a to jak pozitivně, tak i negativně, vymezena v ustanovení § 3 tohoto zákona.

Dle § 3 odst. 2 se ZOOÚ vztahuje na veškeré osobní údaje, bez ohledu na to, zda jsou zpracovávány prostřednictvím výpočetní techniky, jinými automatizovanými prostředky anebo manuálně. Z hlediska osobní působnosti, vymezené v § 3 odst. 1 ZOOÚ, se tento zákon vztahuje na veškeré fyzické i právnické osoby, které zpracovávají osobní údaje, ať jsou veřejnoprávními nebo soukromoprávními subjekty.

V této souvislosti je třeba připomenout, že osobními údaji, na jejichž zpracování se ZOOÚ aplikuje, se rozumí pouze údaje fyzických osob, nikoli osob právnických. Toto vymezení logicky vyplývá ze základního cíle právní úpravy ochrany osobních údajů, kterým je ochrana soukromí, o němž lze hovořit pouze v souvislosti s fyzickými osobami.⁸¹

Uvedené vymezení působnosti ZOOÚ je v souladu s textem Úmluvy 108, jejíž článek 3 odst. 1 zavazuje smluvní strany uplatnit zásady této úmluvy na automatizované soubory osobních údajů a jejich automatizované zpracování ve veřejném a soukromém sektoru, přičemž Česká republika dle svého prohlášení aplikuje principy zde zakotvené rovněž na

⁸¹ Jsou-li osobní údaje fyzických osob součástí jména osoby právnické, jak to u tzv. podnikajících fyzických osob vyžaduje zákon č. 512/1991 Sb., obchodní zákoník, jsou ZOOÚ v určitých situacích chráněny, ale např. adresa sídla právnické osoby nebo její IČO do působnosti ZOOÚ nespádají.

soubory osobních údajů, které se nezpracovávají automatizovaně. ZOOÚ splňuje v tomto směru i požadavky Směrnice 95/46, jejíž působnost je v pozitivním smyslu vymezena v článku 3 odst. 1 tak, že pravidla zde stanovená platí pro zpracování osobních údajů zcela nebo částečně automatizovaná, jakož i – za určitých podmínek – na zpracování jinými než automatizovanými způsoby.⁸²

Vymezení oblastí, na které se ZOOÚ nevztahuje, je poněkud obsáhlejší a především výkladově problematičtější.

Z působnosti ZOOÚ je, podle § 3 odst. 3 tohoto zákona, zaprvé vyloučeno takové zpracování osobních údajů, které provádí fyzická osoba výlučně pro svoji osobní potřebu. Tato výjimka vychází z ustanovení článku 3 odst. 2 Směrnice 95/46, kterým je z působnosti této směrnice vyloučeno „zpracování osobních údajů prováděné fyzickou osobou výlučně v rámci osobních či domácích činností“. Považovat každého, kdo si vede např. osobní adresář, a tedy nepochybně zpracovává osobní údaje svých příbuzných či přátel (a to možná i ve velkém rozsahu) za správce osobních údajů ve smyslu ZOOÚ a požadovat po něm plnění povinností stanovených tímto zákonem, by bylo samozřejmě absurdní. Vzhledem k tomu, že pojem „osobní potřeba“ není ZOOÚ definován, je při výkladu tohoto ustanovení nutno vycházet z obecného chápání jeho obsahu, přičemž vodítkem pro výklad může být i bod 12 preambule Směrnice 95/46, podle kterého se osobní potřebou fyzické osoby rozumí činnosti, které mají výlučně soukromou povahu, jako je korespondence nebo vedení diáře či adresáře.

Výkladově obtížnější je další výjimka z působnosti ZOOÚ, uvedená v § 3 odst. 4, která zní, že ZOOÚ se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto nejsou již dále zpracovávány. Uvedené ustanovení je sporné již jen z toho důvodu, že nahodilé může být jen jednorázové shromáždění, nikoli shromažďování údajů, kdy již sám tento termín indikuje určitou systematickou činnost.

Pojem nahodilé je třeba vykládat tak, že se jedná o údaje shromážděné zcela bez úmyslu, bez předchozího záměru takové údaje získat (např. údaje o rodinných příslušnících obsažené v žádosti o zaměstnání, které uchazeč do žádosti zahrnul z vlastní iniciativy) nebo údaje získané omylem. V případě, kdy si subjekt stanoví určitý cíl, jehož má v úmyslu dosáhnout prostřednictvím shromažďování určitých osobních údajů a jejich následného využití, jedná se o systematické jednání, které ZOOÚ podléhá.⁸³

Nahodilé shromáždění, resp. „obdržení“, údajů je z působnosti ZOOÚ vyloučeno zcela správně, neboť této situaci nelze předejít, a pokud nejsou takto získané údaje dále využívány

⁸² Aplikace Směrnice 95/46 na manuální zpracování osobních údajů je podmíněna zařazením údajů do datového souboru (z čehož vyplývají jisté sporné otázky – viz níže).

⁸³ I v takovém případě by ovšem mohlo dojít k nahodilému shromáždění údajů, a to pokud by správci osobních údajů byly (z iniciativy třetí osoby) sděleny údaje, které k dosažení svého cíle neměl v úmyslu shromažďovat, tedy o které neměl zájem.

či jinak nezpracovány, není důvodné ve vztahu k nim požadovat plnění povinností uložených ZOOÚ.⁸⁴ Obdobně se ZOOÚ neaplikuje ani na shromáždění osobních údajů, k němuž dochází např. v souvislosti s poskytováním jednorázové služby, kdy si např. podnikatel za účelem možnosti kontaktování zákazníka poznamená jeho jméno a adresu (zejména při opravě hodnotnějších věcí jako je mobilní telefon). V takovém případě sice dochází ke shromáždění osobních údajů, ale zcela náhodných osob, kdy předmětem činnosti dotyčného podnikatele není zpracování těchto údajů (nezaznamenal si je za účelem dosažení určitého cíle prostřednictvím jejich zpracování). Za předpokladu, že po vyřízení zakázky nebudou takto získané osobní údaje dále uchovávané (např. jako evidence stálých zákazníků), se ZOOÚ na popsany postup nevztahuje. Obdobný výklad se použije např. i pro činnost advokáta.

Častý je ovšem i názor, že nahodilost zpracování osobních údajů se neodvíjí od původního úmyslu údaje shromáždit (resp. absence takového úmyslu), ale že to je teprve podoba výstupu předmětného zpracování, která musí obsahovat prvky systematickosti.⁸⁵ Tento výklad vychází z článku 3 odst. 1 Směrnice 95/46, který výslovně stanoví, že na manuálně zpracovávané osobní údaje (tj. „údaje zpracovávané jinak než automatizovanými způsoby“) se tato směrnice vztahuje pouze, pokud jsou nebo se mají stát součástí datového systému. Dále podle bodu 15 úvodních ustanovení Směrnice 95/46 se tato směrnice vztahuje na neautomatizované zpracování osobních údajů pouze, pokud mají být takto shromážděné údaje následně uspořádány podle zvláštních kritérií usnadňujících jejich dostupnost. Jinými slovy, dle bodu 27 tamtéž, pokud jde o manuální zpracování, týká se Směrnice 95/46 pouze datových systémů uspořádaných podle specifických hledisek týkajících se jednotlivců, která umožňují vyhledávání osobních údajů, a nikoli nestrukturovaných záznamů.⁸⁶

Tímto výkladem lze však dojít absurdnímu závěru, že na toho, kdo zcela záměrně shromažďuje určité informace za konkrétním účelem, avšak takto shromážděné údaje uchovává neuspořádaně, bez jakéhokoli systému (např. na volných listech bez možnosti vyhledávání podle určitých hledisek), se ZOOÚ nevztahuje. Naopak ten, kdo by shromažďoval tytéž údaje za identickým účelem a vytvářel by kartotéku či evidenci řazenou tak, že by bylo možné v ní vyhledávat podle konkrétního kritéria, by již byl správcem osobních údajů ve smyslu ZOOÚ se všemi povinnostmi, které z tohoto postavení vyplývají.

⁸⁴ Jakým způsobem má subjekt, který nahodile obdrží určité informace, postupovat závisí vždy na konkrétních okolnostech, v úvahu připadá vrácení např. omylem zasláné písemnosti, likvidace nepotřebných údajů nebo nepřihlížení k těmto údajům (to v případě, kdy jsou neoddělitelné od údajů, které správce legálně zpracovává).

⁸⁵ Např. Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, a.s., 2004, s. 186 nebo Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 201.

⁸⁶ Právě s ohledem toto ustanovení Směrnice 95/46 byla zákonem č. 439/2004 Sb. do ZOOÚ nově vložena definice evidence a datového souboru [§ 4 písm. m) ZOOÚ], která však, vzhledem k tomu, že uvedené vymezení působnosti Směrnice 95/46 ZOOÚ zcela nepřijímá, nemá větší význam.

Přitom je zřejmé, že v prvním případě hrozí osobním údajům větší rizika než v případě druhém, neboť systematické uspořádání shromážděných údajů napomáhá jejich správě, tj. i lepšímu plnění povinností podle v – např. posouzení přesnosti zpracovávaných údajů, posouzení účelnosti a nezbytnosti jejich dalšího zpracování či přijetí odpovídajících bezpečnostních opatření.

Směrnice 95/46 paradoxně podporuje i tento závěr, když již v citovaném bodě 27 úvodních ustanovení, uvádí, že rozsah ochrany osobních údajů nesmí být závislý na použitých technických prostředcích, neboť by tak vzniklo riziko obcházení povinností při zpracování osobních údajů. Vyloučení manuálního zpracování osobních údajů neuspořádaných např. do kartotéky řazené podle jména osob z působnosti ZOOÚ toto riziko rozhodně přináší. Správce osobních údajů by se v takovém případě mohl snadno vyhnout povinnostem stanoveným ZOOÚ tak, že by ke zpracování osobních údajů nevyužíval výpočetní techniku a shromážděné informace netřídil podle jednotlivých kritérií, ale „pouze“ uchovával, např. v pořadí v jakém je získal. Jeho činnost by byla samozřejmě takovým postupem ztížena, což ovšem nemůže být důvodem k vyloučení takového zpracování z působnosti ZOOÚ, tj. odepření ochrany takto zpracovávaným osobním údajům.

Systematická procesus následného zpracování údajů tedy nelze považovat za definiční znak „nahodilosti“ podle ZOOÚ. Naopak tímto znakem musí být systematický přístup ke shromáždění potřebných údajů (určitý záměr), resp. jeho nedostatek.

V úvahu je dále nutno vzít také ustanovení Úmluvy 108, která má vzhledem k čl. 10 Ústavy vyšší právní sílu než ZOOÚ, a která se dle článku 3 uplatní bez dalšího omezení i na soubory osobních údajů nezpracovávané automatizovaně. Výše uvedený restriktivní výklad nahodilosti shromáždění osobních údajů podle ZOOÚ (tj. pouze při nedostatku předcházejícího záměru a nikoli při absenci systematického výstupu zpracování) se tak jeví jako vhodnější.⁸⁷

Před novelou ZOOÚ provedenou zákonem č. 439/2004 Sb. obsahovalo ustanovení § 3 odst. 4 ZOOÚ ještě větu druhou, vylučující z působnosti tohoto zákona nahodilé shromažďování osobních údajů v rozsahu nezbytném pro výkon nezávislého povolání. Tato věta však jen opakovala obsah věty první a pouze jej adresovala určitým skupinám (advokátům, notářům apod.), u nichž docházelo v praxi ke sporům, zda se na jejich činnost ZOOÚ vztahuje či nikoli (viz kapitola 2.2.2). Vypuštěním této věty se na skutečnosti, že na

⁸⁷ Za zmínku v této souvislosti stojí srovnání se slovenským zákonem č. 428/2002 Z. z., o ochrane osobných údajov, ktorý upravuje tuto problematiku v § 2a písm. b) tak, že tento zákon se nevztahuje na ochranu osobních údajů, které byly získané náhodně bez předcházejícího určení účelu a prostředků zpracování, bez záměru jejich dalšího zpracování v systému uspořádaném podle osobnostních kritérií a které nejsou dále systematicky zpracovávány.

běžné operace s osobními údaji při výkonu tzv. svobodných povolání se ZOOÚ neuplatní, nic nemění.

Poměrně rozsáhlé výjimky z povinností stanovených správčům osobních údajů jsou dále uvedeny v § 3 odst. 6 ZOOÚ. Jedná se o zpracování osobních údajů prováděná příslušnými orgány státu zjednodušeně řečeno za účelem zajištění bezpečnosti, veřejného pořádku, odhalování a stíhání trestných činů, významného hospodářského či finančního zájmu České republiky nebo Evropské unie nebo zajištění činností souvisejících se zpřístupňováním svazků bývalé Státní bezpečnosti.

Jak bylo uvedeno již v kapitole 2.2.7. koncepce ustanovení § 3 odst. 6 ZOOÚ byla zákonem č. 439/2004 Sb. změněna v tom smyslu, že nadále neobsahuje výčet orgánů, na jejichž činnosti se ZOOÚ neuplatní, ale výčet cílů, při jejichž dosahování se na zpracování osobních údajů ZOOÚ neaplikuje. Původní znění citovaného ustanovení přinášelo jisté pochybnosti o rozsahu oprávnění zde uvedených subjektů (např. zda je ZOOÚ vyloučen i v případě, že zpracovávají údaje svých zaměstnanců z titulu zaměstnavatele). Tato změna byla vedena úmyslem více harmonizovat znění § 3 odst. 6 ZOOÚ s článkem 13 Směrnice 95/46, který upravuje výjimky z její působnosti obdobným způsobem.

Za účelem výše uvedených cílů ovšem nejsou příslušné orgány vyňaty z působnosti ZOOÚ zcela, ale pouze v rozsahu ustanovení § 5 odst. 1, § 11 a odst. 12 tohoto zákona. Bylo by jistě nelogické ukládat např. Policii ČR povinnost podle § 5 odst. 1 písm. c) ZOOÚ zpracovávat pouze přesné osobní údaje, o jejich shromáždění dotyčnou osobu informovat (podle § 11 ZOOÚ) a na její žádost jí kdykoli sdělit, jaké osobní údaje o ní zpracovává, jak stanoví § 12 ZOOÚ. Na druhou stranu i údaje shromážděné při zajišťování těchto tzv. veřejných zájmů je nutno spravovat tak, aby nedocházelo ke zbytečným zásahům do soukromí osob, a proto i v těchto případech platí např. povinnost příslušného správce (podle § 13 ZOOÚ) přijmout odpovídající bezpečnostní opatření.

Novelou č. 439/2004 Sb. byla nově upravena působnost ZOOÚ vůči správčům osobních údajů, kteří jsou, jak je dnes zcela běžné, usazeni ve více zemích. V ustanovení § 3 odst. 5 je deklarováno použití ZOOÚ vůči správci, který není usazen v ČR, ale v daném případě se podle zásad mezinárodního práva veřejného má přednostně použít právní řád České republiky, a dále použití ZOOÚ v případě, kdy správce, který je usazen mimo území EU, zpracovává osobní údaje na našem území. Prostřednictvím tohoto ustanovení jsou v podstatě rozšiřovány standardy ochrany osobních údajů EU i do nečlenských zemí a dále je zaručeno, že veškeré osobní údaje zpracovávané v České republice budou požívat stejnou úroveň ochrany.

Z uvedeného výkladu je zřejmé, že naprostá většina postupů zaměstnavatele, při kterých jakkoli nakládá s osobními údaji svých zaměstnanců, spadá do působnosti ZOOÚ, neboť se jedná o zpracování osobních údajů ve smyslu § 4 písm. e) tohoto zákona, při kterém je zaměstnavatel podle § 4 písm. j) ZOOÚ v pozici správce těchto údajů, jemuž jsou adresovány povinnosti stanovené touto právní normou. Zaměstnanci, který je v roli subjektu údajů podle § 4 písm. d) ZOOÚ, přiznává ZOOÚ určitá práva, jejichž využitím se může i sám zasadit o dosažení žádoucí úrovně ochrany svých osobních údajů.

4. Práva a povinnosti při zpracování osobních údajů v rámci pracovněprávních vztahů

Svoji úlohu v pracovněprávních vztazích nemohou zaměstnavatelé plnit bez znalosti určitých informací o svých zaměstnancích, tj. bez znalosti jejich osobních údajů. Potřeba zpracovávat některá data vyvstává ještě před vznikem pracovněprávního vztahu, v souvislosti s procesem přijímání nových zaměstnanců, a trvá i po jeho zániku, kdy je zaměstnavatel povinen uchovávat po stanovenou dobu některé doklady týkající se bývalých zaměstnanců.

Zpracování osobních údajů zaměstnanců v rámci pracovněprávního vztahu bezpochyby není zpracováním výlučně pro osobní potřebu zaměstnavatele a také, alespoň ve své významné části, není zpracováním nahodilým. Působnost ZOOÚ je zde tedy jednoznačně dána. Zaměstnavatel je z hlediska ZOOÚ správcem osobních údajů podle § 4 písm. j) ZOOÚ, tedy tím, komu jsou touto právní normou zejména ukládány povinnosti, a zaměstnanec je v pozici subjektu údajů ve smyslu § 4 písm. d) ZOOÚ, jehož zájmy jsou prostřednictvím ZOOÚ chráněny a jemuž jsou také poskytována i některá práva, která může aktivně vůči správci osobních údajů uplatňovat.

Některé povinnosti stanovené ZOOÚ jsou (na základě § 7 ZOOÚ) adresovány také zaměstnavatelem zmocněným zpracovatelům osobních údajů, např. společností najatým na zpracování mzdové agendy. Odpovědnost za plnění jednotlivých povinností se odvíjí od konkrétního uspořádání vztahu správce a zpracovatele, tj. závisí na tom, které činnosti daný subjekt skutečně vykonává, které kroky zpracování může fakticky ovlivnit.⁸⁸

ZOOÚ stanoví určité povinnosti také přímo osobám, které zpracování fakticky provádějí, tedy zaměstnancům správce či zpracovatele osobních údajů a jiným osobám v obdobném postavení.

Práva a povinnosti těch, kteří osobní údaje zpracovávají, upravuje hlava II ZOOÚ, tedy ustanovení § 5 až 26. Řada ustanovení této hlavy byla dotčena novelou zákona 101 provedenou zákonem č. 439/2004 Sb., a to buď přímo, nebo nepřímo – v souvislosti se změnami provedenými citovanou novelou v hlavě VII ZOOÚ upravující sankce za nedodržení povinností stanovených tímto zákonem.⁸⁹

⁸⁸ Na zpracovatele osobních údajů se dle § 7 ZOOÚ vztahují konkrétně povinnosti podle § 5 tohoto zákona, který obsahuje základní povinnosti při zpracovávání osobních údajů.

⁸⁹ Přičemž některé z těchto změn měly významný dopad na možnost vymáhání povinností stanovených ZOOÚ (viz níže).

Pro větší přehlednost je možné povinnosti zakotvené v hlavě II ZOOÚ rozdělit podle toho, ve které fázi procesu zpracování osobních údajů daná povinnost správci vzniká. Povinnosti stanovené ZOOÚ lze potom dělit na:

- 1) povinnosti před zahájením zpracování;
- 2) povinnosti v průběhu zpracování;
- 3) povinnosti související s ukončením zpracování.

Z hlediska možnosti volby správce osobních údajů, zda bude údaje zpracovávat či nikoli, lze dále povinnosti podle ZOOÚ rozdělit následovně:

- 1) povinnosti správce osobních údajů, jemuž je zpracování uloženo zákonem a
- 2) povinnosti adresované pouze správci, který zpracování osobních údajů sám stanovil.

Vzhledem k tomu, že zákoník práce neobsahuje speciální úpravu povinností v oblasti zpracování osobních údajů v pracovněprávních vztazích, použije se ZOOÚ vždy, když zaměstnavatel zpracovává osobní údaje svých zaměstnanců, a také když zaměstnanci v rámci své pracovní činnosti s osobními údaji nakládají.

4.1. Povinnosti zaměstnavatele před zahájením zpracování osobních údajů

Jak je uvedeno již výše ZOOÚ rozlišuje mezi správci, kteří si účel zpracování osobních údajů zvolili sami, a správci, jimž je zpracování osobních údajů uloženo zákonem. Ačkoli většina povinností stanovených ZOOÚ se vztahuje na všechny správce bez rozdílu, právě ve fázi před zahájením zpracování je výrazně více požadavků kladeno na správce, který si účel zpracování stanovil sám.

Obecně řečeno je správce osobních údajů ještě před zahájením samotného zpracování osobních údajů, tj. budoucí správce, povinen stanovit účel zpracování osobních údajů, určit prostředky a způsob zpracování, získat souhlas se zpracováním osobních údajů, splnit informační povinnost vůči subjektům údajů, a oznámit zamýšlené zpracování osobních údajů Úřadu pro ochranu osobních údajů.

Logicky zcela prvním krokem každého správce osobních údajů, v podstatě ještě před tím, než se správcem stane, je podle § 5 odst. 1 písm. a) ZOOÚ stanovení účelu, k němuž mají být osobní údaje zpracovány.

Je-li správci osobních údajů – zaměstnavateli uloženo zpracování osobních údajů zákonem, vyplývá z tohoto zákona i jeho účel, který je zde buď přímo vyjádřen, nebo je možno jej odvodit z předmětu úpravy daného právního předpisu. Tento účel je potom zaměstnavatel povinen sledovat a je přinejmenším vhodné, aby dané zpracování prováděl

pod odpovídajícím označením (např. „mzdové účetnictví“), aby bylo zřejmé, že se jedná o zpracování prováděné na základě určitého zákona, nikoli z rozhodnutí správce.⁹⁰

Naprostá většina operací s osobními údaji zaměstnanců prováděná jejich zaměstnavatelem je právě zpracováním uloženým zákonem, kdy tedy správce osobních údajů sám účel zpracování neurčuje. V právním řádu České republiky je řada zákonů (typicky v oblasti sociálního zabezpečení, nemocenského a zdravotního pojištění, daní účetnictví apod.), které stanoví zaměstnavatelům nejružnější povinnosti, jejichž plnění obnáší zpracování osobních údajů. Příkladem může být povinnost zaměstnavatele vést evidenci pro účely nemocenského a důchodového pojištění podle zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, nebo povinnost vést pro každého zaměstnance mzdový list uložená zákonem č. 586/1992 Sb., o daních z příjmů, anebo povinnost evidovat pracovní dobu, práci přesčas, pracovní pohotovost a noční práce u jednotlivých zaměstnanců podle § 94 zákoníku práce.

Ve všech uvedených případech lze z příslušné normy vyvodit účel, k němuž mají být osobní údaje zaměstnance zpracovávány, tj. zajištění úkolů při výběru daně z příjmu fyzických osob, při provádění sociálního zabezpečení nebo při kontrole dodržování pracovní doby. V některých případech stanoví zákon přímo také rozsah potřebných údajů, případně i konkrétní prostředky, které k danému zpracování mají být užity.

Zaměstnavatel však může také sám stanovit, že k určitému účelu bude osobní údaje svých zaměstnanců zpracovávat, aniž by mu to nějaký zvláštní zákon ukládal. Důvody takového rozhodnutí zaměstnavatele mohou být různé např. může po některých svých zaměstnancích žádat poskytnutí čísla soukromého mobilního telefonu, aby pro něj byli lépe dosažitelní, nebo může považovat za vhodné umístit na své internetové stránky fotografie svých zaměstnanců za účelem lepší komunikace se zákazníky anebo považuje za nezbytné zabezpečit vstup na určitá pracoviště zvýšenou kontrolou, např. pomocí otisků prstů zaměstnanců.

V těchto případech zaměstnavatel musí vymezit účel zpracování sám. Stanovení účelu zpracování je definičním znakem správce osobních údajů a způsob, jakým se správce s touto povinností vypořádá, předurčuje obsah řady jeho dalších povinností při následném zpracování osobních údajů. Účel zpracování je tedy pro posuzování plnění povinností podle ZOOÚ zcela zásadní kategorií.

Účel zpracování osobních údajů však nemůže správce zvolit zcela libovolně, stanovený účel musí být legální a legitimní. Ačkoli tyto požadavky z § 5 odst. 1 písm. a) ZOOÚ přímo nevyplývají, je nutno toto ustanovení vykládat v souvislosti s korespondujícím článkem 6 odst. 1 písm. b) Směrnice 95/46, který požaduje, aby stanovené účely zpracování byly

⁹⁰ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 218.

vyjádřeny výslovně a aby byly legitimní, a článkem 5 písm. b) Úmluvy 108 vyžadujícím oprávněnost účelu zpracování. Vyjádření těchto podmínek přinesla do českého právního řádu teprve až zmíněná euronovela ZOOÚ, tj. zákon č. 439/2004 Sb., tím, že v nové úpravě skutkových podstat přestupků a jiných správních deliktů v hlavě VII ZOOÚ (konkrétně v § 44 a § 45) je stanoveno, že správce se dopustí jiného správního deliktu, jestliže mj. stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona. Tím došlo k doplnění, resp. nepřímé novelizaci, povinnosti správce podle § 5 odst. 1 písm. a) ZOOÚ, nicméně zakotvení požadavku na legalitu a legitimitu účelu přímo v citovaném ustanovení by bylo jistě vhodnější.

Legalitu, tj. soulad s platnými právními předpisy, zvoleného účelu zpracování osobních údajů není ve většině případů obtížné posoudit. Legimitu účelu je však nutno hodnotit vždy ad hoc, tj. zejména porovnáním deklarovaného účelu zpracování se skutečným jednáním správce osobních údajů, a to s přihlédnutím ke všem relevantním okolnostem případu. V oblasti pracovně právních vztahů tak lze za legitimní účel zpracování považovat např. využití údajů o datu narození zaměstnance za účelem blahopřání k narozeninám, což může pomoci k vytvoření vhodného pracovního prostředí nebo ke zvýšení identifikace zaměstnance s danou společností.⁹¹ Naopak v rozporu se ZOOÚ by byla např. snaha zaměstnavatele získat detailní přehled o soukromém životě zaměstnanců, byť odůvodněná třeba tím, že má s ohledem na zachování dobrého jména zájem zaměstnávat pouze tzv. „slušné lidi“.

ZOOÚ nestanoví jakou formou má být účel zpracování vyjádřen, ale již vzhledem k případné potřebě prokázat splnění povinnosti podle § 5 odst. 1 písm. a) ZOOÚ, je vhodné zvolit formu, která bude jednoznačné vymezení účelu zpracování dokládat. Obvykle lze tuto povinnost splnit např. zakotvením v interních dokumentech správce osobních údajů. Správce může buď přijmout samostatný dokument věnovaný ochraně osobních údajů, což je vhodné zejména u správce se složitější organizační strukturou a větším objemem zpracovávaných dat, nebo je možné zakomponovat tyto informace do jiných dokumentů, např. do organizačního nebo pracovního řádu.

Deklarování účelu zpracování osobních údajů musí být dostatečně určité, nelze se omezit pouze na obecné konstatování, že osobní údaje budou zpracovávány např. pro podnikatelskou činnost. Pro naplnění povinnosti podle § 5 odst. 1 písm. a) ZOOÚ je nezbytné specifikovat konkrétní důvod, konkrétní cíl zpracování osobních údajů.⁹²

Smyslem povinnosti vymezit účel zpracování osobních údajů je zejména to, aby ještě před započítáním samotného zpracování správce otevřeně deklaroval cíle své činnosti a své úmysly a aby se v podstatě „zamyslel“ nad tím, čeho hodlá pomocí zpracování osobních

⁹¹ To ovšem za předpokladu, že s tímto postupem vyjádří zaměstnanec souhlas – viz níže.

⁹² „Cíl“ zpracování ostatně více odpovídá termínu „purpose“ užitému ve Směrnici 95/46.

údajů dosahovat a podle toho mohl náležitě plnit další povinnosti předcházející samotnému zpracování osobních údajů i povinnosti v jeho průběhu. Dostatečně jasně vymezený účel umožňuje správci mj. vyhodnotit rizika zásahu do soukromí subjektů údajů a přijmout jim odpovídající bezpečnostní opatření.

Bezprostředně poté, co se zaměstnavatel rozhodne, že bude k naplnění určitého záměru zpracovávat osobní údaje zaměstnanců a tento záměr určitým způsobem deklaruje, resp. mu povinnost zpracovávat údaje vyplývá ze zákona, musí stanovit prostředky a způsob zpracování osobních údajů, což mu ukládá § 5 odst. 1 písm. b) ZOOÚ.

Obdobně jako u účelu zpracování, který správci vyplývá ze zvláštního zákona, měly by být příslušným právním předpisem stanoveny alespoň základní prostředky, jejichž prostřednictvím má být daného účelu dosahováno. Povinnost určit prostředky a způsob zpracování platí pouze v té míře, kterou zvláštní zákon již nespecifikuje. Správce tedy musí provést zákonem stanovené požadavky tak, aby zohlednil konkrétní situaci a okolnosti zpracování, zejména by měl určit vnitřní uspořádání činností, odpovědnost konkrétních osob a zvolit adekvátní technická řešení. Prostředkem zpracování osobních údajů je např. evidenční list upravený v zákoně č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, kniha úrazů podle § 133c odst. 3 zákoníku práce nebo písemný doklad o jednotlivých složkách mzdy a o provedených srážkách podle § 120 odst. 4 téhož zákona. Naopak např. pro vedení evidence pracovní doby nebo dovolených není zaměstnavateli žádný konkrétní prostředek či způsob stanoven.

Není-li zpracování osobních údajů povinností správce vyplývající ze zákona, musí definovat prostředky a způsob zpracování sám. ZOOÚ opět nestanoví jakou formu má správce zvolit, ale platí obdobně to, co bylo již uvedeno výše, totiž, že je vhodné se s touto povinností vypořádat způsobem, který správci umožní její splnění následně prokázat. Nejběžnějším a zřejmě nejvhodnějším způsobem stanovení prostředků a způsobu zpracování osobních údajů je opět jejich specifikování v určitém interním předpise správce.

Rozdíl mezi tím, co se rozumí prostředky zpracování a tím, co je způsob zpracování není příliš ostrý. Jako prostředky zpracování se obvykle označují spíše technická zařízení („čím“ je zpracování prováděno) a způsob zpracování je chápán jako určitá metoda („jak“ zpracování probíhá, tj. zejména zda je prováděno manuálně či automatizovaně).

Na rozdíl od účelu zpracování osobních údajů, který v jeho průběhu nelze změnit,⁹³ může správce původně zvolené prostředky či způsob zpracování s ohledem na jejich funkčnost a efektivitu měnit. Projeví-li se zvolené prostředky nebo způsob jako nezpůsobilé k bezpečnému zpracování osobních údajů, je správce fakticky povinen takovou změnu provést. Povinnost stanovit prostředky a způsob zpracování tak bezprostředně souvisí s (již

⁹³ Údaje shromážděné k určitému účelu nelze bez dalšího využít jiným způsobem než právě v souladu s tímto účelem (pro jiné využití by byl zapotřebí zejména souhlas subjektu údajů – viz níže).

několikrát zmíněnou) povinností přijmout nezbytná bezpečnostní opatření podle § 13 ZOOÚ, a je tedy nutno ji vykládat tak, že správce je povinen přijmout nikoli jakékoli, ale vhodné prostředky zpracování.

Další otázkou, kterou musí zaměstnavatel vyřešit ještě před tím, než zpracování osobních údajů zahájí, je otázka, zda je povinen zpracovávat osobní údaje pouze se souhlasem subjektů údajů nebo zda se na něj vztahuje některá z výjimek z této povinnosti.

Povinnost zpracovávat osobní údaje zásadně pouze se souhlasem subjektů údajů je základní zásadou právní úpravy ochrany osobních údajů zakotvenou na mezinárodní úrovni v článku 7 písm. a) Směrnice 95/46.⁹⁴ Tento princip znamená, že rozhodovat o možnosti využití svých osobních údajů je primárně oprávněna osoba, ke které se tyto údaje vztahují.

Obecná povinnost zpracovávat osobní údaje pouze se souhlasem subjektů údajů je vyjádřena v návěti § 5 odst. 2 ZOOÚ. Citované ustanovení dále přináší taxativní výčet výjimek z této povinnosti, tj. situací, kdy souhlas subjektů údajů není zapotřebí. Pro zpracování citlivých osobních údajů je obdobná povinnost, tedy zpracování údajů zásadně na základě souhlasu (resp. výslovného souhlasu), zakotvena v § 9 písm. a) ZOOÚ a výjimky z této povinnosti v následujících ustanoveních § 9 písm. b) až ch).

Veškeré výjimky z povinnosti správce získat před zpracováním osobních údajů souhlas osoby, o jejíž údaje se jedná, jsou vázány na účel daného zpracování, čímž se projevuje zmíněná klíčová role účelu zpracování osobních údajů.

Z povinnosti disponovat souhlasem podle § 5 odst. 2 ZOOÚ, tj. ve vztahu k „obyčejným“ osobním údajům, jsou vyňaty situace vyjmenované v písm. a) až g) citovaného ustanovení. Jedná se o:

- a) zpracování nezbytné pro dodržení právní povinnosti správce;
- b) zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů;
- c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů;
- d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem;
- e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby;
- f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení nebo,

⁹⁴ Úmluva 108 tento požadavek přímo nestanoví a v článku 5 písm. a) pouze odkazuje na národní úpravu s tím, že požaduje, aby osobní údaje byly získány a zpracovány poctivě a v souladu se zákony.

g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.

V pracovněprávních vztazích se zřejmě nejčastěji uplatní výjimky podle § 5 odst. 2 písm. a), b) a e) ZOOÚ.

Ustanovení § 5 odst. 2 písm. b) ZOOÚ se aplikuje v souvislosti s jednáním o vzniku, změně či zániku pracovněprávního vztahu, tedy při uzavírání pracovní smlouvy, (případně dohody o provedení práce nebo dohody o pracovní činnosti), při jednání o změně obsahu těchto smluv nebo při skončení pracovního poměru dohodou, to ovšem za předpokladu, že k jednání dochází z iniciativy subjektu údajů, tedy zaměstnance nebo budoucího zaměstnance. Dále se uvedená výjimka vztahuje na zpracování osobních údajů, které je nutné pro plnění již uzavřené smlouvy, např. při plnění povinnosti zaměstnavatele vyplácet zaměstnanci sjednanou mzdu, kdy je logicky nezbytné určitá osobní data zpracovat.

Tam, kde subjekt údajů dobrovolně vstupuje do smluvního vztahu nebo určité jednání sám vyvolává, by byl požadavek na formální vyjádření souhlasu se zpracováním osobních údajů nezbytných k provedení požadovaného úkonu či služby neúčelný, neboť tento souhlas je již zahrnut v jednání subjektu údajů. Podstatné je omezit shromažďování osobních údajů k tomuto účelu na data skutečně nezbytná k jeho dosažení.

Naprostá většina operací prováděných zaměstnavateli s osobními údaji jejich zaměstnanců bude spadat pod výjimku uvedenou v § 5 odst. 2 písm. a) ZOOÚ.⁹⁵ Citované ustanovení umožňuje správci zpracovávat osobní údaje bez souhlasu subjektů údajů, pokud tímto zpracováním plní své povinnosti vyplývající, přímo či nepřímo, z určitého právního předpisu. Typickým příkladem, kdy je tato výjimka aplikována, je právě zpracování osobních údajů zaměstnanců zaměstnavatelem při plnění jeho povinností stanovených předpisy v oblasti sociálního zabezpečení, nemocenského a důchodového pojištění, daní, účetnictví apod.

Vyžadovat po zaměstnanci souhlas se zpracováním osobních údajů v situaci, kdy účelem předmětného zpracování je plnění povinností zaměstnavatele, je nadbytečné a pro zaměstnance může být pouze matoucí.⁹⁶

Třetí výjimkou z povinnosti zpracovávat osobní údaje zásadně se souhlasem subjektu údajů, která je v pracovněprávních vztazích relevantní, je výjimka podle § 5 odst. 2 písm. e) ZOOÚ, tedy zpracování osobních údajů za účelem ochrany práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Možnost dovolávat se této výjimky je však

⁹⁵ Toto ustanovení bylo zákonem č. 439/2004 Sb. upřesněno, aby nadále neumožňovalo výklad, že je lze aplikovat i na plnění smluvních povinností, a také více odpovídalo znění článku 7 písm. c) Směrnice 95/46.

⁹⁶ Např. začlenění blíže nespecifikovaného souhlasu se zpracováním osobních údajů do pracovní smlouvy na základě § 29 odst. 2 zákoníku práce, který zaměstnavatel považuje pouze za pojistku, ale u zaměstnance může vyvolat nejistotu, zda a k jakému nadstandardnímu účelu jsou jeho osobní údaje zpracovávány.

současně omezena povinností uvedených subjektů nezasahovat svým jednáním do práva subjektu údajů na ochranu jeho soukromého a osobního života.⁹⁷

Uvedené ustanovení tak umožňuje správcům osobních údajů domoci se svých práv prostřednictvím využití nezbytných osobních údajů, současně však zakotvuje určitou vyváženost mezi oprávněnými zájmy správce a subjektu údajů tím, že zakazuje zásah do ústavně zaručeného práva na ochranu soukromí.

Zaměstnavatelé mohou v souladu s touto výjimkou zpracovávat osobní údaje svých zaměstnanců, případně i bývalých zaměstnanců, např. v souvislosti s vymáháním nároků vyplývajících z odpovědnosti zaměstnance za škodu nebo v souvislosti s uplatněním neplatnosti rozvázání pracovního poměru u soudu. Avšak např. uchovávání všech údajů shromážděných v souvislosti s pracovněprávním vztahem i po jeho ukončení s odůvodněním, že v budoucnu může vyvstat potřeba jejich uplatnění k ochraně práv zaměstnavatele je postupem, který rozhodně pod výjimku podle § 5 odst. 2 písm. e) ZOOÚ zahrnout nelze a který je naopak možné kvalifikovat jako správní delikt podle tohoto zákona.

Pro zaměstnavatele – orgány státní správy, je dále relevantní ustanovení v § 5 odst. 2 písm. f) ZOOÚ, které upravuje výjimku z povinnosti disponovat souhlasem se zpracováním osobních údajů při poskytování osobních údajů o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy vypovídajících o jeho veřejné nebo úřední činnosti.

Uvedené ustanovení je zcela novým prvkem a bylo do zákona č. 439/2004 Sb., tj. novely ZOOÚ, vloženo až v průběhu legislativního procesu v Poslanecké sněmovně Parlamentu ČR, a to zřejmě ve snaze provázat ZOOÚ se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím.⁹⁸

Aplikačně problematické je již vymezení osob, jejichž údaje mohou být v souladu s uvedeným ustanovením zveřejněny, zejména pojem veřejně činná osoba je pojmem velice širokým, pod který lze zahrnout jak politiky, tak i populární osobnosti.⁹⁹ Obdobně nejasné jsou pojmy veřejná či úřední činnost, které lze vykládat poměrně extenzivně. Úmyslem zákonodárce však zřejmě bylo umožnit zveřejnění určitých informací o osobách, jejichž činnost je hrazena z veřejných prostředků, kdy má veřejnost právo se se způsobem využití těchto zdrojů seznámit.

V současné době není také zcela zřejmé, které údaje je možné v souladu s § 5 odst. 2 písm. f) ZOOÚ zveřejnit a naopak které informace již pod tuto výjimku nespádají.

⁹⁷ Zákonem č. 439/2004 Sb. došlo k rozšíření okruhu subjektů, které se mohou aplikace této výjimky dovolávat o příjemce a jiné dotčené osoby, což lze považovat za určité oslabení postavení subjektu údajů. Současně byla doplněna uvedená podmínka nezasahovat zpracováním údajů do práva subjektu údajů na ochranu soukromého a osobního života. Obě uvedené úpravy vycházely ze znění článku 7 písm. f) Směrnice 95/46, přičemž zejména absence určitého omezení správců byla při hodnocení úrovně ochrany osobních údajů v ČR kritizována (viz Důvodová zpráva k návrhu zákona č. 439/2004 Sb., zvláštní část, komentář k bodu 21).

⁹⁸ Zákon č. 106/1999 Sb. se však obecně (podle § 2 odst. 3) na přístup k osobním údajům nevztahuje, ustanovení § 5 odst. 2 písm. f) ZOOÚ tak de facto zákon č. 106/1999 Sb. nepřímou novelizuje.

⁹⁹ Mates, P., Bartík, V. Nová úprava osobních údajů. Právní rádce, 2004, č. 9, s. 43.

Jednoznačné stanovisko bude možné zaujmout až po delší aplikaci uvedeného ustanovení. Zřejmě však není možné zpracovávat v souladu s citovaným ustanovením např. údaje o konkrétním platovém ohodnocení jednotlivých zaměstnanců – úředníků, informace o výši osobního ohodnocení anebo o rodinných či majetkových poměrech zaměstnance. Naopak informace o jménu, funkci či pozici, pracovních úkolech, platovém zařazení (tj. obecně o zařazení do určité platové třídy) veřejně činných osob je na základě citované výjimky možno zveřejnit i bez jejich souhlasu s takovým postupem. V souladu s § 5 odst. 2 písm. f) ZOOÚ mohou být zpracovány pouze takové údaje, které mají skutečně vztah k činnosti zaměstnance, kterou lze označit za veřejnou či úřední.

Další výjimkou z povinnosti zaměstnavatele nakládat s osobními údaji pouze se souhlasem subjektu údajů upravenou v § 5 odst. 2 písm. c) ZOOÚ, jejíž uplatnění lze při zpracování osobních údajů v rámci pracovněprávních vztahů předpokládat, je postup správce směřující k ochraně životně důležitých zájmů subjektu údajů.

V tomto případě se však fakticky nejedná o zpracování osobních údajů bez souhlasu subjektu údajů, povinnost získat souhlas je vzhledem k určité krizové situaci pouze odložena na dobu, kdy je její splnění možné. Citované ustanovení totiž ve větě druhé a třetí stanoví správci povinnost získat souhlas se zpracováním osobních údajů bez zbytečného odkladu a v opačném případě údaje zlikvidovat.¹⁰⁰

Konkrétní situace, kdy bude třeba využít osobní údaje zaměstnance (původně shromážděné zejména za účelem plnění povinností zaměstnavatele) k ochraně jeho životně důležitých zájmů mohou být velmi různorodé, obvykle se bude zřejmě jednat o vážné pracovní úrazy apod. Posouzení, kdy se jedná o životně důležitý zájem subjektu údajů, je vždy na konkrétním správci, nicméně by nemělo v praxi činit zásadní potíže.

Zbýlé výjimky, podle § 5 odst. 2 písm. d) a g) ZOOÚ, se v souvislosti se zpracováním osobních údajů zaměstnanců zaměstnavatelem pravděpodobně příliš neuplatní.

První z citovaných ustanovení se vztahuje na oprávněně zveřejněné údaje. ZOOÚ zde vychází z předpokladu, že jsou-li osobní údaje již jednou oprávněně, tzn. v souladu s právním řádem České republiky,¹⁰¹ zveřejněny, subjekt údajů je s jejich případným dalším zpracováním srozuměn a tedy není třeba znovu získávat souhlas s jejich zpracováním. To,

¹⁰⁰ Za účelem dosažení vyšší míry harmonizace se Směrnicí 95/46, kde je obdobná výjimka uvedena v článku 7 písm. d), bylo zákonem č. 439/2004 Sb. do tohoto ustanovení doplněno pouze jedno, nicméně zásadní slovo, a to slovo „životně“, kterým byl zúžen a současně i vyjasněn pojem „důležitý zájem subjektu údajů“, který dříve vyvolával určitý výkladový problém.

¹⁰¹ Podmínky zveřejňování osobních údajů jsou upraveny v řadě různých právních norem, např. v zákoně č. 450/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), nebo v zákoně č. 513/1991 Sb., obchodní zákoník, v souvislosti s vedením obchodního rejstříku. ZOOÚ však odkazuje v poznámce pod čarou k citovanému ustanovení pouze na zákon č. 81/1996 Sb., o periodickém tisku a ostatních informačních prostředcích, který však byl již nahrazen uvedeným zákonem č. 450/2000 Sb. Tento odkaz, i vzhledem k jeho neaktuálnosti (navzdory několika novelám ZOOÚ provedeným již v době po účinnosti zákona č. 450/2000 Sb.) je nutno vykládat pouze jako demonstrativní příklad, neboť oprávněně zveřejnit osobní údaje lze i jiným způsobem než prostřednictvím tisku.

zda údaje, které hodlá zpracovávat, byly zveřejněny skutečně oprávněně, by měl zkoumat správce, jenž hodlá tyto údaje využít.

Ve větě druhé § 5 odst. 2 písm. d) ZOOÚ je zdůrazněno, že zpracováním spadajícím pod tuto výjimku nesmí správce zasáhnout do práva subjektu údajů na ochranu soukromého a osobního života. Situace v České republice, kdy stále existují veřejné seznamy obsahující rozsáhlé množství osobních údajů (zejména obchodní rejstřík a katastr nemovitostí), svádí některé správce osobních údajů ke shromažďování a spojování údajů z těchto veřejně přístupných zdrojů. Takovým propojením údajů však může správce získat informace již zcela odlišné kvality, na jejichž zpracování nelze uvedenou výjimku aplikovat.

Zpracování osobních údajů zaměstnanců s uplatněním posledně zmíněné výjimky zřejmě nebude v praxi obvyklé, nicméně možnost získání osobních údajů zaměstnanců z veřejně přístupných zdrojů existuje i zde. Případné využití takto získaných osobních údajů musí zaměstnavatel řádně zvážit, neboť riziko neoprávněného zásahu do soukromí je v těchto případech poměrně vysoké (zaměstnavatel musí mít pro takové zpracování osobních údajů legální a zejména legitimní důvod, tj. účel zpracování).

Aby bylo možné označit určitý právní úkon subjektu údajů za souhlas se zpracováním osobních údajů, musí být ze strany správce osobních údajů provázen určitými informacemi vztahujícími se k zamýšlenému zpracování údajů (mluví se o tzv. „informovaném souhlasu“). Obsah této informační povinnosti správce je vymezen v § 5 odst. 4 ZOOÚ, kde je stanoveno, že při udělení souhlasu musí být subjekt údajů informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.¹⁰² Zjednodušeně řečeno se musí subjektu údajů dostat informace o tom proč, co, kdo a jak dlouho bude zpracovávat.

Za souhlas podle ZOOÚ lze tedy považovat pouze takový právní úkon subjektu údajů, kterému ze strany správce osobních údajů předchází uvedené informace. V opačném případě, tedy pokud subjekt údajů není ve stanoveném rozsahu poučen, se fakticky jedná o zpracování osobních údajů bez souhlasu, tedy zpracování v rozporu se ZOOÚ.

Smyslem ustanovení § 5 odst. 4 ZOOÚ je, aby se každému subjektu údajů, který je žádán o poskytnutí souhlasu se zpracováním svých osobních údajů, dostalo informací nezbytných k tomu, aby mohl tento úkon skutečně učinit svobodně a vážně, tak jak předpokládá § 37 odst. 1 občanského zákoníku. Uvedené informace musí vykazovat dostatečnou míru určitosti, kdy např. vymezení účelu zpracování jako „obchodní aktivity“ či

¹⁰² Není třeba vždy zvlášť vyjmenovat veškeré tyto kategorie, zejména výčet osobních údajů a osoba správce obvykle dostatečně vyplývají z předložené smlouvy či formuláře. Častějším nedostatkem bývá opomenutí informace o účelu zpracování a o době, na kterou je souhlas poskytován.

„výzkum“ informaci v nezbytné kvalitě neposkytuje, obdobně není možné dobu zpracování vymezit pouze jako „dobu neurčitou“.¹⁰³

Ačkoli konkrétní formu či podobu souhlasu se zpracováním osobních údajů ZOOÚ nepředepisuje, jeví se jako nejvhodnější písemná podoba souhlasu, neboť podle věty druhé § 5 odst. 4 ZOOÚ musí být správce osobních údajů schopen souhlas prokázat po celou dobu, po kterou osobní údaje zpracovává. Obvykle bývá souhlas se zpracováním osobních údajů inkorporován přímo do smlouvy, kterou subjekt údajů se správcem uzavírá, nebo je součástí všeobecných obchodních podmínek, k nimž subjekt údajů přistupuje.¹⁰⁴ Souhlas je nicméně možné zaznamenat i pomocí různých technických prostředků, např. nahrávkou rozhovoru (což je však běžné pouze v oblasti tzv. telemarketingu).

Pro zpracování citlivých osobních údajů, tj. údajů ve smyslu § 4 písm. b) ZOOÚ,¹⁰⁵ platí tentýž princip jako při zpracování „obyčejných“ osobních údajů: jejich zpracování je až na specifikované výjimky možné zásadně na základě souhlasu subjektu údajů.

Tato zásada je zakotvena v § 9 písm. a) ZOOÚ, jehož obsahem je povinnost správce zpracovávat citlivé osobní údaje jen pokud k tomu dal subjekt údajů výslovný souhlas a současně za podmínky splnění informační povinnosti, která je identická s výše uvedenou povinností podle § 5 odst. 4 ZOOÚ. Na rozdíl od obecného souhlasu se zpracováním osobních údajů má souhlas podle § 9 písm. a) ZOOÚ kvalifikovanou podobu, tj. musí se jednat o „výslovný“ souhlas. Tuto charakteristiku souhlasu je třeba vztáhnout k zvláštní povaze citlivých osobních údajů, subjekt údajů se tedy musí výslovně vyjádřit v tom smyslu, že poskytuje souhlas se zpracováním právě citlivých osobních údajů.

Obdobně i tento souhlas musí být správce schopen prokázat po celou dobu zpracování citlivých údajů, proto se opět jako nejvhodnější jeví písemná forma tohoto úkonu.

Výjimky z povinnosti zpracovávat citlivé údaje pouze na základě souhlasu subjektu údajů jsou upraveny v § 9 písm. b) až ch) ZOOÚ, jejichž znění je následující:

- b) je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů;

¹⁰³ Informační povinnost správce je také obsahem § 11 ZOOÚ, kde je vymezen rozsah informací, které musí subjekt údajů obdržet při shromažďování osobních údajů, a to i v případě, že jde o zpracování na základě zákonného zmocnění – viz níže.

¹⁰⁴ Podmínkou platnosti právního úkonu, jímž subjekt údajů souhlasí se zpracováním osobních údajů přímo podpisem určité smlouvy je zejména to, aby text poučení nebyl uveden příliš drobným písmem nebo až pod podpisem subjektu údajů. V případě, kdy je souhlas udělen přistoupením ke všeobecným obchodním podmínkám, musí mít subjekt údajů reálnou možnost se s jejich zněním předem seznámit.

¹⁰⁵ Tedy údajů vypovídajících o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů nebo biometrických a genetických údajů subjektu údajů.

- c) jedná se o zpracování při zajišťování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem;
- d) je zpracování nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem;
- e) jde o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti občanského sdružení, nadace nebo jiné právnické osoby nevýdělečné povahy (dále jen „sdružení“), a které se týká pouze členů sdružení nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů;
- f) jedná se o údaje podle zvláštního zákona nezbytné pro provádění nemocenského pojištění, důchodového pojištění (zabezpečení), státní sociální podpory a dalších státních sociálních dávek, sociální péče a sociálně-právní ochrany dětí, a při zajištění ochrany těchto údajů v souladu se zákonem;
- g) zpracování se týká osobních údajů zveřejněných subjektem údajů;
- h) zpracování je nezbytné pro zajištění a uplatnění právních nároků nebo
- ch) jsou zpracovány výlučně pro účely archivnictví podle zvláštního zákona.

