# VĚSTNÍK
## ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
## 2007

**Částka 45** **10. srpna 2007** **Cena 77,– Kč**


## OBSAH

# ÚVOD

Čtyřicátá pátá částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací v období od 10. 3. 2007 do 15. 7. 2007.

V rubrice Stanoviska Úřadu je publikováno stanovisko k aplikaci práva na ochranu osobních údajů při poskytování informací o činnosti orgánů veřejné správy. Činnost orgánů státní správy a územní samosprávy vykonávají lidé, fyzické osoby, a výkon směřuje v řadě případů rovněž vůči fyzickým osobám. Všechny tyto fyzické osoby mají právo na ochranu svého soukromí, které však může kolidovat s právem veřejnosti na informace. Výše uvedené stanovisko objasňuje možné aplikační nejasnosti zákonů, především zákona o ochraně osobních údajů a zákona o svobodném přístupu k informacím, které konkrétní zákonnou úpravu práva na ochranu soukromí a práva na informace provádějí.

V rubrice Sdělení Úřadu najdete dokument „Praktické otázky provozování kamerových systémů ve školách a školských zařízeních“, jehož cílem je zpřístupnit veřejnosti pohled Úřadu na konkrétní otázky související s instalací kamerových systémů zejména ve školách.

Dalším materiálem této rubriky je informace Úřadu o návrhu nové dohody o předávání dat ze jmenné evidence cestujících – PNR (Passenger Name Records) – leteckých společností do USA a text „Usnesení Evropského parlamentu ze dne 12. července 2007 o dohodě mezi EU a USA o jmenné evidenci cestujících“. V rámci boje proti terorismu přijala vláda USA řadu bezpečnostních opatření, která však většinou současně vedou k určitému omezení základních lidských práv, včetně práva na soukromí a ochranu osobních údajů. Úřad vyjádřil kritické stanovisko k celkovému vyznění nové dohody, při kterém vycházel ze skutečnosti, že navrhovaná dohoda nabízí zhoršení úrovně ochrany osobních údajů cestujících oproti dohodám předchozím.

Rubriku Sdělení dále naplňují dvě stanoviska vytvořená Pracovní skupinou pro ochranu dat podle článku 29 (tj. článku 29 směrnice 95/46/ES), která se zabývá problematikou ochrany osobních údajů a soukromí: Stanovisko č. 8/2006 k přezkumu předpisového rámce pro elektronickou komunikaci a služby s důrazem na směrnici o soukromí a elektronickou komunikaci a Stanovisko č. 9/2006 o provádění směrnice Rady 2004/82/ES o povinnosti dopravců předávat předběžné údaje o cestujících.

Posledním dokumentem rubriky Sdělení Úřadu je Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR). Tento dokument sepsala výše uvedená pracovní skupina s cílem poskytnout vodítko k výkladu právního rámce ochrany údajů použitelného pro systémy elektronických zdravotních záznamů (EHR), stanovit některé obecné zásady a popsat předběžné podmínky vybudování celostátního systému EHR z hlediska ochrany údajů a přispět k jednotnému používání vnitrostátních opatření přijatých podle směrnice 95/46/ES.

Úřad přetiskuje oficiální překlady právně nezávazných dokumentů WP29 v jejich původní podobě a nepřebírá odpovědnost za případné nepřesnosti překladu.

# Přehled zrušených registrací

| Číslo registrace | Subjekt | Datum zrušení |
|---|---|---|
| 00001456/001 | MĚSTSKÁ ČÁST PRAHA 14 | 30. 6. 2007 |
| 00003815/001 | ZO ODB. SVAZ PRAC. HORNICTVÍ, GEOLOGIE, NAFTOVÉHO PRŮMYSLU, OKD A. S. DŮL DOUBRAVA | 8. 5. 2007 |
| 00003886/001 | KŘEČKOVÁ MUDR. JAROSLAVA | 26. 4. 2007 |
| 00004413/001 | SALESIÁNSKÉ STŘEDISKO MLÁDEŽE | 11. 4. 2007 |
| 00004772/009 | MĚSTO NOVÉ MĚSTO NAD METUJÍ | 27. 6. 2007 |
| 00004840/002 | PIVOVARY STAROPRAMEN A. S. | 14. 7. 2007 |
| 00010738/001 | VÍTKOVICE STEEL, A. S. | 4. 7. 2007 |
| 00011220/003 | VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE | 14. 7. 2007 |
| 00019242/001 | MĚSTO LIPNÍK NAD BEČVOU | 8. 6. 2007 |
| 00019296/001 | VALEŠ MARTIN | 8. 5. 2007 |
| 00019525/001 | IPA-ČESKÁ SEKCE, ÚZEMNÍ SKUPINA Č. 114 PŘI MINISTERSTVU VNITRA ČR | 10. 5. 2007 |

# II. STANOVISKA ÚŘADU

## Stanovisko č. 1/2007

červen 2007

**Stanovisko k aplikaci práva na ochranu osobních údajů při poskytování informací o činnosti orgánů veřejné správy**

Listina základních práv a svobod, která je součástí ústavního pořádku České republiky, stanoví mj. dvě lidská práva, jejichž vztah při výkladu nemusí být zcela jasný, přičemž pro dozor nad dodržováním části jednoho z nich byl zřízen Úřad pro ochranu osobních údajů: Na jedné straně je právo na ochranu soukromí a na straně druhé právo na informace.