Z pohledu zaměstnavatele zpracovávajícího osobních údaje svých zaměstnanců má největší význam ustanovení § 9 písm. d) ZOOÚ, na jehož základě je z povinnosti zpracovávat citlivé osobní údaje pouze s výslovným souhlasem subjektů údajů vyňato zpracování citlivých osobních údajů zaměstnanců v rozsahu nezbytném pro dodržení povinností zaměstnavatele stanovených zvláštními zákony. Těmito předpisy se dle odkazu v citovaném ustanovení rozumí především zákoník práce, zákon č. 1/1992 Sb., o mzdě, odměně za pracovní pohotovost a o průměrné výdělku, nebo zákon č. 435/2004 Sb., o zaměstnanosti. Nejčastěji budou zaměstnavatelé v režimu podle citovaného ustanovení zřejmě zpracovávat informace o zdravotním stavu zaměstnanců, např. v souvislosti s pracovními úrazy nebo těhotenstvím zaměstnankyň, anebo o odsouzení zaměstnance či uchazeče o zaměstnání za trestný čin, pokud je tento údaj rozhodujícím požadavkem pro výkon daného zaměstnání.

Jinou situací, která se může v pracovněprávních vztazích vyskytnout a na kterou se vztahuje výjimka podle § 9 písm. h) ZOOÚ, je potřeba zaměstnavatele nakládat s citlivými osobními údaji zaměstnance za účelem zajištění či uplatnění svých nároků, kdy např. v rámci soudního sporu ve věci nároků zaměstnance vyplývajících z odpovědnosti zaměstnavatele

za škodu při pracovních úrazech nebo nemocech z povolání, je pro zaměstnavatele nezbytné, aby mohl disponovat s údaji o zdravotním stavu zaměstnance.

Uplatnění v praxi může najít také zpracování citlivých osobních údajů nezbytné v zájmu záchrany života nebo zdraví zaměstnance či jiné osoby, případně k odvrácení závažného nebezpečí, předpokládané v § 9 písm. b) ZOOÚ. V uvedených situacích bude opět přicházet v úvahu zpracování zejména údajů týkajících se zdravotního stavu zaměstnanců nebo jiných osob.

Poměrně častým případem zpracování citlivých osobních údajů zaměstnavateli je evidování členství zaměstnanců v odborových organizacích, a to v souvislosti s odváděním členských příspěvků členů těchto organizací na základě dohody o srážkách ze mzdy nebo uplatnění zaplacených příspěvků jako odečitatelné položky od daně z příjmu.¹⁰⁶

Zaměstnavatelé tímto způsobem často zpracovávají citlivý osobní údaj vypovídající o členství určitého zaměstnance v odborech, aniž by si uvědomili, že na takové zpracování nelze aplikovat žádnou z výjimek podle § 9 písm. b) až ch) ZOOÚ, a je tedy nezbytné, aby disponovali výslovným souhlasem dotyčného zaměstnance se zpracováním této informace. Přitom uvedená situace zpracování údaje o členství v odborové organizaci nevyžaduje.

Srážky ze mzdy, případně platu, podle § 121 odst. 1 zákoníku práce a § 12 odst. 1 zákona č. 1/1992 Sb., o mzdě, odměně za pracovní pohotovost a o průměrné výdělku, resp. § 18 odst. 1 zákona č. 143/1992 Sb., o platu a odměně za pracovní pohotovost v rozpočtových a v některých dalších organizacích a orgánech, může zaměstnavatel provést pouze na základě dohody o srážkách ze mzdy (platu). Citovaná ustanovení však nevymezují obsah této dohody, postačí tedy, pokud zde budou jednoznačně identifikovány strany a vyjádřen požadavek zaměstnance na provádění srážek v přesné výši a jejich odvádění na určitý účet. Důvod požadavku zaměstnance na provádění srážek ze mzdy nemusí být zaměstnavateli vůbec znám a ten bude za účelem plnění svých smluvních závazků, tedy v souladu s § 5 odst. 2 písm. b) ZOOÚ, zpracovávat pouze osobní údaj o existenci dohody o srážkách ze mzdy, neboť z výše srážky a čísla účtu nemusí zaměstnavateli informace o členství zaměstnance v odborech vyplývat.

Zpracování osobních údajů (ať již „obyčejných“ nebo citlivých) bez souhlasu zaměstnance s tím, že se na takové zpracování vztahuje některá z výjimek uvedených v § 5 odst. 2 nebo § 9 ZOOÚ, je třeba vždy důkladně zvážit. Vzhledem k tomu, že se jedná o výjimky ze základní zásady ochrany osobních údajů, je nezbytná jejich důsledná aplikace pouze na zde vymezené situace, přičemž v pochybnostech je nutno užít spíše restriktivní výklad než extenzivní.

¹⁰⁶ K těmto otázkám vydal Úřad pro ochranu osobních údajů stanovisko č. 2/2001 - zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací, a stanovisko č. 5/2004 - uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky od daně z příjmu (www.uouu.cz).

Ačkoli ZOOÚ vyžaduje svobodný souhlas se zpracováním osobních údajů, který je podmíněný zejména dostatečnou informovaností subjektu údajů, v praxi je tato svoboda často pouze deklaratorní, neboť subjekt údajů je postaven do situace, kdy buď poskytne osobní údaje v požadovaném rozsahu, nebo nezíská to, oč usiluje, případně se vystaví hrozbě určitých následků. Typickým příkladem je uchazeč o zaměstnání, který ve snaze získat zaměstnání obvykle neodmítne poskytnout souhlas se zpracováním jakýchkoli osobních údajů, včetně např. úmyslu založit v blízké době rodinu.¹⁰⁷ V obdobné situaci jsou i někteří zaměstnanci, kteří jsou žádáni o souhlas s předáváním svých osobních údajů do zahraničí tzv. mateřské společnosti jejich zaměstnavatele, ačkoli k tomu není důvod a postačilo by předání anonymizovaných statistických údajů (blíže k tomuto tématu viz kapitola 5.1). Vyskytují se i situace, kdy poté, co Úřad pro ochranu osobních údajů začne prošetřovat způsob, jakým zaměstnavatel nakládal s osobními údaji zaměstnanců (např. je neoprávněně zpřístupnil ostatním zaměstnancům tím, že na nástěnce vyvěsil rozpis povinných zdravotních prohlídek včetně rodných čísel a údaje příslušnosti zaměstnanců ke konkrétní zdravotní pojišťovně), získá zaměstnavatel dodatečně prohlášení zaměstnanců, že s předmětným postupem byli srozuměni a že s ním souhlasili.

Využití institutu souhlasu se zpracováním osobních údajů v pracovněprávních vztazích, kde má zaměstnavatel zjevně silnější postavení, by se tedy mělo omezit zásadně na situace, kdy je zaměstnanci dána skutečně svobodná volba s postupem zaměstnavatele nesouhlasit a možnost následně svůj souhlas odvolat, a to bez jakýchkoli následků.¹⁰⁸

Je také třeba upozornit na to, že sám fakt, že správce zpracovává osobní údaje se souhlasem subjektů údajů, jej nezbavuje ostatních povinností stanovených ZOOÚ, jak se mnozí správci mylně domnívají. Získání souhlasu subjektu údajů je pouze splněním jedné, ač zásadní, povinnosti správce, ten je však dále povinen např. zpracovávat osobní údaje v souladu se stanoveným účelem a pouze v rozsahu pro naplnění tohoto účelu nezbytném. V některých případech tak ani souhlas subjektu údajů nemůže zhojit zjevnou nadbytečnost shromážděných údajů ve vztahu k stanovenému či deklarovanému účelu zpracování nebo zjevné zneužití údajů k jinému účelu. Postup správce osobních údajů lze v takovém případě hodnotit jako porušení ZOOÚ.

¹⁰⁷ V současné době upravuje tuto problematiku také § 12 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti, podle něhož zaměstnavatel obecně nesmí při výběru zaměstnanců vyžadovat informace, které odpovídají definici citlivého osobního údaje podle § 4 písm. b) ZOOÚ, dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele podle zvláštních právních předpisů. Na žádost uchazeče o zaměstnání je zaměstnavatel dále povinen prokázat potřebnost požadovaného osobního údaje.

¹⁰⁸ Tento názor vyjádřila Pracovní skupina 29 ve svém stanovisku č. 8/2001 ke zpracování osobních údajů v pracovněprávních vztazích (Opinion 8/2001 on the processing of personal data in the employment context, www.europa.eu.int). Toto stanovisko je (v anglickém jazyce) uvedeno v Příloze III.

Ustanovení § 16 ZOOÚ upravuje další povinnost zaměstnavatele v pozici správce osobních údajů, kterou musí splnit ještě před zahájením samotného zpracování. Jedná se o oznamovací povinnost vůči Úřadu pro ochranu osobních údajů.

Tato povinnost se však opět vztahuje pouze na ty správce, kteří zjednodušeně řečeno osobní údaje nezpracovávají na základě zvláštního zákona, ale ze svého rozhodnutí (výjimky z oznamovací povinnosti jsou upraveny v § 18 ZOOÚ). Postup některých subjektů, včetně zaměstnavatelů, kteří žádají Úřad pro ochranu osobních údajů o registraci zpracování osobních údajů, které je jejich právní povinností, je nesprávný a Úřad takové žádosti odmítá.¹⁰⁹

Smyslem této povinnosti správce osobních údajů je, aby prezentoval svůj úmysl zpracovávat osobní údaje ještě před samotným zahájením předmětného zpracování a aby Úřad mohl v souladu s § 17 ZOOÚ v případě pochybností, zda při oznámeném zpracování nebude docházet k porušení ZOOÚ, zasáhnout ještě předtím, než k samotnému zpracování fakticky dojde, a tím případně zabránit neoprávněnému zásahu do soukromí osob. V případě, kdy Úřad pro ochranu osobních údajů získá z podaného oznámení pochybnosti o zákonnosti zamýšleného zpracování, zahájí s dotyčným subjektem správní řízení, jehož vyústěním může být i rozhodnutí, kterým se konkrétní zpracování osobních údajů nepovolí. Pokud z oznámení podle § 16 ZOOÚ žádné obdobné podezření nevyplývá (a tedy není zahájeno řízení podle § 17 tohoto zákona), je možné po uplynutí lhůty 30 dní zpracování osobních údajů zahájit, přičemž Úřad vydá správci o provedené registraci osvědčení.¹¹⁰

Dalším cílem oznamovací povinnosti podle § 16 ZOOÚ je zajištění informovanosti veřejnosti o tom, k jakému zpracování osobních údajů u jednotlivých správců dochází. Registr, který Úřad pro ochranu osobních údajů na základě zaregistrovaných oznámení vede, je totiž podle § 35 odst. 2 ZOOÚ veřejně přístupný, a to zejména formou dálkového přístupu (tj. na internetových stránkách Úřadu – www.uoou.cz). Veřejně přístupné nejsou z pochopitelných důvodů pouze informace o konkrétním způsobu zpracování dat a popis bezpečnostních opatření, jejichž zveřejnění by k bezpečnosti osobních údajů příliš nepřispělo.

ZOOÚ dále (v § 16 odst. 2) stanoví náležitosti oznámení o zpracování osobních údajů, přičemž pro splnění oznamovací povinnosti je zřejmě nejvhodnější využít standardizovaný formulář vydaný Úřadem, který je dostupný i prostřednictvím Internetu.

¹⁰⁹ Obzvláště v období těsně po účinnosti ZOOÚ postupovalo značné množství správců osobních údajů tak, že když si nebyli jisti, radši o registraci žádali, což znamenalo, a do jisté míry dosud znamená, pro Úřad značnou administrativní zátěž.

¹¹⁰ Tento dokument však pouze dokládá, že správce splnil povinnost podle § 16 ZOOÚ, a nelze jej považovat za povolení konkrétního zpracování. Na základě informací uvedených v oznámení podle § 16 ZOOÚ může Úřad posoudit pouze to, zda je obecný záměr správce v souladu se ZOOÚ, nikoli zda tak zpracování skutečně bude probíhat. V praxi se však stává, že správci, kterým je vytýkáno porušení ZOOÚ argumentují (ať již během kontroly nebo následujícího správního řízení) tím, že jim Úřad zpracování povolil, a tedy nemohou být za porušení ZOOÚ sankcionováni.

Jednotlivé informace, které musí oznámení o zpracování osobních údajů obsahovat, mohou budoucímu správci také usnadnit splnění jeho povinností ve fázi před zahájením zpracování, neboť obsah oznámení stanovený v § 16 odst. 2 ZOOÚ vyžaduje, aby správce specifikoval účel zpracování, kategorie subjektů údajů a osobních údajů, zdroje těchto údajů, zamýšlený způsob zpracování, další příjemce osobních údajů, případné propojení na jiné správce či zpracovatele, bezpečnostní opatření ve smyslu § 13 ZOOÚ a zvažovaná předání osobních údajů do zahraničí. Tímto je správce v podstatě veden k tomu, aby se ještě před zahájením zpracování důkladně seznámil se svými povinnostmi podle ZOOÚ.

Naprostá většina zpracování osobních údajů prováděná zaměstnavateli, tj. zpracování uložená zvláštními zákony, však spadá pod výjimku z oznamovací povinnosti podle § 18 odst. 1 písm. b) ZOOÚ. Registrace Úřadu pro ochranu osobních údajů tak bude zapotřebí pouze tam, kde zaměstnavatel stanoví účel zpracování sám.

Avšak určitou formu oznamovací povinnosti ukládá ZOOÚ i těm správcům, kteří nemusí Úřadu zpracování oznamovat podle § 16 ZOOÚ. Zákonem č. 439/2004 Sb. bylo totiž ustanovení § 18 ZOOÚ rozšířeno o druhý odstavec ukládající správcům osobních údajů, na kterého se vztahuje výjimka podle § 18 odst. 1 písm. b) tohoto zákona, povinnost zajistit zpřístupnění informací o účelu zpracování, kategoriích osobních údajů a subjektů údajů, o příjemcích a o době uchování údajů, a to dálkovým přístupem nebo jinou vhodnou formou. Zákonodárce se tímto ustanovením zjevně snažil kompenzovat to, že zpracování osobních údajů prováděná na základě zákona nejsou v evidenci vedené Úřadem registrována a zavedení této povinnosti zdůvodňuje právem kohokoli získat informace o zpracování prováděném na základě zákona, zejména proto, aby mu bylo umožněno uplatňovat základní práva podle § 12 a 21 ZOOÚ (tedy např. právo přístupu ke svým údajům nebo právo na námitku).¹¹¹ Důsledné plnění této povinnosti v praxi však představuje nejen nepřiměřené zatížení některých správců, ale právě na příkladu zaměstnavatele jako správce osobních údajů je zjevná neefektivnost tohoto ustanovení. Každý zaměstnavatel by totiž podle § 18 odst. 2 ZOOÚ měl vypracovat dokument obsahující uvedené informace (mj. podrobný seznam všech kategorií údajů, které o svých zaměstnancích na základě zvláštních zákonů zpracovává), přičemž ale informační hodnota takového seznamu, byť umístěného např. na internetových stránkách zaměstnavatele, je téměř nulová. Lze ovšem vyjádřit názor, že v praxi tato povinnost důsledně dodržována nebude, a to i proto, že porušení § 18 ZOOÚ není uvedeno v taxativním výčtu skutkových podstat v hlavě VII tohoto zákona, a tak nedodržení této povinnosti nelze hodnotit jako správní delikt a nelze jej sankcionovat.¹¹²

¹¹¹ Důvodová zpráva k návrhu zákona č. 439/2004 Sb., zvláštní část, komentář k bodu 36.

¹¹² V daném případě není imperfektnost této normy pro aplikaci ZOOÚ zvláště závažnou překážkou, ačkoli k úrovni právního řádu ČR samozřejmě nijak nepřispívá. Jak bude uvedeno dále, jsou však obdobně nedostatečná i některá další ustanovení ZOOÚ, kdy je nemožnost uložení sankce za porušení již zásadnějším nedostatkem.

Při shromažďování osobních údajů je zaměstnavatel podle § 11 odst. 1 ZOOÚ povinen subjekty údajů informovat o tom, jakým způsobem bude s jejich osobními údaji nakládáno, tj. v jakém rozsahu a pro jaký účel budou zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být zpřístupněny. To ovšem jen pokud nejsou zaměstnanci tyto informace již známy. Zaměstnavatel musí dále zaměstnance poučit o jeho aktivních právech, jejichž prostřednictvím může sám své osobní údaje chránit, tj. o právu na přístup k osobním údajům, právu na opravu osobních údajů (upravených v § 12 ZOOÚ), právu požadovat vysvětlení způsobu zpracování osobních údajů, v případě, že zaměstnanec získá pochybnosti o zákonnosti postupu zaměstnavatele, a právu požadovat nápravu vadného stavu (tj. právech zakotvených v § 21 ZOOÚ).

Další informace, které je zaměstnavatel v souvislosti se shromažďováním osobních údajů povinen poskytnout, jsou upraveny v § 11 odst. 2 ZOOÚ, podle kterého musí poučit zaměstnance také o tom, zda je povinen požadované údaje poskytnout nebo zda je jejich poskytnutí dobrovolné. V případě, kdy je subjekt údajů podle zvláštního zákona povinen údaje sdělit, musí jej správce poučit také o následcích případného odmítnutí. Významná je zejména povinnost poučit o dobrovolnosti poskytnutí dat, která má sloužit jako prevence před shromažďováním nadbytečných osobních údajů. Je-li subjekt údajů sděleno, že určitou informaci sdělovat nemusí, lze předpokládat, že ji správci osobních údajů poskytne pouze, pokud správce náležitě vysvětlí důvod, který ho k jeho žádosti vedl, případně i výhody, které z poskytnutí dané informace subjektu údajů vyplynou.

Vzhledem k tomu, že zaměstnavatelé zpracováním osobních údajů obvykle plní pouze své právní povinnosti, lze předpokládat, že většina informací uvedených v § 11 odst. 1 ZOOÚ je zaměstnanci známa, resp. má možnost je získat z příslušných zákonů, a informační povinnost tedy do značné míry odpadá. Vždy je však nutné zaměstnance informovat o veškerých postupech, které nemá možnost z právních předpisů zjistit, jako je např. pověření jiného subjektu (v pozici zpracovatele osobních údajů) faktickým provedením zpracování údajů. Obdobně je vždy nezbytné zaměstnance poučit o jeho právech podle § 12 a 21 ZOOÚ a v souladu s § 11 odst. 2 tohoto zákona také o tom, že je povinen požadované údaje sdělit, resp. že zaměstnavatel je oprávněn je na základě zvláštních zákonů k plnění určitého účelu požadovat a dále zpracovávat.

Pokud zaměstnavatel stanovil zpracování osobních údajů vlastním rozhodnutím a zaměstnanec tedy nemá možnost získat informace o tom, jakým způsobem bude s jeho údaji zacházeno z příslušných právních předpisů, informační povinnost podle § 11 ZOOÚ se na zaměstnavatele vztahuje v plném rozsahu a obvykle nebude možné odkazovat na to, že uvedené informace jsou zaměstnanci již známy. Poučení o tom, že poskytnutí osobních údajů pro tento účel je dobrovolné a z odmítnutí nemohou zaměstnanci vyplynout žádné následky, je přitom podstatně významnější než poučení o povinnosti zaměstnance údaje

poskytnout podle zvláštních zákonů, neboť zaměstnanec obvykle žádost zaměstnavatele z obavy před možnými následky neodmítne, není-li zaměstnavatelem ujištěn o dobrovolnosti a případných výhodách souhlasu se zpracováním předmětných údajů (např. zpracování osobních údajů zaměstnanců a jejich rodinných příslušníků v souvislosti s poskytováním nejruznějších zvýhodněných služeb či slev).

Otázku formy, kterou mají být uvedené informace zaměstnanci prezentovány, ZOOÚ neřeší, nicméně je vhodné, a to zejména v případě zpracování stanoveného zaměstnavatelem, zvolit formu, která umožní případné pozdější prokázání splnění uvedené povinnosti, tedy zřejmě písemnou formu.

4.2. Povinnosti zaměstnavatele v průběhu zpracování osobních údajů

Během zpracování osobních údajů vyplývá jejich správci ze ZOOÚ celá řada povinností. Otázku, od kterého okamžiku se na něj tyto povinnosti vztahují, tedy kterým okamžikem vlastně začíná správce osobních údajů se zpracováním, lze zřejmě nejlépe zodpovědět tak, že ve chvíli, kdy k danému účelu získá osobní údaje v požadovaném rozsahu od prvního subjektu údajů.¹¹³

Všechny povinnosti, které ZOOÚ správci osobních údajů v průběhu zpracování dat ukládá, se aplikují v podstatě současně a pořadí, v jakém budou popsány, je tedy nepředmětné, nicméně zřejmě nejpréhlednějším způsobem je výklad v pořadí, v jakém jsou postupně uvedeny v § 5, § 6, § 10 a § 13 ZOOÚ.

V pořadí první povinností správce (zaměstnavatele) ve vztahu k osobním údajům subjektů údajů (zaměstnanců) je tedy povinnost podle § 5 odst. 1 písm. c) ZOOÚ zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Současně je zaměstnavatel povinen, je-li to nezbytné, osobní údaje aktualizovat a v případě, kdy zjistí, že jím zpracovávané údaje nejsou přesné, musí bez zbytečného odkladu provést přiměřená opatření, o kterých musí informovat i všechny případné příjemce osobních údajů.¹¹⁴ Přiměřeným opatřením se rozumí zejména blokování předmětných údajů a následná oprava či doplnění, v krajním případě, kdy není náprava možná, přichází v úvahu likvidace údajů.

Zákonný způsob získání osobních údajů v daném případě znamená, že zaměstnavatel postupuje na základě zvláštního zákona, který mu ukládá povinnosti, k jejichž splnění je nezbytné zpracování osobních údajů zaměstnanců, anebo osobní údaje získal na základě souhlasu subjektu údajů. Jiný způsob shromáždění údajů než na základě zákona nebo

¹¹³ Matoušová, M., Hejlik, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 234.

¹¹⁴ Tzv. euronovelou ZOOÚ, zákonem č. 439/2004 Sb., bylo toto ustanovení dotčeno tak, že došlo k zúžení povinnosti správce aktualizovat zpracovávané údaje pouze je-li to nezbytné, zatímco dříve byli správci povinni provádět kontrolu přesnosti i pravdivosti údajů prakticky neustále.

souhlasu je již v rozporu se ZOOÚ. Z citovaného ustanovení tak mj. vyplývá, že by nikdy nemělo dojít ke shromáždění osobních údajů nekalým způsobem.

Vzhledem k tomu, že zdrojem osobních údajů zpracovávaných zaměstnavatelem bude ve většině případů sám subjekt údajů (zaměstnanec) je pravděpodobné, že osobní údaje zaměstnavatelem zpracovávané budou dostatečně přesné i včas aktualizované a plnění této povinnosti tedy nebude přinášet vážnější komplikace. Při zpracování osobních údajů pro plnění zákonem stanovených účelů je subjektu údajů někdy přímo stanovena povinnost změnu údajů oznamovat,¹¹⁵ v jiných případech lze tuto povinnost zakotvit smluvně.

Naopak povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu, zakotvená v § 5 odst. 1 písm. d) ZOOÚ, správcům osobních údajů jistě problémy činí.¹¹⁶

Rozsah osobních údajů potřebných k naplnění zákonem stanovené povinnosti by měl být vymezen buď přímo předmětnou právní normou, nebo prováděcím předpisem, a to alespoň výčtem druhů osobních údajů. Příkladem může být ustanovení § 11 odst. 4 zákona č. 1/1992 Sb., o mzdě, odměně za pracovní pohotovost a o průměrném výdělků, které vymezuje rozsah údajů potřebných pro měsíční vyúčtování mzdy, i když nikoli přímým výčtem. Z citovaného ustanovení vyplývá, že pro splnění uvedené povinnosti, musí zaměstnavatel zpracovat (tj. uvést v písemném dokladu, který zaměstnanci vydává) osobní údaje zaměstnance v rozsahu jméno, příjmení a jednotlivé složky mzdy, případně také srážky ze mzdy. Pro bližší identifikaci zaměstnance je dále možné využít např. interní identifikační číslo. V případě, kdy je zaměstnanci mzda zasílána na bankovní účet připadá v úvahu také uvedení čísla účtu, zejména pro oboustrannou kontrolu, zda je mzda zasílána na správný účet. Jiné osobní údaje, např. adresa trvalého pobytu zaměstnance, však již k uvedenému účelu nezbytné nejsou. Taxativní výčet údajů, jejichž zpracování je nezbytné pro plnění povinnosti zaměstnavatele, je uveden např. v § 38j odst. 2 zákona č. 586/1992 Sb., o daních z příjmů, který stanoví, jaké údaje musí pro daňové účely obsahovat mzdový list zaměstnance. Zpracování jiných než zde uvedených osobních údajů k danému účelu je již v rozporu se ZOOÚ.

Zaměstnavatel by měl vyžadovat pouze takové informace, jejichž zpracování má podklad v dané právní úpravě a které skutečně směřují k naplnění stanovené povinnosti. Pokud by např. shromažďoval jména a rodná čísla rodinných příslušníků zaměstnance, který pro tyto osoby neuplatňuje snížení základu daně, jednalo by se zjevně o nadbytečné osobní údaje. Obdobně by bylo nutno posoudit i případ, kdy by zaměstnavatel od zaměstnance vyžadoval předložení výpisu z rejstříku trestů, ačkoli pro danou pozici není bezúhonnost podstatným

¹¹⁵ Např. § 38k odst. 8 zákona č. 586/1992 Sb., o daních z příjmů.

¹¹⁶ Jedná se o jedno z nejčastěji porušovaných ustanovení ZOOÚ.

požadavkem anebo situací, kdy by zaměstnavatel zpracovával číslo bankovního účtu zaměstnance, jemuž je celá mzda vyplácena v hotovosti.¹¹⁷

Porušení citované povinnosti bývá často následkem určité setrvačnosti v činnosti správců osobních údajů, kteří mají pro některé činnosti již zavedené postupy či formuláře ještě z doby před účinností ZOOÚ. Příkladem může být požadavek na vyplnění kolonky „národnost“ v některých personálních formulářích, přičemž tento údaj je z hlediska potřeb zaměstnavatele zjevně nadbytečný. Jako nedůvodné se dále jeví např. i zpracování údaje o místě pobytu během dovolené, který je vyžadován prostřednictvím standardního formuláře žádosti o dovolenou na zotavenou (tzv. dovolenka). Legitimním účelem zpracování takového údaje je pouze potřeba zaměstnavatele mít v naléhavých situacích možnost kontaktovat daného zaměstnance, což se však zřejmě nebude týkat všech zaměstnanců, ale pouze vedoucích pracovníků nebo zaměstnanců, kteří jsou z nějakého důvodu obtížně zastupitelní. Nicméně v době, kdy jsou zejména tito nepostradatelní zaměstnanci vybaveni mobilním telefonem, se i v jejich případě požadavek sdělení informace o místě pobytu během dovolené jeví jako neopodstatněný.

Stanovení rozsahu údajů nezbytného pro dosažení cíle, který si správce určil sám, je v praxi pro mnohé správce dosti obtížné. Splnění uvedené povinnosti vyžaduje důkladný rozbor toho, na základě jakého minimálního rozsahu údajů lze stanoveného účelu dosáhnout. Tam, kde má správce možnost volit mezi několika údaji, které mají obdobnou vypovídací hodnotu (např. datum narození nebo rodné číslo), měl by zvolit ten údaj, jehož zpracování představuje menší zásah do soukromí dané osoby, případně ten údaj, který v sobě latentně nenese mnohem větší rozsah informací, než je nezbytně nutné (v uvedeném příkladě by tedy bylo správné zpracovávat údaj o datu narození a nikoli rodné číslo).

Rozsah nezbytných údajů se samozřejmě liší podle okolností, jiný bude v případě uchazeče o post vrcholového manažera nebo bezpečnostního technika a jiný u uchazeče o místo kuchaře v podnikové jídelně. U uchazeče o zaměstnání, kde je nezbytný např. častý přesun z jednoho pracoviště na jiné, je adekvátní získat informaci o tom, zda vlastní auto, již však nikoli o jaký typ jde či jakou má barvu. Zaměstnavatel tedy musí jednotlivé situace rozlišovat a rozsah shromažďovaných údajů přizpůsobit situaci, přičemž musí vždy volit ten způsob, který pokud možno co nejméně zasahuje do soukromí dotčené osoby.

Další povinností správce osobních údajů, stanovenou v § 5 odst. 1 písm. e) ZOOÚ, je uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Pokud zpracovává zaměstnavatel osobní údaje pouze za účelem plnění povinností stanovených zvláštními zákony, je obvykle těmito normami vymezena i potřebná doba zpracování. Některé právní předpisy tuto dobu stanoví výslovně, jako např. § 35a odst. 4 zákona

¹¹⁷ V obdobných případech se povinnosti zaměstnavatele stanovené ZOOÚ prolínají s povinnostmi podle zákona č. 435/2004 Sb., o zaměstnanosti, konkrétně s povinností podle § 12 odst. 2 tohoto zákona.

č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, kde se určuje doba, po kterou je zaměstnavatel povinen uchovat mzdové listy zaměstnanců (konkrétně 30 kalendářních roků následujících po roce, kterého se mzdový list týká). Doba zpracování osobních údajů může být však stanovena i ve vztahu k určité rozhodné události, jako je tomu např. u evidenčních listů důchodového pojištění, kdy z § 38 odst. 1 zákona č. 582/1991 Sb. vyplývá zaměstnavateli povinnost zpracovávat údaje potřebné pro vyhotovení evidenčního listu po celou dobu, po kterou pojištění daného zaměstnance trvá.

Zákonem stanovenou dobu musí zaměstnavatel samozřejmě dodržet, přičemž je jeho povinností kontrolovat, zda je zpracování konkrétních osobních údajů stále ještě nezbytné nebo zda již uplynula zákonem určená doba a další zpracování již není v souladu s příslušnou právní normou, a tedy může být v rozporu se ZOOÚ. Uplynutím dané doby zpracování vzniká zaměstnavateli další povinnost, totiž dané údaje zlikvidovat, případně s nimi naložit jiným způsobem, pokud tak zákon stanoví (viz níže).

Situace správce, který údaje zpracovává za účelem, jenž si sám stanovil, je opět mnohem obtížnější, neboť musí minimální dobu potřebnou pro zpracování stanovit s přihlédnutím ke všem okolnostem sám. Tento správce musí pravidelně hodnotit, zda jím zpracovávané údaje jsou ještě stále potřebné, nebo zda již účel zpracování pominul, a to u jednotlivých kategorií údajů zvláště (některé osobní údaje, týkající se téže osoby, je důvodné zpracovávat jen po velmi omezenou dobu, naopak jiné je nezbytné uchovávat velmi dlouho).

Věta druhá § 5 odst. 1 písm. e) ZOOÚ umožňuje zpracování osobních údajů i po uplynutí určené doby, jedná-li se o uchování údajů pro účely státní statistické služby, vědecké účely nebo účely archivnictví. Tohoto ustanovení se ovšem lze dovolávat pouze v případech, kdy je plnění uvedených úkolů danému subjektu stanoveno zákonem (zejména zákonem č. 89/1995 Sb., o státní statistické službě, nebo zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů). Správce osobních údajů tedy nemůže po vypršení stanovené doby zpracování osobní údaje i nadále využívat s tím, že takové zpracování je v souladu s § 5 odst. 1 písm. e) ZOOÚ,¹¹⁸ neboť jeho účelem je vytváření statistických přehledů potřebných např. pro přehled o rozvoji jeho podnikatelských aktivit.

Ustanovení § 5 odst. 1 písm. f) ZOOÚ zakotvuje jednu z velmi důležitých povinností správce osobních údajů,¹¹⁹ povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny.

V případě zaměstnavatele, který zpracovává osobní údaje svých zaměstnanců pouze v rozsahu potřebném k naplnění svých právních povinností, jde jinými slovy o povinnost

¹¹⁸ Zákonem č. 439/2004 Sb. bylo ustanovení § 5 odst. 1 písm. e) ZOOÚ upraveno tak, že původní obecný termín „statistické účely“ byl změněn na „účely státní statistické služby“, což jednoznačně odkazuje na činnost podle zákona č. 89/1995 Sb., o státní statistické službě, a tím vylučuje dříve časté argumenty správců, že se toto ustanovení vztahuje i na jejich vnitřní statistické přehledy či evidence.

¹¹⁹ Současně se jedná o jednu z nejčastěji porušovaných povinností podle ZOOÚ.

využít osobní údaje shromážděné podle daného zvláštního zákona pouze k účelu tímto zákonem stanovenému. V souladu se ZOOÚ tedy nebude např. zveřejnění osobních údajů zaměstnance na internetových stránkách zaměstnavatele v případě, kdy náplní práce tohoto zaměstnance není komunikace s veřejností nebo kdy zveřejněné údaje s pracovní náplní nesouvisí (např. věk, platové poměry nebo soukromé telefonní číslo). Obdobně nezákonné by bylo předání adres jednotlivých zaměstnanců, kterými zaměstnavatel disponuje za účelem plnění svých povinností v oblasti daní či sociálního zabezpečení, jinému subjektu např. za účelem oslovení s nabídkou určitých služeb či obchodu, aniž by k tomu zaměstnavatele opravňoval specifický souhlas zaměstnanců.

Jestliže správce stanovil účel zpracování sám, zde se projeví, jak se s povinností stanovit účel zpracování [podle § 5 odst. 1 písm. a) ZOOÚ] vypořádal. Pouze v případě jednoznačně a srozumitelně vymezeného účelu lze totiž povinnost stanovenou v § 5 odst. 1 písm. f) ZOOÚ řádně plnit. Stanovení příliš obecného nebo i zavádějícího účelu zpracování může být samozřejmě i záměrem správce, který se však při kontrole plnění povinnosti podle § 5 odst. 1 písm. f) ZOOÚ obvykle projeví.

Další povinností zaměstnavatele jako správce osobních údajů, vyjádřenou v § 5 odst. 1 písm. g) ZOOÚ, je shromažďovat osobní údaje pouze otevřeně. V citovaném ustanovení je současně upřesněno, že v rozporu s tímto ustanovením je shromažďování osobních údajů pod záminkou jiného účelu nebo jiné činnosti. V pracovněprávních vztazích by citovaná povinnost neměla činit problémy. Riziko porušení této povinnosti existuje zejména v oblasti marketingu, kdy se podnikatelé často snaží získat o svých, případně potenciálních, klientech takové informace, aby mohli svoji nabídku co nejvíce přizpůsobit určité cílové skupině, přičemž mohou inklinovat k získání těchto údajů skrytou formou např. při příležitosti spotřebitelské soutěže.

Zaměstnavatel ze zákona disponuje veškerými osobními údaji zaměstnanců, které potřebuje pro plnění svých povinností, o čemž by zaměstnanci měli mít dostatečné povědomí. Pokus získat další informace o zaměstnanci na základě nějakých zástupných důvodů tedy zřejmě nebude v praxi příliš reálný. Lze si však představit např. požadavek písemně vypracovaného životopisu uchazeče o zaměstnání s tím, že uchazeči není předem znám záměr využít tento dokument k vyhotovení grafologického posudku (tj. shromáždění jeho osobních údajů vypovídajících např. i o zdravotním stavu)¹²⁰ anebo získání otisku prstu zaměstnance za účelem vstupu na pracoviště s tím, že je bez jeho vědomí použit nikoli pouze k verifikaci při vstupu, ale je zařazen do databáze a dochází vždy k identifikaci zaměstnance, a tím je umožněno případné sledování jeho pohybu na pracovišti.

¹²⁰ Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003, s. 250.

Posledním ustanovením § 5 odst. 1 ZOOÚ je písm. h), kde je zakotvena povinnost nesdružovat osobní údaje, které byly získány k rozdílným účelům.

Zakotvení této povinnosti může být považováno za nadbytečné, neboť při dodržení ostatních výše uvedených povinností, zejména povinnosti zpracovávat osobní údaje pouze k účelu, k němuž byly shromážděny, by k porušení citovaného ustanovení dojít nemělo. Na druhou stranu tato norma nepůsobí žádné výkladové ani aplikační problémy a naopak může přispět k upřesnění záměru ZOOÚ a k pochopení principů ochrany osobních údajů.

Je logické, že sdružením evidencí vedených k rozdílným účelům může správce osobních údajů získat kvalitativně zcela odlišné informace, než jakými by disponoval, pokud by soubory dat nepropojil. Ačkoli toto riziko hrozí zejména při zpracování osobních údajů subjekty veřejné správy, které obvykle disponují velmi rozsáhlými soubory osobních údajů, jejichž propojení by znamenalo citelný zásah do soukromí dotčených osob, je nezbytné, aby i správci osobních údajů působící v soukromoprávní sféře dbali na to, že údaje jimi zpracovávané k určitému účelu nejsou, byť neúmyslně, sdružovány s údaji shromažďovanými pro jiný účel. Pro zajištění plnění této povinnosti je zejména vhodné spravovat osobní údaje pod patřičným označením, tak aby bylo zřejmé, že v daném souboru jsou shromažďovány údaje k určitému účelu (např. „evidence pracovní doby“).

Pokud se správce osobních údajů rozhodne, že provedením části anebo i všech operací spojených s konkrétním zpracováním osobních údajů pověří jiný subjekt, je podle § 6 ZOOÚ povinen uzavřít smlouvu o zpracování osobních údajů. Citované ustanovení ZOOÚ stanoví i náležitosti, které smlouva o zpracování osobních údajů musí obsahovat. Zejména zde musí být výslovně uvedeno, na jaký rozsah osobních údajů a na jaký účel zpracování se daná smlouva vztahuje a na jakou dobu se uzavírá. Smlouva o zpracování osobních údajů musí dále obsahovat i záruky zpracovatele ohledně technického a organizačního zabezpečení ochrany osobních údajů.

Pověřit zpracováním osobních údajů zpracovatele je právem každého správce a zejména v případech zpracování velkého množství údajů nebo zpracování vyžadujícího odborné znalosti je pro mnoho správců výhodné převést úkoly s tím spojené na jiný subjekt – zpracovatele. ZOOÚ neomezuje počet zpracovatelů, kteří mohou být do procesu zpracování zapojeni, správce má tak poměrně široké možnosti jak svoji činnost uspořádat. Jedinou podmínkou, kterou ZOOÚ stanoví, je právě povinnost uzavřít s každým zpracovatelem smlouvu podle § 6 tohoto zákona. Tato povinnost směřuje k tomu, aby správce ještě předtím, než zpracovatel zahájí svoji činnost, jednoznačně specifikoval podmínky, kterými se zpracovatel musí při zpracování údajů řídit, a tak minimalizoval riziko zásahu do soukromí osob, jejichž osobních údajů se bude dané zpracování týkat. Tím, kdo za celý proces zpracování osobních údajů po celou dobu primárně odpovídá, je však vždy správce osobních údajů, a to i v případě, kdy zpracovatele pověřil výkonem všech operací se

zpracováním osobních údajů spojených. Tato odpovědnost správce vyplývá z faktu, že je to on, kdo účel zpracování stanovil a kdo stanovil prostředky a způsob, jakým má být zpracování provedeno.¹²¹

Nedodržení povinnosti podle § 6 ZOOÚ však nelze od účinnosti zákona č. 439/2004 Sb. sankcionovat. Touto novelou byla v ZOOÚ mj. zohledněna nová koncepce správního trestání a hlavě VII ZOOÚ byly proto vyjmenovány jednotlivé skutkové podstaty správních deliktů, v jejichž výčtu však porušení ustanovení § 6 ZOOÚ schází. Je nutno konstatovat, že se jedná o poměrně závažný nedostatek ZOOÚ, neboť s rostoucím počtem subjektů zapojených do určitého zpracování osobních údajů roste i riziko nedbalostního i úmyslného zneužití těchto dat, a tedy riziko zásahu do soukromí subjektů údajů. Vymezení vzájemných vztahů a stanovení podmínek činnosti zpracovatele je tak jednou ze základních podmínek ochrany osobních údajů.¹²²

Při zpracování osobních údajů svých zaměstnanců mohou zaměstnavatelé využívat služeb zpracovatelů např. v souvislosti se zajištěním mzdového účetnictví nebo i pro vedení veškeré personální agendy. Tato možnost bude vhodná zejména pro zaměstnavatele, jejichž organizační struktura není natolik rozsáhlá, aby zahrnovala i specializovaná personální či účetní oddělení. Služeb zpracovatele lze využít jak pro zpracování údajů zaměstnanců, kterými musí zaměstnavatel disponovat při plnění svých právních povinností, tak i pro zpracování údajů, u nichž účel zpracování stanovil zaměstnavatel sám.

V této souvislosti je třeba upozornit, že vnitřní organizační složka zaměstnavatele (odbor, oddělení, sekce apod.) či pověřený zaměstnanec zabývající se zpracováním osobních údajů pro zaměstnavatele není zpracovatelem osobních údajů ve smyslu ZOOÚ. Povinnost podle § 6 ZOOÚ se aplikuje pouze v případě pověření jiného subjektu než je správce.

Zvláštní kategorií povinností zaměstnavatele při zpracování osobních údajů je povinnost vyjádřená obecně v § 10 ZOOÚ a v § 5 odst. 3 tohoto zákona adresovaná konkrétně správci, který provádí zpracování na základě zvláštního zákona. V obou případech se jedná o povinnost dbát práva subjektů údajů na ochranu soukromého a osobního života a na zachování lidské důstojnosti. Tato ustanovení jsou do značné míry pouze proklamativní, jen zdůrazňují základní smysl právní úpravy ochrany osobních údajů, tj. provedení ústavně zakotveného práva na ochranu před neoprávněným zásahem do soukromí (čl. 10 Listiny). Citovaná ustanovení lze tedy chápat jako obecná interpretační pravidla ZOOÚ nebo obecné principy ochrany osobních údajů.

¹²¹ Určení účelu a prostředků a odpovědnost za zpracování jsou ostatně definičními znaky správce osobních údajů podle § 4 písm. j) ZOOÚ.

¹²² V praxi lze povinnost uzavřít smlouvu o zpracování osobních údajů zohlednit jako jednu ze složek povinnosti přijmout bezpečnostní opatření podle § 13 ZOOÚ, to ovšem pouze v případě, kdy absence této smlouvy představuje riziko pro bezpečnost osobních údajů. Tam, kde jsou zjištěny pouze formální vady smlouvy, ale zpracování probíhá zcela v souladu se ZOOÚ lze považovat za dostatečné nápravné opatření uložené inspektorem Úřadu.

Zásahem do soukromí subjektů údajů je obvykle zpracování, které přes sledování zákonného účelu, zahrnuje nadbytečné osobní údaje nebo je prováděno nevhodným způsobem. Zaměstnavatel, který by vykonával např. své právo kontrolovat práci zaměstnanců tak, že by je během pracovní doby podrobil permanentní kontrole, by zřejmě porušil právě svoji povinnost zpracovávat osobní údaje tak, aby nezasahoval do soukromého či osobního života zaměstnanců, neboť i na pracovišti během pracovní doby má zaměstnanec právo na zachování určitého soukromí (blíže k této otázce viz kapitola 5.3).

Povinností uvedeným v § 5 odst. 3 a § 10 ZOOÚ však neodpovídá žádná ze skutkových podstat právních deliktů podle § 44 a 45 ZOOÚ. To znamená, že jejich porušení nemůže být sankcionováno, což pouze podtrhuje deklaratorní charakter těchto ustanovení. Z legislativního hlediska se ovšem jedná o nedostatek ZOOÚ, neboť obdobně imperfektní normy k úrovni ZOOÚ a potažmo celého právního řádu ČR příliš nepřispívají.¹²³

Podstatně méně teoretickou povinností zaměstnavatele ve vztahu k ochraně osobních údajů zaměstnanců je povinnost zakotvená v § 13 odst. 1 ZOOÚ. Jedná se o povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování nebo jinému zneužití. Zjednodušeně řečeno lze tuto povinnost vyjádřit jako povinnost přijmout bezpečnostní opatření.

Ustanovení § 13 odst. 1 ZOOÚ ukládá správcům osobních údajů povinnost osobní údaje chránit, jak před jednáním osob, úmyslným i nedbalostním, tak i před událostmi jako je např. požár či povodeň nebo selháním techniky, v jejichž důsledku by mohlo ke zneužití údajů dojít. ZOOÚ tak v citovaném ustanovení pouze stanoví (navíc jen demonstrativně) před čím je nutno osobní údaje chránit, ale již nikoli jakými prostředky. Konkrétní podoba ochrany osobních údajů je tedy ponechána na jednotlivých správcích osobních údajů.¹²⁴

Při hledání základního přístupu pro určení adekvátních bezpečnostních opatření je možno se inspirovat ustanovením č. 46 preambule Směrnice 95/46, kde je vyjádřen požadavek na přijetí odpovídajících technických a organizačních opatření, a to jak při přípravě zpracování osobních údajů, tak i v jeho samotném průběhu, s cílem zajistit bezpečnost dat a zabránit jakémukoli neoprávněnému zpracování. Přijatá opatření přitom musí vykazovat náležitou odbornou úroveň odrážející rizika spojená s konkrétními operacemi s osobními údaji a s povahou zpracovávaných údajů.

¹²³ V daném případě však nevznikají při aplikaci ZOOÚ v praxi závažnější problémy, protože správce, který poruší § 5 odst. 3 nebo § 10 ZOOÚ, tím obvykle poruší i některou z jiných povinností stanovených ZOOÚ. Dojde-li jednáním správce skutečně k zásahu do soukromí dotčených osob, je to možné posoudit jako okolnost zvyšující závažnost jednání správce při zvažování výše sankce za správní delikt.

¹²⁴ Pro srovnání lze uvést, že v ustanovení § 15 a 16 slovenského zákona č. 428/2002 Z. z., o ochrane osobných údajov, jsou jednotlivé oblasti, které musí správce s ohledem na bezpečnost údajů analyzovat, popsány detailněji.

V souvislosti se snahou správců osobních údajů plnit tuto povinnost co nejlépe se Úřad pro ochranu osobních údajů poměrně často setkává s žádostmi, aby stanovil, jaká konkrétní opatření považuje pro splnění povinnosti podle § 13 odst. 1 ZOOÚ za dostatečná. Obdobným žádostem ovšem nemůže Úřad vyhovět, neboť splnění povinnosti stanovené § 13 odst. 1 ZOOÚ závisí na mnoha faktorech, které se u jednotlivých správců osobních údajů velice liší. Opatření, která postačí ve společnosti s deseti zaměstnanci, jejichž údaje jsou uloženy pouze v písemné podobě v kartotéce, neobstojí tam, kde je zaměstnanců deset tisíc, některé jejich údaje jsou dostupné na vnitřní počítačové síti a jsou předávány jiným společnostem, případně i do zahraničí. Opatření zcela jiného charakteru je samozřejmě nutné přijmout pro ty evidence, kde jsou zpracovávány „obyčejné“ údaje a tam, kde jsou o zaměstnancích vedeny i citlivé osobní údaje.

Je tedy zřejmé, že posouzení rizik vyplývajících ze zpracování osobních údajů je otázkou vyhodnocení konkrétní situace daného správce – zaměstnavatele, zejména potom zvolených či stanovených prostředků a způsobů zpracování osobních údajů, druhu a rozsahu těchto údajů atd. Nicméně je možné vymezit určité okruhy, ze kterých lze při plnění povinnosti podle § 13 odst. 1 ZOOÚ vycházet.

Prvním okruhem jsou technická opatření. Jsou-li osobní údaje zpracovávány manuálně, což v současné době znamená zejména uchování nejrůznějších dokumentů např. životopisů zaměstnanců nebo kopií vysvědčení, které sloužily jako zdroj osobních údajů, je nezbytné zajistit, aby kartotéky či skříně, v nichž jsou tyto listiny uloženy, byly uzamykatelné, umístěné na vhodném místě, tedy nikoli ve volně přístupných místnostech apod. V případě zpracování osobních údajů prostřednictvím výpočetní techniky je třeba počítače chránit alespoň vstupním heslem, popř. i jinými přístupovými právy. K tomuto typu opatření patří i náležité zabezpečení prostor a objektů, kde jsou osobní údaje uchovávány, aby k nim nezískaly přístup nepovolané osoby nebo aby nedošlo k jejich odcizení.

Při přijímání těchto opatření se správci osobních údajů mohou případně inspirovat řadou právních předpisů či technických norem, především zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a vyhláškami Národního bezpečnostního úřadu.¹²⁵ Vodítkem může být i příkladný výčet opatření uvedený na formuláři Úřadu pro ochranu osobních údajů „Oznámení o zpracování osobních údajů“, kde jsou uvedena základní bezpečnostní opatření.¹²⁶

Další podstatnou kategorií opatření ve smyslu § 13 odst. 1 ZOOÚ jsou vnitřní organizační opatření, tj. závazné interní normy stanovící odpovědnost konkrétních osob za bezpečnost

¹²⁵ Např. vyhláška Národního bezpečnostního úřadu č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, nebo vyhláška NBÚ č. 526/2005 Sb., o průmyslové bezpečnosti.

¹²⁶ Z hlediska zabezpečení budov a místností se jedná o zámky, mříže apod., centrální pult ochrany, elektronické zabezpečení či bezpečnostní směrnice, v oblasti automatizovaného zpracování potom o přístupová práva, bezpečnostní zálohy, antivirovou ochranu nebo šifrování.

zpracovávaných osobních údajů (např. organizační řád či pracovní řád nebo pracovní náplň zaměstnance). Zvláště u větších společností se osvědčuje vydání zvláštní interní směrnice týkající se přímo ochrany osobních údajů, vymezující konkrétní postupy a oprávnění zaměstnanců a stanovící jejich odpovědnost. Určení podmínek, které jsou jednotliví zaměstnanci, nebo jiné osoby přicházející u zaměstnavatele do styku s osobními údaji, povinni dodržovat, je považováno za jedno ze základních opatření podle § 13 odst. 1 ZOOÚ.

Neméně podstatnou součástí bezpečnostních opatření je důsledná kontrola plnění přijatých opatření a plnění povinností odpovědných osob. Sebelepší technické zabezpečení a organizační uspořádání nelze považovat z hlediska ZOOÚ za dostatečné, nejsou-li tato opatření důsledně v praxi uplatňována a jejich plnění kontrolováno. Výsledky těchto kontrol mohou zaměstnavateli sloužit jako ukazatel efektivity nastavených opatření a mohou ho včas upozornit na situace, které by mohly vyústit v porušení povinností stanovených ZOOÚ. Kontrola plnění bezpečnostních opatření nemusí být nezbytně kontrolou specializovanou na problematiku ochrany osobních údajů, ale může být součástí uplatňování práva, a současně povinnosti, vedoucích zaměstnanců kontrolovat práci zaměstnanců vyjádřená v § 74 písm. a) zákoníku práce.¹²⁷

Zákonem č. 439/2004 Sb., byl do ustanovení § 13 ZOOÚ vložen ještě druhý odstavce ukládající správci osobních údajů povinnost dokumentovat přijatá a provedená opatření k zajištění bezpečnosti osobních údajů, tj. technicko-organizační opatření podle § 13 odst. 1 ZOOÚ. Zákonodárce byl veden snahou minimalizovat rizika spojená se zpracováním osobních údajů tím, že správce osobních údajů bude povinností vypracovat uvedený dokument nucen se více nad hrozícími riziky zamyslet, vyhodnotit je a přijmout odpovídající opatření.¹²⁸ Je však otázkou, zda je toto ustanovení přínosem. Mnohé, zejména menší, správce osobních údajů může tato povinnost zbytečně zatěžovat, přičemž její přínos je minimální. Správci velkých databází naopak obdobné dokumenty obvykle vypracovávají mají, neboť si sami (v souvislosti s plněním požadavků kladených na ně ZOOÚ) uvědomili, že bez stanovení jednoznačných principů není důsledná ochrana osobních údajů možná.¹²⁹ Určitým přínosem je tak tato novelizace pouze z hlediska kontrol prováděných inspektory Úřadu pro ochranu osobních údajů, kterým může značně usnadnit zjištění plnění povinnosti stanovené v § 13 odst. 1 ZOOÚ.