Ochrana soukromí je upravena zejména dvěma následujícími ustanoveními Listiny:

Článek 7, odstavec 1: „Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."

Článek 10, odstavec 3: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě".

Právo na informace je obecně upraveno v článku 17, odstavci 1 Listiny, který uvádí: „Svoboda projevu a právo na informace jsou zaručeny." Odstavec 5 tohoto článku právo na informace promítá do principu publicity veřejné správy: „Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon."

Konkrétní zákonnou úpravu těchto ústavních zásad pak provádějí zejména zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů"), v případě ochrany soukromí, a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím), v otázkách obecného práva na informace a aplikace ústavní zásady veřejnosti státní správy.

Uvedené ústavní zásady se z principu mohou ocitnout v konfliktu, neboť činnost orgánů státní správy a územní samosprávy vykonávají lidé, fyzické osoby, a výkon směřuje v řadě případů rovněž vůči fyzickým osobám. Všechny tyto fyzické osoby mají samozřejmě právo na ochranu soukromí, které však může kolidovat s právem veřejnosti na informace o činnosti státních orgánů a orgánů územní samosprávy.

Tuto případnou aplikační nejasnost se snaží řešit oba výše uvedené zákony, konkrétně zákon o svobodném přístupu k informacím, který v § 8a uvádí: „Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu." Poznámka pod čarou tohoto ustanovení obsahuje demonstrativní výčet dalších právních předpisů a to § 11 až 16 zákona č. 40/1964 Sb., (dále jen „občanský zákoník") či § 5 a 10 zákona o ochraně osobních údajů.

Občanský zákoník v odkazovaných ustanoveních upravuje právo na ochranu osobnosti. Z našeho hlediska je zajímavý zejména § 11 uvedeného zákona: „Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnost, jakož i soukromí, svého jména a projevů osobní povahy." Jedná se o obecnou úpravu ústavního principu ochrany soukromí, jejíž jeden, pro naše téma klíčový, aspekt, tedy ochrana osobních údajů, je rozveden v zákoně o ochraně osobních údajů.

Další odkazovaná ustanovení občanského zákoníku upravují možnost pořizování a zveřejňování písemností osobní povahy, podobizen, obrazových snímků a obrazových a zvukových záznamů týkajících se fyzické osoby nebo jejích projevů osobní povahy a dále pak možnost ochrany fyzické osoby před neoprávněným zásahem do soukromí.

Odkazovaný § 5 zákona o ochraně osobních údajů upravuje práva a povinnosti správce a zpracovatele při zpracování osobních údajů, jako je stanovit účel, prostředky a způsob zpracování, zpracovávat pouze osobní údaje přesné a to jen ke stanovenému účelu. Druhý odstavec uvádí, že zpracování osobních údajů je v zásadě možné pouze se souhlasem subjektů údajů, ale uvádí z tohoto pravidla zároveň několik výjimek. Správce je například bez souhlasu oprávněn zpracovávat osobní údaje, pokud provádí zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou subjekt údajů je, jedná-li se o oprávněně zveřejněné osobní údaje podle zvláštního právního předpisu, pokud je to nezbytné k ochraně životně důležitých zájmů subjektu údajů atd.

Pro naše téma je pak klíčové ustanovení § 5 odst. 2 písm. f) zákona o ochraně osobních údajů, dle kterého může správce osobní údaje bez souhlasu jejich subjektu zpracovávat, „pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení."

Ustanovení § 10 zákona o ochraně osobních údajů, na které také zákon o svobodném přístupu k informacím v poznámce pod čarou odkazuje a které zní: „Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů," je spíše vyjádřením obecného předmětu úpravy zákona o ochraně osobních údajů, ale co do svého významu ve vztahu k popisovanému konfliktu práv patří k těm nejvýznamnějším.

Při poskytování informací o činnosti státní správy či územní samosprávy se můžeme dostat do střetu s právem na ochranu soukromí a to u dvou typů fyzických osob:

1) Osoby, které s orgány státní správy či územní samosprávy přicházejí do styku jako občané (stěžovatelé, svědci, poškození, žadatelé, pachatelé přestupků atd.);
2) Osoby, které se na výkonu státní správy či územní samosprávy přímo podílejí (úředníci, další zaměstnanci správních úřadů nebo samosprávy apod.).

V případě první skupiny občanů by se ze samotného zákona o svobodném přístupu k informacím mohlo jevit, že informace o nich v zásadě poskytovány být mohou. Paragraf 2 odst. 1 tohoto zákona totiž uvádí: „Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti, jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.“ Druhý odstavec ve výčtu povinných subjektů pokračuje: „Povinnými subjekty jsou dále ty subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických osob nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.“

Z dikce samotného zákona o svobodném přístupu k informacím je možno dovodit, že povinné subjekty mohou či mají poskytovat informace také například o účastnících správního řízení, neboť správní řízení je u řady povinných subjektů součástí jejich působnosti. U povinných subjektů dle § 2 odstavce druhého je informační povinnost zúžena, nicméně termín „v rozsahu jejich rozhodovací činnosti“ by bylo možno vyložit také tak, že tyto povinné subjekty poskytují informace o celé své rozhodovací činnosti, tedy i o těch fyzických osobách, kterým svým rozhodnutím založily, změnily či zrušily práva nebo povinnosti.

Ovšem v případě, že povinný subjekt poskytuje informaci o takovéto určené nebo určitelné fyzické osobě, a tím nutně i o jejích osobních údajích, uplatní se zákonný odkaz § 8a zákona o svobodném přístupu k informacím na příslušná ustanovení zákona o ochraně osobních údajů. V této situaci je nutno aplikovat § 5 odst. 2 zákona o ochraně osobních údajů, tedy, že osobní údaje lze zpracovávat pouze se souhlasem jejich subjektu s tím, že zpracováním je dle § 4 písm. e) tohoto zákona mj. i zpřístupňování, šíření a zveřejňování osobních údajů. Poskytnutí osobních údajů těchto fyzických osob nelze podřadit pod žádnou z výjimek § 5 odst. 2. Výše uvedená výjimka v § 5 odst. 2 písm. f) zákona o ochraně osobních údajů hovoří o situaci, kdy je možnost bez souhlasu poskytnout osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, nikoliv tedy o fyzických osobách jiných, které se státní správou nebo územní samosprávou sice přišly do kontaktu, ale rozhodně ji nevykonávají.

V tomto bodě lze shrnout, že orgány či osoby vykonávající státní správu nebo územní samosprávu nesmějí zveřejňovat či na žádost dle zákona o svobodném přístupu k informacím poskytovat osobní údaje, které získaly v souvislosti s výkonem státní správy nebo územní samosprávy bez souhlasu subjektu údajů, není-li zvláštním právním předpisem stanoveno jinak, resp. neobsahuje-li zvláštní právní předpis vlastní úpravu zveřejňování informací včetně osobních údajů (např. zákon č. 183/2006 Sb., o územním plánování a stavebním řádu /stavební zákon/, zákon č. 500/2004 Sb., správní řád, či zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích a o změně zákona č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla a o změně některých souvisejících zákonů /zákon o pojištění odpovědnosti z provozu vozidla/, ve znění zákona č. 307/1999 Sb., včetně prováděcí vyhlášky č. 243/2001 Sb., o registraci vozidel, atd.).

Druhou výše uvedenou skupinou osob, u kterých je při poskytování informací o činnosti státní správy a územní samosprávy nutno vážit právo na ochranu soukromí a osobních údajů na jedné straně a nutnost aplikace principu publicity výkonu veřejné správy na straně druhé, jsou ti, kteří veřejnou správu vykonávají v rámci orgánů veřejné správy, a nebo ti, kterým rozhodování o právech, právem chráněných zájmech nebo povinnostech jiných osob svěřil zvláštní zákon. Zejména u těchto osob se výše uvedené ústavní zásady mohou dostat do konfliktu, kdy na jedné straně stojí zájem veřejnosti o informace z veřejné správy, na straně druhé pak otázka soukromí konkrétní fyzické osoby, která se na výkonu státní správy nebo územní samosprávy podílí či podílela.

Klíčovým pro tuto otázku je již zmíněné ustanovení § 5 odst. 2 písm. f) zákona o ochraně osobních údajů. Podle něj správce může poskytovat osobní údaje bez souhlasu jejich subjektu v případě, že se jedná o osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti a o jeho funkčním nebo pracovním zařazení.

Zákonem nedefinovanými a tedy potencionálně problematickými jsou pojmy „veřejná anebo úřední činnost“. Dle dikce citovaného zákona se jedná o údaje odlišné od funkčního nebo pracovního zařazení, tedy jiné informace než ty, že konkrétní osoba zastává konkrétní funkci nebo je zařazena na určitou pracovní pozici při výkonu veřejné správy, které mohou být na žádost dle zákona o svobodném přístupu k informacím poskytnuty i bez souhlasu dotyčných osob.