¹²⁷ V případě, kdy dojde v souvislosti se selháním bezpečnostních opatření ke ztrátě či zneužití osobních údajů hodnotí Úřad právě to, jak dotýčný správce vyhodnotil rizika a zda přijatá opatření tato rizika pokrývala. Pokud správce prokáže, že vynaložil veškeré úsilí, které po něm bylo možno požadovat, aby osobní údaje ochránil, lze aplikovat § 46 odst. 1 ZOOÚ a tento správce za delikt, kterého se porušením § 13 odst. 1 ZOOÚ dopustil, neodpovídá a není za něj tedy potrestán.

¹²⁸ Důvodová zpráva k návrhu zákona č. 439/2004 Sb., komentář k bodu 34.

¹²⁹ Opět lze srovnat se slovenským zákonem č. 428/2002 Z. z., o ochrane osobných údajov, který v § 16 ukládá správci za určitých podmínek (nikoli vždy, jak je tomu v ČR podle § 13 odst. 2 ZOOÚ) povinnost vytvořit „bezpečnostný projekt“ (jehož struktura i obsah jsou zákonem definovány) anebo povinnost nezávislého auditu odborným pracovníkem.

Vzhledem ke znění ustanovení § 45 odst. 1 písm. h) ZOOÚ nelze však porušení povinnosti zakotvené v § 13 odst. 2 tohoto zákona považovat za správní delikt, a tedy jej nelze sankcionovat. Podle znění skutkové podstaty správního deliktu uvedené v § 45 odst. 1 písm. h) ZOOÚ je totiž správním deliktem pouze nepřijetí či neprovedení opatření pro zajištění bezpečnosti zpracování osobních údajů. Zpracování dokumentace o těchto opatřeních tak již za správní delikt považováno být nemůže. Kromě toho, že je povinnost podle § 13 odst. 2 ZOOÚ poněkud diskutabilní, je tedy navíc i imperfektní normou.

Z uvedeného je zřejmé, že alfou a omegou ZOOÚ je účel zpracování osobních údajů, neboť splnění uložených povinností je často hodnoceno právě ve vztahu k účelu zpracování. Vymezení účelu zpracování osobních údajů, resp. správné provedení účelu stanoveného zvláštním zákonem, je tedy velmi důležitým krokem správce osobních údajů. Je-li účel vymezen či proveden nevhodně, je i plnění ostatních povinností podle ZOOÚ velmi problematické.

4.3. Povinnosti zaměstnavatele v souvislosti s ukončením zpracování osobních údajů

ZOOÚ stanoví správcům určité povinnosti nejen před a v průběhu zpracování osobních údajů, ale také po ukončení předmětného zpracování.

Jednou z těchto povinností, která je vyjádřena v § 13 odst. 1 větě druhé ZOOÚ, je povinnost správce osobních údajů zabezpečit osobní údaje i po ukončení zpracování. Toto ustanovení ZOOÚ je však poněkud zavádějící. Ukončení zpracování není ZOOÚ zvlášť definováno, z definice zpracování uvedené v § 4 písm. e) je ale zřejmé, že zpracováním osobních údajů se rozumí veškeré operace s nimi, tzn. i jejich uchovávání či likvidace. Po celou dobu, co správce osobní údaje uchovává a následně i během jejich likvidace, tyto údaje tedy stále zpracovává. Zpracování lze v souladu s § 4 písm. e) ZOOÚ považovat za ukončené až po likvidaci osobních údajů, kdy však již logicky není nutno přijímat opatření k zabezpečení údajů. Zákonodárce se zde zřejmě odchýlil od vlastní definice zpracování osobních údajů, neboť pod tímto pojmem ve významu, v jakém je použit v § 13 odst. 1 ZOOÚ, je nutno rozumět aktivní nakládání s osobními údaji, tj. jakési zpracování v užším slova smyslu. Povinností zde stanovenou je tedy zabezpečení údajů, i pokud nejsou právě aktivně využívány a jsou jen uchovávány.

Co se týče konkrétních opatření pro bezpečnost uchovávaných údajů, platí obdobně to, co bylo uvedeno výše k povinnosti správce podle § 13 odst. 1 ZOOÚ. Správce osobních

údajů by měl mít, tam kde postup nevyplývá přímo ze zvláštního zákona,¹³⁰ zavedeny určité standardizované postupy ohledně archivace písemností nebo ukládání a zálohování dat v elektronické podobě.

Z hlediska správce – zaměstnavatele, který údaje zpracovával pouze v souvislosti s plněním svých povinností, tj. nebyl registrován Úřadem pro ochranu osobních údajů, je poslední povinností při ukončení zpracování povinnost likvidace osobních údajů vyjádřená v § 20 ZOOÚ.

Tato povinnost se na správce vztahuje od toho okamžiku, kdy pominul účel jím prováděného zpracování osobních údajů, tj. kdy uplynula doba, po kterou mohl osobní údaje v souladu se zákonem zpracovávat. Zaměstnavateli, který zpracovává osobní údaje pouze v rozsahu svých právních povinností, je příslušnými právními předpisy obvykle stanovena i přesná doba, po kterou je povinen osobní údaje shromážděné k danému účelu uchovávat (viz výše). Pokud správci tato doba stanovena není nebo se jedná o správce, který určil účel zpracování osobních údajů vlastním rozhodnutím, musí správce sám vyhodnotit všechny relevantní okolnosti a příslušnou dobu zpracování dovést či vymežit sám.

Poté co pomine účel zpracování osobních údajů je tedy správce povinen osobní údaje zlikvidovat, čímž mj. přestává být správcem osobních údajů podle ZOOÚ (ve vztahu k těmto údajům). Citované ustanovení předpokládá, že správce provede likvidaci osobních údajů vhodným a účinným způsobem tak, že předmětné údaje již skutečně nebudou nadále existovat a nebude je možno dále využívat. Správce, který zpracovává osobní údaje dlouhodobě a soustavně, což je právě případ většiny zaměstnavatelů, by měl mít stanoveny konkrétní postupy pro likvidaci dat, u nichž zanikl účel zpracování. Tyto postupy je vhodné zahrnout do některého interního aktu správce, typicky jde o skartační řád a skartační plán. Samozřejmě, že adekvátní způsob likvidace je nutno zvolit s ohledem na nosič, na kterém jsou údaje zachyceny. Jedná-li se o likvidaci údajů zachycených v písemných dokumentech, je situace správce snadná, neboť likvidaci těchto písemností (nejlépe skartováním za současného pořízení skartačního protokolu) jsou údaje v nich obsažené bezpečně zlikvidovány. Problematičtější je likvidace dat zachycených v elektronické podobě, kdy s ohledem na možnosti obnovení dat běžné vymazání ke skutečné likvidaci nestačí.

Porušení povinnosti podle § 20 ZOOÚ ovšem není správním deliktem podle ZOOÚ, protože tomuto ustanovení ZOOÚ neodpovídá žádná ze skutkových podstat správních deliktů uvedených v taxativním výčtu v hlavě VII tohoto zákona. Obdobně jako v případech některých výše uvedených povinností se tedy i zde jedná o imperfektní normu.¹³¹

¹³⁰ Např. zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

¹³¹ Pokud by správce poté, co pomine účel zpracování osobních údajů, neprovedl jejich likvidaci a údaje tak nadále zpracovával, bylo by nutno jeho jednání kvalifikovat jako porušení povinností stanovené v § 5 odst. 1 písm. e) ZOOÚ.

Další povinností spojenou s ukončením zpracování osobních údajů, která se však týká již pouze správce, na něhož se vztahuje oznamovací povinnost podle § 16 ZOOÚ (tj. správce, který osobní údaje zpracovává na základě vlastního rozhodnutí), je povinnost vyjádřená v § 19 ZOOÚ oznámit, jakým způsobem bylo s osobními údaji naloženo Úřadu pro ochranu osobních údajů. Tímto ustanovením mělo být zřejmě zajištěno, aby správci náležitě ověřili, že údaje, které již dále nehodlají využívat, nemohou být nějakým způsobem zneužity. Vzhledem k tomu, že následující § 20 ZOOÚ stanoví povinnost údaje po ukončení zpracování likvidovat, je obsahem povinnosti podle § 19 tohoto zákona v podstatě informace o tom, jakým způsobem byla likvidace provedena.

Avšak obdobně jako povinnost vyjádřená v § 20 ZOOÚ nelze ani porušení povinnosti správce podle § 19 tohoto zákona kvalifikovat jako správní delikt, neboť žádné z ustanovení hlavy VII upravující sankce za správní delikty neupravuje skutkovou podstatu odpovídající této povinnosti. Význam tohoto ustanovení v praxi je tak jen velmi malý.

S ohledem na uvedené lze shrnout, že v praxi mají správci osobních údajů provádějící zpracování pouze v rozsahu uložených povinností situaci poměrně jednoduchou. Naprostá většina podmínek pro takové zpracování osobních údajů je stanovena v příslušných zvláštních zákonech a jejich povinností je „pouze“ se s těmito normami řádně seznámit a při své činnosti se jimi řídit. Pokud správce postupuje v souladu se zvláštními zákony, plní současně i povinnosti stanovené ZOOÚ. Zřejmě největší problém činí těmto správcům plnění povinnosti podle § 13 odst. 1 ZOOÚ, neboť zde je ponecháno správcům osobních údajů na zvážení, jaká technicko-organizační opatření jsou vhodná právě v jeho situaci. Další povinností, která činí správcům často potíže, je povinnost uvedená v § 5 odst. 1 písm. f) ZOOÚ. Správce často neodolá, aby již jednou shromážděné údaje nevyužil i k jinému účelu a tím si zjednodušil situaci, případně si ani neuvědomí, že účel, k němuž údaje zpracovává, již přesahuje ten, pro který údaje shromáždil.

Naopak pro správce osobních údajů, kteří stanoví účel zpracování sami, je plnění povinností podle ZOOÚ poměrně těžší. Tito správci nemají k dispozici právní předpis, který by jim alespoň v základních rysech stanovil jak má zpracování osobních údajů probíhat. Je tedy zcela na zvážení těchto správců, jak na základě účelu zpracování, který stanovili, vyhodnotí své ostatní povinnosti, např. jaký minimální rozsah údajů je pro dosažení tohoto účelu nezbytný a které údaje jsou naopak již nadbytečné, jak dlouho je třeba údaje uchovávat nebo jakým způsobem a v jaké podobě získat souhlas subjektů údajů se zpracováním. V praxi však těmto správcům osobních údajů činí největší potíže obdobné povinnosti jako správcům, kterým je zpracování uloženo zvláštním zákonem. Jedná se o povinnost podle § 13 odst. 1 ZOOÚ, správci osobních údajů zde obvykle podcení zejména organizační opatření, jako např. správné nastavení povinností a odpovědnosti jednotlivých pracovníků pověřených zpracováním osobních údajů a kontrola těchto opatření. Poměrně

často jsou porušována i ustanovení § 5 odst. 1 písm. d) a e) ZOOÚ, jejichž plnění závisí na adekvátně stanoveném účelu zpracování a vyhodnocení toho, jaký rozsah osobních údajů je k jeho dosažení skutečně zapotřebí a jaká doba uchování údajů je nezbytná. Nevhodně stanový účel zpracování údajů a nedbalost při jeho naplnění je také zřejmě hlavní příčinou správních deliktů, kterých se správci dopouštějí porušením povinnosti podle § 5 odst. 1 písm. f) ZOOÚ.

S výjimkou ustanovení § 5 odst. 3, § 6, § 10, § 13 odst. 2, § 18 odst. 2, § 19 a § 20 ZOOÚ, je porušení všech vyjmenovaných povinností správním deliktem (přesněji jiným správním deliktem) podle tohoto zákona,¹³² tedy naplněním některé ze skutkových podstat uvedených v § 44 nebo § 45 ZOOÚ, za který je možno uložit sankci až do výše pěti milionů Kč a v případě ohrožení citlivých osobních údajů nebo zásahu do práva na ochranu soukromého a rodinného života většího počtu osob až do výše deseti milionů Kč. Správní delikty podle ZOOÚ jsou projednávány Úřadem pro ochranu osobních údajů ve správním řízení.

Co se týče souladu právní úpravy citovaných povinností s mezinárodními dokumenty, lze konstatovat, že veškeré výše uvedené povinnosti více či méně odpovídají obdobným ustanovením v mezinárodních předpisech upravujících ochranu osobních údajů, tj. v Úmluvě 108 a Směrnici 95/46. Právní úprava ochrany osobních údajů v České republice tedy v této oblasti odpovídá požadavkům vyplývajícím z uvedených mezinárodních dokumentů.

4.4. Povinnosti zaměstnanců při zpracování osobních údajů

ZOOÚ neukládá povinnosti pouze správcům a zpracovatelům osobních údajů, ale klade určité požadavky také na zaměstnance, kteří pro tyto subjekty údaje fakticky zpracovávají (např. pracovníky personálních úseků nebo mzdové účetní). Obdobné povinnosti se vztahují i na jiné osoby, které se na zpracování osobních údajů podílejí na základě smlouvy se správcem či zpracovatelem.¹³³ Zaměstnancům i těmto tzv. jiným osobám (dále jen "zaměstnanci") ukládá ZOOÚ sice pouze dvě povinnosti, jejich dodržení je však pro dosažení cílů ZOOÚ neméně významné jako dodržování povinností uložených správcům osobních údajů.

První z nich, kterou upravuje § 14 ZOOÚ, je povinnost zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném. V podstatě se jedná o

¹³² Diskutabilní může být i možnost sankcionování porušení povinnosti podle § 5 odst. 1 písm. g) ZOOÚ (shromažďování osobních údajů pod záminkou jiného účelu nebo jiné činnosti), kdy toto ustanovení je sice v korespondujícím § 45 odst. 1 písm. c) ZOOÚ uvedeno, nicméně znění této skutkové podstaty tomu zcela neodpovídá.

¹³³ Může se jednat o fyzické osoby nebo tzv. fyzické osoby podnikající, pokud údaje zpracovávají na základě jiné smlouvy než smlouvy o zpracování osobních údajů podle § 6 ZOOÚ, tj. na základě smlouvy podle zákona občanského zákoníku, nebo zákona č. 513/1991 Sb., obchodní zákoník.

vyjádření jedné ze základních povinností zaměstnance vyplývající z pracovního poměru,¹³⁴ která je zde vztažena konkrétně k nakládání s osobními údaji.

Z hlediska ochrany osobních údajů je nezbytné, aby všechny osoby, které se zpracování osobních údajů účastní, byly vázány jednoznačnými pravidly, a tím bylo minimalizováno riziko zneužití těchto údajů a s ním související hrozba zásahu do soukromí subjektů údajů.

Podmínkami ve smyslu § 14 ZOOÚ se rozumí jak organizační pokyny zaměstnavatele, tak i pokyny týkající se využití konkrétních prostředků pro zpracování osobních údajů a vhodném způsobu práce s nimi, jako např. uzamykání písemností během nepřítomnosti na pracovišti nebo náležitě využívání přístupových hesel při práci s výpočetní technikou. Současně je nezbytné zaměstnance o podmínkách zpracování a jeho povinnostech poučit, nejlépe formou vnitřních aktů nebo pokynů, z nichž bude zřetelně vyplývat, že dodržování uvedených pokynů je součástí pracovní kázně zaměstnance, tj. povinností podle zákoníku práce (zejména podle § 73 odst. 1 tohoto zákona). V některých případech bude na místě i odborné školení zaměstnanců týkající bezpečného využívání pracovních prostředků z hlediska ochrany osobních údajů, a to zřejmě především při práci s výpočetní technikou.

Pokud jde o tzv. jiné osoby, vykonávajících činnost spočívající ve zpracování osobních údajů pro správce na základě smlouvy, je zřejmě jedinou cestou zajištění dodržování stanovených podmínek smluvní závazek podpořený případně smluvní sankcí.

Jak bylo uvedeno již výše, stanovení pokynů zaměstnancům a jejich vymáhání v praxi je nedílnou součástí bezpečnostních opatření ve smyslu § 13 odst. 1 ZOOÚ. Absence podmínek zpracování osobních údajů stanovených zaměstnavatelem je obvykle hodnocena jako porušení tohoto ustanovení, což znamená naplnění skutkové podstaty správního deliktu podle § 45 odst. 1 písm. h) ZOOÚ. Dojde-li tedy např. k neoprávněnému zpřístupnění osobních údajů jejich odesláním elektronickou poštou na nesprávnou adresu a u příslušného správce osobních údajů je zahájena kontrola plnění povinností podle ZOOÚ, zkoumá inspektor Úřadu, zda příčinou takového neoprávněného zpracování osobních údajů nebyla právě nevhodná či nedostačující opatření ve smyslu § 13 odst. 1 ZOOÚ (např. absence pokynu zaměstnavatele opatřit soubor obsahující osobní údaje před odesláním elektronickou poštou heslem) anebo zda se jednalo o pochybení konkrétního zaměstnance, který správcem vydané pokyny nedodržel.

Z porušení § 14 ZOOÚ může zaměstnancům vyplynout pracovněprávní případně i trestní odpovědnost,¹³⁵ nikoli však odpovědnost ze ZOOÚ, neboť ve výčtu skutkových podstat přestupků podle § 44 ZOOÚ není odpovídající ustanovení uvedeno a porušení § 14 tohoto

¹³⁴ Např. v § 27 odst. 1 nebo § 35 odst. 1 písm. b) zákoníku práce.

¹³⁵ Zaměstnanec, který neoprávněně zpracovává (sdělí, zpřístupní apod.) osobní údaje shromážděné orgánem vykonávajícím státní správu či samosprávu nebo který neoprávněným zpracováním osobních údajů poruší zákonem stanovenou povinnost mlčenlivosti (tj. i podle § 15 ZOOÚ – viz níže) může být odpovědný za trestný čin neoprávněného nakládání s osobními údaji podle § 178 zákona 140/1961 Sb., trestní zákon.

zákonu tedy nelze hodnotit jako přešůpek. Na druhou stranu je třeba uvést, že projednávání porušení § 14 ZOOÚ Úřadem pro ochranu osobních údajů by bylo do jisté míry zásahem do pravomocí zaměstnavatelů, neboť jsou to primárně oni, kdo má právo po zaměstnancích požadovat výkon práce v souladu s udělenými pokyny a kdo může z nedodržení stanovených limitů vyvodit pracovněprávní odpovědnost.¹³⁶

Druhou povinností zaměstnanců správců osobních údajů je povinnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních podle § 15 odst. 1 ZOOÚ.

Tato povinnost se kromě zaměstnanců správce či zpracovatele osobních údajů vztahuje také na osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí s osobními údaji do styku, tedy osoby vykonávající nejrůznější kontrolní nebo inspekční činnosti, auditoři, znalci apod.

Povinnost nesdělovat nepovoleným osobám informace, s nimiž se zaměstnanec seznámil při výkonu své práce, resp. neumožnit, aby k těmto informacím získal přístup někdo nepovolaný, je jedním z nejdůležitějších institutů ochrany osobních údajů a tedy ochrany soukromí subjektů údajů. Současně jsou touto povinností chráněni i správci a zpracovatelé, neboť povinnost mlčenlivosti ohledně bezpečnostních opatření, která pro zajištění ochrany osobních údajů přijali, je nezbytnou podmínkou efektivitv těchto opatření.

Uvedená povinnost mlčenlivosti platí pro vyjmenované osoby přímo ze ZOOÚ, není tedy nezbytné ji zvláště potvrzovat např. formou zvláštního závazku v rámci pracovní smlouvy, jak se v praxi někdy děje. Znalost této povinnosti u zaměstnanců nakládajících s osobními údaji se dle obecné právní zásady *ignorantia iuris non excusat* předpokládá a povinnost dodržovat při práci právní předpisy vztahující se k jejich práci vyplývá zaměstnancům také z § 73 odst. 1 písm. c) zákoníku práce. Nicméně je vhodné příslušné zaměstnance o této povinnosti vhodným způsobem poučit.

Povinnost mlčenlivosti platí dle poslední věty § 15 odst. 1 ZOOÚ i po skončení zaměstnání nebo příslušných prací. Vzhledem k tomu, že ZOOÚ neuvádí, do kdy jsou uvedené osoby povinností mlčenlivosti vázány, je nutno toto ustanovení vykládat tak, že neomezeně. Bylo by nelogické, aby právo subjektů údajů na ochranu soukromí bylo ohroženo či přímo narušeno jen proto, že zaměstnanec správce osobních údajů nebo jiná osoba, která se kdysi s informacemi o něm seznámila, již pro daného správce dále nepracuje. Obdobné platí i v případě bezpečnostních opatření přijatých správcem či zpracovatelem ke splnění povinnosti podle § 13 odst. ZOOÚ.

¹³⁶ Před účinností zákona č. 439/2004 Sb., který přinesl do ZOOÚ novou úpravu sankcí, vedl Úřad řízení o přešůpku v případě jakéhokoli porušení povinnosti podle § 14 ZOOÚ, tedy např. i se zaměstnancem, který z nepozornosti zaměnil písemnosti a nadepsané obálky, a tak způsobil zpřístupnění osobních údajů neoprávněným osobám. Projednávání takového pochybení Úřadem se však nejevív jako účelné, mj. i proto, že příslušný zaměstnavatel takového zaměstnance již obvykle potrestal sám. Pokud nedošlo k pochybení zaměstnance na základě absence jednoznačných pokynů, jak má s osobními údaji nakládat, bylo faktickým výsledkem obdobných řízení opakované sankcionování zaměstnance.

Praktický dopad tohoto ustanovení ZOOÚ je v tom, že by se nemělo stát, aby např. současně s nástupem nového kolegy věděli všichni ostatní zaměstnanci dané společnosti, kterou školu dotyčný studoval, že je rozvedený a kolik má dětí. Tam, kde je zpracování osobních údajů přímo předmětem činnosti správce, je důsledné dodržování této povinnosti neméně důležité. Jistě nelze připustit, aby si např. pracovník pověřený zpracováním výsledků spotřebitelské ankety paralelně vytvářel vlastní evidenci kontaktů s cílem využít takové informace např. pro podnikatelskou činnost některého člena rodiny nebo s cílem tyto informace zpeněžit.

Povinnost mlčenlivosti podle ZOOÚ se nevztahuje pouze na informační povinnost podle zvláštních zákonů, zejména podle § 167 a 168 zákona č. 140/1961 Sb., trestní zákon, nebo § 25a zákona č. 21/1992 Sb., o bankách. Naopak řadě osob, které se při výkonu svého zaměstnání setkávají s osobními údaji, vzniká povinnost mlčenlivosti současně i ze zvláštních zákonů, např. § 14 zákona č. 582/1991 Sb., o organizaci sociálního zabezpečení, nebo § 136 zákona 435/2004 Sb., o zaměstnanosti. Tato zvláštní povinnost mlčenlivosti není ustanovením § 15 ZOOÚ samozřejmě nijak dotčena (a naopak).

Porušením povinnosti podle § 15 odst. 1 ZOOÚ se zaměstnanec dopustí přestupku podle § 44 odst. 1 ZOOÚ, jehož projednání je v kompetenci Úřadu pro ochranu osobních údajů. Za tento přestupek lze potom v řízení o přestupku v souladu s § 44 odst. ZOOÚ uložit pokutu až do výše sto tisíc Kč.

4.5. Práva zaměstnanců jako subjektů údajů

Zaměstnancům nevyplývají ze ZOOÚ pouze povinnosti ve vztahu k ochraně osobních údajů, s nimiž se při výkonu své práce setkávají, ale ZOOÚ jim, jakožto subjektům údajů, přiznává i určitá práva. Každý subjekt údajů, jehož osobní údaje jsou zpracovávány, má na základě ZOOÚ možnost aktivně se na ochraně vlastních osobních údajů, ale i údajů jiných osob, podílet, a tím přispívat k zajištění co nejvyšší úrovně ochrany osobních údajů.

První z těchto práv upravuje § 12 ZOOÚ a je jím právo subjektu údajů na přístup k informacím. Obsahem tohoto práva je možnost požádat správce osobních údajů o sdělení, zda jeho osobní údaje vůbec zpracovává, jaký je účel tohoto zpracování, o jaké konkrétní údaje se jedná, případně alespoň o jaké kategorie údajů, z jakého zdroje tyto údaje získal a jakým příjemcům, resp. kategoriím příjemců, předmětné údaje zpřístupňuje. Jsou-li na základě automatizovaného zpracování údajů činěny správcem určité úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů, potom musí správce poskytnout informaci také o povaze tohoto zpracování, tj. jaký je mechanismus takového automatizovaného zpracování.

Správce oslovený s žádostí podle § 12 ZOOÚ je povinen sdělit tazateli uvedené informace bez zbytečného odkladu, přičemž má právo požadovat přiměřenou úhradu nákladů vzniklých v souvislosti s jejich poskytnutím. Tuto informační povinnost může za správce splnit i zpracovatel, což je zejména v případech, kdy provádí většinu nebo veškeré operace se zpracováním spojené, zřejmě vhodnější. Tím se ale správce nezbavuje odpovědnosti za náležité splnění této povinnosti v případě, kdy by zpracovatel neinformoval subjekt údajů dostatečně včas nebo ve stanoveném rozsahu.¹³⁷

Získání uvedených informací je nezbytnou podmínkou toho, aby subjekt údajů mohl uplatňovat svá další práva směřující k odstranění případných pochybení správce či k zamezení neoprávněného zpracování jeho osobních údajů a je tedy jednou ze záruk zachování práva na ochranu před neoprávněným zpracováním osobních údajů zakotveného v ustanovení čl. 10 odst. 3 Listiny.

Na základě zvláštních zákonů může však být právo subjektu údajů na přístup k údajům omezeno. Je tomu tak např. podle § 42j zákona 283/1991 Sb., o Policii České republiky, nebo podle § 16 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, kdy z důvodů zajištění plnění úkolů těchto orgánů je právo na přístup k osobním údajům v určitých situacích limitováno. Některé právní předpisy mohou také stanovit zvláštní úpravu přístupu k osobním údajům, např. § 8 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), který upravuje otázku poskytnutí údajů z Informačního systému evidence obyvatel. V pracovněprávních vztazích se však obdobná omezení či výjimky nevyskytují.

Další práva subjektů údajů jsou upravena v § 21 ZOOÚ. Toto ustanovení umožňuje dotčeným osobám reagovat na situaci, kdy buď zjistí, nebo se pouze domnívají, že určitý správce nebo zpracovatel nakládá s jejich osobními údaji v rozporu s právními předpisy nebo způsobem, kdy hrozí zásah do jejich soukromého života. ZOOÚ v ustanovení § 21 odst. 1 uvádí jako příklad situaci, kdy subjekt údajů zjistí nepřesnost osobních údajů ve vztahu ke stanovenému či deklarovanému účelu jejich zpracování. Spíše než nepřesnost zpracovávaných údajů je však častější, a také závažnější, případné zpracování nadbytečných údajů nebo zpracování údajů k jinému účelu, např. pokud by zaměstnavatel za účelem možnosti kontaktovat příbuzné svých zaměstnanců shromažďoval nejen adresu nebo telefonní číslo např. manžela, ale i to, kde je zaměstnán, nebo pokud by zaměstnavatel využíval rodné číslo jako obecný identifikátor zaměstnanců i tam, kde zvláštní zákon¹³⁸ jeho zpracování neumožňuje (např. pro účely evidence pracovní doby).

¹³⁷ Správce by měl v této souvislosti zvážit vytvoření mechanismu vyřizování obdobných žádostí, případně stížností.

¹³⁸ Právní úprava využívání rodných čísel je obsažena v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). Problematice zpracování rodných čísel v rámci pracovněprávního vztahu je věnována kapitola 5.2.

V obdobných případech má zaměstnanec na základě § 21 ZOOÚ zejména právo požádat správce nebo zpracovatele o vysvětlení. V některých případech je tímto možné předejít nedorozumění, neboť ne každý subjekt údajů (zaměstnanec) si musí být zcela přesně vědom toho, jaké osobní údaje a k jakému účelu může správce (zaměstnavatel) zpracovávat na základě zmocnění zvláštními zákony.¹³⁹

Pokud vysvětlení nebude pro subjekt údajů uspokojivé a jeho podezření z nezákonného zpracování osobních údajů bude přetrvávat, může požadovat, aby správce závadný stav odstranil. Těto nápravy lze dosáhnout především blokováním, provedením opravy, doplněním nebo i likvidací předmětných osobních údajů, přičemž subjekt údajů může buď obecně požadovat provedení nápravy, nebo může i konkrétně specifikovat jakou operaci má správce s údaji provést.

Shledá-li takto oslovený správce žádost oprávněnou, je podle § 21 odst. 2 ZOOÚ jeho povinností závadný stav neprodleně odstranit. Toto ustanovení se může zdát poněkud nadbytečné, neboť při splnění všech ostatních relevantních povinností stanovených ZOOÚ, by situace, kdy správce zjistí nezákonnost zpracování až na základě žádosti subjektu údajů, nastat neměla. Uvedená povinnost se tak uplatní především u správců, kteří se pochybení v souvislosti se zpracováním osobních údajů dopustí určitou nedbalostí nebo nedůsledností při plnění požadavků stanovených ZOOÚ.

Jestliže správce osobních údajů obdrží žádost subjektu údajů podle § 21 odst. 1 ZOOÚ, je na základě § 21 odst. 7 ZOOÚ povinen o této skutečnosti následně informovat veškeré příjemce osobních údajů, obdobně je povinen je informovat, provede-li na základě této žádosti např. opravu či likvidaci určitých dat. Smysl této povinnosti je zřejmý. Pokud správce předává osobní údaje jiným osobám, měl by stejnému okruhu subjektů předat také informaci, že subjekt údajů uplatňuje některé ze svých práv podle § 21 ZOOÚ. V situaci, kdy na základě podané žádosti dojde k nápravě protiprávního stavu, se význam této povinnosti ještě zvyšuje, neboť logicky není možné, aby správce uvedl zpracování osobních údajů do souladu s právními předpisy, ale příjemci, kterým chybné údaje předal, již nikoli.

Poslední věta ustanovení § 21 odst. 7 ZOOÚ však umožňuje správcům se zde uvedené povinnosti vyhnout, a to v případě, kdy by informování příjemců nebylo možné nebo bylo spojeno s neúměrným úsilím. Tato věta tak význam povinnosti podle § 21 odst. 7 ZOOÚ poněkud relativizuje a nedůvodně obsah povinností správců osobních údajů zmírňuje na úkor práv subjektu údajů, který v uvedených situacích ztrácí možnost dosáhnout nápravy. Není zřejmé, proč by nemělo být možné či únosné informovat příjemce osobních údajů v požadovaném rozsahu, jestliže bylo možné jim osobní údaje předat.

¹³⁹ V případě zpracování osobních údajů na základě souhlasu zaměstnance by teoreticky k žádostem o vysvětlení důvodu zpracování docházet nemělo, protože na zaměstnavatele s v takovém případě vztahuje informační povinnost podle § 11 ZOOÚ.

V případě, kdy správce žádosti subjektu údajů, ať již o vysvětlení nebo o nápravu, nevyhoví, má tato osoba podle § 21 odst. 3 ZOOÚ právo obrátit se na Úřad pro ochranu osobních údajů, který má pravomoc její podnět prošetřit a případně uložit opatření k nápravě či sankci z moci úřední.

Zákonodárce sledoval zavedením tohoto „dvouinstančního“ principu, kdy se má subjekt údajů nejprve obrátit na příslušného správce a teprve poté na Úřad pro ochranu osobních údajů, zejména redukcí sporů mezi správcí a subjekty vyplývajících pouze z neinformovanosti či nedorozumění.¹⁴⁰

Nicméně podle následujícího ustanovení § 21 odst. 4 ZOOÚ může subjekt údajů podat podnět Úřadu i přímo, aniž by správce, o němž se domnívá, že ZOOÚ porušuje, kontaktoval. Rozhodnutí, jak bude postupovat, je tak čistě na subjektu údajů. V situaci, kdy jsou (nebo mají být) jeho osobní údaje nezákonně zpracovávány správcem, k němuž má určitý vztah, např. právě zaměstnavatelem, může obvykle jednání se správcem situaci vyřešit.¹⁴¹ Naopak tam, kde správce odmítá na žádost reagovat, což může být i případ, kdy údaje zpracovává zcela v souladu se zákony, ale subjekt údajů je přesvědčen o opaku, je na místě zásah dozorového orgánu.

Uplatněním práv podle § 21 ZOOÚ samozřejmě není dotčena možnost subjektu údajů domáhat se nároků vyplývajících z práva na ochranu osobnosti podle jiných právních předpisů, zejména podle § 13 občanského zákoníku, upravující právo domáhat se upuštění neoprávněných zásahů do uvedeného práva, odstranění následků a přiměřeného zadostiučinění nebo náhrady nemajetkové újmy v penězích.

Jak je uvedeno již v kapitole 2.2.7. až do novely ZOOÚ provedené zákonem č. 439/2004 Sb. byl Úřad pro ochranu osobních údajů na základě § 21 odst. 2 ZOOÚ kompetentní rozhodovat také o přiznání omluvy nebo jiného zadostiučinění, případně i peněžité náhrady subjektu údajů v souvislosti s porušením jeho práv chráněných ZOOÚ. Tímto byla vytvořena nedůvodná nerovnost mezi osobami, které se domáhaly náhrady nemajetkové újmy způsobené zásahem do práva na ochranu osobnosti podle občanského zákoníku, o jejichž nárocích rozhodoval soud, a osobami, jejichž osobnostní práva byla narušena zásahem do práva na ochranu osobních údajů, kdy bylo rozhodování o přiznání peněžité náhrady svěřeno Úřadu, který by však musel o tomto nároku rozhodovat v jakémsi kvazi správním řízení.¹⁴²

Ustanovení § 21 odst. 6 ZOOÚ zakládá solidární odpovědnost správců a zpracovatelů za porušení ZOOÚ, ke kterým u nich došlo, přičemž tato odpovědnost je objektivní. Uvedené

¹⁴⁰ Důvodová zpráva k návrhu zákona č. 439/2004 Sb., komentář k bodu 37 a 38.

¹⁴¹ Dotyčnému správcí navíc v takovém případě nehrozí postih za porušení ZOOÚ.

¹⁴² Před účinností zákona č. 439/2004 Sb. se vyskytlo jen velmi málo návrhů na přiznání peněžité náhrady, přičemž většinu případů musel Úřad nakonec ukončit, neboť dříve než zahájil řízení vstoupila v účinnost uvedená novela ZOOÚ, která Úřadu tuto kompetenci odejmula.

ustanovení sice posiluje postavení subjektu údajů, na druhou stranu ale nedůvodně zatěžuje odpovědností zpracovatele osobních údajů, ačkoli z definice správce osobních údajů podle § 4 písm. j) je zřejmé, že je to pouze on, kdo nese odpovědnost za celé zpracování. Vzhledem k tomu, že zpracovatel by neměl s údaji nakládat jinak, než v souladu s podmínkami vymezenými zvláštním zákonem nebo smlouvou o zpracování osobních údajů podle § 6 ZOOÚ, je porušení ZOOÚ zpracovatelem obvykle následkem nevhodně stanovených podmínek, tj. pochybením správce. Nicméně v podmínkách českého právního řádu není širší vymezení odpovědných subjektů, vedené zřejmě úmyslem, aby se poškozený svých práv alespoň někde dovolal, ničím neobvyklým.¹⁴³

Porušení povinností, které správčům z práv subjektů údajů podle § 12 a § 21 ZOOÚ vyplývají, je správním deliktem podle hlavy VII tohoto zákona, za který je ve správním řízení možné uložit příslušnému správci pokutu až do výše pěti, resp. deseti milionů Kč. Obdobně, jako je tomu po novele ZOOÚ provedené zákonem č. 439/2004 Sb. u jiných ustanovení, ani zde však nelze sankcionovat všechny případy, kdy správce nepostupuje tak, jak ZOOÚ vyžaduje. Skutková podstata přestupku a správního deliktu vyjádřená v § 44 odst. 2 písm. g) a § 45 odst. 1 písm. g) ZOOÚ zahrnuje pouze neposkytnutí požadované informace, což však nepokrývá povinnosti správce uvedené v § 21 odst. 2 a 7 ZOOÚ, tedy povinnost odstranit na žádost subjektu údajů závadný stav a povinnost informovat o provedených opravách a změnách zpracovávaných údajů ostatní příjemce. Zatímco v prvním případě není tento nedostatek pro vymáhání ZOOÚ příliš velkou překážkou, neboť správce v takovém případě obvykle porušuje jinou z povinností podle ZOOÚ a subjekt údajů se může se svým problémem obrátit na Úřad pro ochranu osobních údajů, v případě § 21 odst. 7 ZOOÚ je situace horší. Správce tak není k předání informace o opravě či likvidaci údajů příjemcům motivován hrozbou případné sankce za porušení této povinnosti.

Ze ZOOÚ vyplývají subjektům údajů i další práva, která odpovídají povinnostem správců a zpracovatelů osobních údajů, ta jsou ale narozdíl od výše uvedených aktivních práv právy pasivními. Mezi nejdůležitější z nich patří právo být náležitě a včas informován ve smyslu § 11 ZOOÚ o základních parametrech zamýšleného či již probíhajícího zpracování. Tyto informace jsou podmínkou toho, aby se subjekt údajů mohl aktivně na ochraně svých osobních údajů podílet a případně se nezákonnému nakládání s údaji bránit. Dalším významným právem subjektu údajů je právo poskytnout souhlas se zpracováním údajů podle § 5 odst. 2 ZOOÚ, resp. právo tento souhlas odmítnout.

¹⁴³ Matoušová, M. Pohled praxe na novelu zákona o ochraně osobních údajů. Právní rádce č. 11/2004, s. 69.

5. Některé aktuální otázky spojené se zpracováním osobních údajů v pracovněprávních vztazích

V souvislosti se zpracováním osobních údajů zaměstnanců zaměstnavateli vyvstává v současné době několik aktuálních otázek, mezi které patří předávání osobních údajů zaměstnanců do zahraničí, zejména tzv. mateřským společnostem, nebo využívání rodných čísel, které bylo s účinností od 1. dubna 2004 nově upraveno. Velmi diskutovanou problematikou je dále zpracování osobních údajů zaměstnanců při kontrole jejich činnosti během pracovní doby, konkrétně využívání připojení k Internetu a elektronické pošty, a problematika kontroly zaměstnanců prostřednictvím kamer či kamerového systému.

Vzhledem ke komplexnosti uvedených oblastí, neboť každá z nich by mohla být tématem samostatné práce, jsou zde tyto aktuální otázky v podstatě pouze nastíněny.

5.1. Předávání osobních údajů zaměstnanců do zahraničí

V dnešní globalizované společnosti je předávání či sdílení nejrůznějších informací, včetně osobních údajů, zcela běžné a pro fungování některých oblastí i nezbytné. Rozdílná úroveň ochrany osobních údajů a poskytovaných garancí v jednotlivých státech však představuje zásadní překážku volného pohybu osobních údajů.¹⁴⁴ Předání dat ze země s přísnější či ucelenější právní úpravou, přičemž zřejmě nejpřísnější podmínky mají v současné době členské státy Evropské unie, do země, kde není garantována odpovídající úroveň, obnáší poměrně velké riziko zásahu do soukromí dotčených subjektů údajů. Na tuto situaci je třeba reagovat stanovením určitých podmínek, bez jejichž naplnění nebude předání osobních údajů do zahraničí možné.

Poskytování osobních údajů zaměstnanců do ciziny je v důsledku toho, jak se v posledních letech v České republice usazují pobočky nejrůznějších zahraničních společností, stále častějším jevem, který nabyl ještě větší intenzity se vstupem ČR do Evropské unie. Nejčastější jsou případy zaměstnavatelů smluvně svázaných se zahraničními podnikatelskými subjekty,¹⁴⁵ které požadují předávání osobních údajů zaměstnanců řídicím orgánům nebo specializovaným personalistickým či jiným útvarům.

¹⁴⁴ Z pohledu dozorových orgánů pověřených ochranou osobních údajů je samozřejmě ideálním stavem, pokud k žádnému toku údajů nedochází. Vzhledem k tomu, že tento stav je logicky nereálný, je nezbytné požadovat záruky adekvátní úrovně ochrany předávaných dat.

¹⁴⁵ Typicky se jedná o vztah tzv. mateřské a dceřinné společnosti, kdy mateřská společnost sídlí v zahraničí a dceřinná v ČR.

Úprava předávání osobních údajů do zahraničí je v českém právním řádu obsažena v § 27 ZOOÚ a je vystavěna na principu, že osobní údaje je zásadně možné předávat pouze do těch zemí, kde je zaručena srovnatelná úroveň jejich ochrany.

Z hlediska úrovně ochrany osobních údajů lze státy rozdělit do čtyř skupin:

- členské státy Evropské unie;
- státy, do nichž lze osobní údaje předávat na základě rozhodnutí orgánů EU;
- státy, s nimiž má ČR uzavřenu mezinárodní smlouvu týkající se volného předávání osobních údajů, a
- ostatní státy s tzv. neadekvátní právní úpravou.

Ustanovení § 27 odst. 1 ZOOÚ obsahuje výslovný zákaz omezování volného pohybu osobních údajů při jejich předání do členských států Evropské unie. Omezením volného pohybu údajů na území Evropské unie by totiž byl ohrožen základní smysl její existence, tj. odstranění překážek volného pohybu osob, kapitálu, zboží a služeb. Požadavek volného předávání osobních údajů však současně přináší potřebu dostatečných záruk ohledně srovnatelné úrovně ochrany osobních údajů v ostatních členských zemích. Touto zárukou je zejména Směrnice 95/46, na jejímž základě došlo k harmonizaci úprav ochrany osobních údajů v rámci EU, a dále některé další předpisy specifikující ochranu dat v určitých oblastech.¹⁴⁶

Předávání osobních údajů do zemí mimo Evropskou unii (tzv. třetích zemí) na základě rozhodnutí jejích orgánů, které je upraveno v § 27 odst. 2 ZOOÚ, bylo zmíněno již v kapitole 1.4.4. Jedná se o případy, kdy právní úprava dané země byla Evropskou komisí¹⁴⁷ posouzena jako odpovídající požadavkům vyplývajícím ze Směrnice 95/46 a následně bylo vydáno rozhodnutí Evropské komise konstatující, že úroveň ochrany osobních údajů v dané zemi umožňuje volné předávání osobních údajů a že tomuto volnému pohybu nesmí být bráněno, např. dalšími požadavky národních dozorových orgánů.

Doposud byla jako adekvátní posouzena úprava ochrany osobních údajů v následujících zemích:

- a) Kanada, za předpokladu, že příjemce údajů podléhá působnosti kanadského zákona o ochraně osobních informací a elektronických dokumentech;
- b) Argentina;
- c) Švýcarsko;
- d) Guernsey;
- e) Ostrov Man a
- f) Spojené státy americké, ovšem pouze pokud:

¹⁴⁶ Např. směrnice 2002/58/EC Evropského parlamentu a Rady ze dne 10. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronické komunikace.

¹⁴⁷ Zejména na základě stanovisek vypracovaných Pracovní skupinou 29 (zřízenou na základě Směrnice 95/46).

- příjemce podléhá kompetenci Federální obchodní komise a Departmentu dopravy USA a současně přistoupil k tzv. zásadám bezpečného přístavu („Safe Harbour“) nebo
- se jedná o předání osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě Úřadu USA pro cla a ochranu hranic.¹⁴⁸

Samostatnou kapitolou předávání osobních údajů do zahraničí na základě rozhodnutí orgánů EU je využití tzv. standardních smluvních doložek, jejichž vzory jsou přílohou příslušných rozhodnutí Evropské komise. V současné době existují tři typy těchto doložek, které se liší podle postavení v jakém vůči sobě předávající a přijímající subjekt vystupují (tj. zda se jedná o vztah správce – zpracovatel nebo vztah správce – správce)¹⁴⁹.

V současné době jsou tyto doložky využívány stále častěji, neboť pro správce představují zjevně nejjednodušší řešení. Je však dlužno říci, že obvykle jsou k předmětné smlouvě připojeny ve formě jakéhosi vyplněného dotazníku, čímž je sice formálně naplněn požadavek § 27 odst. 2 ZOOÚ, ale smysl doložek, tj. skutečně zajistit standardní úroveň ochrany, tím naplněn není.

Dle ustanovení § 27 odst. 2 ZOOÚ je možné předávat osobní údaje také na základě závazné mezinárodní smlouvy, k jejíž ratifikaci dal souhlas Parlament ČR (tj. smlouvy podle čl. 10 Ústavy), která upravuje zákaz omezování volného pohybu osobních údajů mezi smluvními stranami této dohody.

Takovou mezinárodní smlouvou je v současnosti pouze Úmluva 108. Právní předpisy států, které Úmluvu 108 ratifikovaly, by měly zaručovat dostatečnou úroveň ochrany osobních údajů odpovídající všem požadavkům této úmluvy a tedy i Směrnice 95/46 a ZOOÚ. Kromě zemí, které jsou signatáři Úmluvy 108 a současně členskými státy EU, lze na základě této úmluvy volně předávat osobní údaje do Bulharska, Lichtenštejnska, Norska a Rumunska.

Nejedná-li se o žádnou z výše uvedených situací, je předání osobních údajů možné pouze v případě, že údaje mají být předávány pro některý z důvodů vyjmenovaných v § 27 odst. 3 ZOOÚ, tedy:

- a) údaje se předávají se souhlasem nebo na základě pokynu subjektu údajů;

¹⁴⁸ Otázka předávání osobních údajů k tomuto účelu je předmětem poměrně ostrých diskusí mezi EU a USA, které v souvislosti s útoky z 11. září 2001 začaly vyžadovat velmi podrobné informace o cestujících v letadlech, přičemž v případě odepření je daný přepravce přísně sankcionován (např. pokutami nebo odepřením přistávacích práv). Vzhledem k tomu, že se jedná o velkou sumu údajů (až 34 položek, mezi nimiž jsou např. i čísla úvěrových karet nebo informace o jídle objednaném během přepravy), k nimž má přístup poměrně široký okruh amerických úřadů, upozorňuje Pracovní skupina 29 ve svém stanovisku č. 4/2003 k úrovni ochrany osobních údajů cestujících při předání do USA (Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, www.europa.eu.int) mj. na nutnost opakovaného hodnocení nezbytnosti požadovaných údajů či okruhu subjektů, které k nim mají přístup.

¹⁴⁹ Původně byly vydány pouze dva typy doložek (rozhodnutím Evropské komise z června a prosince 2001). S účinností od 1. dubna 2005 je potom možné využít alternativní smluvní doložky při předávání údajů ve vztahu správce – správce, které v určitých ohledech stanoví mírnější požadavky.

- b) ve třetí zemi, kde mají být údaje zpracovávány, jsou vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu;¹⁵⁰
- c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem;
- d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána;
- e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů;
- f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků, nebo
- g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotní péče.

Před předáním osobních údajů na základě některého z výše uvedených důvodů je však ještě zapotřebí požádat Úřad pro ochranu osobních údajů o povolení. Úřad poté podle § 27 odst. 4 ZOOÚ přezkoumá všechny okolnosti související s předáním osobních údajů, a to především zdroj, konečné určení předávaných osobních údajů, kategorie těchto údajů a dále účel a dobu zamýšleného zpracování. Úřad při tomto postupu dále přihlédne k dostupným informacím o právních předpisech upravujících zpracování osobních údajů v dané třetí zemi nebo jiných normách, které by mohly úroveň ochrany osobních údajů ovlivnit.

Problematika předávání osobních údajů do zahraničí není však limitována jen podmínkami stanovenými v § 27 ZOOÚ, je nutno současně aplikovat i další požadavky tohoto zákona. Úřad pro ochranu osobních údajů proto pohlíží na případy předávání dat do zahraničí nejen z hlediska § 27 ZOOÚ, ale také z hlediska dalších povinností, které ZOOÚ pro zpracování předmětných kategorií osobních údajů stanoví. Především je tedy nutno posoudit, zda je předávání osobních údajů v souladu s účelem, k němuž byly shromážděny.

V mnoha případech jsou osobní údaje zaměstnanců předávány do jiných států na základě požadavku tzv. „mateřské“ společnosti, tj. zakladatele či partnera tuzemské společnosti. Tyto zahraniční podnikatelské subjekty mají obvykle zájem pouze o ekonomické

¹⁵⁰ Zde se jedná o smluvní doložky, které by mohl vydat český dozorový orgán (tedy Úřad), za účelem standardizování a zjednodušení procesu povolování předání osobních údajů podle § 27 odst. 3 ZOOÚ. Úřad takové doložky doposud nevydal a vzhledem k tomu, že správcům předávajícím osobní údaje do zahraničí více vyhovuje použití doložek vydaných rozhodnutím Evropské komise (neboť při jejich použití již nemusí žádat Úřad o povolení předání – viz níže), lze předpokládat, že tyto doložky vydány ani nebudou.

výsledky tuzemské společnosti vypovídající o racionalizaci práce, efektivitě činností a trendech dalšího vývoje v daných oblastech. K tomuto účelu tak mohou postačit ekonomické souhrny, statistické údaje a případné informace týkající se zaměstnanců pouze v anonymizované podobě. Zpracování osobních údajů zaměstnanců pro uvedené potřeby by zjevně bylo překročením účelu zpracování osobních údajů zaměstnanců stanoveného právními předpisy.¹⁵¹

Z pohledu ZOOÚ se navíc jedná o předání osobních údajů zpracovateli a na správce osobních údajů (českého zaměstnavatele) se tak vztahuje povinnost podle § 6 ZOOÚ, tedy povinnost uzavřít smlouvu o zpracování osobních údajů.

Předání osobních údajů zaměstnanců přichází v úvahu v případě, kdy jsou předávány údaje konkrétních zaměstnanců např. v souvislosti s jejich vysláním na služební cesty do zahraničí nebo na zahraniční stáž, neboť v takovém případě zaměstnanec plní své pracovní povinnosti a zaměstnavatel je naopak povinen vytvořit mu podmínky pro úspěšné plnění pracovních úkolů, tj. například zajistit dopravu a ubytování v zahraničí. Ke zpracování osobních údajů tak dochází v souladu s účelem, k němuž byly osobní údaje zaměstnavatelem shromážděny.