Určitou pomoc při vyjasnění uvedených pojmů poskytuje rozsudek Ústavního soudu I. ÚS 453/03, který mj. uvádí: „Věcí veřejnou jsou veškeré agendy státních institucí, jakož i činnost politiků místních i celostátních, úředníků, soudců, advokátů, popř. kandidátů či čekatelů na tyto funkce. Tyto veřejné záležitosti, resp. veřejná činnost jednotlivých osob, mohou být veřejně posuzovány.“ Veřejnou činností konkrétních osob podstatnou pro naše téma je tedy výkon agendy státních institucí (samozřejmě i agendy orgánů územní samosprávy) a s ní související činnost úředníků. I v tomto případě je však nutno brát v potaz úpravu zvláštními právními předpisy. Například v případě územní samosprávy je to zákon č. 128/2000 Sb., o obcích (obecní zřízení), který obsahuje vlastní úpravu zveřejňování zápisů ze zasedání rady a zastupitelstva obce, kdy zápis ze zasedání rady je dle § 101 citovaného zákona přístupný k nahlédnutí jen členům zastupitelstva, zatímco zápis z jednání zastupitelstva je dle § 16 tohoto zákona přístupný všem občanům obce či fyzickým osobám starším 18 let, které na území obce vlastní nemovitost.

Dle uvedeného nálezu Ústavního soudu, dikce § 2, odst. 1 a 2 zákona o svobodném přístupu k informacím a § 5 odst. 2 písm. f) zákona o ochraně osobních údajů lze shrnout, že povinné subjekty poskytnou informace o jednotlivých osobách, které vykonávají veřejnou činnost u povinného subjektu, pokud se tato veřejná činnost vztahuje k jeho působnosti. Veřejnou a úřední činností je u povinných subjektů výkon agendy státních institucí a orgánů územní samosprávy včetně činnosti jejich úředníků.

Každý povinný subjekt je zřízen na základě zákona: ministerstva a jiné ústřední správní orgány zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, některé další ústřední správní úřady zvláštními zákony, např. Úřad pro ochranu osobních údajů zákonem o ochraně osobních údajů, krajské úřady zákonem č. 129/2000 Sb., o krajích (krajské zřízení), obecní úřady na základě zákona č. 128/2000 Sb., o obcích (obecní zřízení), atd. Tyto speciální zákony pak definují povinným subjektům předmět a rozsah působnosti a jejich pravomoc. Obecně lze tedy říci, že informace lze poskytovat pouze o činnosti jednotlivých osob právě v rámci této působnosti povinných subjektů.

Ovšem ani s takto úžeji vymezenými podmínkami poskytování informací o osobách, které se podílejí na veřejné správě, nemůže být formulován obecný závěr, jak postupovat v konkrétních případech žádostí o poskytnutí informací dle zákona o svobodném přístupu k informacím, tedy nelze striktně stanovit, které kategorie údajů povinný subjekt poskytovat ještě může a které už ne. Řešení totiž vždy záleží na dané situaci, na jedinečném obsahu žádosti o poskytnutí informací a na posouzení celé věci povinným subjektem.

**Závěr**: Přestože je právo na ochranu soukromí osob, které se podílejí na výkonu státní správy a územní samosprávy, částečně oslabeno, rozhodně nezaniká a při posuzování každé žádosti je třeba pečlivě vážit, co lze o konkrétní osobě sdělit, aby to nadměrným způsobem nezasáhlo do jejího soukromí. V tomto smyslu se vyjádřil i Ústavní soud ve svém rozsudku I. ÚS 321/2006: „Právo na ochranu soukromého života je nezadatelným lidským právem, které bezpochyby zahrnuje, mimo jiné, právo fyzické osoby rozhodnout podle vlastního uvážení zda, popřípadě v jakém rozsahu a jakým způsobem, mají být skutečnosti jejího soukromí zpřístupněny jiným. K omezení takového práva lze nicméně přikročit za účelem ochrany základních práv jiných osob, anebo za účelem ochrany veřejného zájmu, který je v podobě principu či hodnoty obsažen v ústavním pořádku. Přitom je třeba dbát, aby bylo dosaženo co nejširšího uplatnění obou chráněných hodnot.“

Lze říci, že v zásadě je možné omezit právo na ochranu soukromí osoby podílející se na výkonu státní správy či územní samosprávy z důvodu uplatnění ústavního práva na informace. Toto oslabení však neznamená odnětí práva na ochranu soukromí a v každém případě povinný subjekt, který o poskytnutí informací rozhoduje, musí hledat, jak v maximální možné míře naplnit jak zásadu ochrany soukromí a osobních údajů, tak právo na informace o činnosti státní správy a územní samosprávy.