Správci osobních údajů, kteří žádají Úřad pro ochranu osobních údajů o povolení předání osobních údajů podle § 27 odst. 4 ZOOÚ, nejčastěji uvádí, že k předání bude docházet se souhlasem subjektů údajů, tedy v souladu s § 27 odst. 3 písm. a) tohoto zákona. Vzhledem k tomu, že v případě pracovních vztahů lze do jisté míry pochybovat o dobrovolnosti souhlasu zaměstnance se zpracováním jeho osobních údajů (viz kapitola 4.1), je přínosem ZOOÚ, že Úřad může po posouzení kritérií podle § 27 odst. 4 ZOOÚ předání osobních údajů nepovolit, a tak chránit práva zaměstnanců, kteří jsou vůči zaměstnavateli ve slabším postavení.

Mají-li být osobní údaje zaměstnance předány do zahraničí na základě jeho souhlasu, musí tomuto úkonu zaměstnance předcházet informace o tom, proč je nezbytné osobní údaje do zahraničí předat, jakým způsobem tam s nimi bude nakládáno a kterým subjektem. Zaměstnanci se dále musí dostat případně také informace o tom, že se jedná o předání údajů do země, která neposkytuje standardní míru ochrany, jaká rizika z tohoto faktu případně vyplývají a jaká byla přijata opatření k jejich snížení či eliminaci. Nelze tedy připustit paušální souhlas zaměstnance s jakýmkoli budoucím předáním jeho údajů, ale musí se jednat o svolení s náležitě specifikovanou operací s osobními údaji. Zaměstnanci musí být také vždy ponechána možnost takové zpracování osobních údajů odmítnout, a to bez jakýchkoli negativních následků.

¹⁵¹ Pokud by zaměstnavatel sám stanovil jako účel zpracování osobních údajů zaměstnanců jejich předávání do zahraničí, bylo zřejmě nutné posoudit takový účel jako nelegitimní.

Ve srovnání s postupem podle § 27 odst. 1 a 2 ZOOÚ, tj. předávání do členských států EU nebo do signatářských států mezinárodní smlouvy, je režim nastavený v § 27 odst. 3 tohoto zákona citelně přísnější. Důvodem je, že zatímco v prvních dvou případech má předávající subjekt záruky, že osobní údaje budou v průběhu zpracování příjemcem v zahraničí chráněny na odpovídající úrovni, při předání v režimu podle § 27 odst. 3 ZOOÚ tomu tak není. Předání osobních údajů podle § 27 odst. 3 ZOOÚ je v podstatě zásahem do základní zásady adekvátnosti ochrany dat a pro dotčené subjekty údajů představuje ztrátu kontroly nad tím, jak je s jejich údaji nakládáno. Z těchto důvodů musí být žádost o předání do třetí země vždy důkladně přezkoumána, tak aby bylo zaručeno, že rizika hrozící osobním údajům ve třetí zemi jsou zanedbatelná, anebo že v daném případě je vyšší riziko vyváženo důležitým zájmem.¹⁵²

Obecnou zásadou při předávání osobních údajů do zahraničí je, že správce by měl vždy volit takové řešení, které představuje zpracování minimálního rozsahu osobních údajů a současně zachová subjektům údajů jistotu adekvátní ochrany dat. V případě, kdy má zahraniční společnost zájem pouze o ekonomické ukazatele, je vhodnější osobní údaje nepředávat, tj. předávat pouze anonymizované výstupy.¹⁵³

5.2. Využití rodných čísel v pracovněprávních vztazích

Rodné číslo je zcela specifickým, v současné době často diskutovaným, nicméně stále zřejmě nejčastěji užívaným identifikátorem fyzických osob. Jeho specifikum spočívá v tom, že je jedním z mála osobních údajů, které se v průběhu života nemění, a že (až na výjimečné duplicity) umožňuje jednoznačnou identifikaci svého nositele.¹⁵⁴

Rodná čísla byla v České republice zavedena vyhláškou Federálního statistického úřadu č. 55/1976 Sb., o rodném čísle, vydanou k provedení zákona č. 21/1971 Sb., o jednotné soustavě sociálně ekonomických informací. V současné době obsahuje komplexní úpravu vydávání i užívání rodných čísel zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), kterým byl zákon č. 21/1971 Sb. nahrazen.

¹⁵² Pracovní skupina 29 doporučuje národním dozorovým úřadům ve svých stanoviscích restriktivní výklad podmínek, za nichž je možné uskutečnit předání osobních údajů do země s neadekvátní právní úpravou (Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, www.europa.eu.int).

¹⁵³ Shrnutí povinností zaměstnavatele v souvislosti s předáním osobních údajů zaměstnanců do zahraničí je dostupné také na internetových stránkách Úřadu v sekci Zahraničí/Předávání osobních údajů do zahraničí (www.uoou.cz/zahr_pred_2.php3).

¹⁵⁴ Osobní identifikátor existuje v mnoha státech, rodné číslo se však liší tím, že obsahuje informaci o datu narození a pohlaví nositele, přičemž každý ví, jakým způsobem jsou tyto údaje v rodném čísle uvedeny, a tak hrozí poměrně vysoké riziko zneužití těchto informací, tj. diskriminace dané osoby nebo vystavení dehonestujícím poznámkám apod.

Smyslem existence rodných čísel byla od počátku snaha umožnit jednoznačnou identifikaci osob při komunikaci se státem, a to nejdříve jen v oblasti sociálního zabezpečení. Později se využívání rodných čísel rozšířilo i do jiných oblastí veřejné správy.¹⁵⁵ V úředních evidencích vedených orgány státní správy je s pomocí rodného čísla možné získat o jeho nositeli velmi rozsáhlý soubor informací, od změn trvalého bydliště přes údaje o osvojení dítěte k informacím o trestné činnosti apod. Vzhledem ke svému jedinečnému charakteru a snadnému způsobu využití se však rodné číslo rozšířilo i do nejrůznějších evidencí v soukromoprávní sféře, kde slouží jako evidenční pomůcka usnadňující správu a využívání dané evidence, tj. zejména vyhledávání a sdružování informací v ní uložených.

S tím, jak byl postupně (zejména pod vlivem dokumentů přijatých na mezinárodní úrovni) na ochranu soukromí jednotlivce kladen stále větší důraz, včetně ochrany před neoprávněným shromažďováním a dalším zpracováním osobních údajů, e měnil i pohled na rodné číslo. Na jedné straně jde jistě o jedinečný, univerzální identifikátor, jehož využitím lze mnohé postupy usnadnit a zefektivnit, na straně druhé právě charakter rodného čísla výrazně zvyšuje potenciální nebezpečí zásahu do soukromého a osobního života subjektů, jejichž osobní údaje vedené v nejrůznějších evidencích lze teoreticky pomocí rodného čísla shromáždit a jejich sdružením získat údaje kvalitativně zcela odlišné od separátně zpracovávaných informací.

Zmíněný trend se projevil v zákoně č. 53/2004 Sb., kterým se mění některé zákony související s oblastí evidence obyvatel, a kterým bylo s účinností od 1. dubna 2004 do zákona č. 133/2000 Sb. mimo jiné vloženo nové ustanovení § 13 odst. 7, které explicitně stanoví, že rodné číslo je oprávněna užívat nebo o jeho využívání (v mezích stanovených zákonem) rozhodovat výlučně fyzická osoba, které bylo rodné číslo přiděleno, tzv. nositel rodného čísla, případně její zákonný zástupce. Výjimky z tohoto principu jsou pouze dvě a jsou upraveny v § 13c tohoto zákona. Jedná se o využití rodného čísla:

- a) jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí, nebo
- b) stanoví-li tak zvláštní zákon.

Citovaný § 13c zákona č. 133/2000 Sb. upravuje ještě třetí situaci, kdy je možné rodná čísla využívat, a to se souhlasem nositele rodného čísla nebo jeho zákonného zástupce [§ 13c písm. c) zákona č. 133/2000 Sb.]. Toto ustanovení však není výjimkou ze zásady podle § 13 odst. 7 zákona č. 133/2000 Sb., ale naopak jejím zohledněním či potvrzením.

Z hlediska zpracování rodného čísla zaměstnavateli je významný především citovaný § 13 písm. b) zákona č. 133/2000 Sb., který umožňuje zpracování rodného čísla tam, kde

¹⁵⁵ Schelle, K., Šmíd, V. Rodné číslo v informačních systémech. Právní rádce č. 11/2004, s. 45.

zaměstnavateli ze zvláštního zákona vyplývá povinnost poskytovat státním orgánům určité údaje ve formě či způsobem umožňujícím jednoznačnou identifikaci zaměstnanců v informačních systémech veřejné správy.

Z ustanovení § 13 písm. b) zákona č. 133/2000 Sb. lze tedy odvodit oprávnění zaměstnavatele evidovat rodná čísla zaměstnanců, a v některých případech i jejich rodinných příslušníků, ve svých evidencích. Příkladem povinnosti zaměstnavatele zpracovávat rodná čísla zaměstnanců je § 22 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, který ukládá zaměstnavateli povinnost vést pro účely nemocenského pojištění v rámci evidence o zaměstnancích také jejich rodná čísla, dále např. § 38j odst. 2 zákona č. 586/1992 Sb., o daních z příjmů, který stanoví, že mzdový list pro účely daně vedený zaměstnavatelem (jako plátcem daně) pro zaměstnance (jako poplatníky daně) musí obsahovat kromě jiných údajů také rodné číslo poplatníka a také rodné číslo osoby, na kterou poplatník uplatňuje nezdánitelnou část základu daně, anebo zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, který v § 10 ukládá zaměstnavateli oznamovací povinnost (týkající se např. nástupu zaměstnance do zaměstnání nebo změny nahlášených údajů), při jejímž plnění je povinen příslušné zdravotní pojišťovně sdělit mj. i rodné číslo zaměstnance, u něhož oznamovaná skutečnost nastala.

Zpracování rodného čísla v souladu s výjimkou uvedenou v § 13c písm. b) zákona č. 133/2000 Sb. je možné pouze tam, kde zvláštní zákon výslovně stanoví povinnost evidovat právě tento údaj. V případě, kdy je v právní normě uvedeno, že správce naplní svoji povinnost zpracováním rodného čísla nebo data narození,¹⁵⁶ měla by být tato volba, v souladu se základním principem, že k využívání rodného čísla je primárně oprávněn jeho nositel, ponechána na osobě, o jejíž údaje se jedná. Nicméně právní předpisy upravující využívání rodného čísla v souvislosti s pracovníprávními vztahy zaměstnance tuto volbu neumožňují, neboť výslovně stanoví povinnost zaměstnavatele zpracovávat v příslušných evidencích rodná čísla.

Již poměrně brzy po účinnosti zmíněné novely (zákona č. 53/2004 Sb.) se projevilo, že problematickou oblastí bude využívání rodného čísla v souladu s § 13c písm. c) zákona č. 133/2000 Sb., tedy na základě souhlasu jeho nositele.

Zákon č. 133/2000 Sb. totiž nestanoví žádné podmínky, za nichž lze rodné číslo na základě souhlasu jeho nositele zpracovávat, a tak vytváří situaci, kdy mnozí správci osobních údajů žádají rodná čísla v rámci smluvních vztahů (aniž by pro ně obvykle mělo rodné číslo jiný význam než jako efektivní evidenční pomůcka) s tím, že přistoupením ke

¹⁵⁶ Jak je tomu např. podle § 41c odst. 3 zákona č. 21/1992 Sb., o bankách, který ukládá bankám povinnost zabezpečit identifikaci vkladatele při vedení jeho účtu nebo při přijetí jeho vkladu a povinnost vést identifikační údaje o vkladateli ve své evidenci, přičemž u fyzických osob se identifikačními údaji rozumí jméno, příjmení, adresa a datum narození nebo rodné číslo, popřípadě identifikační číslo.

smlouvě subjekt údajů vyjadřuje svou vůli a tedy souhlasí s využitím rodného čísla ve smyslu § 13c písm. c) zákona č. 133/2000 Sb.

Rodné číslo je však bezesporu osobním údajem ve smyslu § 4 písm. a) ZOOÚ a jeho zpracování je tedy možné pouze při naplnění všech požadavků stanovených tímto zákonem pro zpracování „obyčejných“ osobních údajů. Ačkoli zákon č. 133/2000 Sb. na úpravu souhlasu se zpracováním osobních údajů v ZOOÚ neodkazuje, je nezbytné chápat ZOOÚ v otázce využívání rodných čísel jako *lex generalis* vůči zákonu č. 133/2000 Sb., a tedy tam, kde tento zákon nestanoví jinak, využít obecnou úpravu povinností při zpracování osobních údajů podle ZOOÚ.¹⁵⁷

Pokud se tedy určitý subjekt rozhodne rodná čísla pro svou činnost využívat na základě souhlasu jejich nositelů, musí tento souhlas vykazovat náležitosti souhlasu se zpracováním osobních údajů podle § 5 odst. 4 ZOOÚ a při shromažďování rodných čísel musí jejich nositele (tj. subjekty údajů) informovat v rozsahu podle § 11 ZOOÚ, a to zejména o tom, že poskytnutí rodného čísla je dobrovolné, resp. že není právní povinností subjektu údajů.¹⁵⁸

Tím však povinnosti těch, kteří hodlají využívat pro určitý účel rodná čísla, nekončí. Jestliže je rodné číslo osobním údajem, je potom ten, kdo jej využívá, správcem osobních údajů ve smyslu § 4 písm. j) ZOOÚ, na kterého se vztahují veškeré povinnosti stanovené ZOOÚ (popsané v kapitole 4). Tento správce osobních údajů musí tedy zejména v souladu s § 5 odst. 1 písm. a) ZOOÚ jasně vymezit účel zpracování rodného čísla, tedy konkrétní a legitimní důvod, proč hodlá při své činnosti rodná čísla využívat. Současně musí dbát, aby shromažďování rodných čísel k naplnění takto stanoveného účelu nebylo zjevně nadbytečné a tedy v rozporu s § 5 odst. 1 písm. d) ZOOÚ, nebo aby podle § 5 odst. 1 písm. f) ZOOÚ byla rodná čísla využívána pouze k účelu, k němuž byla původně shromážděna. V neposlední řadě je v tomto případě nezbytné splnit oznamovací povinnost vůči Úřadu pro ochranu osobních údajů podle § 16 ZOOÚ.

Vzhledem k tomu, že zpracování rodného čísla ukládají zaměstnavateli mnohé zvláštní zákony, ale zákoník práce mu tuto povinnost (až na jednu výjimku¹⁵⁹) nestanoví, je zpracování rodných čísel v dokumentech upravených tímto právním předpisem, např. v pracovní smlouvě nebo na potvrzení o zaměstnání, možné pouze v souladu s § 13c

¹⁵⁷ Z hlediska právní jistoty nositelů rodných čísel i těch, kteří rodná čísla využívají, je absence takového odkazu poměrně nešťastné řešení, neboť výkladem je nutné dojít k závěru, že je nezbytné použít úpravu obsaženou v ZOOÚ, avšak laikům tato skutečnost nemusí být vždy zřejmá a v praxi tak může v souvislosti se zpracováním rodných čísel snadno docházet k porušování povinností stanovených ZOOÚ.

¹⁵⁸ Zde vyvstává obtížně řešitelný problém, jestliže určitý subjekt poskytnutím rodného čísla podmíní např. uzavření smlouvy (typicky banky). Na jedné straně je zde tedy povinnost podle ZOOÚ informovat o (legitimním) účelu zpracování rodného čísla a dobrovolnosti jeho poskytnutí a na straně druhé však právo smlouvu v případě odmítnutí sdělení tohoto údaje neuzavřít, což staví subjekty údajů do složité situace.

¹⁵⁹ Jedná se o evidenci zaměstnanců, kteří vstupují do kontrolovaných pásem nebo konají práce s azbestem, s chemickými karcinogeny nebo biologickými činidly, kdy je zaměstnavatel podle § 134c odst. 4 zákoníku práce povinen vést v předmětné evidenci také rodná čísla těchto zaměstnanců.

písm. c) zákona č. 133/2000 Sb., tedy se souhlasem zaměstnance. Vzhledem k tomu, že rodné číslo není citlivým osobním údajem podle § 4 písm. b) ZOOÚ, pro jehož zpracování by bylo zapotřebí kvalifikovaného souhlasu, není nutné souhlas s jeho zpracováním vyjadřovat explicitně. Zaměstnanec vyjadřuje svoji vůli, tj. souhlas s využitím rodného čísla, např. podpisem pracovní smlouvy, v níž je rodné číslo uvedeno, to ovšem pouze za předpokladu, že je srozuměn s tím, že rodné číslo není obligatorní součástí daného dokumentu (tj. jestliže zaměstnavatel splnil svou informační povinnost podle § 11 ZOOÚ).

Jak bylo již několikrát uvedeno, je využití souhlasu se zpracováním osobních údajů v pracovněprávních vztazích diskutabilní, a proto je nezbytné, aby měl zaměstnanec vždy možnost se skutečně svobodně rozhodnout. V případě uchazečů o zaměstnání, by zaměstnavatelé neměli žádat rodná čísla vůbec, neboť v době, kdy ani není jisté, zda bude pracovněprávní vztah uzavřen, je zpracování tohoto údaje zcela nadbytečné.

Obecně však platí, že rodné číslo je určeno primárně pro identifikaci občana (případně cizince s povolením k pobytu na území ČR) vůči státním orgánům, které vedou evidence podle zvláštních zákonů. V soukromoprávních vztazích je vhodnější využívat jiné identifikátory, např. unikátní identifikační čísla generovaná pouze pro potřebu daného správce (např. zákaznická čísla nebo osobní čísla zaměstnanců).

Změna přístupu k využívání rodného čísla v praxi, tj. omezení využívání skutečně jen na nezbytné případy, však zřejmě nebude snadná ani rychlá. Doposud přetrvávají postupy, kdy jsou rodná čísla shromažďována čistě proto, že je to pro dané subjekty výhodnější než vytvářet vlastní identifikátory a usnadní si tak některé postupy anebo ze setrvačnosti stále využívají staré formuláře z dob, kdy ochraně osobních údajů nebyla věnována taková pozornost a rodné číslo se automaticky požadovalo v rámci téměř každého právního vztahu. Zákon č. 53/2004 Sb. proto obsahuje v čl. II přechodné ustanovení ukládající právnickým a fyzickým osobám, které do dne nabytí účinnosti tohoto zákona využívaly rodná čísla při plnění svých úkolů nebo v souvislosti s předmětem své činnosti, a nejde o případy uvedené v § 13c zákona č. 133/2000 Sb., povinnost rodná čísla z těchto informačních systémů a evidencí prokazatelně odstranit do 31. prosince 2005. Do tohoto data se využívání rodných čísel nepovažuje za neoprávněné nakládání s rodným číslem. Toto ustanovení se však vztahuje pouze na „staré“ evidence, které vznikly před 1. dubnem 2004, jakékoli shromažďování rodných čísel po tomto datu již musí být v souladu s § 13c zákona č. 133/2000 Sb. Jestliže tedy vede zaměstnavatel např. evidenci bývalých zaměstnanců za účelem sledování životních jubileí podle jejich rodných čísel, měl do 1. ledna 2006 buď zavést jiný identifikátor nebo získat souhlas takto evidovaných osob, nositelů rodných čísel, s využitím rodného čísla k danému účelu.

V souvislosti s popsanou novou úpravu využívání rodných čísel byly zákonem č. 53/2004 Sb. zavedeny také nové skutkové podstaty přestupků a jiných správních deliktů

(§ 17d a § 17e zákona č. 133/2000 Sb.), přičemž projednáním a sankcionováním posledně jmenovaných je na základě § 17e odst. 4 zákona č. 133/2000 Sb. pověřen Úřad pro ochranu osobních údajů (viz kapitola 6).

5.3. Kontrola práce zaměstnance a ochrana osobních údajů

Osobní počítač s přístupem k Internetu, telefonní linka, mobilní telefon nebo elektronická pošta patří v současné době k naprosto standardnímu vybavení velké většiny pracovišť. Kdo ze zaměstnanců občas uvedené prostředky nevyužije k tomu, aby si vyřídil nějakou soukromou záležitost, např. zavolal z práce svým příbuzným nebo známým nebo jim napsal e-mail? V zájmu zaměstnavatele však logicky je, aby zaměstnanci plně využívali pracovní dobu i pracovní prostředky k plnění svých pracovních úkolů a nikoli pro své soukromé účely. To, zda a jak jeho zaměstnanci své úkoly plní, jak hospodaří se svěřenými prostředky, jak ochraňují jeho majetek nebo zda nejednají v rozporu s jeho zájmy, má zaměstnavatel bezesporu právo také kontrolovat (např. podle § 9 odst. 3 zákoníku práce).

Aktuální otázkou však je, jakým způsobem může zaměstnavatel tuto kontrolu provádět. V době, kdy jsou široké veřejnosti dostupná nejrůznější monitorovací zařízení, vyvstává automaticky problém legálnosti jejich využití. Může zaměstnavatel kontrolovat práci svých zaměstnanců pomocí moderní telekomunikační techniky? Je oprávněn, a případně do jaké míry, kontrolovat obsah došlých zásilek, monitorovat činnost zaměstnanců kamerovým systémem nebo sledovat využívání Internetu a elektronické pošty? A naopak do jaké míry má zaměstnanec právo na soukromí na pracovišti, tedy v rámci pracovněprávního vztahu? Zde se střetávají práva a oprávněné zájmy zaměstnavatele s oprávněným očekáváním zaměstnance. Nejlepší řešení uvedených otázek je potom to, které šetří práva obou stran a vytváří mezi nimi určitou rovnováhu.

Vzhledem k tomu, že zákoník práce otázku ochrany soukromí zaměstnanců v podstatě neřeší,¹⁶⁰ je nutné podpůrně aplikovat úpravu ochrany osobnosti podle občanského zákoníku, neboť zaměstnanec samozřejmě na pracovišti svá osobnostní práva nepozbývá. Tam, kde jsou zaměstnavatelem zpracovávány osobní údaje zaměstnanců, je ochrana soukromí zaměstnance zajištěna také ZOOÚ.¹⁶¹

Zásady kontroly používání a využívání pracovních prostředků svěřených zaměstnanci by měly být jednoznačně vymezeny buď v pracovní smlouvě, nebo v interních předpisech

¹⁶⁰ Zákoník práce upravuje pouze zásadu rovného zacházení se zaměstnanci (v § 1 odst. 3), právo odborových orgánů vykonávat u příslušného zaměstnavatele kontrolu dodržování pracovních i interních předpisů (v § 22 odst. 2) a právo zaměstnance domáhat se u soudu opravy obsahu potvrzení o zaměstnání nebo pracovního posudku (v § 60 odst. 4).

¹⁶¹ Zaměstnanec je pro zaměstnavatele osobou bezesporu identifikovanou, a proto je osobním údajem ve smyslu § 4 písm. a) ZOOÚ v podstatě jakákoli informace týkající se zaměstnance, a proto je v pracovních vztazích možnost aplikace ZOOÚ poměrně široká, a to i v oblasti monitorování činnosti zaměstnanců.

zaměstnavatele, přičemž vzájemná dohoda zaměstnance a zaměstnavatele se jeví jako nejvhodnější řešení, kdy lze formu a podmínky této kontroly v rozumné míře vymezit, a tak mj. i předejít negativním reakcím ze strany zaměstnanců na jednostranně přijatá opatření. V této souvislosti je však nutno připomenout, že na základě čl. 1 Listiny jsou základní práva a svobody, mezi něž právo na lidskou důstojnost, právo na ochranu před zasahováním do soukromého života nebo právo na zachování listovního tajemství patří, nezadatelná, nezczitelná, nepromlčitelná a nezrušitelná. Zaměstnanec se tedy nemůže těchto svých práv v rámci smlouvy se zaměstnavatelem platně vzdát, např. nemůže souhlasit s tím, že zaměstnavatel bude automaticky kontrolovat obsah veškeré elektronické pošty došlé na jemu přidělenou adresu.¹⁶²

Základním východiskem pro hodnocení opatření přijatých zaměstnavatelem při kontrole činnosti zaměstnanců, je několik významných rozhodnutí Evropského soudu pro lidská práva (dále jen „Evropský soud“), který byl zřízen na základě čl. 19 Evropské úmluvy. Tento soud se již několikrát ve svých judikátech zabýval obsahem práva na respektování soukromého a rodinného života, obydlí a korespondence,¹⁶³ které je zaručeno v čl. 8 Evropské úmluvy. Stěžejním judikátem k této problematice je rozhodnutí ve věci Niemietz v. Německo (z roku 1992), kde Evropský soud vyslovil, že přesně oddělit soukromý a profesionální život není dost dobře možné, neboť právě v rámci svých pracovních aktivit má většina lidí největší příležitost navazovat a rozvíjet vztahy s vnějším okolím, a proto právo na respektování soukromého života zahrnuje i právo na respektování soukromí v zaměstnání. Tento názor zopakoval Evropský soud v témže roce ještě v rozhodnutí Cambell v. Spojené království, v němž vyslovil, že ochraně soukromí podléhá i korespondence profesní povahy. Rozhodnutím ve věci Halford v. Spojené království (z roku 1997) Evropský soud judikoval, že i v rámci pracovních vztahů je každý oprávněn očekávat jistou míru soukromí a monitorování činnosti (v daném případě odposlouchávání telefonních hovorů za účelem získání informací pro probíhající pracovněprávní spor) bez legálního podkladu a předchozího oznámení tohoto úmyslu je porušením čl. 8 Evropské úmluvy.¹⁶⁴

Z citovaných rozhodnutí Evropského soudu jednoznačně vyplývá, že zaměstnanec svá práva na ochranu soukromí, a tedy i osobních údajů, neztrácí každé ráno při příchodu do práce, ale naopak má právo do určité míry očekávat respektování svého soukromí i na pracovišti. Tato „určitá míra“ je dána nezbytným kompromisem mezi tímto oprávněným

¹⁶² Takový úkon zaměstnance by byl neplatný i podle § 242 odst. 1 písm. c) zákoníku práce.

¹⁶³ Přičemž pod pojmem korespondence je dle Evropského soudu nutno rozumět nejen „papírové“ dopisy, ale i veškeré formy komunikace, včetně telefonních hovorů nebo e-mailových zpráv (viz rozhodnutí Halford v. Spojené království, www.echr.coe.int). Mladší Charta základních práv Evropské unie (z roku 2000) již nové technické možnosti zohledňuje a v čl. 7 zakotvuje právo na respektování všech forem komunikace.

¹⁶⁴ Evropský soud tyto své postoje opakovaně potvrzuje i v dalších svých rozhodnutích např. Amann v. Švýcarsko nebo Leander v. Švédsko. Znění citovaných rozhodnutí (www.echr.coe.int).

očekáváním zaměstnance na straně jedné a právy a zájmy zaměstnavatele na straně druhé (zejména jeho práva kontrolovat činnost svých zaměstnanců a práva chránit svůj majetek).

Uvedené základní východisko by měl každý zaměstnavatel při přijímání opatření, jejichž cílem je kontrola práce zaměstnanců respektovat. Konkrétní postupy zaměstnavatele budou vždy ovlivněny podmínkami na daném pracovišti, nicméně lze vymezit určité obecné zásady pro přístup zaměstnavatele k této problematice (z hlediska ochrany osobních údajů zaměstnanců), a to zejména na základě dokumentů vypracovaných orgány a pracovními skupinami působícími v rámci Evropské unie.¹⁶⁵

Jestliže zaměstnavatel zamýšlí vykonávat kontrolu práce zaměstnanců prostřednictvím určitých monitorovacích zařízení, měl by nejdříve, ještě před jejich zavedením v praxi, důkladně zvážit některé otázky,¹⁶⁶ a to:

- a) zda je přijetí těchto opatření skutečně nezbytné, tedy zda nelze obdobných výsledků dosáhnout tradičními metodami (otázka proporcionality)¹⁶⁷ a
- b) zda jsou zaměstnanci s tímto úmyslem zaměstnavatele a podmínkami, za nichž bude k monitorování práce zaměstnanců a případnému zpracování osobních údajů s tím spojenému docházet, dostatečně obeznámeni (otázka transparentnosti).¹⁶⁸

Úpravou zpracování osobních údajů získaných v souvislosti s monitorováním práce zaměstnanců se zabývá také Mezinárodní organizace práce („MOP“) ve svém Kodexu o ochraně osobních údajů zaměstnanců¹⁶⁹ z roku 1997, ve kterém MOP formuluje základní standardy, jimiž by se zaměstnavatelé měli při zpracování osobních údajů zaměstnanců řídit. Jakékoli monitorování činnosti zaměstnanců by se mělo dle čl. 6.14 uvedeného dokumentu dít pouze za současného splnění dvou podmínek:

- a) zaměstnanci jsou o této skutečnosti předem řádně informováni, včetně důvodů, časového rozvržení sledování, použitých technických prostředků a využití takto získaných dat a
- b) zaměstnavatel zvolí takové prostředky, které budou co nejméně zasahovat do soukromí zaměstnanců.

Nepřetržité či utajené sledování činnosti zaměstnanců musí být dle MOP podrobena ještě přísnějším požadavkům. Nepřetržité sledování zaměstnanců je, vzhledem k tomu, že může

¹⁶⁵ V oblasti ochrany osobních údajů se jedná především o již dříve zmíněnou pracovní skupinu zřízenou podle čl. 29 Směrnice 95/46 - Pracovní skupinu 29.

¹⁶⁶ Vyjádření Pracovní skupiny 29 ke sledování elektronické komunikace na pracovišti ze dne 29. května 2002 (Working document on the surveillance of electronic communications in the workplace), www.europa.eu.int. Některá ustanovení tohoto dokumentu (v anglickém jazyce) jsou obsahem Přílohy IV.

¹⁶⁷ Z hlediska ZOOÚ se jedná o plnění povinností stanovit účel zpracování osobních údajů a jemu odpovídající prostředky a s tím spojené povinnosti zpracovávat osobní údaje pouze v rozsahu nezbytném pro naplnění stanoveného účelu – tj. povinností podle § 5 odst. 1 písm. a), b) a d) ZOOÚ.

¹⁶⁸ Tj. otázka splnění informační povinnosti podle § 11 ZOOÚ.

¹⁶⁹ Code of Practice on protection of workers' personal data (www.unionnetwork.org).

vést ke stresu a s ním spojeným zdravotním komplikacím, obvykle přípustné pouze, je-li nezbytné k ochraně zdraví a bezpečnosti zaměstnanců nebo majetku. Utajené sledování lze v souladu se standardy MOP připustit jen, jestliže je v souladu s právní úpravou nebo pokud má zaměstnavatel vážné podezření na trestnou činnost zaměstnance nebo jiné závažné porušování pravidel (například tzv. sexual harassment).

Citované standardy MOP dále doporučují (v čl. 12) konzultovat zavedení automatického zpracování osobních údajů zaměstnanců nebo elektronických monitorovacích prostředků a jejich účel a možnosti využití se zástupci zaměstnanců, a tím vymezit způsob provádění kontroly tak, aby byl pro obě strany přijatelný.

Z hlediska aplikace ZOOÚ je podstatné, že při sledování činnosti zaměstnanců (tradičními způsoby i pomocí elektronických zařízení) shromažďuje zaměstnavatel informace o činnosti zaměstnanců, tj. osob, které jsou vůči němu zcela jistě identifikovány nebo identifikovatelné, a tak zpracovává osobní údaje ve smyslu § 4 písm. a) ZOOÚ. Vzhledem k uvedenému musí zaměstnavatel při této činnosti postupovat také v souladu se ZOOÚ, což znamená plnit veškeré povinnosti správce osobních údajů popsané v předchozí kapitole.

Zaměstnavatel tedy musí zvolit takové prostředky, které zasahují do soukromí zaměstnanců co nejméně (umožňují získání pouze nezbytných dat), přičemž by se měl obvykle vyvarovat prostředků umožňujících soustavné nebo utajené sledování. Tam, kde lze stejného cíle dosáhnout pomocí tradičních postupů, by monitorovací zařízení neměla být zaváděna vůbec. Zvolený cíl kontroly zaměstnanců musí být legální a legitimní, zejména nesmí zasahovat do základních práv zaměstnanců. Takovým cílem je např. ochrana zájmů zaměstnavatele proti hrozbám jako je zpřístupnění důvěrných informací konkurenci, majetková trestná činnost zaměstnanců nebo ochrana informačních systémů před viry nebo jiným poškozením.

Dalším základním požadavkem vyplývajícím ze ZOOÚ je transparentnost jednání zaměstnavatele, což zahrnuje jednak poskytnutí úplných a pravdivých informací zaměstnancům a jednak případné oznámení dozorovému orgánu (tj. oznámení o zpracování osobních údajů Úřadu podle § 16 ZOOÚ). Zaměstnanci by měli být informováni především o důvodech a cílech sledování jejich činnosti na pracovišti a o tom, kdo je kontrole podroben, jakým způsobem a kdy nebo za jakých okolností je prováděna a dále jakým způsobem bude řešeno zjištěné porušení pravidel, tj. jak budou osobní údaje shromážděné tímto způsobem využívány.

Zaměstnavatel je také povinen umožnit zaměstnancům přístup k osobním údajům, které o nich v souvislosti s monitorováním jejich činnosti zpracovává, a o tomto jejich právu a dále o právu žádat nápravu případného vadného stavu je musí poučit. Informace získané při monitorování činnosti zaměstnanců mohou být uchovávány pouze po dobu nezbytnou k dosažení stanoveného účelu, jejíž délka by se měla obecně pohybovat v řádu několika dní

potřebných pro zjištění, zda došlo či nedošlo ke sledovanému jevu, a jaké byly jeho okolnosti. Samozřejmostí je také přijetí adekvátních bezpečnostních opatření k ochraně takto shromážděných osobních údajů.

Výkon kontroly činnosti zaměstnanců na pracovišti je postupem v souladu se zákoníkem práce, a tedy i v případě, kdy zaměstnavatel k této kontrole využívá technické prostředky, jedná se o postup v souladu s § 5 odst. 2 písm. a) ZOOÚ. Zaměstnavatel tedy nepotřebuje ke zpracování osobních údajů, ke kterému při monitorování činnosti zaměstnanců nezbytně dochází, souhlas zaměstnanců. Aplikovat lze případně i ustanovení § 5 odst. 2 písm. e) ZOOÚ, neboť zavedením opatření určených ke sledování činnosti zaměstnanců, případně i jiných osob, které se na pracovišti pohybují, může zaměstnavatel sledovat ochranu svých práv a právem chráněných zájmů, zejména ochranu majetku. Obvykle bude také možné aplikovat ustanovení § 18 odst. 1 písm. b) ZOOÚ¹⁷⁰ a zaměstnavatel tedy nebude povinen oznamovat předmětné zpracování osobních údajů Úřadu pro ochranu osobních údajů podle § 16 ZOOÚ.¹⁷¹

Případné zpracování citlivých osobních údajů prostřednictvím monitorování činnosti zaměstnanců (ve smyslu monitorování jejich aktivit zaměřené speciálně na zpracování citlivých údajů) by bylo z hlediska ZOOÚ problematické, neboť účel takového zpracování by zřejmě nebyl legitimní a zaměstnavatel by jej tedy nemohl uskutečnit ani na základě souhlasu zaměstnanců. Ustanovení § 9 písm. d) ZOOÚ, umožňující zpracovávat citlivé osobní údaje potřebné pro plnění povinností zaměstnavatele v oblasti pracovního práva a zaměstnanosti bez souhlasu subjektů údajů, také nelze v uvedené situaci aplikovat, neboť potřebné citlivé osobní údaje zaměstnanců může zaměstnavatel získat vhodnějšími prostředky než technickým zařízením určeným k monitorování jejich činnosti. Shromáždění citlivých osobních údajů tak přichází v úvahu pouze jako vedlejší produkt kontroly činnosti zaměstnanců, kdy platí, že pokud je zaměstnavatel dále nezpracovává, jsou tyto údaje údají shromážděnými nahodile ve smyslu § 3 odst. 4 ZOOÚ, na něž se ochrana poskytovaná tímto zákonem nevztahuje.

Při kontrole využívání jednotlivých komunikačních prostředků je třeba zohlednit jak specifika těchto technických prostředků, tak i situaci na daném pracovišti. Nicméně lze zmínit několik základních východisek a požadavků, které by měl zaměstnavatel v souvislosti s ochranou soukromí a osobních údajů při kontrole elektronické komunikace nebo při instalování kamerových systémů uvážit.

¹⁷⁰ Tj. výjimka z oznamovací povinnosti v případě, kdy je zpracování osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona.

¹⁷¹ Zpracování osobních údajů v rámci tradičních metod kontroly činnosti zaměstnanců a při aplikaci technických zařízení pro kontrolu využívání přístupu k Internetu a elektronické poště lze považovat za zpracování potřebné k uplatnění práv zaměstnavatele vyplývajících ze zvláštního zákona.

Co se týče připojení k Internetu, je zcela na rozhodnutí zaměstnavatele, v jakém rozsahu zaměstnancům umožní jeho využití pro soukromé účely.¹⁷² Zaměstnavatel tak může přistoupit i k úplnému zákazu využití Internetu k jiným než čistě pracovním aktivitám, což však v současné době nelze považovat za vhodné řešení mj. proto, že takový požadavek je do značné míry nerealistický (obdobně jako by byl např. zákaz hovoru s kolegy na jiné než pracovní téma). Zaměstnavatel by měl vždy jasně vymezit podmínky využití připojení k Internetu, případné zákazy přístupu k určitým stránkám a rozsah, v jakém je přístup k Internetu sledován (např. zda je monitoring zaměřen vůči jednotlivcům nebo sekcím či oddělením), tedy způsob zajištění detekce porušení daných pravidel. O těchto pravidlech by měl zaměstnavatel zaměstnance náležitě informovat, opět nejlépe formou vnitřních předpisů nebo ustanovení v pracovní smlouvě. Dále by měl zaměstnance seznámit s tím, jakým způsobem bude naloženo s osobními údaji, které tímto monitorováním získá,¹⁷³ tedy k jakému účelu budou zpracovány, a také jak dlouho budou pořízené informace uchovávány.

Obecně platí, že zaměstnavatel by měl vždy upřednostnit preventivní opatření proti zneužití přístupu k Internetu před následným monitorováním takového zneužití [dle zásady zpracovávat vždy jen minimální rozsah osobních údajů vyplývající z § 5 odst. 1 písm. d) ZOOÚ]. Určité kategorie webových stránek lze např., místo sledování přístupu k nim, přímo blokovat nebo lze instalovat automatické výstrahy, které se při otevření příslušných stránek zaměstnanci zobrazí. Obvykle může být zneužití přístupu k Internetu zjištěno i bez znalosti obsahu navštívených stránek (podle času stráveného touto činností) nebo podle stránek nejčastěji navštěvovaných zaměstnanci určitého úseku jako celku. Jestliže z této obecné kontroly využívání Internetu, zaměřené na sledování času nebo na skupinu zaměstnanců, vyplyne podezření z porušování stanovených pravidel, může zaměstnavatel následně přijmout adekvátní opatření, např. ve formě dalšího sledování již více zaměřeného na konkrétní osoby.

Zaměstnavatel by měl zaměstnanci vždy bezprostředně oznámit jakékoli zjištění neoprávněného využití Internetu a před tím, než tuto informaci využije jako podklad pro určité své rozhodnutí, by měl dát zaměstnanci možnost se k danému zjištění vyjádřit, neboť je nutno brát v úvahu i fakt, že mnohé stránky lze navštívit nevědomky nebo nechtěně. Ohrožením zájmů zaměstnavatele také jistě není, pokud zaměstnanec občas sleduje zpravodajství nebo si vyhledá nějakou informaci, pokud své pracovní úkoly plní dostatečně rychle a v potřebné kvalitě.

¹⁷² Také touto problematikou se zabývala Pracovní skupina 29 ve svém Vyjádření ke sledování elektronické komunikace na pracovišti ze dne 29. května 2002 (Working document on the surveillance of electronic communications in the workplace), www.europa.eu.int. Viz Příloha IV.

¹⁷³ Jestliže zaměstnavatel monitoruje činnost konkrétního zaměstnance, potom veškeré informace, které takto získá, jsou osobními údaji ve smyslu § 4 písm. a) ZOOÚ a na jejich zpracování je nutno aplikovat režim tímto zákonem stanovený.

Každé monitorování přístupu zaměstnanců k Internetu, tj. zvolené postupy a prostředky, musí odpovídat rizikům, která zaměstnavateli ze zneužití přístupu k Internetu hrozí. Současné technologie jistě umožňují zaměstnavateli chránit své zájmy a současně i soukromí zaměstnanců. Zaměstnavatel by měl z nabízených možností vybrat vždy tu, která za daných okolností umožňuje co největší ochranu soukromí zaměstnanců.

Další oblastí je kontrola korespondence zaměstnance, a to jak té klasické, tak i té elektronické.¹⁷⁴ Zde je však právo zaměstnavatele kontrolovat jakým způsobem využívají zaměstnanci pracovní dobu a pracovní prostředky značně limitováno ochranou listovního tajemství zaručenou v čl. 13 Listiny. Povinnost zachovávat listovní tajemství se vztahuje na každého, tedy i na zaměstnavatele, a zaměstnanec (v souladu s čl. 1 Listiny) nemůže platně souhlasit s omezením či zrušením svého práva na ochranu obsahu jeho korespondence, včetně té elektronické. Případné porušení listovního tajemství může vést i k naplnění skutkové podstaty trestného činu porušování tajemství dopravovaných zpráv (podle § 239 a 240 zákona č. 141/1961 Sb., trestní zákon).

Vzhledem k tomu, že informace obsažené v doručených či odeslaných písemnostech a zprávách obvykle naplňují definici osobního údaje podle § 4 písm. a) ZOOÚ (neboť se vztahují k identifikované či identifikovatelné osobě – zaměstnanci), je obsah dopisů či elektronických zpráv chráněn i tímto zákonem. Ačkoli ve vztahu k ochraně osobních údajů obecně platí, že data je možno zpracovávat pouze na základě zákonného zmocnění nebo souhlasu dotčené osoby, v daném případě nelze souhlasem zaměstnance prolomit nezadatelné, ústavně zaručené právo. Zaměstnavatel tak má sice právo kontrolovat činnost svých zaměstnanců, nikoli ale obsah jim doručených nebo jimi odesílaných dopisů či e-mailů.

Pro náležitou ochranu obsahu dopisů doručených do sídla zaměstnavatele či došlých prostřednictvím technických zařízení v jeho vlastnictví je zásadní správné rozlišení, zda je doručená pošta určena zaměstnavateli či zda se jedná o zásilku či zprávu určenou konkrétnímu zaměstnanci.¹⁷⁵

V případě klasických poštovních zásilek byla otázka, zda je doručená písemnost určena primárně zaměstnavateli nebo konkrétnímu zaměstnanci, řešena vyhláškou č. 286/2004 Sb., kterou se stanoví poštovní podmínky základních služeb a základní požadavky kvality při jejich zajišťování držitelem poštovní licence (vyhláška o základních službách držitele poštovní licence), kterou vydalo Ministerstvo informatiky k provedení zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách). Citovaná vyhláška stanovila pravidlo, že je-li na prvním místě adresy uvedena obchodní firma či jméno zaměstnavatele, je doručená zásilka určena jemu a naopak, je-li na prvním

¹⁷⁴ Otázce kontroly elektronické korespondence se mj. věnuje i Úřad pro ochranu osobních údajů ve svém stanovisku k problémům z praxe č. 1/2003 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců (www.uoou.cz)

¹⁷⁵ V případě odesílaných zásilek a zpráv platí přiměřeně totéž, nicméně situace je zde o poznání jednodušší.

nepřípustné, aby zaměstnavatel bez vědomí zaměstnance monitoroval poštu doručenou a odeslanou prostřednictvím této adresy.

Při kontrole využití elektronické pošty by se měl zaměstnavatel primárně omezit na zpracování údajů o počtu odeslaných a obdržených zpráv, případně typu jejich příloh nebo čase stráveném touto činností, což současné technologie zaměstnavateli umožňují. Jak bylo uvedeno již výše, obsah zpráv zásadně kontrolovat nesmí. V úvahu je dále nutno brát právo na ochranu soukromí té osoby, která je „na druhé straně“, a která o sledování využívání elektronické pošty a stanovených podmínkách informována není.

Kromě již uvedeného trestného činu porušování tajemství dopravovaných zpráv může nevhodným přístupem ke kontrole využívání elektronické pošty zaměstnanci dojít také k naplnění skutkové podstaty trestného činu poškození a zneužití záznamu na nosiči informací (podle § 257a zákona č. 140/1961 Sb., trestní zákon).

Zaměstnavatelem přidělený telefon, ať již pevná linka nebo mobilní přístroj, je dalším technickým prostředkem, který dnes při své pracovní činnosti využívá naprostá většina zaměstnanců. Způsob jeho využití tak může být další oblastí, kterou může zaměstnavatel kontrolovat, přičemž i zde platí, že zaměstnanec má právo na zachování určité míry soukromí i na pracovišti. Zásady ochrany soukromí, vymezené zejména judikaturou Evropského soudu, se uplatní bez ohledu na to, zda zaměstnanec právě vyřizuje soukromé či pracovní záležitosti.¹⁷⁸

Obdobně jako v případě připojení k Internetu nebo využití elektronické pošty v zaměstnání by měl zaměstnavatel v první řadě jednoznačně vymežit, za jakých podmínek je využití tzv. služebního telefonu možné k soukromým účelům, neboť i zde platí, že absolutní zákaz takového využití je nereálný, až kontraproduktivní.

Při provádění kontroly plnění těchto podmínek by potom měl zaměstnavatel shromažďovat pouze data nezbytná k identifikaci uživatele daného přístroje, typu uskutečněných hovorů (zda jde o lokální či meziměstské hovory apod.), jejich délky a ceny a volaného čísla.¹⁷⁹ Pokud se tyto údaje týkají přístroje, který využívá pouze jeden zaměstnanec, jedná se o osobní údaje ve smyslu § 4 písm. a) ZOOÚ, které podléhají režimu tímto zákonem stanovenému. S ohledem na právo zaměstnavatele kontrolovat činnost zaměstnanců během pracovní doby a způsob jakým hospodaří se svěřenými prostředky, je takové zpracování osobních údajů zaměstnanců (pokud je prováděno adekvátními prostředky a přiměřeném rozsahu) v souladu se ZOOÚ, a to zejména podle § 5 odst. 2 písm. e) tohoto zákona i bez souhlasu dotčených zaměstnanců.

¹⁷⁸ To, že se ochrana soukromí vztahuje ve stejném rozsahu na soukromé i obchodní telefonáty stanovil Evropský soud ve svém rozhodnutí ve věci *Huvig v. Francie* z roku 1989 (www.echr.coe.int).

¹⁷⁹ Tyto údaje získá zaměstnavatel obvykle prostřednictvím výpisů od provozovatele dané sítě či poskytovatele služby.

Nepřípustným by však již bylo např. tajné sledování nebo nahrávání hovorů, neboť tajemství zpráv dopravovaných telefonem je chráněno obdobně jako listovní tajemství podle čl. 13 Listiny. Dále je třeba zmínit, že právo zaměstnavatele kontrolovat výpisy hovorů neznámá, že zaměstnavatel má právo zjišťovat neznámá čísla např. tak, že by na ně volal.¹⁸⁰ V případě zjištění jakýchkoli nesrovnalostí by měl zaměstnavatel nejprve požadovat vysvětlení dotyčného zaměstnance, až poté přistupovat k určitým opatřením či závěrům.

Při monitorování využívání telefonů zaměstnanci by se měl zaměstnavatel řídit všemi výše uvedenými obecnými pravidly, zejména tedy využívat postupy a opatření, které zasahují do soukromí zaměstnanců co nejméně a jejichž využitím shromáždí co nejmenší kvantum osobních údajů.

V souvislosti s tím, jak jsou nejrůznější technická zařízení stále lépe dostupná široké veřejnosti, je v současné době další aktuální problematikou monitorování prostranství v okolí budov i jejich interiérů pomocí kamerových systémů. Úvodem je nutno zdůraznit, že narozdíl od výše popsaných oblastí, tj. sledování využití telefonů nebo přístupu na Internet, kdy je zpracování osobních údajů zaměstnanců s tím spojené (v rozsahu nezbytném pro zajištění kontroly jejich činnosti), právem zaměstnavatele, instalaci kamer na pracovišti nelze provést bez souhlasu zaměstnanců, kteří se na daném pracovišti pohybují.¹⁸¹

Jak bylo již několikrát zmíněno, dochází při monitorování činnosti zaměstnanců ke zpracování osobních údajů a na veškerá tímto způsobem pořízená data se tedy vztahuje režim stanovený ZOOÚ.¹⁸² V případě sledování využívání elektronické pošty, Internetu nebo telefonu lze, při splnění uvedených požadavků vyplývajících ze ZOOÚ, takové zpracování osobních údajů považovat za zpracování nezbytné pro ochranu práv a právem chráněných zájmů zaměstnavatele, který dané technické prostředky vlastní, a tedy má právo kontrolovat jejich využití. Zaměstnavatel tak v souladu s § 5 odst. 2 písm. e) ZOOÚ může přijmout potřebná opatření a zpracovávat jejich prostřednictvím osobní údaje zaměstnanců, aniž by musel disponovat jejich souhlasem podle § 5 odst. 4 ZOOÚ.

Monitorování určitých prostor kamerami lze však stěží označit za nezbytné k ochraně práv nebo zájmů zaměstnavatele, a to zejména proto, že obvykle lze stejného účelu dosáhnout prostředky, které do soukromí zaměstnanců, případně dalších osob, které se na pracovišti vyskytují, nezasahují, resp. zasahují v menší míře. Instalaci kamerového systému tak může zaměstnavatel v souladu se základní zásadou ochrany osobních údajů, vyjádřenou v § 5 odst. 2 ZOOÚ, uskutečnit pouze s předchozím souhlasem zaměstnanců. Žádost o

¹⁸⁰ Hyška, M. Velký bratr zaměstnavatel. Lidové noviny, 25. května 2005, s. 1.

¹⁸¹ Úřad pro ochranu osobních údajů připravuje v současné době k problematice zpracování osobních údajů prostřednictvím kamerových systémů stanovisko.

¹⁸² Prostřednictvím kamer jsou shromažďovány informace o osobách, které jsou pro zaměstnavatele identifikované či identifikovatelné, a tyto informace tak naplňují definici osobního údaje podle § 4 písm. a) ZOOÚ.

tento souhlas musí být samozřejmě provázena patřičnými informacemi o důvodech, které zaměstnavatele k přijetí takového opatření vedou, o tom, jakým způsobem bude monitorování probíhat nebo jakým způsobem bude nakládáno s pořízenými záběry, tj. jak budou využívány a zda a jak dlouho budou uchovávány. Jinými slovy zaměstnanec musí před udělením souhlasu obdržet informace v rozsahu vymezeném v § 11 ZOOÚ. Další povinností, kterou musí zaměstnavatel, ještě předtím než začne prostřednictvím kamer osobní údaje shromažďovat, splnit, je oznamovací povinnost vůči Úřadu pro ochranu osobních údajů podle § 16 ZOOÚ.¹⁸³

Problematika souhlasu zaměstnanců se zpracováním osobních údajů byla již několikrát zmíněna výše (viz kapitola 4.1). Považovat určitý právní úkon zaměstnance za souhlas se zpracováním osobních údajů podle ZOOÚ, je možné pouze, pokud mu bylo umožněno se skutečně svobodně rozhodnout, o čemž by však bylo v podmínkách mnoha pracovně právních vztahů možné s úspěchem pochybovat.