# III. SDĚLENÍ ÚŘADU

## Praktické otázky provozování kamerových systémů ve školách a školských zařízeních

*Sdělení úvodem:*
*Úřad pro ochranu osobních údajů se v poslední době několikrát vyjadřoval k právním otázkám souvisejícím s provozováním kamerových systémů se záznamem (viz poznámka). Jedním z velmi sledovaných problémů je instalace těchto systémů ve školách a školských zařízeních (dále jen „školy“). Zmíněná vyjádření Úřadu však dosud nevedla k úplnému vyjasnění současné situace a Úřad se stále setkává s řadou oznámení škol o zpracování osobních údajů prostřednictvím kamer, které jsou zcela evidentně v rozporu se základními povinnostmi správce stanovenými zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon“). K praktickému řešení této, z hlediska ochrany soukromí nežádoucí situace, by měl přispět následující text, který si klade za cíl zpřístupnit veřejnosti pohled Úřadu na konkrétní otázky související s instalací kamer zejména ve školách.*

K instalaci a provozu kamerových systémů lze obecně uvést, že s ohledem na jejich zvláštní charakter spočívající ve sledování prostor, kde se pohybují i lidé, a který tak může představovat hrubý zásah do soukromého a osobního života subjektu údajů, je jejich využití možné především na základě výslovného zákonného zmocnění, nebo (což je i případ školních budov) se jejich nasazení jeví jako poslední možnost, kdy již všechny dříve použité a méně invazivní prostředky dozoru selhaly. To znamená, že se vždy jedná o zvláštní situaci, kdy se jiná opatření fyzické povahy směřující k stejnému účelu prevence, ochrany nebo zabezpečení osob a majetku, která neobsahují pořizování obrazových nebo zvukových záznamů, ukáží být s ohledem na legitimní účely jejich nasazení (zejména zajištění ochrany osob i majetku) nedostatečnými či nepoužitelnými, nebo jde o situaci, kdy lze, vzhledem k okolnostem, předem vyloučit účinnost méně invazivních prostředků.

Při instalaci a plánovaní režimu provozu kamerového systému je nutné přistupovat odlišně ke způsobu užívání jednotlivých monitorovaných prostor či objektů, a to i ve vztahu k různému dennímu režimu v daném prostoru. Z hlediska ochrany osobních údajů a ochrany soukromí subjektů údajů tak lze odlišit rozsah a dobu monitorování pláště budovy, vnějších prostor anebo prostor, do nichž není běžně povolen přístup, od prostorů vnitřních – chodeb, šaten, učeben, kabinetů, sborovен, jídelen či sálů. Obdobně je také nezbytné rozlišovat, zda monitorování kamerovým systémem probíhá pouze v době, kdy se v daném prostoru nemají vyskytovat žádné osoby (tj. po nebo naopak během vyučování, resp. po nebo během pracovní doby učitelů a dalšího personálu, o víkendu nebo během prázdnin), anebo zda má být systém v provozu nepřetržitě, tedy i v době, kdy se v dané budově běžně vyskytují osoby v souvislosti s plněním svých úkolů a povinností. Nastavení systému tak, aby snímal prostory v době, kdy se v nich nemá žádná osoba vyskytovat, přitom z hlediska ochrany osobních údajů a soukromí nic nebrání, přičemž v současné době běžně dostupná technická zařízení takové nastavení funkčnosti bezpochyby umožňují.

Za základní povinnosti z hlediska instalace kamerového systému lze považovat ty, které jsou stanoveny v § 5 odst. 1 písm. e) a odst. 2, § 10, § 11 odst. 1 a 5 a § 16 zákona. Projděme si je tedy postupně:

K § 5 odst. 1 písm. e)

Podle tohoto ustanovení je správce povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Doba uchovávání záznamů musí být stanovena tak, že nepřesáhne dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno dále prošetřit a zajistit další nezbytné informace, například potřebné k předání případu k vyšetření příslušným orgánům, což lze běžně učinit nejpozději den následující po zjištění bezpečnostního incidentu, a v případě, že budova není přes víkend využívána, pak nejpozději třetí den po incidentu. Doba uchování informací by tedy při běžném provozu kamerového systému neměla přesáhnout délku 3 dnů, přičemž v opačném případě nelze než dospět k závěru, že déle stanovená doba pro uchovávání záznamů je nepřiměřená a neodpovídá ve spojení s nejčastěji stanoveným účelem zpracování (ochrana osob a majetku a prevence proti vandalismu) ze strany správce zákonnému požadavku nezbytnosti. Ve vztahu k uchovávání záznamů pořizovaným například během prázdnin, tj. mimo běžný provoz budovy, lze připustit i delší dobu uchovávání záznamů.

K § 5 odst. 2, 4 a § 10

Podle § 5 odst. 2 zákona může správce osobních údajů zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat pouze v případech uvedených v § 5 odst. 2 písm. a) až g) zákona. Při instalaci kamerových systémů ve školách se nejčastěji diskutuje o možnosti zpracovávat osobní údaje bez souhlasu subjektu údajů s odkazem na ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby ve smyslu ustanovení § 5 odst. 2 písm. e) zákona.