Zpracováním osobních údajů prostřednictvím kamer se věnuje také Pracovní skupina 29, která se k této otázce vyjádřila ve svém stanovisku č. 4/2004.¹⁸⁴ V rámci pracovního poměru by dle tohoto dokumentu měly být kamerové systémy zaměřené na kontrolu kvality či objemu práce jednotlivých zaměstnanců zpravidla nepřipustné. Naopak v souladu s principy ochrany soukromí a osobních údajů může být instalace monitorovacího zařízení, je-li účelem sledování bezpečnosti práce nebo ochrana majetku zaměstnavatele nebo zaměstnanců (to však zejména sledováním vnějších prostor a vstupů do budov; v případě vnitřních uzamykatelných prostor by instalace kamer byla účelná pouze za určitých okolností, jako např. pohybuje-li se v daném prostoru velký počet osob, a pouze v těch místnostech, které nejsou určeny pro čistě soukromé potřeby).

Pro hodnocení adekvátnosti instalace kamer je dále významná technická úroveň zvoleného systému. Z hlediska ochrany soukromí zaměstnanců je jistě rozdíl v tom, zda je využíváno technicky jednoduché zařízení anebo např. digitální kamery s možností velkého rozlišení a s propojením na výpočetní techniku. Zvláštní pozornost je také třeba věnovat včasné likvidaci pořízených záběrů, která by měla (pokud pořízené záběry nevypovídají např. o trestné činnosti nebo o úrazu zaměstnance) obvykle proběhnout v rámci hodin, maximálně několika dnů, nikoli týdnů.

Obecně by však zaměstnavatel měl k instalaci kamer či kamerového systému přistoupit až jako k meznímu řešení, neboť – z hlediska ochrany soukromí – se jedná o prostředek,

¹⁸³ Úřad věnuje v poslední době, v souvislosti s rozmachem těchto postupů, oznámení týkající se instalace kamerového systému zvýšenou pozornost a v souladu se svou pravomocí podle § 17 ZOOÚ důsledně sleduje, zda by v daném případě zpracováním osobních údajů nedocházelo k porušení pravidel stanovených ZOOÚ, tj. k nedůvodnému zásahu do soukromí osob.

¹⁸⁴ Stanovisko č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování (Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance), www.europa.eu.int. Toto stanovisko je uvedeno v Příloze V.

který je vzhledem k obvyklým oprávněným zájmům zaměstnavatelů neadekvátní. Prostřednictvím kamer je o zaměstnancích a ostatních osobách pohybujících se v daném prostoru obvykle shromažďováno větší množství údajů, než zaměstnavatel nezbytně potřebuje např. pro ochranu svého majetku (což je zřejmě nejobvyklejší důvod, proč subjekty k instalaci kamer přistupují).

S ohledem na to, že s vývojem stále nových technologií se budou vyvíjet i nejrůznější monitorovací prostředky, a dále vzhledem k tomu, že určité procento zaměstnavatelů bude vždy zřejmě inklinovat k tomu, mít nad svými zaměstnanci maximální kontrolu, je zřejmé, že výše naznačená problematika ochrany soukromí na pracovišti, a tedy i osobních údajů zaměstnanců zpracovávaných v souvislosti s monitorováním činnosti zaměstnanců bude nabývat na významu. Úřad pro ochranu osobních údajů se tak jistě bude této problematice věnovat intenzivněji, jak ve svých stanoviscích či vyjádřeních k problémům z praxe, tak i ve své kontrolní činnosti.

6. Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů byl zřízen ustanovením § 2 ZOOÚ, jakožto ústřední správní úřad¹⁸⁵ pro oblast ochrany osobních údajů se sídlem v Praze.¹⁸⁶

Existence orgánu, který dohlíží na plnění povinností směřujících k ochraně osobních údajů a má pravomoc jejich plnění případně i vymáhat, je nezbytným prvkem efektivní ochrany osobních údajů. Zřízení obdobného orgánu je ostatně jedním ze základních požadavků jak Úmluvy 108 (čl. 13), tak i Směrnice 95/46 (čl. 28), a tím i jednou z podmínek přijetí České republiky do Evropské unie. Existence Úřadu pro ochranu osobních údajů je dále nezbytná z hlediska začlenění ČR do Schengenského systému, neboť čl. 114 tzv. Schengenské Prováděcí úmluvy¹⁸⁷ ukládá smluvním stranám zřídit kontrolní orgán pověřený výkonem nezávislé kontroly zpracování osobních údajů ve vnitrostátní části Schengenského informačního systému. Tímto orgánem bude po zapojení České republiky do Schengenského informačního systému právě Úřad pro ochranu osobních údajů. Význam nezávislého dozorového orgánu pro oblast ochrany osobních údajů vyplývá také z řady judikátů Evropského soudu, které se týkají ochrany soukromí jednotlivce v souvislosti se zpracováním osobních údajů zpravodajskými službami nebo sporů o právo přístupu k údajům v nejrůznějších úředních evidencích.¹⁸⁸

Postavení a působnost Úřadu jsou upraveny v hlavě IV ZOOÚ, základy jeho vnitřního uspořádání jsou definovány v hlavě V tohoto zákona a následující hlava VI upravuje některé činnosti Úřadu a oprávnění osob, které se na jejich výkonu podílejí.

Úřad pro ochranu osobních údajů je dle § 28 odst. 1 ZOOÚ nezávislým orgánem, který se při své činnosti řídí pouze zákony a jinými právními předpisy. Uvedené znamená, že Úřad není zařazen do resortu žádného ministerstva, a že orgány moci výkonné nemohou do jeho činnosti zasahovat. Činnost Úřadu může být v souladu s § 28 odst. 2 ZOOÚ limitována pouze zákonem.¹⁸⁹ Nezávislost Úřadu je zabezpečena také tím, že na základě § 28 odst. ZOOÚ jsou náklady spojené s jeho činností hrazeny ze samostatné kapitoly státního rozpočtu České republiky.

¹⁸⁵ Tato nezvyklá definice byla zmíněna již v úvodu kapitoly 3 s tím, že Úřad je fakticky ústředním orgánem státní správy a definice uvedená v § 2 ZOOÚ tedy nezakládá žádné specifické postavení.

¹⁸⁶ V současné době sídlí Úřad na adrese Pplk. Sochora 27, Praha 7, v době svého vzniku však sdílel prostory s Úřadem pro veřejné informační systémy v Havelkově 22, Praha 3.

¹⁸⁷ Úmluva k provedení dohody podepsané dne 14. června 1985 o postupném odstraňování kontrol na společných hranicích, ze dne 19. června 1990.

¹⁸⁸ Např. rozsudek *Hewit v. Spojené království, Leander v. Švédsko* nebo *Gaskin v. Spojené království* (www.echr.coe.int).

¹⁸⁹ Pozici Úřadu lze zřejmě nejlépe přirovnat k pozici Nejvyššího kontrolního úřadu nebo Úřadu pro ochranu hospodářské soutěže.

Deklarovaná nezávislost Úřadu pro ochranu osobních údajů je samozřejmě jen relativní. Úřad nemůže svoji činnosti vykonávat v naprosté izolaci a fakticky je tedy ovlivňován především jinými orgány státní správy, s nimiž při plnění svých úkolů spolupracuje, a stejně tak nejrůznějšími politickými otázkami (zejména s ohledem na způsob jmenování předsedy Úřadu a inspektorů).

Personálně sestává Úřad pro ochranu osobních údajů z předsedy Úřadu, inspektorů a ostatních zaměstnanců, přičemž předseda a inspektoři jsou jmenováni prezidentem republiky na návrh Senátu Parlamentu České republiky.

Předseda Úřadu je takto jmenován na dobu pěti let a může být ve funkci pouze dvě po sobě jdoucí období.¹⁹⁰ ZOOÚ klade určité požadavky na osobu předsedy, zejména bezúhonnost, vysokoškolské vzdělání či české občanství, a současně stanoví neslučitelnost funkce předsedy Úřadu s funkcí poslance, senátora, jakoukoli funkcí ve veřejné správě nebo s funkcí člena orgánů územní samosprávy. Předseda Úřadu také nesmí být členem žádné politické strany či hnutí a dále nesmí zastávat žádnou jinou placenou funkci, být v jiném pracovním poměru či vykonávat jinou výdělečnou funkci (až na obvyklé výjimky týkající se vědecké či literární činnosti nebo správy vlastního majetku, pokud tato činnost neovlivní jeho nezávislost).

Tato omezení odpovídají standardům pro obdobně významné pozice,¹⁹¹ kde je nezbytné zajistit maximální nestrannost a nezávislost vedoucího představitele, a tak potažmo celé instituce, v jejímž čele stojí.

Významnou roli v rámci Úřadu pro ochranu osobních údajů mají inspektoři Úřadu, kteří jsou do své funkce jmenováni (stejným procesem jako předseda Úřadu) na deset let, a kteří jsou pověřeni výkonem kontroly plnění povinností stanovených ZOOÚ. Inspektoři musí naplnit obdobné předpoklady jako předseda Úřadu a jejich funkce je v tomtéž rozsahu neslučitelná s jinou pozicí ve veřejné správě nebo členstvím v politických stranách. Dle ustanovení § 33 odst. 4 ZOOÚ působí na Úřadě pro ochranu osobních údajů celkem sedm inspektorů.¹⁹²

¹⁹⁰ Od vzniku Úřadu do roku 2005 vykonával tuto funkci RNDr. Karel Neuwirt, k 1. září 2005 byl předsedou Úřadu jmenován RNDr. Igor Němec.

¹⁹¹ Viz např. § 10 zákona č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, nebo § 1 zákona 273/1966 Sb., o působnosti Úřadu pro ochranu hospodářské soutěže.

¹⁹² Přestože inspektoři nesmějí být členy politických stran, politické zájmy se vzhledem k tomu, že jsou navrhováni Senátem, při jejich jmenování samozřejmě projevují. Obdobné politické tlaky jsou zjevné i v případě jmenování předsedy Úřadu.

6.1. Kompetence Úřadu pro ochranu osobních údajů podle zákona č. 101/2000 Sb.

Výčet oblastí, v nichž Úřad pro ochranu osobních údajů působí je uveden v § 29 ZOOÚ následujícím způsobem:

- a) dozor nad dodržováním povinností stanovených tímto zákonem;
- b) vedení registru zpracování osobních údajů;
- c) přijímání podnětů a stížností na porušení ZOOÚ a informování o jejich vyřízení;
- d) zpracování a zpřístupnění výroční zprávy o své činnosti;
- e) výkon dalších působností stanovených zákonem (tj. ZOOÚ i jinými zákony);
- f) projednávání přestupků a jiných správních deliktů a udělování pokut podle ZOOÚ;
- g) zajištění plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána;
- h) poskytování konzultací v oblasti ochrany osobních údajů;
- i) spolupráce s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů.

Bezpochyby základní činností Úřadu je provádění dozoru nad dodržováním povinností při zpracování osobních údajů správci, zpracovateli i jinými osobami, které se procesu zpracování osobních údajů účastní. Kontrolní činnost provádí Úřad prostřednictvím kontrol nebo prověřování stížností na porušení ZOOÚ.

Ustanovení § 31 ZOOÚ předpokládá existenci kontrolního plánu, na jehož základě mají být kontroly prováděny.¹⁹³ Kontroly podle tohoto plánu obnášejí prověření plnění veškerých povinností stanovených ZOOÚ, které se na daného správce či zpracovatele vztahují. Kromě těchto plánovaných kontrol však Úřad provádí také tzv. incidenční kontroly, kdy je zkoumáno plnění jen určitých povinností, jejichž porušení je předmětem stížnosti či podnětu podaného Úřadu.

Povinnosti i oprávnění kontrolujících jsou poměrně detailně upraveny v § 37 a § 38 ZOOÚ, kde je kontrolujícím mj. přiznáno oprávnění vstupovat do všech objektů kontrolovaného subjektu, požadovat předložení nejruznějších dokladů, seznamovat se s utajovanými skutečnostmi nebo se skutečnostmi chráněnými povinností mlčenlivosti. Naopak mezi jejich povinnosti patří prokázat se kontrolovanému průkazem, náležitě zahájení kontroly oznámit, řádně ochraňovat převzaté doklady, šetřit práva a právem chráněné zájmy kontrolovaných nebo zachovávat mlčenlivost o skutečnostech zjištěných při výkonu kontroly.

¹⁹³ ZOOÚ však již nestanoví další podrobnosti ohledně procesu sestavování tohoto plánu, ani jaké období má zahrnovat. V současné době je kontrolní plán sestavován každoročně (zejména inspektory Úřadu) s tím, že při jeho sestavování se přihlíží také k došlým stížnostem a podnětům, které mohou naznačit, že některým oblastem je třeba věnovat zvýšenou pozornost.

Pro průběh kontroly plnění povinností vyplývajících ze ZOOÚ, kdy je třeba zjistit skutečný stav věci, je dále významná povinnost poskytnout při výkonu kontroly potřebnou součinnost, upravená ustanovení § 39 ZOOÚ, která se bez dalšího omezení vztahuje na každého. Tomu, kdo potřebnou součinnost neposkytne, lze (i opakovaně) uložit pořádkovou pokutu až do výše 25.000 Kč. Ačkoli tak ZOOÚ přímo nestanoví, je zřejmé, že v souladu s ústavními principy (zejména čl. odst. 3 Ústavy) lze vyžadovat součinnost podle citovaného ustanovení pouze v případech, kdy je to pro účinné provedení kontroly nezbytné, a dále způsobem a v rozsahu, který bude dožádanou osobu zatěžovat co nejméně.

Závěrem každé provedené kontroly musí být vyhotoven kontrolní protokol, který shrnuje průběh kontroly a zjištěné skutečnosti, včetně uvedení případných nedostatků. V rámci kontrolního protokolu mohou být v souladu s § 40 ZOOÚ kontrolovanému uložena také opatření k nápravě závadného stavu, a to včetně lhůty k jejich provedení. Tato opatření mají efekt zejména tam, kde jsou zjištěna systémová pochybení, tj. nedostatky v zavedeném postupu, kdy hrozí, že by k porušení ZOOÚ mohlo dojít opakovaně.

Obecná úprava postupu osob vykonávajících kontrolní činnost Úřadu pro ochranu osobních údajů je obsažena v zákoně č. 552/1991 Sb., o státní kontrole, který se podle § 43 ZOOÚ použije tam, kde ZOOÚ nestanoví jinak, což znamená vždy kromě otázek oprávnění a povinností kontrolujících a povinnosti součinnosti.

Výkonem kontroly dodržování povinností stanovených ZOOÚ jsou, přímo tímto zákonem (konkrétně § 33 odst. 3) pověřeni inspektoři Úřadu, nicméně na kontrole se v případě potřeby může na základě pověření předsedy Úřadu podílet každý zaměstnanec Úřadu, případně lze přibrat i externí specialisty.

Jak bylo uvedeno již výše, kontroly dodržování povinností stanovených ZOOÚ mohou být jednak kontroly plánované a jednak tzv. „ad hoc“ neboli incidenční kontroly – reagující na konkrétní podnět. Prověřování došlých podnětů a stížností je další ze základních činností Úřadu pro ochranu osobních údajů, jejímž prostřednictvím Úřad přispívá k ochraně soukromí osob. Správci osobních údajů musí vždy počítat s tím, že jejich postup může být podroben kontrole a naopak subjekty údajů vědí, že zde existuje nezávislá instituce, na kterou se mohou obrátit, pokud se domnívají, že nezákonným zpracováním osobních údajů došlo či může dojít k zásahu do jejich soukromého života. Úřad pro ochranu osobních údajů je ze zákona povinen se každým podnětem vážně zabývat a případně přijmout veškerá potřebná opatření.

Prověřováním nejrůznějších stížností a podnětů Úřad dále získává přehled o aktuálních problematických oblastech, k nimž se může poté vyjádřit v některém ze svých stanovisek či vyjádření k problémům z praxe, a tak mj. předcházet výskytu obdobných nezákonných či nevhodných postupů v budoucnu.

S kontrolní činností Úřadu a s prověřováním podnětů bezprostředně souvisí další z důležitých oblastí činnosti Úřadu, a to vedení správních řízení, případně řízení o přestupku, se správci či zpracovateli, kteří porušili povinnosti stanovené ZOOÚ. Tento zákon, obdobně jako mnohé jiné právní předpisy v oblasti správního práva, definuje skutkové podstaty správních deliktů (resp. jiných správních deliktů) a přestupků, a tak umožňuje správce či zpracovatele sankcionovat za porušení zde stanovených povinností. Konkrétně lze podle ZOOÚ za správní delikt nebo přestupek uložit pouze pokutu, jiné sankce ZOOÚ totiž nepřipouští.¹⁹⁴ Spolu s opatřením k nápravě, které může být uloženo v průběhu kontroly (§ 40 ZOOÚ), je sankce za správní delikt či přestupek institutem určeným k vymáhání plnění povinností podle ZOOÚ, tedy nástrojem umožňujícím efektivně chránit osobní údaje a soukromí osob.

Zákonem č. 439/2004 Sb. byla hlava VII ZOOÚ, která obsahuje úpravu sankcí, výrazně novelizována. Správní trestání podle ZOOÚ přejalo s účinností této novely (tj. od 26. července 2004) novou koncepci spočívající v rozepsání jednotlivých skutkových podstat, které zrcadlově odráží povinnosti stanovené ZOOÚ v předchozích částech, tj. v hlavě II a III. Tato úprava nahrazuje dřívější pojetí, kdy bylo (v § 46 odst. 1 ZOOÚ) pouze obecně stanoveno, že porušení povinností stanovených tímto zákonem je správním deliktem. Avšak, jak bylo již zmíněno na několika místech v kapitole 4, některým povinnostem uvedeným v hlavě II a III ZOOÚ¹⁹⁵ žádné ustanovení skutkové podstaty správního deliktu podle hlavy VII tohoto zákona neodpovídá, což z hlediska vymáhání povinností stanovených ZOOÚ představuje v praxi určité komplikace.¹⁹⁶

Pokuta za jiný správní delikt uložená správci – právnické osobě může být až pět milionů Kč, případně až deset milionů Kč, pokud správce ohrozí svým jednáním soukromí většího počtu osob anebo pokud nezákonně zpracovává citlivé osobní údaje. Správci osobních údajů v pozici fyzické osoby lze za přestupek podle ZOOÚ uložit pokutu do výše jednoho milionu Kč, resp. pěti milionů Kč. Správní delikty projednává Úřad ve správním řízení podle zákona č. 500/2004 Sb. správní řád, neboť ZOOÚ zvláštní procesní úpravu neobsahuje, přestupky jsou projednávány podle zákona č. 200/1990 Sb., o přestupcích.

¹⁹⁴ ZOOÚ přímo stanoví uložit pokutu pokaždé, kdy je zjištěno a ve správním řízení prokázáno porušení tohoto zákona. Možnost delikt pouze projednat či uložit napomenutí ZOOÚ nepřipouští, ačkoli jsou poměrně časté případy správců, kteří se deliktu dopustili nedbalostí či špatným výkladem ZOOÚ nebo jiné právní normy, jejich jednání nemělo žádné následky v podobě ohrožení soukromí subjektů údajů a závadný stav byl již zcela napraven (buď správcem samotným nebo prostřednictvím uložených opatření k nápravě), a u nichž tedy uložení pokuty nemá žádoucí efekt.

¹⁹⁵ Z povinností popsanych v kapitole 5 jde o ustanovení § 5 odst. 3, § 6, § 10, § 13 odst. 2, § 18 odst. 2, § 19 a § 20 ZOOÚ.

¹⁹⁶ Zřejmě nejzávažnější je nemožnost sankcionovat nedodržení podmínek při postupu podle § 5 odst. 6 ZOOÚ, tj. při předání osobních údajů získaných za účelem nabízení obchodu a služeb jinému správci, kdy může dojít k nekontrolovanému předání osobních údajů řadě dalších správců. Tato situace se však zpracování osobních údajů zaměstnanců zaměstnavatelem příliš netýká.

Úřad pro ochranu osobních údajů doposud ukládal pokuty spíše při dolní hranici uvedených zákonných sazeb, čímž zejména zpočátku své existence zohledňoval skutečnost, že problematika ochrany osobních údajů byla pro české subjekty zcela novou oblastí. V současné době, po pěti letech platnosti ZOOÚ, není již pro obdobnou shovívavost důvod, nicméně Úřad při stanovení výše sankce musí hodnotit veškeré okolnosti předmětného zpracování osobních údajů i poměry subjektu odpovědného za správní delikt či přestupek, a proto jsou i nadále ukládané pokuty obvykle při dolní hranici zákonné sazby (která je ostatně nastavena velmi „velkoryse“).

Odpovědnost správců a zpracovatelů za správní delikt podle ZOOÚ je odpovědností objektivní (za následek) s možností liberace. Tato možnost vyplývá z § 46 odst. 1 ZOOÚ, který stanoví, že správce či zpracovatel osobních údajů za správní delikt neodpovídá, jestliže prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení ZOOÚ zabránil.

Úřad pro ochranu osobních údajů má dále pravomoc vést řízení o přestupku s fyzickou osobou, která je ke správci osobních údajů v pracovním nebo obdobném vztahu, vykonává pro něj činnosti na základě dohody anebo přichází u správce s osobními údaji do styku při plnění svých úkolů, a která poruší povinnost mlčenlivosti podle § 15 ZOOÚ. Povinnosti zaměstnance či osoby v obdobném postavení zpracovávat osobní údaje pouze v souladu s pokyny správce, vyjádřené v § 14 ZOOÚ, žádná skutková podstata přestupku podle hlavy VII neodpovídá a její porušení tak nelze jako přestupek hodnotit. V řízení o přestupku může být uložena pokuta až do výše sto tisíc Kč a Úřad v tomto řízení postupuje podle zákona č. 200/1990 Sb., o přestupcích.¹⁹⁷

Dalším úkolem Úřadu je, podle § 35 ZOOÚ, vedení registru zpracování osobních údajů, který vzniká na základě oznámení správců osobních údajů podaných v souladu s jejich oznamovací povinností podle § 16 ZOOÚ. Smyslem vedení tohoto registru je získání přehledu o existujícím zpracování osobních údajů, a to především pro účely plánování a provádění kontrol. Současně je prostřednictvím registru informována o probíhajícím zpracování osobních údajů u daných správců i veřejnost, neboť registr je (s výjimkou údajů týkajících se konkrétního způsobu zpracování a bezpečnostních opatření) veřejně přístupný, a to i prostřednictvím internetových stránek Úřadu (www.uouu.cz).

Důležitou oblastí působnosti Úřadu pro ochranu osobních údajů, která představuje značně rozsáhlou agendu, je poskytování konzultací v oblasti ochrany osobních údajů, tedy zejména výklad ZOOÚ, Směrnice 95/46 a otázky interakce těchto norem s nejrůznějšími právními předpisy. Tato možnost je široce využívána jak subjekty ze soukromého sektoru, tak i těmi veřejnoprávními, přičemž konzultace se provádí nejčastěji telefonicky nebo

¹⁹⁷ Úpravu sankcí za přestupky v ZOOÚ je však nutno brát jako *lex specialis* k obecné úpravě sankcí podle § 11 zákona č. 200/1990 Sb., a tedy i fyzickým osobám lze za přestupek podle ZOOÚ uložit pouze pokutu.

písemnou formou, případně i formou osobní konzultace (zejména jedná-li se o složitější případ, kdy je zapotřebí zaujmout zásadnější výkladové stanovisko). Tato působnost Úřadu je významná z hlediska předcházení zásahů do soukromí osob nevhodným či nezákonným zpracováním osobních údajů, neboť správce, který si není svým postupem zcela jist nebo se setkal s výkladovým či aplikačním problémem, má možnost kontaktovat přímo Úřad a získat potřebné informace, jakým způsobem sladit své postupy se ZOOÚ, a tím předejít případným stížnostem subjektů údajů, následným kontrolám ze strany Úřadu a sankcím za porušení povinností podle ZOOÚ.¹⁹⁸

ZOOÚ uvádí ve výčtu činností Úřadu pro ochranu osobních údajů uvedeném v § 29 také zpracování a zveřejnění výroční zprávy o činnosti Úřadu. Výroční zpráva je zveřejňována ve Věstníku Úřadu pro ochranu osobních údajů i jako samostatná brožura a je předkládána Senátu a Poslanecké sněmovně Parlamentu České republiky k projednání, čímž je zajištěna kontrola činnosti Úřadu jak ze strany Parlamentu ČR, tak i ze strany veřejnosti. Veškeré doposud vydané výroční zprávy jsou také dostupné na internetových stránkách Úřadu. Požadavek na vypracování výroční zprávy vychází přímo z čl. 28 odst. 5 Směrnice 95/46, přičemž základním smyslem této povinnosti je rozšiřování povědomí o právech a povinnostech spojených s ochranou osobních údajů.

Informace o své činnosti i o zajímavostech v oblasti ochrany osobních údajů v České republice, Evropské unii i jinde ve světě publikuje Úřad pro ochranu osobních údajů také v Bulletinu, který vychází čtvrtletně, a ve Věstníku, který je vydáván nejméně šestkrát do roka, a kde jsou zveřejňována i stanoviska Úřadu, dokumenty EU týkající se ochrany osobních údajů nebo seznam subjektů, které v uplynulém období podaly oznámení o zpracování osobních údajů podle § 16 ZOOÚ nebo naopak svoji činnost správce ukončily.

Nedílnou součástí činnosti Úřadu je připomínkování návrhů zákonů či novelizací, které se týkají oblasti ochrany osobních údajů, a dále navrhování legislativních úprav za účelem implementace mezinárodních norem v oblasti ochrany osobních údajů. Při této činnosti může Úřad pro ochranu osobních údajů využívat zkušenosti obdobných dozorových orgánů v zemích EU, s nimiž má intenzivní kontakty.¹⁹⁹

¹⁹⁸ Výstupy z konzultací však nelze vykládat jako povolení Úřadu k danému zpracování. Komplexní posouzení legality zpracování osobních údajů pouze na základě (často neúplných) informací poskytnutých v žádosti o stanovisko či konzultaci není samozřejmě možné.

¹⁹⁹ Úřad je povinným připomínkovým místem v rámci legislativního procesu, sám ovšem legislativní iniciativu nemá.

6.2. Kompetence Úřadu pro ochranu osobních údajů podle jiných zákonů

Vedle ZOOÚ vykonává Úřad pro ochranu osobních údajů v současné době působnost ještě na základě tří dalších norem, a to konkrétně podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti) a podle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

První z uvedených norem zakládá kompetenci Úřadu dohlížet nad využíváním rodných čísel, která lze s účinností od 1. dubna 2004 (tj. s účinností zákona č. 53/2004 Sb., kterým se mění některé zákony související s oblastí evidence obyvatel) využívat jen v případech taxativně vymezených v § 13c zákona č. 133/2000 Sb.²⁰⁰

Úřad pro ochranu osobních údajů projednává podle § 17e zákona č. 133/2000 Sb. správní delikty, kterých se dopustí právnické osoby nebo fyzické osoby – podnikatelé tím, že neoprávněně nakládají s rodným číslem nebo rodná čísla neoprávněně využívají, přičemž těmto subjektům lze ve správním řízení uložit pokutu až do výše jednoho, resp. deseti milionů Kč.

Druhá z uvedených norem, zákon č. 480/2004 Sb., pověřuje Úřad pro ochranu osobních údajů výkonem dozoru nad šířením nevyžádaných obchodních sdělení.²⁰¹

Zákon č. 480/2004 Sb. stanoví v § 7 podmínky, za nichž je možné využívat informace o elektronickém kontaktu (tj. zejména adresu elektronické pošty, ale i telefonní číslo) k šíření obchodních sdělení, tedy sdělení, která mají za cíl podpořit určitý produkt, službu či image konkrétní právnické osoby nebo podnikající fyzické osoby. Zjednodušeně lze říci, že zákon č. 480/2004 Sb. povoluje pouze šíření obchodních sdělení v tzv. systému opt-in, tedy vyžádaných sdělení, kdy odesílatel předem disponuje souhlasem adresáta se zasláním obchodního sdělení, a dále zakazuje veškeré skryté formy obchodních sdělení.

Výkonem dozoru nad dodržováním podmínek pro šíření obchodních sdělení podle § 7 zákona č. 480/2004 Sb. je pověřen právě Úřad pro ochranu osobních údajů, který může při jejich porušení uložit ve správním řízení pokutu až do výše deseti milionů Kč.

Zákon č. 127/2005 Sb. zakládá ve svém § 87 kompetenci Úřadu vykonávat dozor nad dodržováním povinností při zpracování osobních údajů podle tohoto zákona. Vzhledem k tomu, že se jedná o kompetenci zcela novou (zákon č. 127/2005 Sb. nabyl účinnosti 1. května 2005), nemá Úřad zatím s výkonem této kompetence žádné praktické zkušenosti.

²⁰⁰ Problematice využití rodných čísel v pracovněprávních vztazích je věnována kapitola 5.2.

²⁰¹ Jedná se o problematiku tzv. SPAMů, která je v současné době celosvětově velmi aktuální, neboť množství rozeslaných nevyžádaných sdělení i počet osob, které se takovým jednáním cítí dotčeny, neustále roste.

Závěr

Závěrem lze říci, že současná právní úprava ochrany osobních údajů v České republice v zásadě odpovídá mezinárodním požadavkům v této oblasti. Nicméně v souvislosti s tím, jak roste důraz na zajištění náležité úrovně ochrany dat ve stále se rozšiřujícím počtu oblastí (přičemž i obsah této „náležité úrovně“ se neustále rozšiřuje), je zřejmé, že nelze usnout na vavřínech. Česká republika bude vzhledem ke svému členství v Evropské unii nucena problematice ochrany osobních údajů věnovat neustále pozornost a přizpůsobovat se trendům v tomto oboru a vypořádávat se s novými riziky.

Mezi tato rizika patří zejména nové komunikační a informační technologie, které na jednu stranu přinášejí nesporný pokrok v oblasti shromažďování a zpracování informací, na druhou stranu právě pro tyto své vlastnosti představují z hlediska ochrany soukromí osob určitou hrozbu, a to tím spíše, že v současné době není přístup k moderním technologiím výsadou státních orgánů, které jsou (i přes nikdy nekončící snahu o získání většího přehledu o všem a o všech) přeci jen podrobeny většímu dohledu než subjekty soukromoprávní sféry.

V oblasti pracovněprávních vztahů bude riziko zásahu do soukromí zaměstnanců spojené s možnostmi, které nové technologie přinášejí, ještě znásobeno tím, že zaměstnanci jsou na zaměstnavateli existenčně závislí, a proto alespoň navenek i méně citliví na zachování svých základních práv. Vzhledem k tomu, že nové technologie stírají hranice mezi pracovním a soukromým životem, např. tím, že umožňují pracovat z domova, bude také zřejmě stále obtížnější odlišit, kdy se jedná o oprávněný zájem zaměstnavatele na kontrole činnosti jeho zaměstnanců, a kdy jde již o neodůvodněný zásah do jejich soukromí.

Další velmi rychle se rozvíjející oblastí je využívání biometrických, případně i genetických údajů k identifikaci osob, což bylo ještě před nedávnem považováno za téma patřící do sci-fi publikací. V dnešní době se však biometrické údaje již běžně používají pro kontrolu pohybu osob na pracovištích se zvláštním režimem a v brzké době se započne s vydáváním cestovních dokladů s čipem, na němž bude uložena biometrická fotografie a posléze i otisk prstu.

Úroveň ochrany osobních údajů je v současné době také jednou ze základních oblastí hodnocených v souvislosti s chystaným vstupem České republiky do tzv. Schengenského prostoru, tedy připojení k Schengenskému informačnímu systému, v němž jsou zpracovávány rozsáhlé soubory osobních údajů velkého počtu osob a na jehož vytváření a využívání se podílí velké množství nejrůznějších orgánů členských států. S ohledem na jedinečnost tohoto systému, zejména ve smyslu rozsahu zpracovávaných dat, musí Česká republika před přistoupením prokázat jednak připravenost poskytnout osobním údajům efektivní ochranu na vysoké úrovni (zejména v rámci složek policie), a jednak existenci

skutečně nezávislého orgánu pověřeného dozorem nad zpracováním osobních údajů ve vnitrostátní části tohoto systému.

Co se týče dalšího vývoje úpravy ochrany osobních údajů v právním řádu České republiky, lze vyjádřit názor, že v dohledné době nedozná zásadních změn. V současné době je v Parlamentu České republiky projednáván vládní návrh nového zákoníku práce (sněmovní tisk č. 1153, Poslaneckou sněmovnou byl schválen dne 8. února 2006 a 28. února 2006 byl postoupen Senátu), obdobně jako platný zákoník práce však tento návrh neobsahuje zvláštní úpravu ochrany osobních údajů v pracovněprávních vztazích, v tom smyslu, že by přinášel systematickou úpravu práv a povinností účastníků pracovněprávních vztahů při zpracování osobních údajů. Nadále bude tedy ochrana dat v této oblasti regulována ZOOÚ s tím, že nový zákoník práce bude upravovat pouze dílčí povinnosti či oprávnění zaměstnavatele zpracovávat o svých zaměstnancích určitý soubor údajů k určitému účelu.²⁰²

Samotný ZOOÚ by měl být, jak bylo uvedeno již výše, také – již po jedenácté – novelizován s tím, že by měly být vyjasněny některé problematické otázky vyplývající z platného znění tohoto zákona a z dosavadní praxe Úřadu, zejména imperfektnost některých ustanovení. O přesném obsahu této novely ZOOÚ však není ještě definitivně rozhodnuto.

Jisté však je, že otázka ochrany osobních údajů se bude nadále prolínat všemi oblastmi našeho života a právní úprava této problematiky se bude i nadále dynamicky rozvíjet, zřejmě v tom smyslu, že se postupně bude prosazovat podrobnější úprava do všech oblastí regulovaných doposud pouze obecnými předpisy, pro něž je dnes nutné přijímat výkladová stanoviska. Je tedy možné, že se například dočkáme zvláštní úpravy ochrany osobních údajů při zpracování dat prostřednictvím moderních technologií, jako jsou kamerové systémy nebo prostředky monitorování elektronické komunikace.

Budoucnost ochrany osobních údajů bude také bezesporu i nadále ve znamení věčného vyvažování práv těch, kteří pro svou činnost potřebují (nebo jsou přesvědčeni, že potřebují) zpracovávat určité údaje, a těch, o jejichž údaje se jedná. Zejména v souvislosti s tzv. bojem proti terorismu je již dnes velmi aktuální otázka, zda a do jaké míry jsme ochotni se ve jménu bezpečnosti vzdát části svého soukromí.

Obdobně přetrvává i neustálé hledání kompromisu mezi právem na ochranu osobních dat a soukromí a právem na informace o činnosti určitých subjektů, zejména orgánů státní

²⁰² Rostoucí důraz na ochranu soukromí se však v projednávaném zákoníku práce projevil, a to zejména zakotvením zákazu narušovat soukromí zaměstnance na pracovišti v souvislosti s kontrolou jeho práce a zákazem vyžadování informací, které nesouvisí bezprostředně s výkonem práce, nemá-li k tomu zaměstnavatel závažné důvody, a dále detailnější úpravou povinností zaměstnavatele při nakládání s osobním spisem zaměstnance a s dokumenty v něm obsaženými (tyto principy jsou uvedeny v závěrečné části obsahující společná ustanovení).

správy, přičemž právě v této oblasti (tj. možnosti jednotlivce domoci se informace o shromažďovaných a zpracovávaných údajích o jeho osobě, důvodu takového zpracování a rozsahu údajů, kterých se týká, a případně i nápravy závadného stavu) má Česká republika ve srovnání s vyspělejšími zeměmi Evropské unie ještě co dohánět.

Jedním z nejdůležitějších úkolů, které má Úřad pro ochranu osobních údajů před sebou, je zvýšení veřejného povědomí o důležitosti ochrany osobních údajů a o možnostech subjektů údajů aktivně k ochraně vlastních dat přispět. Dobře informovaný občan je totiž partnerem ochránců osobních údajů. Pokud takový občan ví, že by neměl kdekomu poskytovat údaje o svém soukromí, neměl by vyplňovat dotazníky neznámého původu pro neznámého sběratele, a že v případě, kdy neuspěje se svými požadavky u příslušného správce či zpracovatele, je zde nezávislá instituce, na kterou se může obrátit, je práce ochránců dat o polovinu snazší.

Ochrana osobních údajů a soukromí bude tedy bezesporu jedním ze základních témat v demokratické společnosti třetího tisíciletí.

Literatura

Monografie a odborné publikace

- Jouza, L. Zákoník práce s komentářem. 5 vydání. Praha: BOVA POLYGON, 2004.
- Klíma, K. Ústavní právo. Praha: Bohemia Iuris Kapitál, a.s., 1997.
- Knapp, V. Teorie práva. Praha: C. H. Beck, 1. vydání, 1995.
- Kužilek, O., Žantovský, M. Svoboda informací. Praha: Linde Praha, a.s., 2002.
- Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J. Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2003.
- Mates, P. Ochrana soukromí ve správním právu. Praha: Linde Praha, a.s., 2004.
- Mates, P., Neuwirt, K. Právní úprava ochrany osobních údajů v ČR. Druhé, doplněné a rozšířené vydání. Praha: IFEC, 2000.
- Matoušová, M., Hejlík, L. Osobní údaje a jejich ochrana. Praha: ASPI Publishing, s.r.o., 2003.
- Matoušová, M., a kol. Ochrana osobních údajů v otázkách a odpovědích. Praha: ASPI Publishing, s.r.o., 2004.
- Výroční zprávy Úřadu pro ochranu osobních údajů za rok 2000 až 2004.
- Věstník Úřadu pro ochranu osobních údajů, 2002, č. 20

Stanoviska a standardy

- Stanovisko Úřadu pro ochranu osobních údajů k problémům z praxe č. 1/2001 – K pojmu osobní údaj, www.uoou.cz.
- Stanovisko Úřadu pro ochranu osobních údajů č. 2/2001 - Zpracování citlivého osobního údaje členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací, www.uoou.cz.
- Stanovisko Úřadu pro ochranu osobních údajů k problémům z praxe č. 4/2002 – Používání rodného čísla, www.uoou.cz.
- Stanovisko Úřadu pro ochranu osobních údajů k problémům z praxe č. 6/2002 – Poskytování osobních údajů o zaměstnancích, www.uoou.cz.
- Stanovisko Úřadu pro ochranu osobních údajů k problémům z praxe č. 1/2003 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců, www.uoou.cz.
- Stanovisko Úřadu pro ochranu osobních údajů č. 5/2004 - Uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky od daně z příjmu, www.uoou.cz.

Vyjádření Pracovní skupiny 29 k jednotnému výkladu článku 26 (1) Směrnice 95/46/ES ze dne 24. října 1995 (Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24. October 1995), www.europa.eu.int.

Stanovisko Pracovní skupiny 29 č. 8/2001 ke zpracování osobních údajů v pracovněprávních vztazích (Opinion 8/2001 on the processing of personal data in the employment context), www.europa.eu.int.

Vyjádření Pracovní skupiny 29 ke sledování elektronické komunikace na pracovišti ze dne 29. května 2002 (Working document on the surveillance of electronic communications in the workplace), www.europa.eu.int.

Stanovisko Pracovní skupiny 29 č. 4/2003 k úrovni ochrany osobních údajů cestujících při předání do USA (Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data), www.europa.eu.int.

Stanovisko Pracovní skupiny 29 č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování (Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance), www.europa.eu.int.

Doporučení portugalského úřadu pro ochranu osobních údajů (Comissão Nacional de Protecção de Dados) k monitorování zaměstnanců na pracovišti (Recommendations of The Portuguese DPA regarding the monitoring of employees at the workplace), www.cnpd.pt.

Mezinárodní organizace práce - Kodex o ochraně osobních údajů zaměstnanců (Code of Practice on protection of workers' personal data), www.unionnetwork.org.

Články

D'Ambrosová, H. K některým povinnostem zaměstnavatelů při ochraně osobních údajů. *Mzdy a personalistika v praxi*, 2004, č. 9, s. 32.

D'Ambrosová, H. K problematice potvrzení o zaměstnání, tzv. zápočtových listů. *Mzdy a personalistika v praxi*, 2003, č. 6, s. 26.

D'Ambrosová, H. Ochrana osobních údajů v personalistické praxi - II. *Mzdy a personalistika v praxi*, 2002, č. 7, s. 12.

Hanušová, A. Ochrana osobních údajů – rozpory právní úpravy. *Právní rozhledy*, 1996, č. 6, s. 252.

Hlásenský, V. Soukromí v přímém přenosu. *Týden*, 4. 4. 2005, s. 36.

Hyška, M. Velký bratr zaměstnavatel. *Lidové noviny*, 25. 5. 2005, s. 1.

Jakubka, J. Potvrzení o zaměstnání a pracovní posudky. *Práce a mzda*, 2001, č. 9, s. 14.

Jakubka, J. Interní předpisy zaměstnavatele v pracovněprávních vztazích – II. *Mzdy a personalistika v praxi*, 2003, č. 6, s. 18.

Jouza, L. Kamery na pracovišti nesmí narušovat soukromí. *Hospodářské noviny*, 10. 11. 2004, s. 26.

Jouza, L. Ochrana soukromí na pracovišti. *Právní rádce*, 2003, č. 5, s. 29.

- Jouza, L. Pracovní posudek nebo informace o zaměstnanci?. Právní rádce, 2004, č. 4, s. 34.
- Jouza, L. Legislativa Evropské unie v českém pracovním právu – 2. část. Právní rádce, 2004, č. 5, s. 62.
- Kolman, P. Nové správní sankce týkající se ochrany osobních údajů. Právní rádce, 2005, č. 7, s. 41.
- Kučerová, A. Úvaha nad novelou zákona o ochraně osobních údajů. Právní zpravodaj, 2004, č. 12, s. 9.
- Maštalka, J. Osobní údaje v právním řádu české republiky a zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Obchodní právo, 1993, č. 6, s. 17.
- Maštalka, J. Nástin koncepce ochrany osobních dat v našem právním řádu. Průmyslové vlastnictví, 1994, č. 2, s. 48.
- Maštalka, J. Co a k čemu je osobní údaj?. Daně a právo v praxi, 2002, č. 4, s. 41.
- Maštalka, J. Zpracování osobních údajů z pohledu správce. Právní rozhledy, 2003, č. 9, s. 44.
- Mates, P. Zamyšlení nad ochranou osobních údajů a o rozporech právní úpravy. Právní rozhledy, 1996, č. 9, s. 407.
- Mates, P. Ochrana osobních údajů v českém právním řádu. Bulletin advokacie, 2000, č. 9, s. 32.
- Mates, P., Bartík, V. Nová úprava ochrany osobních údajů. Právní rádce, 2004, č. 9, s. 42.
- Mates, P., Smejkal, V. Spam a legální zasílání hromadných zásilek. Právní zpravodaj, 2005, č. 1, s. 9.
- Matoušová, M. Pohled praxe na novelu zákona o ochraně osobních údajů. Právní rádce, 2004, č. 11, s. 69.
- Schelle, K., Šmíd, V. Rodné číslo v informačních systémech. Právní rádce, 2004, č. 11, s. 44.
- Sokol, T. Zákon o ochraně osobních údajů se na advokáta nevztahuje. Bulletin advokacie, 2000, č. 10, s. 23.
- Štědroň, B. Kontrola práce zaměstnance prostřednictvím telekomunikační techniky. Právní rádce, 2004, č. 12, s. 39.
- Tuháček, M. Sto šest neznamena vždy více než sto jedna. Podle jakého zákona postupovat při poskytování informací. Via Iuris, 2003, č. 3, s. 8.
- Veselý, J. Právní úprava ochrany osobních údajů v ČR. Právní rozhledy, 1997, č. 3, s. 105.

- Jouza, L. Pracovní posudek nebo informace o zaměstnanci?. Právní rádce, 2004, č. 4, s. 34.
- Jouza, L. Legislativa Evropské unie v českém pracovním právu – 2. část. Právní rádce, 2004, č. 5, s. 62.
- Kolman, P. Nové správní sankce týkající se ochrany osobních údajů. Právní rádce, 2005, č. 7, s. 41.
- Kučerová, A. Úvaha nad novelou zákona o ochraně osobních údajů. Právní zpravodaj, 2004, č. 12, s. 9.
- Maštalka, J. Osobní údaje v právním řádu české republiky a zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Obchodní právo, 1993, č. 6, s. 17.
- Maštalka, J. Nástin koncepce ochrany osobních dat v našem právním řádu. Průmyslové vlastnictví, 1994, č. 2, s. 48.
- Maštalka, J. Co a k čemu je osobní údaj?. Daně a právo v praxi, 2002, č. 4, s. 41.
- Maštalka, J. Zpracování osobních údajů z pohledu správce. Právní rozhledy, 2003, č. 9, s. 44.
- Mates, P. Zamyšlení nad ochranou osobních údajů a o rozporech právní úpravy. Právní rozhledy, 1996, č. 9, s. 407.
- Mates, P. Ochrana osobních údajů v českém právním řádu. Bulletin advokacie, 2000, č. 9, s. 32.
- Mates, P., Bartík, V. Nová úprava ochrany osobních údajů. Právní rádce, 2004, č. 9, s. 42.
- Mates, P., Smejkal, V. Spam a legální zasilání hromadných zásilek. Právní zpravodaj, 2005, č. 1, s. 9.
- Matoušová, M. Pohled praxe na novelu zákona o ochraně osobních údajů. Právní rádce, 2004, č. 11, s. 69.
- Schelle, K., Šmíd, V. Rodné číslo v informačních systémech. Právní rádce, 2004, č. 11, s. 44.
- Sokol, T. Zákon o ochraně osobních údajů se na advokáta nevztahuje. Bulletin advokacie, 2000, č. 10, s. 23.
- Štědroň, B. Kontrola práce zaměstnance prostřednictvím telekomunikační techniky. Právní rádce, 2004, č. 12, s. 39.
- Tuháček, M. Sto šest neznamená vždy více než sto jedna. Podle jakého zákona postupovat při poskytování informací. Via Iuris, 2003, č. 3, s. 8.
- Veselý, J. Právní úprava ochrany osobních údajů v ČR. Právní rozhledy, 1997, č. 3, s. 105.

Základní právní předpisy a soudní rozhodnutí

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a důvodová zpráva k návrhu tohoto zákona.

Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a důvodová zpráva k návrhu tohoto zákona.

Zákon č. 65/1965 Sb., zákoník práce.

Zákon č. 435/1999 Sb., o zaměstnanosti, a důvodová zpráva k návrhu tohoto zákona.

Zákon č. 428/2000 Z. z., o ochrane osobných údajov (Slovenská republika).

Bundesdatenschutzgesetz, BGBl. I, S. 2954.

Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů.

Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat.

Doporučení č. R (89) 2 výboru ministrů Rady Evropy členským státům o ochraně osobních údajů používaných pro účely zaměstnání, www.uouu.cz.

Evropský soud pro lidská práva, Niemietz v. Německo, Halford v. Spojené království, Huvig v. Francie, Cambell v. Spojené království, Amann v. Švýcarsko, www.echr.coe.int.

Seznam použitých zkratk

ZOOÚ – zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Listina – zákon č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

Zákoník práce – zákon č. 65/1965 Sb., zákoník práce.

Úřad – Úřad pro ochranu osobních údajů.

Deklarace – Všeobecná deklarace lidských práv.

MOP – Mezinárodní organizace práce.

OECD – Organizace pro hospodářskou spolupráci a rozvoj.

Evropská úmluva – Evropská úmluva o ochraně lidských práv a základních svobod.

Ústava – zákon č. 1/1993 Sb., Ústava České republiky.

Úmluva 108 – Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat.

Evropská ústava – Smlouva o Ústavě pro Evropu.

Směrnice 95/46 – Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů.

Pracovní skupina 29 – Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů (podle čl 29 Směrnice 95/46).

Směrnice č. 2002/58/ES – Směrnice č. 2002/58/ES Evropského parlamentu a rady ze dne 10. července 2002 o zpracování osobních údajů a ochraně soukromí v oblasti elektronické komunikace.

Občanský zákoník – zákon č. 40/1964 Sb., občanský zákoník.

Evropský soud – Evropský soud pro lidská práva.

Resume

The purpose of this work, which title sounds "The Protection of the personal data in the labour relations", is to give a synoptically view of processing of the personal data in the employment context.

Protection of personal data is relatively young discipline (in general begun attract attention at the beginning of 90's, but in the Czech Republic rather in the end of this decade). The younger this discipline is, the more dynamic is its development; the data protection issue is of raising importance in all spheres in our life and the employment relationships are not an exemption.

Today, when information concerning our way of life are valuable commodity and any misuse of them can lead to very serious impact not only on the privacy or the property, but also on the execution of the fundamental rights, the protection of personal data gains still more importance. In consequence of the globalization and the possibilities of new communication means and new technologies are the risks for everyone's privacy growing higher and higher.

The best protection of any data is no processing (collection, recording, storage or transfer) at all. However in today's society is processing of personal data a necessity. In most of relations we enter is necessary to identify each party and so the processing of personal data is inseparable part of most, if not all, human's activities.

The necessity of personal data use leads logically to the necessity of rules for their processing and protecting. There must be clear principles lay down to protect personal information and private life of those, who are subjects of such data.

In the Czech Republic are the general rules for processing of the personal data settled in the Act n. 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts (further "Act n. 101/2000"), which is *lex generalis* for this area. This act develops the fundamental right on personal data protection expressed in article 10 of the Declaration of Basic Rights and Freedoms of the Czech Republic.

The rules for personal data processing are also involved in many special acts (*lex specialis*) both in private and public sector. The protection of personal data is granted in the Criminal Code as well.

Some provisions for personal data processing are also in the Act n. 65/1965, the Labour Code, which allows the processing of employee's data by the employer.

In the first chapter of this work are mentioned the most important international documents, on which are the national legislation provisions on personal data protection built.

The very first document mentioning the right on protection of privacy is the Universal Declaration of Human Rights proclaimed by the United Nations Organisation in 1948. The

same organisation created in 1966 another important document – International Pact about Civil and Political Rights, which is despite of the above-mentioned Declaration for the member states legally binding. The International Labour Organisation, which is since 1946 operative within the system of the OSN, published in 1997 its Code of Practice on Protection of Worker's Personal Data, where the rules on processing personal data in employment context are specified.

The first specific provisions on personal data protection were issued by the Organisation for Economic Cooperation and Development in 1980. The Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data defined for the first time the main terms of personal data protection and the basic principles.

The Council of Europe published in 1950 the Convention for the Protection of Human Rights and Fundamental Freedoms settled the right on protection of privacy and family life. In 1980 issued this body one of the most important international documents in the area of personal data protection the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108 (further "Convention n. 108"). The Czech Republic ratified this treaty on 24 September 2003. The Council of Europe published since then thirteen recommendations to further explain or specify the provisions of the Convention n. 108, one of these is the Recommendation R(89)2E of 18 January 1989 on the protection of personal data used for employment purposes.

The European Union, which pays great attention to the protection of privacy, involves provisions on personal data protection to all basic documents and agreements. On the international level it's above all the Charter of Fundamental Rights (issued in 2000), the principles for data protection are also involved the vetoed European Constitution. The most relevant act of *acquis communautaire* is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (further "Directive 95/46/EC"). This directive settles the obligation to involve it's provisions to the national law system of each member state and it was one of the acts the Czech Republic had to implement before it's entry to the EU.

There are some other acts of European law, which are of importance for personal data protection: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Decision No 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July

2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties or decisions concerning transfer of personal data to third countries.

The history of regulation of the personal data processing in the Czech Republic is described in the second chapter.

The first act regulating personal data processing was issued in 1992 (the Act n. 256 of June 1, 1992 on the Protection of Personal data in Information systems). This act was due its closely defined subject due the absence of an independent supervisory authority of small importance. On 1 June 2000 came into the force the Act n. 101/2000, which fully corresponds to all binding international documents, especially Convention n. 108 a Directive 95/46/EC. The Act n. 101/2000 was since then ten times amended and the eleventh amendment is now in legislative process.

The theme of the third chapter is the definitions of the terms relevant for personal data protection and the scope of the Act n. 101/2000. Concerning the definitions the Act n. 101/2000 brings description of all basic terms as "personal data", "processing of personal data", "the controller" and "the processor" of personal data or "the data subject". All the definitions in the Act n. 101/2000 as well as its scope correspond more or less with Convention n. 108 a Directive 95/46/EC. Still there are some inaccuracies in both the definitions and the description of the scope of the Act n. 101/2000, but these don't cause significant troubles with explanation or application of this act.

Due to absence of special provisions on data processing in the Labour Code, the Act n. 101/2000 applies fully on the processing of employees' data by the employer.

The description and explanation of the obligations, which the Act n. 101/2000 imposes on the controllers and processors, and of the rights given by this act to the data subjects makes the content of chapter four.

The obligations of the employer (as the controller of employee' personal data) put by the Act n. 101/2000 could be divide as follows:

- 1) obligations applied before beginning of the data processing;
- 2) obligations applied during the processing and
- 3) obligations applied during the ending of the processing.

In the first group belongs obligation to: specify the purpose for which personal data are to be processed and the means and manner of personal data processing; get the consent of data subject; provide the data subject with necessary information about the processing and notify the processing to the Office for Personal Data Protection.

During the processing is the employer obliged to: process only accurate personal data; collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary; preserve personal data only for a period of time that is necessary for the

purpose of their processing; process personal data only in accordance with the purpose for which the data were collected.; collect personal data only in an open manner; ensure that personal data that were obtained for different purposes are not grouped; conclude with the processor (if any) an agreement on personal data processing; adopt measures preventing unauthorised or accidental access to personal data and respect the right to protection of private and personal life of the data subject while processing the data.

And finally while ending the processing of any personal data the employer has obligation to: announce to the Office for Personal Data Protection how he handled personal data and carry out liquidation of personal data as soon as the purpose for which personal data were processed ceases to exist.

It's not only the employer, whom the Act n. 101/2000 addresses obligations. The employees, who in fact process the personal data for their employer, have some obligations too. Firstly they have to process personal data only under the conditions and in the scope specified by the controller or the processor and secondly they're obliged to maintain confidentiality of personal data and security measures.

On the other side the employees, as the data subjects, have on the basis of the Act n. 101/2000 also some rights. These rights are: requests information on the processing of his personal data; ask the controller or processor for explanation or require the remedy of the arisen state of affairs.

Some actual questions concerning personal data processing and protecting are mentioned in the fifth chapter.

The first subchapter describes the problematic of the transfer of the personal data to other countries. The Act n. 101/2000 has several different provisions, which applies according to the level of the protection granted in the receiving country.

The Act n. 101/2000 recognizes four situations of transborder data flows, which are:

- 1) transfer of the personal data to the EU country (where is no restriction of the free movement of the data allowed);
- 2) transfer of the personal data allowed by the decisions of EU authorities (these decisions allows free transfer to specified countries or under specified conditions);
- 3) transfer of the personal data to the member state of an binding international agreement, which settles free movement of personal data (such agreement is today only the Convention n. 108);
- 4) transfer of the personal data to other countries (here is the authorization of the Czech data protection authority necessary).

Second described actual question on the field of data protection in the Czech Republic is processing of the personal identification number ("PIN"). All citizens of the Czech Republic have such a number, which contains information about the date of birth and the sex. PIN is

unique and primary serves for easy identification of the bearer for the purposes of the public sector. For its unique character and its easy usage is PIN widely used in both public and private sector as a mere evidence aid, which raises the risk of intrusion to the privacy of the bearer.

PIN not only involved personal information, it's a key to many public evidences, which contained huge amount of personal data, some of them very sensitive. A misuse of PIN could cause big troubles to its bearer and so its use should be restricted only on the situations exactly specified in law (use of PIN is since 1 March 2004, when an amendment of the Act n. 133 on the Evidence of Citizens and the Personal Identification Number, more strict).

The last actual theme mentioned in the chapter five is the problem of surveillance of the employees and the protection of the personal data processed in this context.

The question is, whether or under which conditions are the employers justified to controlling the way, how their employees use Internet access, e-mail or phone in the workplace. On basis of some decisions of the European Court of Human Rights (concerning the right on protection of privacy), standards of International Labour Organisation and standards issued by the Article 29 Working Group (established in the article 29 of the Directive 95/46/EC) on the surveillance of electronic communications in the workplace is possible to set some principles for controlling the employees.

The main rules are:

- necessity;
- finality;
- transparency (including notification to the supervising authority, information to the data subject and the worker's right of access to the data);
- legitimacy;
- proportionality;
- accuracy and clear retention period and
- security of the processed data.

Following all these principles, the employers are allowed to process the personal data of their employees collected by the means of monitoring the use of Internet access and e-mail. The same principles apply on the monitoring of phone calls.

Specific situation is with the surveillance by camera systems. Here also apply the above mentioned principles, but – because of the higher risk of intrusion to the employees privacy – could be the use of camera surveillance in the workplace much more restricted (it's settled e.g. the Article 29 Working Party Opinion on the Processing of Personal Data by Means of Video Surveillance).

The last chapter is giving account of the Czech data protection authority, The Office for Personal Data Protection, its organisational structure and competences.

The Office is independent supervision body for the area of personal data processing. It also executes supervision on processing the PIN, of using means of electronic communication for sending unasked business messages and processing personal data while using these means.

Where the law, regulated mentioned areas, was broken, the Office imposes fines up to 10 million CZK (cca 300.000 €).

The Office also provides explanations of the provisions and application of the Act 101/2000 and consultations on the problematic of personal data protection.

The conclusions of this work are that the protection of personal data in the Czech Republic is on high level and in accordance with all international requirements. However there still remain some problems to solve, especially in the area of public awareness of the issue of personal data protection.

As the legislation of data protection develops very quickly, there's high probability it'll soon be specific provisions on personal data protection in concrete areas, maybe including employment relations too.

The future of data protection will certainly be colourful and this issue becomes (if it already isn't) with no doubt one of the most important themes for the 21st century.

Seznam příloh¹

- I. Doporučení výboru ministrů Rady Evropy č. R (89) 2 členským státům o ochraně osobních údajů používaných pro účely zaměstnání.
- II. Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů
- III. Article 29 Working Party opinion 8/2001 on the processing of personal data in the employment context
- IV. Working document on the surveillance of electronic communications in the workplace.
- V. Article 29 Working Party opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.

¹ S ohledem na to, že uvedené dokumenty, lze získat pouze v elektronické podobě (ve formátu pdf), nebylo možné číslovat pořadí stran v rámci tohoto seznamu příloh.

Přílohy III, IV a V nejsou (vzhledem ke svému rozsahu) uvedeny v plném znění; jsou vybrány jen některé pasáže. Úplné znění těchto dokumentů je na příloženém CD.

**DOPORUČENÍ VÝBORU MINISTRŮ RADY EVROPY Č. R (89) 2 ČLENSKÝM STÁTŮM
O OCHRANĚ OSOBNÍCH ÚDAJŮ POUŽÍVANÝCH PRO ÚČELY ZAMĚSTNÁNÍ**
(Schváleno výborem ministrů dne 18. ledna 1989 na 423. zasedání zástupců ministrů)

PREAMBULE

Výbor ministrů, podle podmínek stanovených v článku 15.b Statutu Rady Evropy, má na zřeteli, že cílem Rady Evropy je dosažení větší jednoty mezi jejími členy; vědom si rostoucího používání automatizovaného zpracování dat ve vztazích mezi zaměstnavateli a zaměstnanci a tomu odpovídajících výhod; přesvědčen však, že užívání metod automatizovaného zpracování dat zaměstnavateli by se mělo řídit zásadami, které jsou navrženy k minimalizaci jakýchkoli rizik, která by takové metody případně mohly představovat pro práva a základní svobody zaměstnanců, zejména pokud jde o právo na soukromí; má ve této věci na paměti ustanovení Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981 a potřebu přizpůsobit je zvláštním požadavkům v oblasti zaměstnání; uznáváje též, že zájmy, které je třeba mít na paměti při zpracování zásad pro oblast zaměstnání, jsou jak individuální, tak kolektivní povahy; vědom si rozdílných tradic existujících v členských státech, jimiž se řídí různé aspekty vzájemných vztahů mezi zaměstnavatelem a zaměstnancem, přičemž úprava zákonem je pouze jednou z metod regulace; připomíná v této souvislosti článek 6 Evropské sociální charty ze dne 18. října 1961, doporučuje, aby vlády členských států:

- zajistily, aby se zásady obsažené v tomto doporučení odrážely v provádění vnitrostátních právních předpisů o ochraně dat v oblasti zaměstnání, jakož i v ostatních částech právního řádu týkajících se používání osobních údajů pro účely zaměstnání;
- zajistily k tomuto účelu, aby na toto doporučení byly upozorněny orgány zřízené podle vnitrostátních předpisů o ochraně dat, v jejichž působnosti je dozor nad prováděním těchto právních předpisů;
- podporovaly přijetí a uplatňování zásad obsažených v tomto doporučení tím, že zajistí jejich šíření mezi orgány zastupujícími jak zaměstnavatele, tak zaměstnance.

1. Oblast působnosti a definice

1.1 Zásady stanovené v tomto doporučení se vztahují na shromažďování a používání osobních údajů pro účely zaměstnání jak ve veřejném, tak v soukromém sektoru. Tyto zásady se vztahují na automatizovaně zpracovávaná data, jakož i na jiné údaje o zaměstnancích vedené zaměstnavateli, pokud jsou to informace nezbytné k tomu, aby automatizovaně zpracovávaná data byla srozumitelná. Ruční zpracování dat by zaměstnavatelé neměli používat k obcházení zásad obsažených v tomto doporučení.

1.2 Bez ohledu na zásadu stanovenou v odst. 1.1, druhý pododstavec, může členský stát rozšířit zásady tohoto doporučení na ruční zpracování obecně.

1.3 Pro účely tohoto doporučení:

¹ Jedná se o překlad Úřadu pro ochranu osobních údajů, který má pouze neoficiální, informační charakter (viz www.uouu.cz).

Výraz „osobní údaje“ zahrnuje jakoukoli informaci o určeném nebo určitelném jednotlivci. Jednotlivec není považován za „určitelného“, pokud jeho identifikace vyžaduje nepřiměřené množství času, nákladů a lidského úsilí.

Výraz „účely zaměstnání“ se týká vztahů mezi zaměstnavateli a zaměstnanci, které souvisejí s náborem zaměstnanců, plněním pracovní smlouvy, řízením včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, jakož i s plánováním a organizací práce.

1.4 Pokud ustanovení vnitrostátních právních předpisů neurčí jinak, zásady tohoto doporučení se uplatní tam, kde je to vhodné, pro činnosti personálních agentur, ať už ve veřejném nebo soukromém sektoru, které shromažďují a používají osobní údaje, aby bylo možno uzavřít pracovní smlouvu mezi osobami u nich registrovanými a budoucími zaměstnavateli.

1.5 Toto doporučení se v rozsahu nezbytném pro ochranu bezpečnosti státu, veřejnou bezpečnost a potlačování trestné činnosti nevztahuje na důvěrné informace shromažďované nebo vedené zaměstnavateli pro účely zaměstnání o osobách přijímaných na místa nebo pracujících v zaměstnáních, která úzce souvisejí s uvedenými oblastmi.

2. Respekt k soukromí a lidské důstojnosti zaměstnanců

2.1 Respektování soukromí a lidské důstojnosti zaměstnance, zejména možnosti navazovat a udržovat sociální a individuální vztahy na pracovišti, by mělo být zaručeno při shromažďování a používání osobních údajů pro účely zaměstnání.

3. Informování zaměstnanců a konzultace

3.1 V souladu s vnitrostátními právními předpisy nebo s praxí a tam, kde je to vhodné v souladu s příslušnými kolektivními smlouvami, by zaměstnavatelé měli předem plně informovat své zaměstnance nebo zástupce zaměstnanců nebo s nimi konzultovat ve věci zavedení nebo úpravy automatizovaných systémů pro shromažďování dat a využívání osobních údajů o zaměstnancích.

Tato zásada se rovněž vztahuje na zavádění nebo úpravy technických zařízení určených ke sledování pohybu nebo produktivity zaměstnanců.

3.2 Souhlas zaměstnanců nebo jejich zástupců by měl být vyžádán před zavedením nebo úpravou těch systémů nebo zařízení, kde postup konzultace, uvedený v odstavci 3.1, odhalí možnost porušení práva zaměstnanců na respektování soukromí a lidské důstojnosti, pokud vnitrostátní právní předpisy nebo praxe neposkytují jiná náležitá ochranná opatření.

4. Shromažďování dat

4.1 Osobní údaje by měly být zásadně získávány od jednotlivých zaměstnanců. Jestliže je vhodné použít informace ze zdrojů mimo rámec pracovních vztahů, příslušný jednotlivec by měl být informován.

4.2 Osobní údaje shromažďované zaměstnavateli pro účely zaměstnání by měly být přiměřené a míru nepřesahující, v závislosti na typu zaměstnání nebo na vývoji informačních potřeb zaměstnavatele.

4.3 Během náborem zaměstnanců by shromažďovaná data měla být omezena na údaje nezbytné k vyhodnocení vhodnosti budoucích kandidátů a jejich předpokladů profesionálního růstu.

V průběhu takového postupu by osobní údaje měly být získávány pouze od dotyčného jednotlivce. S výhradou ustanovení vnitrostátních právních předpisů lze využívat jiných

zdrojů než těch, kterými jsou dotyční jednotlivci, pouze s jejich souhlasem, nebo pokud byli předem o této možnosti informováni.

4.4 Využívání zdrojů, jako jsou testy, analýzy a podobné postupy koncipované pro posouzení charakteru nebo osobnosti jednotlivce by nemělo být přípustné bez jeho souhlasu nebo jestliže vnitrostátní právní předpisy neposkytují jiná přiměřená ochranná opatření. Pokud si tak přeje, měl by být informován o výsledcích těchto testů.

5. Ukládání dat

5.1 Ukládání osobních údajů je přípustné pouze pokud data byla shromážděna v souladu s pravidly uvedenými v odstavci 4 a pokud ukládání má sloužit pro účely zaměstnání.

5.2 Ukládaná data by měla být přesná, tam kde je to nutné aktualizovaná, a měla by věrně odrážet situaci zaměstnance. Neměla by být ukládána nebo kódována způsobem, který by zasahoval do práv zaměstnance tím, že by ho bez jeho vědomí umožňoval charakterizovat nebo profilovat.

5.3 Pokud jsou ukládána data hodnotící výkon nebo potenciál jednotlivých zaměstnanců, měla by taková data být založena na korektním a čestném hodnocení a nesmějí být urážlivá ve způsobu, jakým jsou formulována.

6. Interní používání dat

6.1 Osobní údaje shromažďované pro účely zaměstnání by měly být použity zaměstnavateli pouze pro tyto účely.

6.2 Pokud mají být data použita pro účely zaměstnání, které jsou odlišné od účelu, pro něž byla původně shromážděna, měla by být přijata odpovídající opatření, aby nedošlo k mylné interpretaci dat v jiném kontextu a aby se zajistilo, že nebudou použita způsobem neslučitelným s původním účelem. V případě, že mají být na základě takto použitých dat učiněna důležitá rozhodnutí s dopadem na zaměstnance, měl by být informován.

6.3 Propojování souborů obsahujících osobní údaje shromažďované a ukládané pro účely zaměstnání podléhá ustanovením odstavce 6.2.

7. Sdělování dat zástupcům zaměstnanců

V souladu s vnitrostátními právními předpisy a praxí nebo s podmínkami kolektivních smluv mohou být osobní údaje sdělovány zástupcům zaměstnanců do té míry, v jaké jsou tato data nezbytná pro zastupování zájmů zaměstnanců.

8. Externí sdělování dat

8.1 Osobní údaje shromážděné pro účely zaměstnání by měly být sdělovány veřejným orgánům pro účely jejich úředního poslání pouze v rozsahu vymezeném zákonnými povinnostmi zaměstnavatelů nebo v souladu s jinými ustanoveními vnitrostátních právních předpisů.

8.2 Ke sdělování osobních údajů veřejným orgánům pro účely jiné než je výkon jejich úředního poslání nebo stranám jiným než veřejným orgánům, včetně podniků v téže skupině, by mělo docházet pouze: pokud je sdělení nezbytné pro účely zaměstnání, které nejsou neslučitelné s účely, pro které byla data původně shromážděna a pokud zaměstnanci nebo jejich zástupci jsou o tom informováni; nebo

s výslovným a informovaným souhlasem jednotlivého zaměstnance; nebo pokud je sdělování povoleno vnitrostátními právními předpisy.

9. Přeshraniční toky dat

Přeshraniční přenos osobních údajů shromažďovaných a ukládaných pro účely zaměstnání by se měl řídit zásadami uvedenými v odstavcích 6 a 8.

10. Zvláštní kategorie dat

10.1 Osobní údaje týkající se rasového původu, politických názorů, náboženského nebo jiného přesvědčení, pohlavního života nebo odsouzení za trestné činy, uvedené v článku 6 Úmluvy o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat, by měly být shromažďovány a ukládány pouze ve zvláštních případech v rozsahu vymezeném vnitrostátními právními předpisy a v souladu s náležitými, jimi stanovenými, ochrannými opatřeními. Pokud taková ochranná opatření chybějí, měla by být tato data shromažďována a ukládána jen s výslovným a informovaným souhlasem zaměstnanců.

10.2 Zaměstnanec nebo uchazeč o zaměstnání smí být dotazován pouze na zdravotní stav a být lékařsky vyšetřován za účelem: stanovení vhodnosti zaměstnance nebo uchazeče o zaměstnání pro jeho současné nebo budoucí zaměstnání; splnění požadavků preventivního lékařství; nebo přiznání sociálních výhod.

10.3 Zdravotní data nesmějí být shromažďována ze zdrojů jiných než od příslušného zaměstnance s výjimkou, kdy udělil svůj výslovný a informovaný souhlas nebo je to v souladu s ustanoveními vnitrostátních právních předpisů.

10.4 Zdravotní data, na která se vztahuje lékařské tajemství, by měla být ukládána pouze personálem, který je vázán pravidly lékařského tajemství. Informace by měly být sdělovány pouze ostatním zaměstnancům personálního útvaru, pokud je to nezbytné pro jeho rozhodování a v souladu s ustanoveními vnitrostátních právních předpisů.

10.5 Zdravotní data, na která se vztahuje lékařské tajemství, by měla být ukládána odděleně od ostatních kategorií osobních údajů vedených zaměstnavatelem. Měla by být učiněna bezpečnostní opatření, aby se předešlo přístupu jiných osob, než těch, které vykonávají lékařskou službu.

10.6 Právo subjektu údajů na přístup k jeho zdravotním datům by nemělo být omezováno kromě případů, kdy by přístup k takovým datům mohl subjekt údajů vážně poškodit, a v takovém případě mu smějí být data sdělena prostřednictvím lékaře, kterého si vybere.

11. Sdělování informací týkajících se osobních údajů

11.1 Informace týkající se osobních údajů vedených zaměstnavatelem by měla být poskytnuta dotyčnému zaměstnanci přímo nebo prostřednictvím jeho zástupců, nebo by mu měla být dána na vědomí jinými vhodnými prostředky. Tato informace by měla specifikovat hlavní účely ukládání dat, druh ukládaných dat, kategorie osob nebo orgánů, kterým jsou data pravidelně sdělována a účely a právní základ pro takové sdělování.

11.2 Informace by také měla uvádět práva zaměstnance týkající se jeho dat, jak jsou stanovena v odstavci 12 tohoto doporučení a rovněž tak i způsoby a prostředky pro výkon práva na přístup.

12. Právo na přístup a opravu

12.1 Každému zaměstnanci by na požádání měl být umožněn přístup ke všem osobním údajům vedeným jeho zaměstnavatelem, které se ho týkají a popřípadě zajištěna oprava nebo vymazání těchto dat, pokud jsou vedena v rozporu se zásadami stanovenými v tomto doporučení. V případě hodnotících dat by každý zaměstnanec měl mít právo v souladu s vnitrostátními právními předpisy hodnocení zpochybnit.

12.2 Výkon práv uvedených v odstavci 12.1 může být, v případě vnitřního šetření prováděného zaměstnavatelem, odložen do ukončení šetření, pokud by jinak výsledek šetření byl ohrožen.

12.3 Když je zaměstnanec seznamován s rozhodnutím vycházejícím z automatizovaného zpracování dat vedených zaměstnavatelem, měl by mít právo přesvědčit se, že data byla zpracována zákonným způsobem.

12.4 Pokud ustanovení vnitrostátních právních předpisů nestanoví jinak, zaměstnanec by měl být oprávněn pověřit jím vybranou osobu, aby mu byla nápomocna při výkonu práva na přístup nebo aby toto právo uplatňovala jeho jménem.

12.5 Pro případ, kdy je přístup k datům odmítnut, nebo kdy je požadavek na opravu nebo vymazání odepřen, vnitrostátní právní předpisy by měly stanovovat opravný prostředek.

13. Bezpečnost dat

13.1 Zaměstnavatelé nebo firmy, které mohou zpracovávat data jejich jménem, by měli zavést vhodná technická a organizační opatření koncipovaná k zajištění bezpečnosti a důvěrnosti osobních údajů, ukládaných pro účely zaměstnání, proti neoprávněnému přístupu, použití, sdělování nebo změně.

13.2 Personální útvar, jakož i jakékoli další osoby zabývající se zpracováním dat by měly být průběžně informovány o takových opatřeních a o nutnosti jejich dodržování.

14. Uchovávání dat

14.1 Osobní údaje by neměly být uchovávány zaměstnavatelem po období delší než k jakému opravňují účely vymezené v odstavci 1.3 nebo jaké vyžadují zájmy současného nebo bývalého zaměstnance.

14.2 Osobní údaje předložené v souvislosti se žádostí o zaměstnání by měly být za normálních okolností vymazány, jakmile je zřejmé, že nabídka zaměstnání nebude učiněna.

14.3 Jsou-li takováto data uchovávána s ohledem na další žádosti o zaměstnání, měla by být tato data vymazána, když o to dotýčný uchazeč požádá.

Tam, kde je nezbytné uchovávat data předložená v souvislosti se žádostí o zaměstnání za účelem obhajoby v právních sporech, měla by být uchovávána pouze po odůvodnitelnou dobu.

Při schválení tohoto doporučení si zástupce Irska s uplatněním článku 10.2.c jednacího řádu pro zasedání zástupců ministrů vyhradil právo jeho vlády omezit oblast působnosti tohoto doporučení pouze na automatizovaně zpracovávané údaje a vyloučit z oblasti jeho působnosti zaměstnání v domácnosti a rodinné podniky, kde zaměstnanci jsou pouze členové rodiny.

Směrnice Evropského parlamentu a Rady 95/46/ES

ze dne 24. října 1995

o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 100a této smlouvy,

s ohledem na návrh Komise¹,

s ohledem na stanovisko Hospodářského a sociálního výboru²,

v souladu s postupem podle článku 189b Smlouvy³,

1. vzhledem k tomu, že cíle Společenství, vyjádřené ve Smlouvě ve znění pozměněném Smlouvou o Evropské unii, spočívají ve vytváření stále užšího svazku evropských národů, ve vytváření stále těsnějších vztahů mezi státy, které Společenství sdružuje, v zajišťování hospodářského a sociálního pokroku společným jednáním vedoucím k odstraňování překážek rozdělujících Evropu, v podpoře neustálého zlepšování životních podmínek svých národů, v zachování a posilování míru a svobody, a v podpoře demokracie z hlediska základních práv stvrzovaných ústavami a zákony členských států a ustanoveními Evropské úmluvy o lidských právech a základních svobodách;
2. vzhledem k tomu, že systémy zpracování údajů mají sloužit lidem; že musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat jejich základní svobody a práva, zejména právo na soukromí, a přispívat k hospodářskému a sociálnímu pokroku, k rozvoji obchodu, jakož i dobrých životních podmínek jednotlivců;
3. vzhledem k tomu, že vytvoření a fungování vnitřního trhu, v němž je zajištěn, v souladu s článkem 7a Smlouvy, volný pohyb zboží, osob, služeb a kapitálu, vyžaduje nejen možnost volného pohybu osobních údajů z jednoho členského státu do druhého, ale rovněž ochranu základních práv jednotlivců;
4. vzhledem k tomu, že ve Společenství se stále častěji využívá zpracování osobních údajů v různých oblastech hospodářské a sociální činnosti; že vývoj informačních technologií podstatně usnadňuje zpracování a výměnu těchto údajů;
5. vzhledem k tomu, že hospodářská a sociální integrace vyplývající z vytvoření a z fungování vnitřního trhu ve smyslu článku 7a Smlouvy nezbytně povede k citelnému zvýšení přeshraničního toku osobních údajů mezi všemi účastníky hospodářského a sociálního života členských států, soukromými či veřejnými; že se dále bude zvyšovat výměna osobních údajů mezi subjekty podnikajícími v různých členských státech; že na základě práva Společenství se od správních orgánů členských států vyžaduje, aby spolupracovaly a vyměňovaly si osobní údaje, aby tak mohly plnit své poslání nebo provádět úkoly ve prospěch správních orgánů jiného členského státu v rámci prostoru bez vnitřních hranic vytvořeného vnitřním trhem;
6. vzhledem k tomu, že i posílení vědecké a technické spolupráce a koordinované zavádění nových telekomunikačních sítí ve Společenství vyžadují a usnadňují přeshraniční toky osobních údajů;
7. vzhledem k tomu, že rozdíly mezi členskými státy, pokud jde o úroveň ochrany práv a svobod jednotlivců, zejména práva na soukromí, mohou s ohledem na zpracování osobních údajů zabránit přenosu těchto údajů z území jednoho členského státu na území jiného členského státu; že tyto rozdíly mohou napříště vytvářet překážku výkonu celé skupiny hospodářských činností na úrovni Společenství, narušit hospodářskou soutěž a bránit správním orgánům ve výkonu odpovědnosti, kterou mají na základě práva Společenství; že tyto rozdíly v úrovni ochrany vyplývají z rozdílů mezi vnitrostátními právními a správními předpisy;
8. vzhledem k tomu, že pro odstranění překážek toku osobních údajů musí být úroveň ochrany práv a svobod jednotlivců v souvislosti se zpracováním těchto údajů rovnocenná ve všech členských státech; že tohoto cíle, pro vnitřní trh životně důležitého, nemůže být dosaženo pouze jednotlivými členskými státy, zejména s

¹ Zdroj: www.uouu.cz

přihlednutím k množství odlišností, které se v současné době vyskytují mezi vnitrostátními právními předpisy z této oblasti, a k nezbytnosti koordinovat právní předpisy členských států, aby přeshraniční tok osobních údajů byl upraven koherentně a v souladu s cílem vnitřního trhu ve smyslu článku 7a Smlouvy; že je tedy nezbytný zásah Společenství směřující ke sblížení právních předpisů;

9. vzhledem k tomu, že v důsledku rovnocenné ochrany vyplývající ze sblížení vnitrostátních právních předpisů nebudou moci členské státy nadále bránit mezi sebou volnému pohybu osobních údajů z důvodů ochrany práv a svobod jednotlivců, zejména práva na soukromí; že členské státy budou mít k dispozici volný prostor, kterého budou moci v souvislosti s prováděním směrnice využít hospodářští a sociální partneři; že budou moci upřesnit ve svých právních předpisech obecné podmínky zákonnosti zpracování údajů; že členské státy budou přitom usilovat o zlepšení ochrany zajišťované až dosud jejich právními předpisy; že v mezích tohoto volného prostoru a v souladu s právem Společenství může při provádění směrnice dojít ke vzniku odlišností a že to může mít dopad na pohyb údajů jak uvnitř jednotlivých členských států, tak ve Společenství;
10. vzhledem k tomu, že předmětem vnitrostátních právních předpisů o zpracování osobních údajů je chránit základní práva a svobody, zejména právo na soukromí uznané v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod i v obecných zásadách práva Společenství; že z tohoto důvodu sblížení těchto právních předpisů nesmí vést k oslabení ochrany, kterou zajišťují, ale musí mít naopak za cíl zajištění vysoké úrovně ochrany ve Společenství;
11. vzhledem k tomu, že zásady ochrany lidských práv a svobod, zejména práva na soukromí, obsažené v této směrnici upřesňují a rozšiřují zásady obsažené v Úmluvě Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat;
12. vzhledem k tomu, že zásady ochrany se musí vztahovat na veškerá zpracování osobních údajů kteroukoli osobou, jejíž činnosti spadají do působnosti práva Společenství; že je třeba vyloučit zpracování údajů fyzickou osobou při výkonu činností, které mají výlučně osobní povahu, jako je korespondence nebo vedení adresáře;
13. vzhledem k tomu, že činnosti uvedené v hlavě V a VI Smlouvy o Evropské unii týkající se veřejné bezpečnosti, obrany, bezpečnosti státu nebo činností státu v oblasti trestní nespádají do oblasti působnosti práva Společenství, aniž jsou tím dotčeny povinnosti členských států vyplývající z čl. 56 odst. 2 a článků 57 a 100a Smlouvy; že zpracování osobních údajů nezbytné pro zachování hospodářské stability státu nespádá do působnosti této směrnice, pokud je toto zpracování spojeno s otázkami bezpečnosti státu;
14. vzhledem k tomu, že s ohledem na význam současného rozvoje technologií pro příjem, přenos, úpravu, zaznamenání, uchování či sdělování zvukových a obrazových údajů týkajících se fyzických osob v rámci informační společnosti, má se tato směrnice vztahovat i na zpracování těchto údajů;
15. vzhledem k tomu, že tato směrnice se vztahuje na zpracování těchto údajů, pouze pokud jsou automatizované nebo pokud jsou zpracovávány údaje obsaženy nebo mají být obsaženy v datovém systému uspořádaném podle zvláštních hledisek týkajících se jednotlivců, aby byl umožněn snadný přístup k dotčeným osobním údajům;
16. vzhledem k tomu, že tato směrnice se nevztahuje na zpracování údajů tvořených zvuky či obrazy, jako například údajů zjištěných při dohledu pomocí videokamer, pokud byly zavedeny pro zajištění veřejné bezpečnosti, obrany a bezpečnosti státu, nebo pro výkon činností státu v oblasti trestní nebo pro výkon jiných činností, které nespádají do působnosti práva Společenství;
17. vzhledem k tomu, že na zpracování zvuků a obrazů pro účely žurnalistiky nebo literárního či uměleckého vyjádření, zejména v audiovizuální oblasti, se zásady této směrnice uplatní jen omezeným způsobem podle článku 9;
18. vzhledem k tomu, že z důvodu, aby se zamezilo případům, kdy jednotlivcům nebude poskytnuta ochrana, která jim je zaručena na základě této směrnice, je nezbytné, aby veškeré zpracování osobních údajů uskutečněné ve Společenství dodržovalo právní předpisy některého členského státu; že v této souvislosti je třeba podřídit zpracování údajů prováděné v rámci odpovědnosti správce, který je zřízen v členském státě, právním předpisům tohoto státu;
19. vzhledem k tomu, že zřízení na území členského státu předpokládá účinný a skutečný výkon činnosti prostřednictvím stálého zařízení; že právní forma takového zřízeného subjektu, ať jde o pobočku nebo dceřinou společnost s vlastní právní subjektivitou, není z tohoto hlediska rozhodující; že pokud je stejný správce zřízen na území několika členských států, zejména formou dceřiné společnosti, musí zajistit, aby všechny zřízené subjekty plnily povinnosti stanovené národními právními předpisy, které se vztahují na jejich činnost, zejména s cílem vyloučit jejich obcházení;
20. vzhledem k tomu, že zpracování údajů subjektem zřízeným ve třetí zemi nesmí mařit ochranu jednotlivců stanovenou v této směrnici; že v takovýchto případech je třeba podřídit zpracování dotčených údajů právním předpisům členského státu, ve kterém jsou umístěna zařízení pro zpracování údajů, a přijmout záruky, aby

práva a povinnosti uvedené v této směrnici byly v praxi dodržovány;

21. vzhledem k tomu, že tato směrnice se nedotýká zásad teritoriality platných v oblasti trestního práva;
22. vzhledem k tomu, že členské státy upřesní ve svých právních předpisech nebo při zavádění opatření přijatých k provedení této směrnice obecné podmínky, za kterých je zpracování údajů přípustné; že zejména článek 5 spolu s články 7 a 8 umožňuje členským státům stanovit, nezávisle na obecných pravidlech, zvláštní podmínky pro zpracování údajů ve zvláštních oblastech a pro různé kategorie údajů uvedených v článku 8;
23. vzhledem k tomu, že členské státy jsou zmocněny zajistit zavádění ochrany jednotlivců jak obecným právním předpisem o ochraně jednotlivců v souvislosti se zpracováním osobních údajů, tak právními předpisy pro jednotlivé obory, jako například předpisy platnými pro statistické instituce;
24. vzhledem k tomu, že se tato směrnice nevztahuje na právní předpisy týkající se ochrany právnických osob v souvislosti se zpracováním údajů;
25. vzhledem k tomu, že zásady ochrany se musí odrazit jednak v povinnostech osob, úředních orgánů, podniků, agentur nebo jiných subjektů odpovědných za zpracování údajů, zejména z hlediska kvality údajů, technického zabezpečení, oznamování okolností, za jakých může být zpracování provedeno, orgánu dozoru, jednak v právu poskytnutému jednotlivcům, jejichž údaje jsou zpracovávány, být informován o tom, že jsou zpracovávány, právu přístupu k údajům, právu žádat jejich opravu a právu odmítnout za určitých okolností zpracování;
26. vzhledem k tomu, že zásady ochrany se musí vztahovat na veškeré informace týkající se identifikované či identifikovatelné osoby; že pro určení, zda je osoba identifikovatelná, je třeba přihlídnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jinou osobou pro identifikaci dané osoby; že zásady ochrany se nevztahují na údaje, které byly učiněny anonymními tak, že subjekt údajů již není identifikovatelný; že etické kodexy ve smyslu článku 27 mohou být užitečným nástrojem pro poskytování pravidel pro způsoby, kterými mohou být údaje učiněny anonymními a uchovány v podobě, která již neumožňuje identifikaci dotyčného subjektu údajů;
27. vzhledem k tomu, že ochrana jednotlivců se musí vztahovat jak na automatizované, tak na manuální zpracování údajů; že rozsah této ochrany nesmí být závislý na použitých technických prostředcích, jinak by se vytvořilo vážné riziko jejího obcházení; že nicméně, pokud jde o manuální zpracování, týká se tato směrnice pouze datových systémů a nikoli nestrukturovaných záznamů; že obsah datového systému musí být zejména uspořádán podle specifických hledisek týkajících se jednotlivců, která umožňují snadný přístup k osobním údajům; že v souladu s vymezením v čl. 2 písm. c) mohou být různá hlediska umožňující určit prvky uspořádaného souboru osobních údajů a jednotlivá hlediska upravující přístup k tomuto souboru údajů vymezena každým členským státem; že záznamy nebo soubory záznamů, stejně jako jejich indexace, které nejsou uspořádány podle specifických kritérií, nespádají v žádném případě do oblasti působnosti této směrnice;
28. vzhledem k tomu, že jakékoli zpracování osobních údajů musí být prováděno zákonným a korektním způsobem vůči dotčeným jednotlivcům; že zpracováváné údaje zejména musí být přiměřené, odpovídající a v množství úměrném účelům zpracování; že tyto účely musí být výslovné a legitimní a musí být stanoveny při sběru údajů; že účely zpracování následujícího po jejich sběru nesmějí být neslučitelné s původně stanovenými účely;
29. vzhledem k tomu, že následné zpracování osobních údajů pro historické, statistické nebo vědecké účely se obecně nepovažuje za neslučitelné s účely, pro které byly předtím údaje sbírány, za předpokladu, že členské státy poskytují vhodná ochranná opatření; že tato ochranná opatření musí zejména vyloučit využití údajů na podporu opatření nebo rozhodnutí přijatých vůči kterémukoli jednotlivci;
30. vzhledem k tomu, že zpracování osobních údajů, aby bylo zákonné, musí být také prováděno se souhlasem subjektu údajů nebo musí být nezbytné pro uzavření nebo plnění smlouvy zavazující subjekt údajů, nebo musí být prováděno na základě požadavku právních předpisů, nebo pro splnění úkolu ve veřejném zájmu či vyplývajícího z výkonu veřejné moci, nebo musí být prováděno v právním zájmu fyzické či právnické osoby za podmínky, že zájmy nebo práva a svobody subjektu údajů nejsou převažující; že pro zajištění rovnováhy dotčených zájmů, při zaručení účinné soutěže, mohou členské státy zejména upřesnit podmínky, za kterých mohou být osobní údaje použity nebo zpřístupněny třetí straně v rámci oprávněné běžné podnikatelské činnosti společnosti a jiných subjektů; že členské státy mohou rovněž upřesnit podmínky, za kterých je možno zpřístupňovat třetí straně osobní údaje pro účely marketingu, ať už prováděného komerčně nebo charitativními organizacemi nebo jinými sdruženími či nadacemi, například politické povahy, při dodržení ustanovení umožňujících subjektu údajů vznést námitku proti zpracování údajů, které se ho týkají, aniž by mu vznikly náklady a aniž by musel uvádět důvody;
31. vzhledem k tomu, že zpracování osobních údajů musí být rovněž považováno za zákonné, pokud je

uskutečňováno s cílem chránit zájem důležitý pro život subjektu údajů;

32. vzhledem k tomu, že národním právním předpisům přísluší určit, zda správce zabývající se úkolem vykonávaným ve veřejném zájmu nebo úkolem vyplývajícím z výkonu veřejné moci, musí být správním orgánem nebo jinou fyzickou nebo právnickou osobou podléhající veřejnému nebo soukromému právu, jako například profesionálním sdružením;
33. vzhledem k tomu, že údaje, které svou povahou mohou porušit základní svobody nebo soukromí, by neměly být předmětem zpracování, pokud k tomu nedá subjekt údajů výslovný souhlas; že odchylky z tohoto zákazu nicméně musejí být jednoznačně stanoveny, aby se vyhovělo zvláštním potřebám, zejména pokud je zpracování těchto údajů prováděno k určitým lékařským účelům osobami, které podléhají povinnosti zachovávat služební tajemství, nebo pro výkon povolených činností některých sdružení či nadací, jejichž cílem je umožnit uplatnění základních svobod;
34. vzhledem k tomu, že členské státy musejí být rovněž oprávněny odchýlit se od zákazu zpracovávat kategorie citlivých údajů, pokud to opodstatňuje důležitý veřejný zájem v oblastech jako je zdravotnictví a sociální péče, zejména pro zajištění kvality a rentability postupů používaných pro vyřizování nároků na plnění a služby v rámci zdravotního pojištění, vědecký výzkum a veřejné statistiky; že jim nicméně přísluší, aby poskytly specifická a vhodná ochranná opatření na ochranu základních práv a soukromí jednotlivců;
35. vzhledem k tomu, že zpracování osobních údajů úředními orgány za účelem dosahování cílů stanovených ústavními předpisy nebo mezinárodním veřejným právem ve prospěch oficiálně uznaných sdružení náboženské povahy se uskutečňuje z důležitého veřejného zájmu;
36. vzhledem k tomu, že tam, kde v rámci činností spojených s volbami si fungování demokratického systému v některých členských státech vyžádalo, aby politické strany shromažďovaly údaje týkající se politických názorů občanů, může být zpracování těchto údajů povoleno z důležitého veřejného zájmu za podmínky, že jsou stanovena náležitá ochranná opatření;
37. vzhledem k tomu, že zpracování osobních údajů pro účely žurnalistiky nebo uměleckého či literárního vyjádření, zejména v audiovizuální oblasti, by mělo opravňovat k výjimce z některých ustanovení této směrnice v míře nezbytné pro vytvoření souladu základních práv jednotlivců s informační svobodou, zejména se svobodou získávat a sdělovat informace, jak to zejména zaručuje článek 10 Evropské úmluvy na ochranu lidských práv a základních svobod; že tedy přísluší členským státům, aby stanovily výjimky a omezení, nezbytné pro vytvoření rovnováhy mezi základními právy z hlediska obecných opatření zakládajících oprávněnost zpracování údajů, opatření v oblasti přenosu údajů do třetích zemí a pravomocí orgánů dozoru, aniž by to nicméně vedlo členské státy k tomu, aby zaváděly výjimky z opatření zajišťujících bezpečnost zpracování; že by bylo rovněž vhodné svěřit příslušnému orgánu dozoru v této oblasti alespoň některé pravomoci uplatňované zpětně, které budou spočívat například v pravidelném zveřejňování zprávy nebo v předávání věcí soudním orgánům;
38. vzhledem k tomu, že má-li být zpracování údajů korektní, musí se subjekt údajů o probíhajícím zpracování dozvědět a, pokud jsou údaje získávány od něho, musí dostat přesné a úplné informace o okolnostech jejich shromažďování;
39. vzhledem k tomu, že se některé postupy zpracování týkají údajů, které správce neshromažďoval přímo od subjektu údajů; že navíc údaje mohou být legitimně zpřístupněny třetí straně, i když to nebylo předem stanoveno při jejich získávání od subjektu údajů; že ve všech těchto případech má být subjekt údajů informován při zaznamenávání údajů nebo nejpozději, když jsou údaje poprvé zpřístupňovány třetí straně;
40. vzhledem k tomu, že není ostatně nezbytné ukládat tuto povinnost, pokud je subjekt údajů již informován; že navíc se tato povinnost neuplatní, pokud je zaznamenávání nebo zpřístupnění výslovně stanoveno zákonem nebo pokud není informování subjektu údajů možné nebo by vyžadovalo neúměrné úsilí, což může být případ zpracování pro historické, statistické či vědecké účely; že z tohoto hlediska je možno přihlídnout k počtu subjektů údajů, ke stáří údajů, jakož i k přijatým kompenzačním opatřením;
41. vzhledem k tomu, že každá osoba musí mít možnost uplatnit právo na přístup k údajům, které se jí týkají a které jsou předmětem zpracování, aby především ověřila jejich přesnost a oprávněnost jejich zpracování; že ze stejných důvodů musí mít každý subjekt údajů právo znát postup automatizovaného zpracování údajů, které se ho týkají, alespoň v případě automatizovaných rozhodnutí uvedených v čl. 15 odst. 1; že toto právo nesmí prolomovat obchodní tajemství ani duševní vlastnictví, zejména autorské právo chránící programové vybavení; že to nicméně nesmí vést k odmítnutí poskytnout subjektu údajů veškeré informace;
42. vzhledem k tomu, že členské státy mohou v zájmu nebo za účelem ochrany práv a svobod druhých omezit právo na přístup a na informace; že mohou například specifikovat, že přístup k lékařským údajům může být zajištěn pouze prostřednictvím odborného zdravotnického pracovníka;
43. vzhledem k tomu, že členské státy mohou omezit právo na přístup a na informace a některé povinnosti

správce v míře nezbytné například pro zachování bezpečnosti státu, obrany, veřejné bezpečnosti a významného hospodářského nebo finančního zájmu členského státu nebo Evropské unie, dále také pro vyšetřování a postihování trestných činů nebo pro akce proti porušování etiky v regulovaných profesích; že je vhodné uvést mezi výjimkami a omezeními monitorovací, inspekční či regulační úkoly nezbytné ve třech zmíněných oblastech, které se týkají veřejné bezpečnosti, hospodářských či finančních zájmů a prevence kriminality; že tento přehled úkolů z uvedených tří oblastí se nedotýká legitimacy výjimek a omezení z důvodu bezpečnosti státu a obrany;

44. vzhledem k tomu, že členské státy mohou na základě práva Společenství přijmout výjimky z ustanovení této směrnice týkající se práva na přístup, povinnosti informovat jednotlivce a kvality údajů, aby byly zachovány některé z výše uvedených cílů;
45. vzhledem k tomu, že v případech, kdy by údaje mohly být předmětem oprávněného zpracování z důvodu veřejného zájmu, výkonu veřejné správy nebo právního zájmu fyzické nebo právnické osoby, měl by nicméně každý subjekt údajů mít právo podat ze závažných a legitimních důvodů týkajících se jeho specifické situace námitky proti zpracování jakýchkoli údajů, které se ho týkají; že členské státy mají nicméně možnost stanovit odchylné vnitrostátní předpisy;
46. vzhledem k tomu, že ochrana práv a svobod subjektů údajů v souvislosti se zpracováním osobních údajů vyžaduje, aby byla přijata příslušná technická a organizační opatření, jak při přípravě systému zpracování, tak v průběhu vlastního zpracování, s cílem zajistit především bezpečnost a tím také zabránit jakémukoli neoprávněnému zpracování; že přísluší členským státům dbát na dodržování těchto opatření správci; že tato opatření musejí zajistit odpovídající úroveň bezpečnosti s ohledem na odbornou úroveň a náklady na jejich zavádění v souvislosti s riziky spojenými se zpracováním a s povahou údajů, které mají být chráněny;
47. vzhledem k tomu, že pokud je zpráva obsahující osobní údaje předávána prostřednictvím telekomunikací nebo elektronickou poštou, jejichž jediným účelem je přenos zpráv tohoto typu, bude za správce ve vztahu k údajům obsaženým ve zprávě obvykle považována spíše osoba, která zprávu podává, nežli osoba, která nabízí službu pro její přenos; že nicméně osoby, které nabízejí tyto služby, jsou obvykle považovány za správce ve vztahu ke zpracování doplňujících osobních údajů nezbytných pro fungování služby;
48. vzhledem k tomu, že mechanismy oznámení orgánu dozoru jsou koncipovány tak, aby objasnily účel a vlastnosti všech zpracovatelských operací s cílem ověřit, zda jsou tyto operace ve shodě s vnitrostátními opatřeními přijatými podle této směrnice;
49. vzhledem k tomu, že k vyloučení neodpovídajících administrativních formalit mohou členské státy zavést výjimky z oznamovací povinnosti a zjednodušení požadovaného oznámení v případech, kdy zpracování neohrožuje práva a svobody subjektů údajů, za podmínky, že je v souladu s příslušným vymežujícím opatřením členského státu; že členské státy mohou rovněž zavést výjimku nebo zjednodušení, pokud osoba určená správcem zaručuje, že prováděná zpracování nehrozí poškozením práv a svobod subjektů údajů; že osoba takto určená pro ochranu údajů, ať je zaměstnancem správce či nikoli, musí mít možnost vykonávat svou činnost zcela nezávisle;
50. vzhledem k tomu, že výjimka nebo zjednodušení mohou být zavedeny v případě zpracovatelských operací, jejichž jediným účelem je vedení registru určeného v souladu s vnitrostátním právem pro informování veřejnosti, který je přístupný veřejnosti či jakékoli osobě, která osvědčí právní zájem;
51. vzhledem k tomu, že zjednodušení nebo výjimka z oznamovací povinnosti nezbavují správce žádné další povinnosti vyplývající z této směrnice;
52. vzhledem k tomu, že v této souvislosti dodatečná kontrola provedená kompetentními orgány musí být obecně považována za dostatečné opatření;
53. vzhledem k tomu, že některé zpracovatelské operace mohou nicméně představovat zvláštní rizika pro práva a svobody subjektů údajů z důvodu jejich povahy, jejich rozsahu nebo jejich účelů, jako například vyloučení jednotlivce z užívání práva, výhody nebo smlouvy, nebo z povahy zvláštního použití nové technologie; že náleží členským státům, pokud si to přejí, aby ve svých právních předpisech tato rizika upřesnily;
54. vzhledem k tomu, že s ohledem na veškerá zpracování, k nimž ve společnosti dochází, by měl být objem zpracování spojených s těmito zvláštními riziky omezen; že členské státy musejí zajistit, aby orgán dozoru nebo osoba určená pro ochranu údajů ve spolupráci s orgánem dozoru kontrolovaly takováto zpracování ještě před jejich uskutečněním; že na základě tohoto předběžného šetření může orgán dozoru v souladu s národním právem zaujmout stanovisko nebo vydat povolení ke zpracování údajů; že toto šetření může být rovněž uskutečněno během přípravy legislativního opatření národního parlamentu nebo opatření založeného na tomto legislativním opatření, které vymezuje povahu zpracování a upřesňuje vhodné záruky;
55. vzhledem k tomu, že v případě nedodržování práv subjektů údajů správcem, musí národní právní předpisy stanovit opravné prostředky; že škody, které mohou vzniknout osobám v důsledku nepřípustného zpracování

musí být nahrazeny správcem, který může být zproštěn svého závazku, pokud prokáže, že za škodu není odpovědný, zejména pokud dokáže chybu subjektu údajů nebo v případě vyšší moci; že sankce se musí vztahovat na každou osobu soukromého nebo veřejného práva, která nedodrží národní opatření přijatá na základě této směrnice;

56. vzhledem k tomu, že přeshraniční toky osobních údajů jsou nezbytné pro rozvoj mezinárodního obchodu; že ochrana jednotlivců zaručená ve Společenství touto směrnicí není překážkou přenosům osobních údajů do třetích zemí zajišťujících odpovídající úroveň ochrany; že odpovídající úroveň ochrany poskytovanou třetími zeměmi je třeba hodnotit z hlediska všech okolností souvisejících s jednotlivým přenosem nebo sérií přenosových operací;
57. vzhledem k tomu, že v případě, kdy třetí země naopak neposkytuje odpovídající úroveň ochrany, musí být přenos osobních údajů do této země zakázán;
58. vzhledem k tomu, že výjimky z tohoto zákazu mohou být stanoveny za určitých okolností: pokud subjekt údajů udělil svůj souhlas, pokud je přenos nezbytný v souvislosti se smlouvou anebo se soudním řízením, pokud to vyžaduje ochrana důležitého veřejného zájmu - například v případě mezinárodních přenosů údajů mezi daňovými nebo celními orgány nebo mezi orgány s působností v oblasti sociálního zabezpečení - nebo pokud je přenos prováděn z registru zřízeného právními předpisy, přístupného veřejnosti nebo osobám osvědčujícím právní zájem; že v tomto případě by se takovýto přenos neměl týkat všech údajů nebo celých kategorií údajů obsažených v tomto registru, a že v případě, kdy je registr přístupný osobám osvědčujícím právní zájem by měl být přenos uskutečněn pouze na žádost těchto osob nebo pokud jsou tyto osoby jeho adresáty;
59. vzhledem k tomu, že mohou být přijata zvláštní opatření, aby došlo k náhradě škod způsobených nedostatečnou ochranou ve třetí zemi v případech, kdy správce poskytuje náležitá ochranná opatření; že kromě toho musí být k dispozici mechanismy jednání mezi Společenstvím a takovouto třetí zemí;
60. vzhledem k tomu, že v každém případě mohou být přenosy do třetích zemí uskutečňovány pouze při úplném dodržování předpisů přijatých členskými státy na základě této směrnice a zejména jejího článku 8;
61. vzhledem k tomu, že členské státy a Komise v rámci svých pravomocí musí podněcovat obchodní sdružení a jiné významné zainteresované organizace, aby vypracovaly etické kodexy s cílem podpořit provádění této směrnice, s ohledem na specifickou povahu zpracování v některých oblastech a při dodržování národních předpisů přijatých k jejímu provedení;
62. vzhledem k tomu, že zřízení orgánů dozoru v členských státech, vykonávajících zcela nezávisle své úkoly, je zásadním prvkem ochrany jednotlivců v souvislosti se zpracováním osobních údajů;
63. vzhledem k tomu, že tyto orgány musejí mít nezbytné prostředky pro plnění svých úkolů, včetně pravomoci provádět šetření a zasahovat, zejména pokud jsou těmto orgánům podány stížnosti občanů, nebo pravomoci obrátit se na soud; že musejí přispět k průhlednosti zpracování prováděného ve členském státu, jehož jurisdikci podléhají;
64. vzhledem k tomu, že tyto orgány v různých členských státech se neobejdou při provádění svých úkolů bez vzájemné pomoci s cílem zajistit dodržování pravidel ochrany v celé Evropské unii;
65. vzhledem k tomu, že na úrovni Společenství musí být zřízena Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů a že musí své úkoly plnit zcela nezávisle; že s přihlédnutím ke své specifické povaze musí poskytovat rady Komisi a zejména také přispívat k jednotnému provádění národních předpisů přijatých na základě této směrnice;
66. vzhledem k tomu, že v případě přenosu údajů do třetích zemí, vyžaduje provádění této směrnice, aby Komisi byla udělena výkonná pravomoc a aby byl vytvořen mechanismus v souladu s rozhodnutím Rady 87/373/EHS⁴;
67. vzhledem k tomu, že 20. prosince 1994 došlo k dohodě o modu vivendi mezi Evropským parlamentem, Radou a Komisí v oblasti opatření k provádění dokumentů přijatých postupem podle článku 189b Smlouvy ES;
68. vzhledem k tomu, že zásady uvedené v této směrnici, které se týkají ochrany práv a svobod jednotlivců, zejména jejich práva na soukromí, v souvislosti se zpracováním osobních údajů, mohou být upřesněny nebo doplněny, zejména pro některé obory, zvláštními předpisy odpovídajícími těmto zásadám;
69. vzhledem k tomu, že je vhodné nechat členským státům lhůtu v délce nepřekračující tři roky od nabytí účinnosti národních opatření provádějících tuto směrnici, aby měly možnost potupně uplatnit na všechna již probíhající zpracování údajů nové výše zmíněné národní předpisy; že pro usnadnění jejich efektivního a co nejméně nákladného zavádění bude členským státům poskytnuta další lhůta v délce do dvanácti let od data přijetí této směrnice pro zajištění souladu stávajících manuálních datových systémů s některými ustanoveními

této směrnice; že pokud jsou údaje obsažené v těchto datových systémech během tohoto rozšířeného přechodného období zpracovávány manuálně, musí být uvedení těchto systémů do souladu s těmito ustanoveními provedeno v době provádění tohoto zpracování;

70. vzhledem k tomu, že není nutné, aby subjekt údajů udělil správci znovu souhlas, aby mohl po nabytí účinnosti národních předpisů přijatých k provedení této směrnice pokračovat ve zpracování citlivých údajů nezbytných k provádění smlouvy uzavřené na základě svobodného a vědomého souhlasu před nabytím účinnosti výše zmíněných ustanovení;
71. vzhledem k tomu, že tato směrnice nebrání tomu, aby členský stát reguloval činnosti v oblasti marketingu zaměřeného na spotřebitele, kteří mají bydliště na jeho území, pokud se tato regulace netýká ochrany jednotlivců v souvislosti se zpracováním osobních údajů;
72. vzhledem k tomu, že tato směrnice při provádění zásad v ní stanovených umožňuje vzít v úvahu zásadu práva na přístup veřejnosti k oficiálním dokumentům,

PŘIJALY TUTO SMĚRNICI:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět směrnice

1. Členské státy zajišťují v souladu s touto směrnicí ochranu základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů.
2. Členské státy nemohou omezit ani zakázat volný pohyb osobních údajů mezi členskými státy z důvodů ochrany zajištěné podle odstavce 1.