Při aplikaci této výjimky však současně platí věta za středníkem citovaného ustanovení, která uvádí, že takovéto zpracování nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. V případě provozu kamerového systému umístěného ve škole, jehož objektem monitorování jsou i děti a mladiství, je přitom nutno tuto podmínku posuzovat zvlášť pečlivě. Lze tedy konstatovat, že je-li systém instalován ve vnitřních prostorách školy, kde se učitelé i další zaměstnanci pohybují v rámci své pracovní doby a žáci během vyučování (ale i například o přestávkách) a kde mají současně nárok na uplatňování svého práva na soukromí, dochází prin-

cipiálně k porušení tohoto ustanovení zákona, protože s aplikací těchto principů je úzce spojeno i ustanovení § 10 zákona, podle kterého správce dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

V úvahu je nutno vzít nové ustanovení § 316 odst. 2 zákona č. 262/2006 Sb., zákoník práce, které zakazuje zaměstnavateli bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že jej podrobuje otevřenému nebo skrytému sledování. S ohledem na skutečnost, že toto ustanovení představuje lex specialis ve vztahu k zákonu a současně jde o kogentní ustanovení zákoníku práce, škola fakticky nemůže v případě svých zaměstnanců naplnit podmínku § 5 odst. 2 zákona, tedy zpracovávat osobní údaje subjektu údajů s jejich souhlasem, neboť tento souhlas by byl v daném případě z hlediska zákona neúčinný jako úkon směřující k obcházení zákona. Je nutno zdůraznit, že je ve vztahu k § 316 odst. 2 zákoníku práce nerozhodné, že škola zamýšlí zpracovávat osobní údaje k naprosto odlišným účelům, než cíleně zpracovávat osobní údaje svých zaměstnanců, resp. je podrobovat otevřenému sledování, neboť při provozu kamerového systému by fakticky k tomuto sledování zaměstnanců na pracovišti docházelo. Za pracoviště je přitom třeba považovat nejen třídy, sborovnu a kabinety, ale též chodby, jídelny a schodiště, případně další prostory, kde mohou učitelé vykonávat část své pracovní činnosti (pedagogický dozor apod.).

Při aplikaci zákonem očekávaných podmínek pro zpracování osobních údajů se často objevuje představa budoucího správce, že je možné k problematice zpracování osobních údajů žáků a studentů prostřednictvím kamerového systému přistoupit tak, že zpracování bude probíhat se souhlasem těchto osob. Pro platnost souhlasu subjektu údajů se zpracováním osobních údajů je významné splnění několika zákonných podmínek. Zejména se jedná o podmínky uvedené v § 4 písm. n) zákona (musí se tedy jednat o svobodný a vědomý projev vůle subjektu údajů) a v § 5 odst. 4 zákona (musí se jednat o informovaný souhlas), tzn. že souhlas se zpracováním osobních údajů, který by byl podmíněn například poskytnutím určité služby, plnění ze smlouvy zejména v případě soukromých škol, nebo při jeho vyžadování nebyly subjektu údajů sděleny všechny potřebné informace ve smyslu § 5 odst. 4 zákona, by mohl být považován za vynucený projev vůle, který nelze v žádném případě považovat za svobodně učiněný, a tedy platný. Osobní údaje, které škola potřebuje pro plnění smlouvy, totiž může na základě ustanovení § 5 odst. 2 písm. b) zákona zpracovávat přímo bez souhlasu subjektu údajů. Logicky tak lze dospět k závěru, že má-li škola potřebu o subjektu údajů získávat další osobní údaje, může tak učinit na základě svobodné volby subjektu údajů, a to pouze s jeho souhlasem, který však nesmí být vázán na další podmínku.

Vedle obecného rámce podmínek souhlasu subjektu údajů je nezbytné odkázat na úzkou souvislost tohoto ustanovení s ustanovením § 8 občanského zákoníku, který upravuje obecné podmínky pro posuzování zákonnosti projevů vůle, a to i s ohledem na právní subjektivitu (způsobilost k právům a povinnostem) fyzické osoby, která má souhlas se zpracováním svých osobních údajů učinit. Ne nepodstatnou se proto jeví otázka, čí souhlas ke zpracování osobních údajů žáků a studentů škola vlastně potřebuje (zda od žáků a studentů samotných nebo jen od jejich zákonných zástupců). Obecně by měla platit zásada uplatňovaná v občanském právu, která vychází z předpokladu, že tento souhlas poskytuje subjekt údajů, jehož se zpracování týká, přičemž se jedná o právní úkon, na který je nutné ve vztahu k žákům a studentům školy nahlížet ve smyslu ustanovení § 9 zákona č. 40/1964 Sb., občanský zákoník. Podle tohoto ustanovení mají nezletilí způsobilost pouze k takovým právním úkonům, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku.

Úřad je v této souvislosti přesvědčen, že dnešní studenti jsou od dosažení hranice 15 let věku již dostatečně rozumově a volně vyspělí, aby po řádném poučení dokázali s náležitou odpovědností posoudit, zda chtějí, aby jejich osobní údaje byly ve škole, ve které tráví většinu dne, zpracovávány prostřednictvím kamerového systému, a že by proto v tomto případě měl správce (škola) získávat souhlasy přímo od těchto studentů a nikoliv od jejich zákonných zástupců. Přičemž se však nedá vyloučit ani ta možnost, že rovněž rodiče „náctiletých“ studentů budou náležitě informováni o nasazení kamerového sledování, o jeho účelu, době provozu a dalších skutečnostech, které školu k instalaci kamerového systému vedly.

Závěrem však lze konstatovat, že i toto zpracování by bylo v rozporu se zákonem v případě, pokud by všichni studenti nebo všichni rodiče nebo zákonní zástupci žáků neposkytli škole souhlas s tímto zpracováním. Pro školu by tak vznikl těžko řešitelný problém, jak zajistit, aby v případě provozu kamerového systému byly zpracovávány osobní údaje jen těch osob, které souhlas poskytly.

K § 11

V návaznosti na shora uvedenou informační povinnost správce v případě získávání souhlasu subjektu údajů, má správce podle § 11 odst. 1 zákona vždy při shromažďování osobních údajů povinnost informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy (například v době získávání souhlasu jako informovaného projevu vůle). Dále jej musí informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona.

Při zpracování prováděném na základě výjimky zakotvené v § 5 odst. 2 písm. e) zákona nemusí být informační povinnost splněna pokaždé před zahájením zpracování v plném rozsahu; správce je v této situaci na základě § 11 odst. 5 zákona povinen informovat subjekt údajů o zpracování jeho osobních údajů bez zbytečného odkladu.

V případě kamerového systému ve škole tak mohou pro správce nastat rozdílné situace ve vztahu k odlišným skupi-

nám monitorovaných osob – subjektů údajů – a s tím související rozdílná úroveň informací pro tyto skupiny osob. U žáků a zaměstnanců školy, případně dalších subjektů, které do sledovaného prostoru pravidelně vstupují, je nutné splnit informační povinnost například prostřednictvím vnitřního předpisu – školního řádu, a to ještě před zahájením zpracování, a v plném rozsahu požadovaném zákonem, neboť tento okruh subjektů údajů je správci předem znám a ten má tak možnost je bez zbytečného odkladu informovat.

V případě dalších subjektů údajů, které do školy budou přicházet nepravidelně, resp. nepředvídatelně, je správce povinen splnit informační povinnost např. umístěním informačních tabulek u vstupu do sledovaných prostor. K náležitostem této informační tabulky lze dodat, že musí obsahovat informaci, že prostor je sledován kamerovým systémem, musí zde být uveden správce – provozovatel kamerového sytému, resp. kontaktní osoba nebo sdělení, kde bude subjektu údajů poskytnuta informace o zpracování v rozsahu požadovaném § 11 odst. 1 a § 12 zákona (tj. kde si může např. vyzvednout v písemné podobě další informace o kamerovém systému).

K § 16

Správce je povinen, a to ještě před zahájením zpracovávání dat prostřednictvím kamerového systému, oznámit zamýšlené zpracování osobních údajů Úřadu. Z dosavadních zkušeností Úřadu plyne, že při zpracování dat prostřednictvím kamerových systémů ve školách přitom nelze uplatnit žádnou z výjimek z registrační povinnosti stanovených v § 18 odst. 1 zákona.

K dalším povinnostem

Mimo tyto povinnosti je správce osobních údajů samozřejmě povinen dodržovat i další povinnosti upravené v zákoně, jako je zejména povinnost zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny (§ 5 odst. 1 písm. f) zákona; jsou-li záznamy pořízené za účelem ochrany majetku, nelze je použít např. pro kontrolu docházky).

Další významnou povinností správce je povinnost přijmout a dokumentovat taková technicko-organizační opatření týkající se provozu kamerového systému, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k uchovávaným osobním údajům (§ 13 zákona).

Poznámka: Plná znění materiálů pojednávajících o postojích Úřadu k právním otázkám souvisejícím s provozováním kamerových systémů jsou k dispozici na webových stránkách Úřadu v rubrice Kamerové systémy: http://www.uoou.cz/index.php?l=cz&m=bottom&mid=01:11&u1=&u2=&t=.