Článek 2

Definice

Pro účely této směrnice se rozumí:

- a. "osobními údaji" veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, která může být identifikována, přímo či nepřímo, především na základě identifikačního čísla nebo jednoho či více prvků, specifických pro její fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu;
- b. "zpracováním osobních údajů" (zpracování) jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, zpřístupnění prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, vymazání nebo zničení;
- c. "datovými systémy s osobními údaji" (datový systém) jakýkoli uspořádaný soubor osobních údajů přístupných podle specifických kritérií, ať již je tento soubor centralizován, decentralizován nebo rozložen podle funkčního či zeměpisného hlediska;
- d. "správcem" fyzická nebo právnická osoba, úřední orgán, agentura nebo jakýkoli jiný útvar, který sám nebo společně s jinými určuje účel a způsoby zpracování osobních údajů; pokud jsou účel a způsoby zpracování stanoveny národními nebo komunitárními zákony a předpisy, je možné určit správce nebo zvláštní kritéria pro jeho určení prostřednictvím zákonných předpisů jednotlivých států nebo Společenství;
- e. "zpracovatelem" fyzická nebo právnická osoba, úřední orgán, agentura nebo jakýkoli jiný útvar, který zpracovává osobní údaje pro správce;
- f. "třetí osobou" fyzická nebo právnická osoba, úřední orgán, agentura nebo jakýkoli jiný útvar jiný než subjekt údajů, správce, zpracovatel a osoby přímo podléhající správci nebo zpracovateli, které jsou zmocněny ke zpracování údajů;
- g. "příjemcem" fyzická nebo právnická osoba, úřední orgán, agentura nebo jakýkoli jiný útvar, kterým jsou údaje zpřístupněny, ať se jedná či nikoli o třetí osobu; orgány, které mohou získávat údaje v rámci zvláštního šetření, však nejsou považovány za příjemce;
- h. "souhlasem subjektu údajů" jakýkoli svobodný, zřejmý a vědomý projev vůle, kterým subjekt údajů dává najevo

své svolení se zpracováním osobních údajů, které se ho týkají.

Článek 3

Působnost

1. Tato směrnice se vztahuje na zpracovávání osobních údajů zcela nebo částečně automatizovaná, jakož i na zpracovávání jinými než automatizovanými způsoby, které jsou nebo se mají stát součástí datového systému.
2. Tato směrnice se nevztahuje na zpracování osobních údajů:
 - prováděné pro výkon činností, které nespádají do oblasti působnosti práva Společenství a jsou uvedeny v hlavě V a VI Smlouvy o Evropské unii, a v každém případě na zpracovatelské operace, které se týkají bezpečnosti občanů, obrany, bezpečnosti státu (včetně hospodářské stability státu, pokud má tato zpracovatelská operace vazbu na otázky bezpečnosti státu) a činnosti státu v oblasti trestního práva,
 - prováděné fyzickou osobou výlučně v rámci osobních či domácích činností.

Článek 4

Uplatňování národního práva

1. Každý členský stát uplatní při zpracování osobních údajů národní ustanovení, která přijme na základě této směrnice, pokud:
 - a. zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je správce usazen na území několika členských států, musí přijmout nezbytná opatření, aby zajistil, že každá z těchto provozoven bude postupovat v souladu s povinnostmi zakotvenými v relevantních národních zákonech;
 - b. správce není usazen na území členského státu, ale v místě, kde se příslušné národní právní předpisy uplatňují na základě veřejného mezinárodního práva,
 - c. správce není usazen na území Společenství a používá za účelem zpracování osobních údajů prostředky, automatizovaným nebo jiným způsobem, umístěné na území zmíněného členského státu, nejsou-li však tyto prostředky použity pouze pro účely tranzitu přes území Společenství.
2. V případě uvedeném v odst. 1 písm. c) správce musí určit zástupce usazeného na území zmíněného členského státu, aniž je tím dotčena možnost podniknout právní kroky proti správci samotnému.

KAPITOLA II

OBEČNÁ PRAVIDLA PRO ZÁKONNOST ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Článek 5

Členské státy upřesní v mezích ustanovení této kapitoly podmínky, za kterých je zpracovávání osobních údajů zákonné.

ODDÍL I

ZÁSADY PRO KVALITU ÚDAJŮ

Článek 6

1. Členské státy stanoví, že osobní údaje musejí být:
 - a. zpracovány korektně a zákonným způsobem;
 - b. shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Dodatečné zpracování pro historické,

- statistické nebo vědecké účely není považováno za neslučitelné, pokud členské státy poskytnou náležitá ochranná opatření;
- c. přiměřené, relevantní a míru nepřesahující s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány;
 - d. přesné, a je-li to nezbytné, i aktualizované; musí být podniknuty veškeré rozumné kroky k vymazání nebo opravení údajů, které jsou nepřesné nebo neúplné ve smyslu účelů, pro které byly shromážděny nebo dále zpracovávány;
 - e. uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány. Členské státy stanoví náležitá ochranná opatření pro osobní údaje, které jsou uchovávány po dobu delší než výše uvedeno pro historické, statistické či vědecké účely.

2. Dodržování odstavce 1 zajistí správce.

ODDÍL II

ZÁSADY PRO ZPRACOVÁNÍ ÚDAJŮ ZÁKONNÝM ZPŮSOBEM

Článek 7

Členské státy stanoví, že zpracování osobních údajů může být provedeno pouze pokud:

- a. subjekt údajů nezpochybnitelně poskytl souhlas;
nebo
- b. je zpracování nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, nebo se tak děje na žádost subjektu údajů před uzavřením smlouvy;
nebo
- c. je nezbytné pro dodržení povinnosti ze zákona, které podléhá správce;
nebo
- d. je nezbytné pro ochranu důležitých zájmů subjektu údajů;
nebo
- e. je nezbytné k provedení úkolu ve veřejném zájmu nebo uskutečnění úředního výkonu lyvajícího z výkonu veřejné moc, jímž je pověřen správce nebo třetí strana, které jsou údaje zpřístupněny;
nebo
- f. je nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje zpřístupněny, kromě případů, kdy nad těmito zájmy převažují ohledy na základní práva a svobody subjektu údajů, která vyžadují ochranu podle čl. 1 odst. 1.

ODDÍL III

ZVLÁŠTNÍ KATEGORIE ZPRACOVÁNÍ

Článek 8

Zpracování zvláštních kategorií údajů

1. Členské státy zakáží zpracování osobních údajů, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního života.
2. Odstavec 1 se nepoužije, pokud:
 - a. subjekt údajů udělí výslovný souhlas k takovému zpracování, kromě případů, kdy právní předpisy členského státu stanoví, že zákaz uvedený v odstavci 1 nelze zrušit udělením souhlasu subjektem údajů;
nebo
 - b. zpracování je nezbytné pro dodržení povinností a zvláštních práv správce v oblasti pracovního práva, pokud je k tomu zmocněn národními právními předpisy, které stanoví odpovídající ochranná opatření;
nebo
 - c. zpracování je nezbytné na ochranu důležitých zájmů subjektu údajů nebo jiné osoby v případě, že

- subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas;
nebo
- d. zpracování je v rámci jejich legitimních činností a s patřičnými zárukami prováděno nadací, sdružením nebo jakoukoli jinou institucí nevýdělečné povahy, která sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že zpracování se vztahuje pouze na členy této instituce nebo na osoby udržující s ní pravidelné styky související s jejími účely a že tyto údaje nejsou zpřístupňovány třetím osobám bez souhlasu subjektu údajů;
nebo
 - e. zpracování se týká údajů očividně zveřejňovaných subjektem údajů nebo je nezbytné pro založení, uplatnění nebo obranu právních nároků.
3. Odstavec 1 se nepoužije, pokud je zpracování údajů nezbytné pro účely zdravotní prevence, lékařských diagnóz, lékařské péče a ošetřování nebo správy zdravotnických služeb a pokud zpracování těchto údajů provádí odborný zdravotnický pracovník, který je na základě národního práva nebo právních předpisů přijatých příslušnými národními orgány vázán služebním tajemstvím, nebo jiná osoba rovněž podléhající stejné povinnosti dodržovat tajemství.
 4. Za předpokladu poskytnutí vhodných ochranných opatření mohou členské státy z důvodu významného veřejného zájmu stanovit i další výjimky, než jaké jsou uvedeny v odstavci 2 buď prostřednictvím národních právních předpisů, nebo rozhodnutím orgánu dozoru.
 5. Zpracování údajů týkajících se přestupků, rozsudků v trestních věcech nebo bezpečnostních opatření lze provádět pouze pod kontrolou úředního orgánu nebo pokud národní zákony stanoví vhodná specifická ochranná opatření, s výhradou výjimek, které mohou být uděleny členským státem na základě národních předpisů poskytujících vhodná specifická ochranná opatření. Úplný rejstřík rozsudků v trestních věcech musí být v každém případě veden pod kontrolou úředního orgánu. Členské státy mohou stanovit, že údaje týkající se správních sankcí nebo rozsudků v občanských věcech budou rovněž zpracovávány pod kontrolou úředního orgánu.
 6. Odchytky z odstavce 1 stanovené v odstavcích 4 a 5 se oznamují Komisi.
 7. Členské státy určí podmínky, za kterých může být předmětem zpracování národní identifikační číslo nebo jakýkoli jiný obecně užívaný identifikátor.

Článek 9

Zpracování osobních údajů a svoboda projevu

Členské státy stanoví pro zpracování osobních údajů, prováděné výlučně pro účely žurnalistiky nebo uměleckého či literárního projevu, odchytky a výjimky z této kapitoly a z kapitol IV a VI pouze bude-li to nezbytné pro uvedení práva na soukromí v soulad s předpisy upravujícími svobodu projevu.

ODDÍL IV

INFORMOVÁNÍ SUBJEKTU ÚDAJŮ

Článek 10

Informování v případě shromažďování dat od subjektu údajů

Členské státy stanoví, že správce nebo jeho zástupce musí poskytnout subjektu údajů, od něhož shromažďuje údaje, které se ho týkají, alespoň níže uvedené informace, pokud už je subjekt údajů nemá:

- a. totožnost správce a popřípadě jeho zástupce;
- b. účely zpracování, pro které jsou údaje určeny;
- c. jakékoli další informace jako:
 - příjemci nebo kategorie příjemců údajů,
 - skutečnost, zda odpovědi na otázky jsou povinné nebo dobrovolné a případné důsledky neposkytnutí odpovědi,
 - existence práva přístupu a práva na opravu údajů, které se dané osoby týkají, v míře, v jaké jsou tyto další informace nezbytné pro zajištění řádného zpracování dat vůči subjektu údajů, s ohledem na specifické okolnosti jejich shromažďování.

Článek 11

Informování v případě, že data nejsou shromažďována od subjektu údajů

1. Pokud údaje nebyly shromážděny od subjektu údajů, stanoví členské státy, že správce nebo jeho zástupce musí po zaznamenání údajů, nebo pokud se počítá se zpřístupněním údajů třetí osobě, nejpozději při jejich prvním zpřístupnění, poskytnout subjektu údajů alespoň níže uvedené informace, pokud už je subjekt údajů nemá:
 - a. totožnost správce, popřípadě jeho zástupce;
 - b. účely zpracování;
 - c. veškeré další informace jako :
 - kategorie dotčených údajů;
 - příjemci nebo kategorie příjemců údajů,
 - existence práva přístupu a práva na opravu údajů, které se daného subjektu údajů týkají, v míře, v jaké jsou tyto další informace nezbytné pro zajištění řádného zpracování dat vůči subjektu údajů s ohledem na specifické okolnosti jejich shromažďování.
- 2.
3. Odstavec 1 se nepoužije, pokud se ukáže, zejména u zpracování pro účely statistiky nebo historických či vědeckých výzkumů, že poskytnutí takových informací není možné nebo by vyžadovalo neúměrné úsilí, nebo pokud zaznamenávání a sdělování je výslovně upraveno zákonem. V těchto případech členské státy poskytnou patřičná ochranná opatření.

ODDÍL V

PŘÁVO SUBJEKTU ÚDAJŮ NA PŘÍSTUP K DATŮM

Článek 12

Právo přístupu

Členské státy zaručí každému subjektu údajů právo získat od správce:

- a. bez omezení, v rozumných intervalech a bez prodlení nebo nadměrných nákladů:
 - potvrzení, že údaje, které se ho týkají, jsou či nejsou zpracovávány, jakož i informace týkající se alespoň účelu zpracování, kategorií dotčených údajů, a příjemců nebo kategorií příjemců, kterým jsou údaje zpřístupňovány,
 - sdělení srozumitelnou formou, jaké údaje jsou zpracovávány, včetně veškerých dostupných informací o jejich zdroji,
 - oznámení postupu automatického zpracování údajů, které se ho týkají, alespoň v případě automaticky přijímaných rozhodnutí uvedených v čl. 15 odst. 1;
- b.
- c. podle dané situace opravu, vymazání nebo zablokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů;
- d. oznámení třetím stranám, kterým byly údaje sděleny, o jakékoli opravě, vymazání nebo zablokování provedeném v souladu s písmenem b), pokud se to neukáže jako nemožné nebo nevyžaduje neúměrné úsilí.

ODDÍL VI

VÝJIMKY A OMEZENÍ

Článek 13

Výjimky a omezení

1. Členské státy mohou přijmout legislativní opatření s cílem omezit rozsah povinností a práv uvedených v čl. 6 odst. 1, čl. 10, čl. 11 odst. 1, čl. 12 a čl. 21, pokud toto omezení představuje opatření potřebné pro zajištění:
 - a. bezpečnosti státu;
 - b. obrany;
 - c. bezpečnosti občanů;
 - d. předcházení, vyšetřování, odhalování a stíhání trestných činů nebo porušení etických pravidel pro regulované profese;
 - e. významného hospodářského nebo finančního zájmu členského státu nebo Evropské unie, včetně oblasti měnové, rozpočtové a daňové;
 - f. kontrolní, inspekční nebo regulační funkce spojené, i pouze příležitostně, s výkonem veřejné správy v případech uvedených v písmenech c), d) a e);
 - g. ochrany subjektu údajů nebo práv a svobod druhých.

2. S výhradou přiměřených právních záruk vylučujících zejména, že údaje mohou být použity pro účely opatření nebo rozhodnutí vztahujících se na konkrétní osoby, mohou členské státy, pokud jednoznačně neexistuje nebezpečí narušení soukromí subjektu údajů, omezit legislativním opatřením práva uvedená v článku 12, jestliže jsou údaje zpracovávány výlučně pro účely vědeckého výzkumu nebo jsou uchovávány formou osobních záznamů po dobu nepřesahující období nezbytné pro vypracování statistik.

ODDÍL VII

PRÁVO SUBJEKTU ÚDAJŮ NA NÁMITKU

Článek 14

Právo subjektu údajů na námitku

Členské státy přiznávají subjektu údajů právo:

- a. alespoň v případech uvedených v čl. 7 písm. e) a f) vznést kdykoli z vážných a legitimních důvodů souvisejících s jeho osobní situací námitku vůči zpracování údajů, které se ho týkají, pokud národní legislativa nestanovuje jinak. Jde-li o oprávněnou námitku, nesmí zpracování zahájené správcem tyto údaje nadále zahrnovat;
- b. na požádání a bezplatně vznést námitku proti zpracování osobních údajů, které se ho týkají, a které správce hodlá zpracovávat pro účely přímého marketingu, nebo být informován dříve než jsou osobní údaje poprvé zpřístupněny třetím stranám nebo použity jejich jménem pro účely přímého marketingu a musí mu být výslovně nabídnuto právo na bezplatné podání námitky proti takovému zpřístupnění nebo použití údajů.
Členské státy přijmou nezbytná opatření, aby zaručily, že subjekty údajů budou mít povědomí o existenci práva uvedeného v písm. b) prvního pododstavce.

Článek 15

Automatizovaně podložená rozhodnutí

1. Členské státy poskytnou všem osobám právo nestat se subjektem rozhodnutí, zakládajícího právní účinky vůči nim nebo dotýkající se jejich významným způsobem a přijatého pouze na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jejich osobnosti, jako například pracovního výkonu, důvěryhodnosti, spolehlivosti, chování, atd.
2. Členské státy stanoví, aniž jsou tím dotčena jiná ustanovení této směrnice, že osoba může být subjektem rozhodnutí uvedeného v odstavci 1, pokud je toto rozhodnutí:
 - a. přijato v rámci uzavírání nebo plnění smlouvy za podmínky, že žádosti o uzavření nebo o plnění smlouvy podané subjektem údajů bylo vyhověno, nebo že existují vhodná opatření k zabezpečení jeho oprávněných zájmů, jakým je možnost projevit svůj názor; nebo
 - b. povoleno právním předpisem, který rovněž upřesňuje opatření zajišťující ochranu legitimních zájmů subjektu údajů.

ODDÍL VIII

DŮVĚRNOST A BEZPEČNOST ZPRACOVÁNÍ

Článek 16

Důvěrnost zpracování

Jakákoli osoba, která jedná z pověření správce nebo zpracovatele, jakož i sám zpracovatel, který má přístup k osobním údajům, je smí zpracovávat pouze podle pokynů správce, pokud mu zákon neukládá jinak.

Článek 17

Bezpečnost zpracování

1. Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nepřipustnému zničení, náhodné ztrátě, změně, nepovolenému rozšíření nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné formě nepřipustného zpracování.
Tato opatření mají zajistit, s ohledem na stav technického rozvoje a náklady na jejich zavedení, zabezpečení na takové úrovni, aby odpovídalo rizikům, jaké představuje zpracování a povaha údajů, které mají být chráněny.
2. Členské státy stanoví, že správce, pokud toto zpracování neprovádí sám, musí si vybrat zpracovatele poskytujícího dostatečné záruky s ohledem na technická bezpečnostní opatření a organizační opatření usměrňující zpracování, které má být provedeno a zajišťujícího dodržování těchto opatření.
3. Zpracování údajů zpracovatelem musí být upraveno smlouvou nebo právním aktem, který zavazuje zpracovatele vůči správci a který zejména stanoví, že:
 - zpracovatel jedná pouze podle pokynů správce;
 - povinnosti vymezené v odstavci 1 ve smyslu, jak je definují právní předpisy členského státu, ve kterém zpracovatel sídlí, jsou pro něj rovněž závazné.
- 4.
5. Pro zachování důkazů mají být ustanovení smlouvy nebo právního aktu o ochraně údajů a požadavků souvisejících s opatřeními uvedenými v odstavci 1 potvrzena písemně nebo jinou rovnocennou formou.

ODDÍL IX

OZNÁMENÍ

Článek 18

Oznamovací povinnost vůči orgánu dozoru

1. Členské státy stanoví, že správce nebo jeho případný zástupce musí zaslat oznámení orgánu dozoru uvedenému v článku 28, a to před zahájením zcela nebo částečně automatizovaného zpracování nebo řady těchto zpracování sloužícího jednomu nebo několika souvisejícím účelům.
2. Členské státy mohou připustit zjednodušení povinnosti nebo výjimku z této povinnosti pouze v následujících případech a za následujících podmínek:
 - pokud upřesní pro kategorie zpracování, které s přihlédnutím ke zpracovávaným údajům nemohou poškodit práva a svobody subjektu údajů, účely zpracování, údaje nebo kategorie zpracovávaných údajů, kategorii nebo kategorie subjektů údajů, příjemce nebo kategorie příjemců, kterým mají být údaje zpřístupněny a dobu uchování údajů a/nebo
 - pokud správce jmenuje, v souladu s národním právem, kterému podléhá, zmocněnce odpovědného za ochranu osobních údajů, který je zejména pověřen:
 - zajistit nezávislým způsobem interní uplatňování národních předpisů přijatých k provedení této směrnice,
 - vést seznam zpracování provedených správcem, který obsahuje informace uvedené v čl. 21 odst. 2, a zajistí tímto způsobem, že zpracování nemohou poškodit práva a svobody subjektu údajů.

- 3.
4. členské státy mohou stanovit, že se odstavec 1 nevztahuje na zpracování, jejichž jediným účelem je vedení registru, který je podle právních předpisů určen pro informování veřejnosti a je přístupný veřejnosti v obecném smyslu nebo jakékoli osobě, která projeví oprávněný zájem.
5. členské státy mohou stanovit výjimku z oznamovací povinnosti nebo zjednodušení oznámení pro zpracování uvedená v čl. 8 odst. 2 písm. d).
6. členské státy mohou stanovit, že jistá zpracování nebo veškerá neautomatizovaná zpracování zahrnující osobní údaje mají být oznámena nebo učinit tyto zpracovatelské operace předmětem pro zjednodušené oznámení.

Článek 19

Obsah oznámení

1. členské státy upřesní informace, které musí být uvedeny v oznámení. Mají obsahovat alespoň:
 - a. jméno a adresu správce a jeho případného zástupce;
 - b. účel nebo účely zpracování;
 - c. popis kategorie nebo kategorií subjektů údajů a dat nebo kategorií dat, které se na ně vztahují;
 - d. příjemce nebo kategorie příjemců, kterým mohou být údaje zpřístupněny;
 - e. zamýšlené předávání údajů do třetích zemí;
 - f. obecný popis umožňující předběžně posoudit vhodnost opatření přijatých pro zajištění bezpečnosti zpracování ve smyslu článku 17.
2. členské státy upřesní postupy oznámování změn majících vliv na informace uvedené v odstavci 1 orgánu dozoru.

Článek 20

Předběžné kontroly

1. členské státy vymezí ty zpracovatelské operace, které by mohly představovat zvláštní rizika z hlediska práv a svobod subjektu údajů, a dbají na to, aby tato zpracování byla před jejich započítím prošetřena.
2. Tato předběžná šetření jsou prováděna orgány dozoru po obdržení oznámení od správce nebo zmocněnce odpovědného za ochranu údajů, který musí v případě pochybností konzultovat orgán dozoru.
3. členské státy mohou tato šetření provádět rovněž v souvislosti s přípravou opatření národního parlamentu nebo kroků založených na takovém legislativním opatření, které vymezuje povahu zpracování a stanovuje náležitá ochranná opatření.

Článek 21

Zveřejnění zpracování

1. členské státy přijmou opatření, kterými zajistí zveřejnění zpracování.
2. členské státy stanoví, že orgány dozoru povedou registr zpracování oznámených na základě článku 18. Registr má obsahovat alespoň informace vyjmenované v čl. 19 odst. 1 písm. a) až e). Tento registr je přístupný komukoli.
3. Pokud jde o zpracování, která nepodléhají oznámení, členské státy stanoví, že správce nebo jiný subjekt jmenovaný členským státem, poskytnou vhodnou formou komukoli, kdo o to požádá, alespoň informace uvedené v čl. 19 odst. 1 písm. a) až e). členské státy mohou stanovit, že toto ustanovení se nebude vztahovat na zpracování, jejichž jediným účelem je vedení datového souboru, který je na základě právních předpisů určen pro informování veřejnosti a je přístupný veřejnosti nebo jakékoli osobě, která projeví oprávněný zájem.

KAPITOLA III

OPRAVNÉ PROSTŘEDKY, ODPOVĚDNOST A SANKCE

Článek 22

Opravné prostředky

Aniž je tím dotčena možnost opravného prostředku ve správním řízení, který je možno podat, zejména orgánu dozoru uvedenému v článku 28, před předáním věci soudnímu orgánu, stanoví všechny členské státy, že každá osoba má právo na využití opravného prostředku v případě porušení práv, které jí jsou zaručeny národními předpisy, které se vztahují na dotčené zpracování.

Článek 23

Odpovědnost

1. Členské státy stanoví, že kdokoli, kdo byl poškozen neoprávněným zpracováním nebo jinou činností neslučitelnou s národními předpisy přijatými k uplatňování této směrnice, má právo na náhradu utrpěné škody od správce.
2. Správce může být částečně nebo zcela zbaven této odpovědnosti, pokud prokáže, že za vznik škody neodpovídá.

Článek 24

Sankce

Členské státy přijmou vhodná opatření, kterými zajistí uplatňování ustanovení této směrnice, a zejména určí sankce, které se uplatní v případě porušení ustanovení přijatých k provedení této směrnice.

KAPITOLA IV

PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ

Článek 25

Zásady

1. Členské státy stanoví, že k předávání osobních údajů, které jsou předmětem zpracování nebo které mají být předmětem zpracování po předání, do třetích zemí, může dojít, aniž by tím byl dotčen soulad s národními předpisy přijatými podle ostatních ustanovení této směrnice, pouze pokud dotyčná třetí země zajistí odpovídající úroveň ochrany.
2. Odpovídající úroveň ochrany poskytovaná třetí zemí se posoudí s ohledem na všechny okolnosti související s předáním nebo předáváním údajů; zejména se vezme v úvahu povaha údajů, účel a trvání předpokládaného či předpokládaných zpracování, země původu a země konečného určení, právní předpisy, obecné nebo zvláštní, platné v dotčené třetí zemi, jakož i profesní předpisy a bezpečnostní opatření, která jsou zde dodržována.
3. Členské státy a Komise se vzájemně informují o případech, kdy se domnívají, že některá třetí země nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2.
4. Pokud Komise zjistí, postupem podle čl. 31 odst. 2, že třetí země nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku, přijmou členské státy opatření nezbytná pro zamezení jakémukoli předávání údajů stejného druhu do dotčené třetí země.
5. Ve vhodný okamžik Komise zahájí jednání s cílem napravit stav vyplývající ze zjištění podle odstavce 4.
6. Postupem podle čl. 31 odst. 2 Komise může konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku na základě svých národních předpisů nebo svých mezinárodních závazků sjednaných zejména na závěr jednání uvedených v odstavci 5 s cílem zajistit ochranu soukromého života a základních svobod a práv jednotlivců.

Členské státy přijmou opatření nezbytná pro dosažení souladu s rozhodnutím Komise.

Článek 26

Výjimky

1. Odchylně od článku 25 a s výhradou opačných ustanovení jejich národního práva upravujících zvláštní případy členské státy stanoví, že předání nebo vícenásobné předání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2, může být provedeno za podmínky, že:
 - a. subjekt údajů nezpochybnitelně udělil svůj souhlas se zamýšleným předáním; nebo
 - b. předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro splnění předmluvních opatření přijatých na žádost subjektu údajů; nebo
 - c. předání je nezbytné pro uzavření nebo plnění smlouvy, která byla uzavřena nebo má být uzavřena v zájmu subjektu údajů mezi správcem a třetí stranou; nebo
 - d. předání je nezbytné nebo se stává právně závazným pro zachování důležitého veřejného zájmu nebo pro založení, uplatnění nebo obranu právních nároků; nebo
 - e. předání je nezbytné pro ochranu životních zájmů subjektu údajů; nebo
 - f. k předání dochází z veřejného souboru dat, který je na základě právních předpisů určen pro informování veřejnosti a je přístupný veřejnosti nebo jakékoli osobě, která projeví oprávněný zájem, pokud jsou v daném případě splněny právní podmínky tohoto přístupu.
2. Aniž je tím dotčen odstavec 1, může členský stát povolit předání nebo předávání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2, pokud správce poskytne náležitá ochranná opatření pro ochranu soukromí a základních práv a svobod jednotlivců, jakož i pro výkon odpovídajících práv; tato ochranná opatření mohou zejména vyplývat z náležitých smluvních doložek.
3. Členský stát informuje Komisi a ostatní členské státy o povoleních, která udělí podle odstavce 2. Pokud jiný členský stát nebo Komise podají námitky a řádně je odůvodní z hlediska ochrany soukromí a základních lidských práv a svobod, přijme Komise vhodná opatření postupem podle čl. 31 odst. 1. Členské státy přijmou opatření nezbytná pro dosažení souladu s rozhodnutím Komise.
4. Pokud Komise rozhodne postupem podle čl. 31 odst. 2, že určité standardní smluvní doložky představují dostatečná ochranná opatření uvedená v odstavci 2, přijmou členské státy opatření nezbytná pro dosažení souladu s rozhodnutím Komise.

KAPITOLA V

ETICKÉ KODEXY

Článek 27

1. Členské státy a Komise podporují vypracování etických kodexů, které mají přispět s ohledem na specifika různých odvětví k řádnému uplatňování národních právních předpisů přijímaných členskými státy k uplatňování této směrnice.
2. Členské státy stanoví, že profesní sdružení a další organizace zastupující ostatní kategorie správců, které vypracovaly návrhy národních pravidel chování nebo které mají v úmyslu změnit nebo prodloužit platnost stávajících národních etických kodexů, je mohou předložit k posouzení národnímu orgánu. Členské státy stanoví, že tento orgán se mimo jiné ujistí o souladu návrhů, které jsou mu předloženy, s národními předpisy přijatými k uplatnění této směrnice. Pokud to považuje za účelné může si tento orgán vyžádat připomínky subjektů údajů nebo jejich zástupců.
3. Návrhy pravidel ve Společenství, jakož i změny či prodloužení platnosti stávajících pravidel ve Společenství, mohou být předloženy Pracovní skupině podle článku 29. Tato pracovní skupina se kromě jiného vyjádří k souladu předložených návrhů s národními předpisy přijatými k uplatňování této směrnice. Považuje-li to za účelné, vyžádá si připomínky subjektů údajů nebo jejich zástupců. Komise může zajistit vhodnou publicitu kodexům, která tato pracovní skupina schválila.

KAPITOLA VI

ORGÁN DOZORU A PRACOVNÍ SKUPINA PRO OCHRANU JEDNOTLIVCŮ V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Článek 28

Orgán dozoru

1. Každý členský stát pověří jeden nebo několik úředních orgánů dohledem nad dodržováním, na svém území, ustanovení přijatých členskými státy k uplatňování této směrnice.
Tyto orgány jsou při výkonu svěřených funkcí zcela nezávislé.
2. Každý členský stát zajistí, aby orgány dozoru byly konzultovány při přípravě správních opatření nebo předpisů týkajících se ochrany práv a svobod jednotlivců v souvislosti se zpracováním osobních údajů.
3. Každý orgán dozoru má zejména:
 - pravomoci provádět šetření, jako například právo přístupu k údajům, které jsou předmětem zpracování, a shromažďovat veškeré informace nezbytné pro splnění svého kontrolního úkolu,
 - pravomoci účinně zasáhnout, jako například zaujmout stanovisko před zahájením zpracování v souladu s článkem 20 a zajistit vhodné zveřejnění těchto stanovisek nebo pravomoc nařídit zajištění, vymazání nebo zničení údajů nebo dočasně nebo trvale zakázat zpracování nebo pravomoc zaslat správci údajů upozornění či napomenutí nebo pravomoc obrátit se na národní parlament či jiné politické instituce,
 - pravomoc obrátit se na soud v případě porušení národních předpisů přijatých k uplatňování této směrnice nebo pravomoc oznámit toto porušení soudním orgánům.Protí rozhodnutím orgánu dozoru, která dala vzniknout stížnostem, je možné se odvolat k soudu.
- 4.
5. Na orgán dozoru se může obrátit jakákoliv osoba nebo sdružení tuto osobu zastupující se žádostí týkající se ochrany svých práv a svobod v souvislosti se zpracováním osobních údajů. Dotčená osoba je informována o způsobu vyřízení své žádosti.
Na orgán dozoru se může zejména obrátit kdokoli s žádostí o ověření přípustnosti zpracování, pokud se uplatní národní předpisy přijaté na základě článku 13 této směrnice. Osoba je za každých okolností informována, zda k ověření došlo.
6. Orgány dozoru mají v pravidelných lhůtách vypracovat zprávu o své činnosti. Tato zpráva bude zveřejněna.
7. Nezávisle na národním právu, které lze uplatnit pro dané zpracování, je orgán dozoru oprávněn vykonávat na území vlastního členského státu pravomoci, které mu byly uděleny v souladu s odstavcem 3. Každý orgán může být vyzván, aby vykonával své pravomoci na žádost orgánu jiného členského státu.
Orgány dozoru vzájemně spolupracují v míře nezbytné pro plnění svých úkolů, zejména výměnou veškerých prospěšných informací.
8. Členské státy stanoví, že členové a personál orgánů dozoru podléhají povinnosti dodržovat služební tajemství v souvislosti s důvěrnými informacemi, ke kterým mají přístup, a to i po skončení své činnosti.

Článek 29

Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů

1. Zřizuje se Pracovní skupina pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů, dále jen "skupina".
Skupina má poradní a nezávislý status.
2. Skupinu tvoří zástupce orgánu nebo orgánů dozoru určených jednotlivými členskými státy, zástupce orgánu nebo orgánů vytvořených pro instituce a subjekty Společenství a zástupce Komise.
Každý člen skupiny je jmenován institucí, orgánem nebo orgány, které zastupuje. Pokud členský stát určí několik orgánů dozoru, jmenují tyto orgány společného zástupce. Obdobně je tomu v případě orgánů vytvořených pro instituce a subjekty Společenství.
3. Skupina přijímá rozhodnutí prostou většinou zástupců orgánů dozoru.
4. Skupina zvolí svého předsedu. Funkční období předsedy je dva roky. Může být zvolen opakovaně.
5. Sekretariát skupiny zajišťuje Komise.
6. Skupina přijme svůj jednací řád.
7. Skupina projednává otázky zařazené na pořad jednání jejím předsedou buď z jeho podnětu, nebo na žádost zástupce orgánů dozoru nebo Komise.

Článek 30

1. Skupina má tyto úkoly:
 - a. posuzovat veškeré otázky týkající se uplatňování národních předpisů přijatých podle této směrnice s cílem přispívat k jejich jednotnému provádění;
 - b. zaujímat pro Komisi stanovisko o úrovni ochrany ve Společenství a ve třetích zemích;
 - c. poskytovat Komisi poradenství o všech pozměňovacích návrzích k této směrnici, o všech doplňujících nebo zvláštních opatřeních, která by měla být přijata pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů, jakož i o všech ostatních navrhovaných opatřeních ve Společenství, která mají vliv na tato práva a svobody;
 - d. zaujmout stanovisko k etickým kodexům vypracovaným na úrovni Společenství.
2. Pokud skupina zjistí, že mezi právními předpisy a praxí členských států vznikají rozpory, které by mohly narušit rovnocennost ochrany osob v souvislosti se zpracováním osobních údajů ve Společenství, uvedomí o tom Komisi.
3. Skupina může z vlastního podnětu podat doporučení k jakékoli otázce týkající se ochrany osob v souvislosti se zpracováním osobních údajů ve Společenství.
4. Stanoviska a doporučení skupiny jsou předávána Komisi a výboru uvedenému v článku 31.
5. Komise uvedomí skupinu o způsobu zpracování předaných stanovisek a doporučení. Za tím účelem vypracuje zprávu, která je rovněž předána Evropskému parlamentu a Radě. Tato zpráva je zveřejněna.
6. Skupina vypracuje roční zprávu o stavu ochrany fyzických osob v souvislosti se zpracováním osobních údajů ve Společenství a třetích zemích, kterou předá Komisi, Evropskému parlamentu a Radě. Tato zpráva je zveřejněna.

KAPITOLA VII

PROVÁDĚCÍ OPATŘENÍ VE SPOLEČENSTVÍ

Článek 31

Výbor

1. Komisi je nápomocen výbor složený ze zástupců členských států, kterému předsedá zástupce Komise.
2. Zástupce Komise předloží výboru návrh opatření, která mají být přijata. Výbor zaujme stanovisko k návrhu ve lhůtě, kterou může určit předseda s ohledem na naléhavost záležitosti.

Stanovisko je přijato většinou stanovenou v čl. 148 odst. 2 Smlouvy. Při hlasování v rámci výboru je hlasům zástupců členských států přidělena váha vymezená ve zmíněném článku. Předseda nehlasuje. Komise přijímá opatření, která mají být uplatněna okamžitě. Pokud však tato opatření nejsou v souladu se stanoviskem výboru, sdělí je Komise neprodleně Radě. V takovém případě:

- Komise odloží zavedení opatření, o nichž rozhodla, na dobu tří měsíců ode dne sdělení,
- Rada může kvalifikovanou většinou přijmout jiné rozhodnutí ve lhůtě stanovené v první odrážce.

ZÁVĚREČNÁ USTANOVENÍ

Článek 32

1. Členské státy uvedou v účinnost právní a správní opatření nezbytná pro dosažení souladu s touto směrnicí nejpozději do tří let od jejího přijetí. Přijímají-li členské státy tato opatření, musí v nich být učiněn odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
2. Členské státy dbají, aby zpracování probíhající v den nabytí účinnosti národních předpisů přijatých k uplatňování této směrnice byla uvedena v soulad s těmito předpisy nejpozději tři roky po tomto datu. Odchylně od předchozího pododstavce mohou členské státy stanovit, že zpracování údajů, která jsou ke dni nabytí účinnosti národních předpisů přijatých k provedení této směrnice již obsažena v manuálních kartotékách, budou uvedena do souladu s články 6, 7 a 8 této směrnice ve lhůtě dvanácti let od jejího přijetí. Členské státy však umožní subjektu údajů, aby na svou žádost a zejména při výkonu práva na přístup, dosáhla

opravy, vymazání nebo zajištění údajů neúplných, nepřesných nebo uchovávaných způsobem neslučitelným s legitimními účely sledovanými správcem.

3. Odchylně od odstavce 2 mohou členské státy stanovit s výhradou vhodných ochranných opatření, že údaje uchovávané výlučně pro účely vědeckého výzkumu nebudou uvedeny v soulad s články 6, 7 a 8 této směrnice.
4. Členské státy sdělí Komisi znění ustanovení národního práva, která přijmou v oblasti upravené touto směrnicí.

Článek 33

Komise bude pravidelně podávat Evropskému parlamentu a Radě zprávu o uplatňování této směrnice poprvé nejpozději tři roky po dni stanoveném v čl. 32 odst. 1 a popřípadě ji doplní vhodnými pozměňovacími návrhy. Tato zpráva bude zveřejněna.

Komise posoudí zejména uplatňování této směrnice na zpracování údajů tvořených zvuky nebo obrazy, které se týkají fyzických osob, a předloží vhodné návrhy, které se projeví jako nezbytné s ohledem na rozvoj informačních technologií a úroveň pokroku informační společnosti.

Článek 34

Tato směrnice je určena členskými státy.

V Lucemburku dne 24. října 1995.

Za Evropský parlament
předseda
K. HANSCH

Za Radu
předseda
L. ATIENZA SERNA

- (1) OJ (Official Journal) č. C 277, 5. 11. 1990, str. 3 a OJ č. C 311, 27. 11. 1992, str.30
- (2) OJ č. C 159, 17. 6. 1991, str.38
- (3) Názor Evropského parlamentu ze dne 11. března 1992 (OJ č. C 94, 13. 4. 1992, str. 198), potvrzené 2. prosince 1993 (OJ č. C 342, 20. 12. 1993, str.30)
Společné stanovisko Rady ze dne 20. února 1995 (OJ č. C 93, 13. 4. 1995, str.1)
a Rozhodnutí Evropského parlamentu ze dne 15. června 1995 (OJ č. C 166, 3. 7. 1995).
- (4) OJ č. L 197, 18. 7. 1987, str.33

ARTICLE 29 - DATA PROTECTION WORKING PARTY



5062/01/EN/Final
WP 48

Opinion 8/2001

on the processing of personal data in the employment context

Adopted on 13 September 2001

The Working Party has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 14 of Directive 97/66/EC. The Secretariat is provided by:

The European Commission, Internal Market DG, Functioning and impact of the Internal Market. Coordination. Data Protection.
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100-6/136.
Telephone: direct line (+32-2)295.72.58 or 299.27.19, switch-board 299.11.11. Fax: 296.80.10
Internet address: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

Supervisory authorities have regularly dealt with a range of data protection issues in employment. These include:

- accuracy of employee data
- monitoring of personal telephone use
- access to medical information
- use of information on trade union membership
- processing in the course of business mergers or acquisitions

Data Protection laws in the EU confer individual rights to any person concerned by the processing of personal data (e.g.: right of access, right to rectify). As a general rule, these rights apply fully to the employee-employer relationship, and the only possible exceptions are those allowed by Directive 95/46/EC. However, as the provisions of the Directive are rather general, some guidance will be helpful to clarify certain aspects of the application of the above provisions in the employment context.

The European Commission, in the framework of the Social Policy Agenda, has launched a consultation with social partners on data protection in the employment context.

In order to contribute to the uniform application of the national measures adopted under Directive 95/46/EC, the Working Party has set up a subgroup to examine this question¹⁴ and has adopted this opinion.

The subgroup is currently working on a specific opinion which will focus on the application of Directive 95/46/EC to the surveillance and monitoring of electronic communications in the workplace .

2. Processing of personal data at the workplace

Employers and workers, both in the public and the private sector, must be aware that many activities performed routinely in the employment context entail the processing of personal data of workers, sometimes of sensitive information.

In fact, employers are collecting personal data from their workers for many different purposes since the very beginning of the employment relationship or even before. During the recruitment process, individuals applying for a job have to provide personal information to their potential employer who, at the same time, usually processes this personal information in order to assess the merits of the candidates.

The collection and further processing of personal data of workers continues during the whole employment relationship. These processing activities concern in normal circumstances all personal information the employer has requested and/or obtained from his workers.

All employers collect payroll and tax information of their workers. The processing of this personal data is necessary for the performance of the employment relationship or for

¹⁴ The following supervisory authorities have contributed to the work of this subgroup: AT, BE, DE, EL, ES, FR, IR, IT, NL, UK.

compliance with legal obligations (social security, payment of taxes), to which the employer is subject. In some Member States, employers collect and process medical information that they store in sickness records; in other Member States, this information is limited to absence data because of illness.

Employers, indeed, assess their workers' performance by collecting personal information directly from the individuals or by other means, including surveillance and monitoring carried out electronically.

Finally, although the collection of personal data of a given worker normally finishes at the end of his/her employment relationship, the processing of his personal information by the former employer may continue. Employers usually keep employment records for a certain period of time, in many cases for mere compliance with a legal obligation of storing employment records for a prescribed period of time.

Examples of employment records usually involving the processing of personal data covered by Directive 95/46/EC
<i>Application forms and work references</i>
<i>Payroll and tax information-tax and social benefits information</i>
<i>Sickness records</i>
<i>Annual leave records</i>
<i>Unpaid leave/special leave records</i>
<i>Annual appraisal/assessment records</i>
<i>Records relating to promoting, transfer, Training, disciplinary matters.-</i>
<i>Records relating to promoting, transfer, Training, disciplinary matters</i>
<i>Records relating to accident at work</i>
<i>Information generated by computer systems</i>
<i>Attendance records</i>
<i>Family members¹⁵</i>
<i>Reimbursement of expenses, e.g. travel</i>

As the European Court of Human Rights has pointed out in the case *Niemitz v. Germany*:

"Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not."¹⁶

¹⁵ Data processed in order to facilitate access to certain services such as nursery schools, studies, transport/travel, etc

¹⁶ ECHR, 23 November 1992, Series A No. 251/B, para. 29.

United Kingdom

- General Law: Data Protection Act 1998⁵⁶

b) EEA Member States

Norway

- General Law: Personal Data Protection Act⁵⁷
- Specific provisions in the main collective agreement regulate the matter of monitoring the workplace, with consultation and information procedures with Trade Union representatives.

Iceland

- General Law: Act on Protection of Individuals with regard to the Processing of Personal Data No. 77/2000⁵⁸

5. Scope and implementation of the Directive

Directive 95/46/EC applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a relevant filing system or are intended to form part of a filing system. "Personal data" means any information relating to an identified or identifiable natural person. Processing is very widely defined. Thus any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the Directive.

The monitoring of workers' email or Internet access by the employer falls within the Directive's scope. The monitoring of email necessarily involves the processing of personal data. The monitoring of Internet access, unless conducted as such a high level, that access to particular sites or patterns of access cannot be linked to specific individuals, and only aggregated information is produced necessarily involves the processing of personal data about the worker gaining access. The processing of sound and image data in the employment context falls within the scope of the Directive and video surveillance of workers is covered by its provisions.

Not all manual records necessarily fall within the Directive's scope. They only do so if they form part of a 'personal data filing system'. This is defined as any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. Most employment records are likely to fall within this definition. However, in some countries, the implementing measures may exclude some hand-written notes retained outside any form of filing system but given the necessarily structured nature of employment records will include most information kept about workers whether centrally or by line managers.

⁵⁶ <http://wood.ccta.gov.uk/dpr/dpdoc.nsf>

⁵⁷ <http://www.datatilsynet.no/>

⁵⁸ <http://www.personuvernd.is/tolvunefnd.nsf/pages/1E685B166D04084D00256922004744AF>

In addition to the general Data Protection Directive (95/46/EC) the Telecommunications Data Protection Directive (97/66/EC) might also be relevant. This particularises and complements Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector. As well as falling within the scope of Directive 95/46/EC monitoring of electronic communications by employers, including email and Internet access, might also fall within the scope of Directive 97/66/EC, which is being revised in the context of the review of community legal framework on telecommunications.

The Working Party would like to point out that data protection law does not operate in isolation from labour law and practice, and labour law and practice does not operate in isolation from data protection law. There is necessarily an interaction between the two. The precise nature of this interaction varies between Member States, but it is generally the case that:

- the developing use of information and communications technology in employment increases the extent of this interaction because employment practices rely more and more on the processing of personal data to which general data protection principles apply;
- not all problems that arise in the employment context and involve the processing of personal data are exclusively data protection ones;
- the interaction is necessary and valuable and should assist the development of solutions that properly protect workers' interests.

6. Lawfulness of the processing of personal data

Any processing of personal data, including in the employment context, must meet the requirements of Section II of Directive 95/46/EC to be lawful. In any case, it is necessary to establish a lawful basis for processing under Articles 6, 7 and 8 of the Directive (this last Article in the case of sensitive data).

The data controller must also observe other requirements which include:

FURTHER REQUIREMENTS IN ADDITION TO ARTICLES 6, 7 AND 8
INFORMATION TO BE GIVEN TO THE DATA SUBJECTS (ARTICLES 10 AND 11)
THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA (ARTICLE 12)
THE DATA SUBJECT'S RIGHT TO OBJECT TO PROCESSING (ARTICLES 14 AND 15)
CONFIDENTIALITY AND SECURITY OF PROCESSING (ARTICLES 16 AND 17)
NOTIFICATION TO THE SUPERVISORY AUTHORITY (ARTICLES 18,19,20,21)

The Directive allows some limited exemptions from some of the above requirements but not from Article 7 or 8 (Articles 9 and 13).

7. Criteria for making data processing legitimate. Article 7.

At least one of the criteria set out in Article 7 must be satisfied if personal data are to be processed in the employment context. Each of these criteria requires that in any case, in which it is relied on the processing that takes place is actually “necessary for” the achievement of the objective in question rather than merely incidental to its achievement.

Those most likely to be relevant are:

PROCESSING IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY...
(ARTICLE 7.1.B)

Employment relationships are very often based on a contract of employment between the employer and worker. To meet its obligations under the contract to, for example, pay the worker, the employer must process some personal data.

PROCESSING IS NECESSARY FOR COMPLIANCE WITH A LEGAL OBLIGATION...
(ARTICLE 7.1.C)

Employment law may impose legal obligations on the employer, which necessarily require the processing of personal data. The employer may be under a legal obligation to make certain disclosures of personal data, for example, to the tax authorities or to process data or in connection with social security payments.

PROCESSING IS NECESSARY FOR THE PURPOSES OF THE LEGITIMATE INTERESTS PURSUED BY THE CONTROLLER OR BY THE THIRD PARTY OR PARTIES TO WHOM THE DATA ARE DISCLOSED, EXCEPT WHERE SUCH INTERESTS ARE OVERRIDDEN BY THE INTERESTS FOR FUNDAMENTAL RIGHTS AND FREEDOMS OF THE DATA SUBJECT ...
(Article 7.1.F).

This criterion requires a balance to be struck between the interests of the employer and the interests of workers. Some supervisory authorities have issued guidance on how the balance between the interests of the data controller and the interests of the data subject should be struck. It is important to remember that if this criterion is relied on the worker retains the right to object to the processing on compelling legitimate grounds (Article 14).

Other criteria that are less likely to be relevant in the employment context are:

- **PROCESSING IS NECESSARY IN ORDER TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT.**
(Article 7.1.D)

This may be relevant in the context of the protection of safety.

- **PROCESSING IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST...**

(Article 7.1.E).

The circumstances, in which this criterion is relevant in the employment context, are likely to be very limited.

If none of the criteria are applicable to the processing of a worker's data by an employer, the employer can, alternatively, obtain the worker's unambiguous consent to the processing. The meaning of "consent" is discussed further in Section 11.

8. The processing of sensitive data. Article 8.

The Directive identifies special categories of data, which are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and those concerning health or sex life. The Directive also affords special protection to data relating to offences, criminal convictions or security measures. Member States do not have freedom to add to this list nor to reduce it. They can of course establish special safeguards for certain categories of data, such as genetic data.

Article 8 starts from the proposition that the processing of data in the special categories ("sensitive data") is prohibited. There are then several exceptions, which set out particular circumstances in which the prohibition does not apply. The national laws of some Member States may limit the extent to which employers can take advantage of these exceptions. Thus Member States make more or less extensive use of these exceptions. The Directive allows Member States to lay down additional exceptions for reasons of substantial public interest.

If none of the other exceptions apply an employer can rely on the explicit consent of the data subject for processing sensitive data unless the law of its member state provides that the prohibition on processing sensitive data may not be lifted by the data subject's consent as it is the case, under certain circumstances, for example in Belgium. The extent to which consent can be used in the employment relationship is however limited, as is outlined in section 11.

Example:

Circumstances in which the processing of sensitive data by an employer is limited by national law even though it might fall within one of the exceptions in Article 8 are the processing of data on a worker's medical condition in France and of genetic data in Austria. An example of additional exceptions laid down by Member States is the processing of sensitive data as to racial or ethnic origin for the purpose of ensuring equality of treatment. Several Member States make specific provision for this.

As additional examples, in the employment context the sensitive data most likely to be held by employers, if permitted by national law and provided the purpose limitation principle is respected, include

9. Principles relating to data quality. Article 6.

A data controller must meet the requirements of its national law implementing Article 6 of the Directive as well as satisfying an Article 7 criteria and in the case of sensitive data an Article 8 exception. Article 6 establishes that personal data must be:

- (a) processing fairly and lawfully
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
- (c) adequate, relevant and not excessive
- (d) accurate and, where necessary, kept up-to-date
- (e) kept in a form, which permits identification of data subjects for no longer than is necessary.

These principles apply to the processing of personal data in an employment context as they do elsewhere. They take account of the circumstances in which personal data are processed, including where they are processed by an external subcontractor.

Example:

A record held by a bank that includes a customer's social insurance number may be excessive but if an employer's record does not include this information about workers it may not be sufficient for its purpose. Several supervisory authorities have taken the view that the collection of social insurance numbers from all applicants for jobs is likely to be excessive and thereby breach data protection requirements. It is only the successful applicant who should be required to supply these details.

The requirement that personal data are processed fairly and lawfully provides significant protection. For personal data to be processed lawfully they must be processed in a way that does not bring about a breach of either data protection law or other legal requirements. These may be general legal requirements that are relevant in the employment context, for example a duty of confidence that an employer owes to its workers, or specific legal requirements applying to employment, for example a law prohibiting particular types of discrimination in employment.

For personal data to be processed fairly they must be processed in a way that does not bring about unfairness to the data subject. This is potentially a very wide-ranging requirement. For example worker monitoring, even if it meets the requirements of the Directive in all other respects, must nevertheless be conducted in a way that is "fair" to the workers being monitored. This is an additional proportionality test.

It is important to remember that Articles 6, 7 and 8 have a cumulative effect. The principles set out in Article 6 are a vital element of the protection the Directive gives to workers in relation to the processing of their personal data. Personal data held by an employer may be excessive even if they have been volunteered by a worker who has given consent to their being held. The national laws of some Members States may, in any case, prevent the collection of some data even with consent.

Processing of personal data in the context of worker monitoring may be unfair even if the worker has consented to the monitoring or one of the other Article 7 criteria is met. The fact that consent has been given may be taken into account in determining whether processing satisfies Article 6. How far this is the case varies between members states but the existence of consent is never an overriding consideration.

9.1. Main principles to bear in mind when considering data protection in the employment context

Workers do not leave their right to privacy at the door of their workplace every morning. However, privacy is not an absolute right. It needs to be balanced with other legitimate interests or rights or freedoms. This also applies to the employment context.

Workers, as long as they form part of an organisation, have to accept a certain degree of intrusion in their privacy and they must share certain personal information with the employer. The employer has a legitimate interest in processing personal data of his workers for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the business operation.

The question, therefore, is never whether data processing at the workplace *per se* are lawful activities or not. The real question is what are the limits that data protection imposes to such activities or, the other way around, which are the reasons that may justify the collection and further processing of personal data of any given worker.

Of course, there are not absolute answers to these questions *a priori*. The level of tolerated privacy's intrusion will very much depend on the nature of the employment as well as on the specific circumstances surrounding and interacting with the employment relationship which may have an influence.

Example:

What amount of personal information about a potential worker should be an employer allowed to collect?

The answer to this question would be very different for a security supervisor of the European Investment Bank than for one of the workers in the cafeteria in the same building.

The Working Party would like to identify certain principles extracted from the Directive 95/46/EC, which must govern all personal data processing activities in the employment context. Supervisory Authorities in the Member States are called to play a fundamental role in the application of these general principles to the concrete case, taking properly into account the peculiarities of national legislation.

BASIC DATA PROTECTION PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA OF WORKERS
FINALITY
TRANSPARENCY
LEGITIMACY
PROPORTIONALITY
ACCURACY AND RETENTION OF THE DATA
SECURITY
AWARENESS OF THE STAFF

FINALITY

Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. The Working Party is presently working to provide some guidance in this regard.

Example:

The personal addresses of workers collected for payroll purposes cannot be further used or processed for direct marketing purposes without specific consent. A compatible purpose could be, however, to further process these data in order to calculate and include new travel allowances in the salary.

TRANSPARENCY

It should govern everything. Many processing operations in the employment context in the Member States may be in breach of data protection rules not because such processing is *per se* unlawful, but because workers have not been properly informed about them. As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future.

Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.

Example:

An employer may have a legitimate interest in checking the performance of his clerks by assessing workers' output (for instance, how many cases has a worker dealt with, how many telephone calls has he answered, etc.). In addition to the application of the principles mentioned below, in particular, the proportionality principle, the employer will only be able to process this kind of data, if the workers have been properly informed. If such a surveillance took place without proper information to the staff, the processing of workers' data would be in contradiction with the provisions of Directive 95/46/EC.

LEGITIMACY

Any processing operation, even carried out with full transparency towards workers, can only take place if it is legitimate. Although we have already analysed in depth this question in a separate chapter, it is however important to remind here that Article 7, letter f) of the Directive⁵⁹ does not give employers a blank cheque for any kind of processing with workers' data. Processing not only still needs to pass the test of proportionality, but cannot unjustifiably prejudice the rights and freedoms of the data subjects.

⁵⁹ This Article states: *Member States shall provided that personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the controller, in this case the employer.*

Example:

An employer has a legitimate interest in assessing the performance of its workers, and it will often be necessary for the employer to process personal data to do so. This criterion will only be satisfied if any performance monitoring does not unjustifiably prejudice the rights and freedoms of the data subject. The way, in which it might do so, for example, with some types of email or Internet access monitoring, is discussed in Section 12.

PROPORTIONALITY

Finally, assuming that workers have been informed and the processing is legitimate, the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed⁶⁰.

Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker⁶¹

This requirement of proportionality is potentially wide-ranging and presents several sides in the employment context. However, the most important of its effects is that employers should always process the personal data in the least-intrusive way. Different elements should be considered when looking for the least intrusive way: the risks at stake, the amount of data involved, the purpose of processing, etc.

Example:

Employers may need to know (for certain posts) if applicants have a car and a driver licence. The potential employer is entitled to request such information, but it would go against this principle to ask for the model or the color of applicants' cars.

ACCURACY AND RETENTION OF THE DATA

Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data are not inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified. Employment records must be kept in a form which permits identification of workers for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

⁶⁰ Article 6.1.c) of Directive 95/46/EC

⁶¹ Article 6: *Member States shall provide that personal data must be processed fairly and lawfully.*

Example:

The annual assessment of a worker contains information regarding a concrete date and a given contact. After some years, there is no need in principle to store the information regarding such evaluations. Therefore, the retention period should be limited to two or three years maximum after the evaluation.

Employers can safeguard the accuracy of the workers' personal data, for instance, by providing employees with an annual print-out of their employment record.

SECURITY

The employer must implement appropriate technical and organisational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access. Personal data must remain safe from the curiosity of other workers or third parties. Nowadays, the technology offers reasonable means for preventing such unauthorised access or disclosure, allowing in any case the identification of the staff accessing the files. Where a data processor is used, there must be a contract between the employer and the third party providing security guarantees and ensuring that the processor acts only on the employer's instructions.

Examples of security measures at the workplace:

- Password/identification systems for access to computerised employment records
- Login and tracing of access and disclosures
- Backup copies
- Encryption of messages, in particular when the data is transferred outside the organisation

AWARENESS OF THE STAFF

Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. It would be desirable that employment contracts of this staff include a professional secrecy clause. They need to be alert of the possible consequences of unlawful processing for them, the organisation and, of course, the privacy of other colleagues. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

10. Consent

It should be clear from the preceding discussion that the processing of personal data in the employment context, particularly if sensitive data are not involved, need not in many cases rely on the consent of the worker. Consent should be a fall back position if no other Article 7 criteria or Article 8 exception is applicable. Even where consent is relied on, it must be valid and the employer must still satisfy other requirements of the Directive including Article 6, and Article 15, which addresses automated decisions. Furthermore the worker must have information on the processing as required by Articles 10 and 11.

The Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". In the context of sensitive data consent must, in addition, be explicit. The Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice.

An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment.

THE ARTICLE 29 WORKING PARTY TAKES THE VIEW THAT WHERE AS A NECESSARY AND UNAVOIDABLE CONSEQUENCE OF THE EMPLOYMENT RELATIONSHIP AN EMPLOYER HAS TO PROCESS PERSONAL DATA IT IS MISLEADING IF IT SEEKS TO LEGITIMISE THIS PROCESSING THROUGH CONSENT. RELIANCE ON CONSENT SHOULD BE CONFINED TO CASES WHERE THE WORKER HAS A GENUINE FREE CHOICE AND IS SUBSEQUENTLY ABLE TO WITHDRAW THE CONSENT WITHOUT DETRIMENT.

In other cases the worker should also clearly be provided with information (Article 10) and the Article 7 and Article 8 criteria should be sufficiently broad to legitimise the processing on grounds other than consent.

The Working Party is aware that several Member States' laws have conferred on the local workers' representatives the role of contributing to the protection of workers' rights in the field of data protection. E.g., in some Member States companies must have the agreement of work councils before introducing controls at the workplace.

11. Individual Rights with Regard to Data Protection

As Data Subject, workers benefit from the rights provided by Directive 95/46/EC.

The most important of these rights is the right of access provided for in Article 12 of the Directive by virtue of which every data subject - is entitled to obtain from the controller (the employer in this case):

- a) without constraint at reasonable intervals and without excessive delay or expense:
 - Confirmation as to whether or not data relating to the worker are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed,
 - Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
 - Knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions
- b) as appropriate the rectification, erasure or blocking of data the provisions of which does not comply with data protection law, in particular because of the incomplete or inaccurate nature of the data;
- c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the previous obligation, unless this proves impossible or involves a disproportionate effort.

Data subjects have also the right to object on compelling legitimate grounds relating to his particular situation to the processing by the employer of data relating to him, save where otherwise provided by national legislation (Article 14 of the Directive) and to receive compensation by damages as a result of unlawful processing operation or of any act incompatible with data protection legislation.

The Working Party has already provided a recommendation on employee evaluation data⁶² and may give further guidance in the future.

12. Surveillance and monitoring

Several aspects of the application of both Directives 95/46/EC and 97/66/EC to the surveillance and monitoring of workers have been previously discussed. There should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, internet access, video cameras or location data.

⁶² See Recommendation 1/2001 on Employee Evaluation Data, adopted by the Working Party on 22 March (WP 42, 5008/01).

The application of the Directive to monitoring and surveillance, and the importance attached to the subject is evidenced by developments in Member States, such as those reports and initiatives mentioned in the Introduction.

It should be also clear that

- **any monitoring**, especially if it is conducted on the basis of Article 7(f) of Directive 95/46/EC and, in any case, to satisfy Article 6 **must be a proportionate** response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers.
- **Any personal data** held or used in the course of monitoring must be **adequate, relevant and not excessive for the purpose for which the monitoring is justified**. Any monitoring must be carried out in the least intrusive way possible. It must be targeted on the area of risk, taking into account that data protection rules and, where applicable, the principle of secrecy of correspondence⁶³.
- **Monitoring**, including surveillance by camera, **must comply with the transparency requirements of Article 10**. Workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing. The Directive does not treat less strictly monitoring of an worker's use of an Internet and email system if the monitoring takes place by means of a camera located in the office.

Example:

A specific example which workers may not be aware of is related to **location data**. It is true that the proposed Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector will include protection of location data. This Directive is intended to replace 97/66/EC. Although location data will be specifically mentioned in the new Directive such data **nevertheless fall within the scope of both Directive 95/46/EC and Directive 97/66/EC**. The requirements of proportionality discussed in the previous paragraph apply fully to an employer's processing of location data relating to workers.

The Article 29 Working Party recognises that there is a need for **further guidance on the application of the Directive to the surveillance and monitoring electronic communications of workers (e.g. e-mail, Internet)**. The production of such guidance is challenging and therefore the Working Party has nevertheless asked the sub group that drew up this preliminary opinion to start work on its development.

⁶³ See also Articles 7 and 8 of the EU Charter of Fundamental Rights, signed and proclaimed in Nice on 7 December 2000.

13. Transfer of workers' data to third countries

Article 25 of the Directive establishes that **transfers of personal data to a third country** outside the EU **can only take place** where the third country ensures an **adequate level of protection for the data**.

It must be remembered that whatever the basis of the transfer under Articles 25 and 26 processing involved in the transfer must still satisfy Article 6 to 8 and all the other provisions of the Directive.

Article 26 sets out **derogations** including where:

- the data subject has given his consent unambiguously to the proposed transfer (the same considerations of chapter 10 remain applicable here), or
- the transfer is necessary for the performance of a contract between the data subject and the controller, or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
- the transfer is on the basis of contractual solutions as authorised by a member state as providing adequate safeguards, or
- the transfer is on the basis of standard contractual clauses approved by the Commission as providing adequate safeguards.

The Working Party believes that **it is preferable to rely on** adequate protection in the **ofcountry of destination rather than relying on the derogations listed in Article 26, for example the workers' consent**. Where consent is relied on, it must be unambiguous and freely given. Employers would be ill-advised to rely **solely** on consent other than in cases where, if consent is subsequently withdrawn, this will not cause problems.

If the third country does not ensure an adequate level of protection and none of the derogations apply the employer can, alternatively, obtain the worker's unambiguous consent to the proposed transfer.

The Article 29 Working Party recognises the importance of these provisions in the employment context. It is apparent that a significant proportion of international transfers involves worker data processed by multi-national businesses or groups of businesses. It should be borne in mind that many transfers are from a data controller in the EU to a processor outside. In this case, the employer in the EU remains a data controller required to respond to a request from a worker for access to his/her data and to respect his/her other rights.

14. Conclusions

Directive 95/46/EC applies fully and comprehensively to personal data about workers. Although the Directive gives each Member State a certain margin of manoeuvre to particularise the conditions of such processing operations, the application of the principles contained in this opinion is common and generally recognised. This opinion is aimed at contributing to the uniform application of the national measures adopted under Directive 95/46/EC.

There is a necessary and welcome interaction between data protection law and labour law and practice. Not all problems that involve the processing of personal data are exclusively data protection ones but this interaction is important in ensuring solutions that properly protect the interest of workers.

The legitimate interests of the employer justify certain limitations to the privacy of individuals at the workplace. Sometimes it is the law or the interests of others which impose these limitations. However, no business interest may ever prevail on the principles of transparency, lawful processing, legitimisation, proportionality, necessity and others contained in Directive 95/46/EC. Workers can always object to the processing when it is susceptible of unjustifiably overriding his/her fundamental rights and freedoms.

Given the specificity of the employment relationship, consent will not normally be a way to legitimise the processing in the employment context. Where it is relied on, consent must always be freely given, specific and informed.

The Working Party is considering further guidance on the surveillance and monitoring at the working place, but all the principles described in this opinion fully apply to these activities.

Done at Brussels, 13 September 2001

For the Working Party

The Chairman

Stefano RODOTA

ARTICLE 29 – Data Protection Working Party



5401/01/EN/Final
WP 55

Working document
on the surveillance of electronic communications in the workplace

Adopted on 29 May 2002

Comments:

* national chapters might be further changed in agreement with national delegations

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate A (Functioning and impact of the single market - Coordination - Data protection) of the European Commission's, Internal Market Directorate-General, B-1049 Brussels, Belgium. Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

4. E-MAIL MONITORING

4.1. THE SECRECY OF CORRESPONDENCE

As explained earlier in the working document, the Working Party is of the view that on-line and off-line situations should not be treated differently without reason and as such e-mails benefit from the same protection of fundamental rights as traditional paper mail²¹. The jurisprudence of the European Court of Human Rights has provided some guidance on the application of the principle of the right of secrecy of correspondence in a democratic society. However, Member States' legal systems interpret this principle slightly differently, in particular as regards its scope of application to professional communications, both as regards its content and the traffic data. From the data protection issue it does have important consequences when considering the degree of tolerable intrusion in workers' e-mail.

The Article 29 Working Party is of the view that electronic communications made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention. There is little margin for interpretation as this respect as this issue has been clearly settled by the Court in the case **Halford v. the United Kingdom** mentioned above.

What remains to be seen and indeed allows for certain margin of interpretation is to what extent this principle can be subject to derogations or limitations in particular when it is confronted with the rights and freedoms of others similarly protected by the Convention (e.g. legitimate interests of the employer). In any case, location and ownership of the electronic means used do not rule out secrecy of communications and correspondence as laid down in fundamental legal principles and constitutions.

The Article 29 Working Party would like nevertheless to recall that this is not a specific problem for the processing of personal data in the employment context but a general one, which arises from the fact that data protection laws and regulations do not apply in abstract. Data Protection rights are supposed to apply to different legal systems with other laws in place stipulating other rights and obligations for individuals (e.g. employment law). The Article 29 Working Party is nevertheless convinced that the solutions proposed in this working document can be useful when conducting this difficult balance of interest.

²¹ One of the first recommendations issued by the Working Party, Recommendation 3/97 "Anonymity in Internet", already said that on-line and off-line situations should be treated in the same way.

See http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6en.pdf

The Internet Task Force Paper, most important document adopted by the Working Party on privacy in the Internet, insisted on this idea in its Chapter number 3, page 21:

See http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf

4.2. LEGITIMISATION UNDER DIRECTIVE 95/46/EC

E-mails contain personal data covered by the provisions of Directive 95/46/EC and therefore employers must have a legitimate ground for processing this data. As it was extensively explained in Opinion 8/2001, consent of workers must be freely given and fully informed and employers should not rely on consent as a general means of legitimising such processing.

The most likely legitimisation for e-mail monitoring can be found in Article 7 (f) of the Directive, that is, where processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed. Before considering the application of this provision to the points at issue, it must be pointed out that such legitimisation cannot override fundamental rights and freedoms of the worker. This includes, where applicable, the fundamental right to secrecy of correspondence.

The Working Party has already taken the view that²²:

" Where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment"

Given that e-mails contain personal data of both the sender and the recipient, and employers can only generally obtain the consent of one of these parties without major difficulty (unless the e-mails comprise inter-staff correspondence), the possibility of legitimising the monitoring of e-mails on the basis of such consent is very limited. Similar considerations apply to Article 7 (b) of the Directive as one of the parties to the letter would never have a contract with the data controller within the meaning of this provision, i.e. to monitor the mail.

It should at this juncture, be pointed out, that where a worker is given an e-mail account for purely personal use or is allowed access to web-mail account, opening of e-mails in this account by his employer (apart from scanning viruses) can only be justified in very limited circumstances²³ and cannot under normal circumstances be justified on the basis of Article 7 (f) because it is not in the legitimate interests of the employer to have access to such data. Instead the fundamental right to secrecy of correspondence prevails.

Therefore, the question of the extent to which Article 7 (f) allows the monitoring of e-mails depends on the application on a case by case basis of the fundamental principles explained in Chapter 3.2. As already indicated in chapter 3.1.4 (legitimacy) when

²² See paragraph in a framework in page 23 of Opinion 8/2001.

²³ Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is liable for the actions of the worker, or where he is the victim of the criminal activity.

conducting this balance test proper account should be taken of the privacy of those outside the organisation affected by the monitoring.

4.3 RECOMMENDED MINIMUM INFORMATION THAT THE COMPANY SHOULD PROVIDE TO ITS WORKERS

In drawing up their policy employers must comply with the principles set out in Chapter 3.1.3 under the general Transparency principle²⁴, in the light of the necessities and the size of the organisation.

And more specifically in relation to e-mail the following points should be addressed;

- a) Whether a worker is entitled to have an e-mail account for purely personal use, whether use of web-mail accounts is permitted at work and whether the employer recommends the use, by workers, of a private web-mail account for the purpose of using e-mail for purely personal use (see Chapter 4.4).
- b) The arrangements in place with workers to access the contents of an e-mail, i.e. when the worker is unexpectedly absent, and the specific purposes for such access.
- c) When a backup copy of messages are made, the storage period of it.
- d) Information as to when e-mails are definitively deleted from the server.
- e) Security issues
- f) The involvement of representative of workers in formulating the policy.

It should be noted that there is a continual obligation on the employer to ensure that his policy is kept up to date in line with technological developments and the opinion of his workers.

4.4 WEBMAIL²⁵

24

1. E-mail/Internet policy within the company describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
2. Reasons and purposes for which surveillance, if any, is being carried out. Where the employer has allowed the use of the company's communication facilities for express private purposes, such private communications may under very limited circumstances be subject to surveillance, e.g. to ensure the security of the information system (virus checking).
3. The details of surveillance measures taken, i.e. who? what? when?
4. Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them

²⁵ Webmail is a web e-mail system, which provides web based e-mail from any POP or IMAP server, which is generally user name and password protected.

The Working Party is of the opinion that such a policy of allowing workers the use of a private account or web-mail could contribute to a pragmatic solution of the problem at issue. Such a working document on the part of the employer would clarify the distinction between e-mails for professional and for private use, and would reduce the possibility of employers invading their workers' privacy. Furthermore it would involve no, or minimal, extra cost to the employer.

If an employer adopts such a policy then it would be possible, in specific cases where there is a serious suspicion about the behaviour of a worker, to monitor the extent to which that worker is using their PC for personal purposes by noting the time spent in web-mail accounts. In this way the employers interests would be served without any possibility of worker's personal data, and in particular, sensitive data, being disclosed.

Furthermore such a policy may be of benefit to workers as it would provide certainty for them as to level of privacy they can expect which may be lacking in more complex and confusing codes of conduct. Having said that, it is also necessary to stress that:

- a) the fact that the use of web-mail or private account is allowed does not prejudice the full application of previous sections of this chapter to other e-mail accounts in the workplace
- b) when allowing the use of web-mail, companies should be aware that their use might challenge the security of companies' networks, especially as regards the spreading of viruses.
- c) workers should be aware that sometimes servers of web-mail are located in third countries where there could not be adequate protection of the personal data of individuals.

It should be born in mind that these considerations apply to standard employer-employee relationships. Special rules might need to be applied to the communication of those employees who are bound by obligations of professional secrecy.

5. MONITORING OF INTERNET ACCESS

5.1 PRIVATE USE OF THE INTERNET AT WORK

First and foremost it should be emphasised that it is up to the company to decide if workers are allowed to use the Internet for personal reasons and the extent to which this is permissible.

That point considered however, the Working Party is of the opinion that a blanket ban on personal use of the Internet by employees may be considered to be impractical and slightly unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life.

5.2. PRINCIPLES RELATING TO INTERNET MONITORING

There are some principles, which can be applied when considering the question of monitoring workers access to the Internet.

Wherever possible **prevention should be more important than detection**. In other words the interest of the employer is better served in preventing Internet misuse through technical means rather than in expending resources in detecting misuse. To the extent reasonably possible Internet policy should rely on technical means to restrict access rather than on monitoring behaviour, i.e. by having some sites blocked or installing automatic access warnings.

The delivering of prompt information to the worker on the detection of a suspicious use of the Internet is important in order to minimise problems. Even if a necessary measure, any monitoring must be a **proportionate response** to the risk faced by the employer. In most cases Internet misuse can be detected without the necessity of analysing the content of the sites visited. For example, a check on the time spent, or a check on the sites most frequently visited by a department may suffice to reassure an employer that their facilities are not being misused. If these general checks reveal possible misuse of the Internet, then the employer may consider the possibility of additional monitoring of the area at risk.

When assessing Internet use by workers employers **should try to exercise caution in coming to conclusions**, taking into account the ease with which websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising and miskeying. In any case, workers must have the facts presented to them and be given full opportunity to contest the misuse alleged by the employer.

5.3 RECOMMENDED MINIMUM CONTENT OF COMPANY'S INTERNET POLICY

1. The information specified in Chapter 3.1.3 under the Transparency principle²⁶.
And more specifically in relation to Internet use in particular the following points should be addressed;
2. The employer must set out clearly to workers the conditions on which private use of the Internet is permitted as well as specifying material, which cannot be viewed or copied. These conditions and limitations have to be explained to the workers.
3. Workers need to be informed about the systems implemented both to prevent access to certain sites and to detect misuse. The extent of such monitoring should be specified, for instance, whether such monitoring may relate to individuals or particular sections of the company or whether the content of the sites visited is viewed or recorded by the employer in particular circumstances. Furthermore, the policy should specify what use, if any, will be made of any data collected in relation to who visited what sites.
4. Inform workers about the involvement of their representatives, both in the implementation of this policy and in the investigation of alleged breaches.

26

1. E-mail/Internet policy within the company describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
2. Reasons and purposes for which surveillance, if any, is being carried out. Where the employer has allowed the use of the company's communication facilities for express private purposes, such private communications may under very limited circumstances be subject to surveillance, e.g. to ensure the security of the information system (virus checking).
3. The details of surveillance measures taken, i.e. who? what? when?
4. Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them.

CONCLUSION

The Working Party has drafted this working document to contribute to the uniform application of the national measures adopted under Directive 95/46/EC on the area of surveillance and monitoring of electronic communications in the workplace. (Please see summaries of national legislation in Annex to this document).

The Working Party has noticed some divergences between the national laws, mainly in related areas to data protection dealing with the derogations allowed to the fundamental right to secrecy of correspondence and related to the scope and effect of collective representation and co-decision. The Article 29 Working Party would like to stress, nevertheless, that any divergences between Member States' laws implementing Directive 95/46/EC do not serve as major obstacles to a common approach, which is contained in the principles and good practices outlined in this working document.

The Subgroup on Employment shall keep this working document under review in the light of the experience and further developments in this area during the years 2002- 2003.

Done at Brussels, 29 May 2002

For the Working Party

The Chairman

Stefano RODOTA

ARTICLE 29 Data Protection Working Party



11750/02/EN
WP 89

**Opinion 4/2004 on the Processing of Personal Data
by means of Video Surveillance**

Adopted on 11th February 2004

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: www.europa.eu.int/comm/privacy

artistic expression, in particular in the audio-visual field (see recital no. 17). Only the exceptions necessary to reconcile the right to privacy with the rules governing freedom of expression must be provided¹³. In this connection, special care will be required in particular when installing web cams and/or cameras on line, in order to prevent flaws and gaps in the protection of individuals under video surveillance for purposes that may be found to consist in advertising and/or tourist promotion activities¹⁴.

6. VIDEO SURVEILLANCE AND PROCESSING OF PERSONAL DATA

In the light of the diverse situations mentioned, the Working Party is of the opinion that attention should be drawn to the fact that Directive 95/46/EC applies to the processing of personal data, including image and sound data by means of CCTV and other video surveillance systems, wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

Image and sound data that relate to identified or identifiable natural persons is personal data:

- a) even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars,
- b) even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers,
- c) irrespective of the media used for the processing – e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or BW images -, the technique used – cabled or fibre optic devices -, the type of equipment – stationary, rotating, mobile -, the features applying to image acquisition – i.e. continuous as opposed to discontinuous, which may be the case if image acquisition only occurs in case a speed limit is not respected and has nothing to do with video shootings performed in a wholly casual, piecemeal fashion – and the communication tools used, e.g. the connection with a “centre” and/or the circulation of images to remote terminals, etc. .

Identifiability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices.

Hence, one of the first precautions to be taken by the data controller is to check whether the video surveillance entails the processing of personal data as it relates

¹³ See Recommendation 1/97 of the Working Party on data protection law and the media.

¹⁴ A webcam that had been installed surreptitiously near the stairs leading out of a subway station in Milan showed directly on the Net images of the private parts of women in transit for purposes only seemingly related to journalistic activities. The fact that the persons involved could not be identified did not allow the national data protection authority to take steps in this connection.

to identifiable persons. If so, the Directive applies regardless of national provisions requiring, in addition, authorisation for public security purposes.

This may be the case, for instance, with equipment located either at the entrance of or inside a bank, where said equipment allows identification of customers; conversely, in certain circumstances the applicability of the Directive may be ruled out for air survey images that cannot be usefully magnified or else do not include information related to natural persons – as may be collected to identify water sources or waste disposal areas – as well as for equipment providing sweeping images of motorway traffic.

7. OBLIGATIONS AND APPROPRIATE PRECAUTIONS APPLYING TO THE DATA CONTROLLER

A) Lawfulness of the Processing

Also in the light of the requirement that processing must be lawful (as per Article 6 (a) of the Directive), the data controller must verify in advance whether the surveillance is compliant with the general and specific provisions applying to this sector – such as laws, regulations, codes of conduct having legal relevance. These provisions may also be laid down in connection with public security purposes as well as with purposes other than those related to personal data protection – e.g. the need to obtain ad-hoc authorisations by specific administrative bodies and comply with their instructions.

All suitable measures must be taken in order to ensure that video surveillance is in line with data protection principles, and inappropriate references to privacy should be avoided¹⁵.

In this regard, account should also be taken of best practices as may be set forth in recommendations issued by supervisory authorities as well as in other self-regulatory instruments.

It is also necessary to check the remaining domestic law provisions – including constitutional principles, civil and criminal law provisions – as regards, in particular, those applying to the “droit à l’image”¹⁶ or the protection of one’s domicile; account must be taken of the relevant case law, which may have ruled that premises other than those related to one’s household – such as hotel rooms, offices, restrooms, cloakrooms, in-house phone booths, etc. – are to be regarded as private premises.

Where the equipment has been installed either by private entities or by public bodies, especially local authorities, allegedly for purposes of security or else for detecting, preventing and controlling offences, special care will have to be taken, when determining and informing on said purposes, as to the tasks that may be lawfully

¹⁵ Recently, a bank and a local police station failed to comply with a customer’s request to extract, from the images recorded by a camera also filming an ATM device, those relating to a thief who, after stealing the customer’s bank card, had used it to unlawfully collect money via the cash dispenser – on grounds allegedly related to “privacy”.

¹⁶ This right requires in France and Belgium “prior consent”.

discharged by the data controller – given that certain public functions may only be exercised under the law by specific non-administrative bodies such as, in particular, law enforcement agencies.

This issue has been raised specifically in respect of a few local authorities having no direct competence over public order and public security matters, which nevertheless carry out auxiliary activities for surveillance purposes. Likewise, surveillance that is often accounted for on grounds of crime control is actually aimed at making available evidence in case criminal offences are committed.

B) Specificity, Specification and Lawfulness of Purposes

The data controller should ensure that the purposes sought are neither unclear nor ambiguous, also in order to be provided with a precise criterion when assessing compatibility of the purposes aimed at by the processing (see Article 6 b) of the Directive).

This clarification is also necessary with a view to listing the purposes both in the information to be provided to data subjects and in the relevant notification, as well as in connection with the prior checking to be possibly carried out with regard to the processing in pursuance of Article 20 of the Directive.

It should be clearly ruled out that the images collected may be used for further purposes with particular regard to the technical reproduction opportunities – e.g. by expressly prohibiting copying.

The relevant purposes should be referred to in a document where other important privacy policy features should be also summarised – in respect of such major issues as documenting the time when images are deleted, possible requests for access by data subjects and/or lawful consultation of the data.

C) Criteria Making the Processing Legitimate

The data controller should verify that the video surveillance complies not only with the specific provisions referred to under A), but also with at least one of the criteria making the processing legitimate under Article 7 of the Directive – as regards specifically personal data protection.

Apart from the less frequent cases in which a legal obligation is to be fulfilled – reference has been made to the activities in a casino – or where processing is necessary to protect vital interests – e.g., for the distance monitoring of patients in resuscitation units -, it often happens that a data controller is required to perform a task in the public interest or in the exercise of official authority possibly by complying with specific regulations – e.g. to detect road traffic offences or violent conduct on public transportation means in high-crime areas – as per Article 7 e) of the Directive; alternatively, the data controller may pursue a legitimate interest which is not overridden by the data subject's interests or fundamental rights and freedoms (see Article 7 f)).

In both cases, though especially in the latter one, the sensitive nature of the processing operations requires careful consideration of the scope of the tasks, powers

and legitimate interests concerning the data controller. Superficiality and the groundless extension of the scope of such tasks and powers should be absolutely banned in carrying out this analysis.

As regards, in particular, the balancing of different interests, special attention will have to be paid, also by hearing the parties concerned in advance, to the possibility that an interest deserving protection may be in conflict either with installation of the system or with certain data retention arrangements or other processing operations¹⁷.

Finally, as regards obtaining the data subject's consent, the latter will have to be unambiguous and based on clear-cut information. Consent will have to be provided separately and specifically in connection with surveillance activities concerning premises where a person's private life is led¹⁸.

Lawfulness of the processing should be also assessed by taking account of the provisions in the Directive laying down specific safeguards for the data relating to offences (see Article 8(5) of the Directive)¹⁹.

Additional measures and arrangements might result from the preliminary assessment of the processing in accordance with the prior checking mechanism, if video surveillance carries specific risks for individuals' rights and freedoms (see Article 20 of Directive 95/46/EC).

Processing operations by means of video surveillance should always be grounded on express legal provisions if they are carried out by public bodies.

D) Proportionality of the Recourse to Video Surveillance

The principle that data must be adequate and proportionate to the purposes sought means, in the first place, that CCTV and similar video surveillance equipment may only be deployed on a subsidiary basis, that is to say:

for purposes that actually justify recourse to such systems.

The proportionality principle entails that these systems may be deployed if other prevention, protection and/or security measures, of physical and/or logical nature, requiring no image acquisition – e.g. the use of armoured doors to fight vandalism, installation of automatic gates and clearance devices, joint alarm systems, better and stronger lighting of streets at night etc. – prove clearly insufficient and/or inapplicable with a view to the above legitimate purposes.

¹⁷ Under Section 6b of the new German federal data protection act, which came into force on 23 May 2001, the observation of publicly accessible areas by means of optical and electronic devices is allowed if, inter alia, there are no grounds to believe that it is to be overridden by interests of the data subject deserving protection.

¹⁸ Specific attention should be given to the real possibility to express a valid consent in the meaning of Article 2 h) of Directive 95/46/EC ("any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed") in case of installation of video surveillance in co-ownership (condominiums etc.).

¹⁹ Reference can be made here to Article 8 of the Portuguese Act no. 67/98 as regards the data concerning persons suspected of participation in unlawful and/or criminal activities.

The same principle also applies to the selection of the appropriate technology, the criteria for using the equipment in concrete, and the specification of data processing arrangements as also related to access rules and retention period.

It should be avoided, for instance, that an administrative body may install VS equipment in connection with minor offences – e.g. in order to reinforce the ban on smoking in schools and other public places or else the prohibition to leave cigarette stumps and litter about in public places.

In other words, it is necessary to apply, on a case by case basis, the *principle of adequacy* in respect of the purposes sought, which entails a sort of *data minimisation duty* on the controller's part.

Whilst a proportionate video surveillance and alerting system may be considered lawful if several episodes of violence occur in an area close to a stadium, or if repeated assaults are committed on board buses in peripheral areas or near bus stops, this is not the case with a system aimed either at preventing insults against bus drivers and the dirtying of vehicles – as described to a data protection authority -, identifying citizens liable for minor administrative offences such as the fact of leaving waste disposal bags outside litter bins and/or in areas where no litter is to be left about, or detecting the persons responsible for occasional thefts at swimming halls.

Proportionality should be assessed on the basis of even stricter criteria as regards non-publicly accessible premises.

The exchange of information and experiences among the competent authorities of different Member States may be helpful in this regard ²⁰;

The above considerations apply, in particular, to the increasingly frequent use of video surveillance for the purpose of self-defence and protection of property – above all near public buildings and offices including the surrounding areas. This type of implementation requires assessing, from a more general viewpoint, the indirect effects produced by the massive recourse to video surveillance – i.e., whether the installation of several devices is really an effective deterrent, or whether the offenders and/or vandals may simply move to other areas and activities.

E) Proportionality in Carrying Out Video Surveillance Activities

The principle under which data must be adequate, relevant and not excessive entails careful assessment of the *proportionality of the arrangements* applying to the data processing once the lawfulness of the latter has been validated.

The *filming arrangements* will have to be taken into account in the first place, by having regard, in particular, to the following issues:

²⁰ This would also allow better harmonisation of both regulatory approaches and administrative decisions, which have sometimes diverged – as has been the case, for instance, with Bingo halls.



- a) the visual angle as related to the purposes sought ²¹ - e.g., if the surveillance is performed in a public place, the angle should be such as not to allow visualising details and/or somatic traits that are irrelevant to the purposes sought, or else the areas inside private places located nearby, especially if zooming functions are implemented,
- b) the type of equipment used for filming, i.e. whether fixed or mobile,
- c) actual installation arrangements, i.e. location of cameras, use of fixed-view and/or movable cameras, etc.,
- d) possibility of magnifying and/or zooming in images either at the time the latter are filmed or thereafter, i.e. as regards stored images, and possibility to blur and delete individual images,
- e) image-freezing functions,
- f) connection with a "centre" to send sound and/or visual alerts,
- g) the steps taken as a result of video surveillance, i.e. shutting down of entrances, calling up surveillance staff, etc. .

Secondly, it is necessary to consider the *decision to be taken as to retention of images and retention period* – the latter having to be quite short and in line with the specific features of the individual case.

Whilst in a few cases a system only enabling closed circuit visualisation of images, which are not recorded, may be sufficient – e.g., in the case of the tills at a supermarket –, in other cases - e.g. to protect private premises – it may be justified to record the images for a few hours and automatically erase them, no later than at the end of the day and at least at the end of the week. An exception to this rule will obviously be the case in which an alert has been issued or else a request has been made deserving specific attention; in such cases there are reasonable grounds to await, for a short time, the decision to be possibly taken by either police or judicial authorities.

To quote another instance, a system aimed at detecting unauthorised accesses of vehicles to city centres and restricted traffic areas should only record images in case a breach is committed.

The proportionality issue should also be taken into due account whenever less short retention periods are deemed to be necessary which should not be in excess of one week²² – e.g., as regards video surveillance images that may be used to

²¹ Examples of specific precautions to be taken as regards visual angle may be found in two provisions issued by the Italian Data Protection Authority. A health care body planning introduction of a service allowing relatives to continuously observe, from a distance, patients in a coma, quarantined and/or seriously ill at an emergency care unit was made aware of the need for making suitable arrangements in order to prevent simultaneous visualisation of other patients as well. In another case, the Authority pointed out to police administrative bodies that it was necessary for a system detecting speed limit breaches to only film the relevant plates rather than the inside of vehicles as well.

²² The Danish and Swedish DPA expressed the view that video recording may only be stored in a short period and this period should not exceed 30 days.

identify the persons frequenting the premises of a bank prior to performing a robbery.

Thirdly, attention will have to be paid to the *cases in which identification of a person is facilitated* by associating the images of the person's face with other information concerning imaged conduct and/or activities – e.g., in the case of the association between images and activities performed by clients in a bank at an easily identifiable time.

In this regard, account will have to be taken of the clear-cut difference existing between temporary retention of video surveillance images obtained by means of equipment located at the entrance of a bank and the definitely more intrusive establishment of data banks including photographs and fingerprints provided by bank clients with the latter's consent.

Finally, consideration will have to be given to the decisions to be made in respect of both the *possible communication of the data to third parties* – which in principle should not involve entities that are unrelated to the video surveillance activities – and their total or partial disclosure possibly abroad or even online – also in the light of the provisions concerning adequate protection, see Article 25 and ff. of the Directive.

Obviously, the requirement that images should be relevant and not excessive also applies to the matching of information held by different controllers of video surveillance systems.

The above safeguards are meant to implement, also operationally, the principle referred to in the domestic laws of a few countries as the *principle of moderation in the use of personal data* – which is aimed at preventing or reducing, to the greatest possible degree, the processing of personal data.

This principle should be implemented in all sectors by also having regard to the fact that many purposes can be actually achieved without making recourse to personal data, or by using really anonymous data, even though they may initially seem to require the use of personal information.

The above considerations also apply in the presence of the justified need to streamline business resources²³ or else improve the services delivered to users²⁴.

²³ This may be the case, for instance, with the need to calculate the number of tills to be kept simultaneously open in a supermarket depending on the number of incoming customers, or else with the requirement of building optimised shopping routes for customers in a supermarket.

²⁴ To facilitate access to a working place and/or a specific transportation means requiring identity controls, personal cards with photographs may be enough, possibly on computerised media, without implementing a facial recognition system.

F) Information to Data Subjects

Openness and appropriateness in the use of video surveillance equipment entail the provision of adequate information to data subjects pursuant to Articles 10 and 11 of the Directive.

Data subjects should be informed in line with Article 10 and 11 of the Directive. They should be aware of the fact that video surveillance is in operation, even where the latter is related to public events and shows or else to advertising activities (web cams); they should be informed in a detailed manner as to the places monitored.

It is not necessary to specify the precise location of the surveillance equipment, however the context of surveillance is to be clarified unambiguously.

The information should be positioned at a reasonable distance from the places monitored – unlike what has been done in a few cases, in which location of information plates at 500 metres from the areas under surveillance has been considered acceptable – also in the light of the filming arrangements.

The information should be visible and may be provided in a summary fashion, on condition that it is effective; it may include symbols that have already been proved useful in connection with video surveillance and no-smoking information – which may differ depending on whether the images are recorded or not. The purposes of the video surveillance and the relevant controller will have to be specified in all cases. The format of the information should be adjusted to the individual location.²⁵

Specific, well-grounded limitations to the information requirements may only be allowed in the cases referred to in Articles 10, 11 and 13 of the Directive – e.g., a temporary limitation may apply in respect of the data collected in the course of investigations carried out lawfully by defence counsel, or else with a view to exercising the right of defence, for as long as provision of the information may jeopardise achievement of the specific purposes sought.

Finally, specific attention should be given to the appropriate way to furnish blind persons with the information.

G) Additional Requirements

In connection with such additional requirements, precautions and safeguards as are referred to in data protection legislation and are summarised under point 3) above - also with regard to the need for the processing of personal data to be notified to and subject to the supervision of an independent authority in line with Articles 18, 19 and 28 of the Directive -, the Working Party would like to draw attention, in particular, to the following issues:

- a) A limited number of natural persons, to be specified, should be allowed to view or access the recorded images, if any, exclusively for the purposes sought by means of the video surveillance or else with a view to

²⁵ This could be termed a “layered” approach.

maintenance of the relevant equipment in order to only verify its proper operation; alternatively, this may occur on the basis of either a data subject's request for access or the lawful order issued by police or judicial authority for crime detection purposes.

Whenever video surveillance is only aimed at preventing, detecting and controlling offences, the solution consisting in the use of two access keys – of which one would be held by the controller and the other one by the police – may prove useful in many cases to ensure that images are only viewed by police staff rather than by unauthorised staff – without prejudice to the data subject's legitimate exercise of his right of access by means of a request made during the short image retention period.

- b) Appropriate security measures should be implemented in order to prevent occurrence of the events referred to in Article 17 of the Directive, including dissemination of information that may be helpful to protect a right of the data subject, a third party or the data controller himself – also with a view to preventing manipulation, alteration or destruction of data and related items of evidence.
- c) Quality of the images recorded, if any, is also fundamental – in particular if the same recording media are used repeatedly, which entails the risk of failing to fully erase previously recorded images.
- d) Finally, it is fundamental for the operators concretely involved in video surveillance activities to be adequately trained in and made aware of the steps to be taken to fully comply with the relevant requirements. Training of controllers and operators as also related to the relevant risks and the mechanisms to correctly identify the imaged individuals can be considered to be a useful measure as well.

H) Data Subjects' Rights

The peculiar features of the personal data collected do not rule out exercise by data subjects of the rights referred to in Articles 13 and 14 of the Directive, with particular regard to the right to object to the processing. Directive 95/46 indeed allows the data subject to object at any time to the processing of data relating to him²⁶ on compelling legitimate grounds relating to his particular situation.

The data subjects' right to oblivion and the usually short retention period of the images do narrow the scope of application of the data subjects' right to access personal data that make them identifiable; however, this right is to be safeguarded especially if a detailed request is made such as to allow the relevant images to be easily retrieved. Account will have to be also taken of the need to temporarily safeguard the rights of third parties.

Any limitations grounded on the efforts to be made for retrieving the images, where such efforts are found to be clearly disproportionate in terms of researches, costs and resources on account of the short retention period of the images, should

²⁶ Except where otherwise provided by national legislation

07 6C

be laid down exclusively by primary legislation (see Article 13(1) of the Directive) with due regard for the data subject's right to defence in respect of specific events that may have occurred in the period considered.

I) Additional Safeguards in connection with Specific Processing Operations

It should be prohibited to perform video surveillance exclusively on account of the racial origin of the persons imaged, their religious or political opinions, their membership in trade unions or sexual habits (Article 8 of the Directive).

Without aiming at an exhaustive list of the multifarious applications of video surveillance, the Working Party would like to stress the need to pay greater attention – in principle, where appropriate, within the framework of the prior checking of processing operations mentioned in Article 20 of the Directive – to a few contexts in which images concerning identified or identifiable persons are collected, since these contexts should be evaluated on a case-by-case basis.

Reference is made, in particular, to the following cases as resulting from experiences and/or tests already in progress:

- a) permanent interconnection of video surveillance systems as managed by different data controllers,
- b) possible association of image and biometric data such as fingerprints (e.g. at the entrance of banks),
- c) use of voice identification systems,
- d) implementation, in line with proportionality principles and based on specific provisions, of indexing systems applying to recorded images and/or systems for their simultaneous automatic retrieval, especially via identification data,
- e) use of facial recognition systems that are not limited to identifying camouflages of persons in transit, such as fake beards and wigs, but are based on the targeting of suspected offenders – i.e. on the ability of the system to automatically identify certain individuals on the basis of templates and/or standard identity-kits resulting from certain outward features (such as colour of a person's skin, eyes, protruding cheekbones, etc.), or else on the basis of pre-defined abnormal behaviour (sudden movements, repeated transit even at given intervals, way of parking a vehicle, etc.). In this connection, human intervention is appropriate also in the light of mistakes possibly occurring in these cases as also mentioned with regard to point f) below,
- f) possibility to automatically trace routes and trails and/or reconstruct or foresee a person's behaviour,
- g) taking of automated decisions based either on a person's profile or on intelligent analysis and intervention systems unrelated to standard alerts - such as the fact of accessing a place without the required identification or else a fire alert.

8. VIDEO SURVEILLANCE IN THE EMPLOYMENT CONTEXT

In its *Opinion no. 8/2001 on the Processing of Personal Data in the Employment Context*, adopted on 13 September 2001, and in its *Working Document on the Surveillance of Electronic Communications in the Workplace*, adopted on 29 May 2002²⁷, this Working Party has already drawn attention, in more general terms, to a few principles aimed at safeguarding data subjects' rights, freedoms and dignity in the employment context.

In addition to the considerations made in the above documents, to the extent that they are actually applicable to video surveillance, it is appropriate to point out that video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities, therefore entailing the processing of personal data in this context, should not be permitted as a rule.

The case is different as regards video surveillance systems that are deployed, subject to appropriate safeguards, to meet production and/or occupational safety requirements and also entail distance monitoring - albeit indirectly²⁸.

The implementing experience has shown additionally that surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks - such as toilets, shower rooms, lockers and recreation areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected.

Information must be given to employees and every other person working on the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject, for instance in which cases the recordings would be examined by the management of the company, the recording period and when the recording would be disclosed to the law enforcement authorities. The provision of information for instance through a symbol can not be considered as sufficient in the employment context.

9. CONCLUSION

The Working Party has drafted this working document to contribute to the uniform application of the national measures adopted under Directive 95/46/EC on the area of video surveillance.

* * *

²⁷ Both documents are available at the following address:
www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

²⁸ In these cases, in addition to the considerations made in this document, account should also be taken specifically of the need to respect the rights referred to in collective agreements, which are sometimes based on the collective information of employees and/or their respective trade union organisations - i.e. apart from the information to be provided on an individual basis in pursuance of data protection laws; in other cases, a prior agreement is to be sought either with employees' representatives or trade union organisations as to installation arrangements, also with regard to duration of the surveillance and other filming arrangements. In a few countries, the State's intervention may be required if no agreement is reached between the parties concerned.

In this framework, it is also fundamental that Member States provide guidance as regards the activity of producers, service providers and distributors, and researchers with a view to the development of technologies, software and technical devices that are in line with the principles referred to in this document.

* * *

Done at Brussels, on 11 February 2004
For the Working Party
The Chairman
Stefano RODOTA