# Usnesení Evropského parlamentu ze dne 12. července 2007 o dohodě mezi EU a USA o jmenné evidenci cestujících[1)]

*Sdělení úvodem:*
*Evropský parlament se vyslovil k návrhu nové dohody o předávání dat PNR do USA[2)].*

*O záležitosti předávání osobních údajů cestujících leteckých společností úřadům v USA jsme již veřejnost mnohokrát informovali. Pouze tedy stručně připomínáme: V rámci boje proti terorismu přijala vláda USA celou řadu bezpečnostních opatření, která většinou současně vedou k určitému omezení základních lidských práv, včetně práva na soukromí a ochranu osobních údajů. Patří mezi ně také povinnost leteckých dopravců (týká se i ČSA) dopravujících cestující do a z USA poskytnout určitým americkým úřadům osobní údaje pasažérů ze svých počítačových rezervačních či odbavovacích systémů, tzv. „data PNR". 17. května 2004 uzavřela Evropská komise s USA první dohodu o povinnosti dopravců údaje dodávat a podmínkách, za jakých budou v USA využívány a chráněny. Na základě podání Evropského parlamentu rozhodl Evropský soudní dvůr o zrušení dohody pro chybný právní základ, na kterém byla uzavřena. Rozsudek se nezabýval hlavním důvodem, pro který EP žalobu podal, tedy porušováním evropského práva v oblasti ochrany osobních údajů. V časové tísni byla v říjnu 2006 uzavřena dohoda druhá, a to dočasná a prozatímně prováděná (ve většině států si vyžaduje ratifikaci, která dosud v ČR nebyla provedena), s téměř totožným obsahem.*

*Platnost dočasné dohody vyprší koncem července 2007. Proto se od jara urychleně, avšak obtížně sjednávala dohoda třetí s předpokládanou dlouhodobou platností. Jednání byla uzavřena 29. června 2007 a během července by měla Rada EU schválit její podepsání.*

*Svým usnesením, které předkládáme i našim čtenářům, se k návrhu nové dohody vyslovil velice kriticky Evropský parlament:*

Evropský parlament,

- s ohledem na článek 6 Smlouvy o Evropské Unii, článek 8 Listiny základních práv Evropské Unie a článek 8 Evropské úmluvy o ochraně lidských práv a základních svobod,
- s ohledem na svá usnesení o jmenné evidenci cestujících ze dne 7. září 2006 (1) a ze dne 14. února 2007 (2) ,
- s ohledem na předchozí dohody o jmenné evidenci cestujících mezi Evropským společenstvím a Spojenými státy americkými ze dne 28. května 2004 a mezi Evropskou unií a Spojenými státy americkými ze dne 19. října 2006,
- s ohledem na návrh dohody ze dne 28. června 2007 mezi Evropskou unií a Spojenými státy americkými o zpracování údajů jmenné evidence cestujících leteckými dopravci a jejich předávání ministerstvu vnitřní bezpečnosti (DHS) Spojených států, který úřadující předseda Rady Wolfgang

Schäuble neoficiálně předal předsedovi Výboru pro občanské svobody, spravedlnost a vnitřní věci,

– s ohledem na rozsudek Evropského soudního dvora ze dne 30. května 2006 ve společné věci C-317/04 a C-318/04

– s ohledem na dopis DHS ze dne 28. června 2007 o ujištěních ohledně zabezpečení údajů PNR, který úřadující předseda Rady W. Schäuble neoficiálně předal předsedovi Výboru pro občanské svobody, spravedlnost a vnitřní věci,

– s ohledem na dopis Evropského inspektora ochrany údajů úřadujícímu předsedovi Rady W. Schäublemu ze dne 27. června 2007, který se týká nové dohody o jmenné evidenci cestujících se Spojenými státy (nová dohoda o PNR) a na odpovědi, které obdržel od ministra Schäubleho a generálního ředitele Komise pro justici a vnitro Jonathana Faulla ze dne 29. června a 3. července 2007,

– s ohledem na článek 2 Dodatkového protokolu Rady Evropy k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních údajů o orgánech dozoru a předávání údajů přes hranice,

– s ohledem na směrnici Rady 2004/82/ES o povinnosti dopravců předávat údaje o cestujících (3) ,

– s ohledem na čl. 103 odst. 2 jednacího řádu,

A. vzhledem k tomu, že deklarovaným účelem nové dohody o PNR je na jedné straně poskytnout právní základ pro předávání údajů jmenné evidence cestujících EU Spojeným státům a na straně druhé zajistit občanům EU jak přiměřenou ochranu jejich osobních údajů, tak procedurální záruky,

B. vzhledem k tomu, že účelem nové dohody o PNR je pomoc při prevenci a boji s terorismem a mezinárodním zločinem,

C. vzhledem k tomu, že nová dohoda o PNR druhý cíl nesplňuje, neboť vykazuje závažné nedostatky s ohledem na právní jistotu, ochranu údajů a opravné prostředky, které jsou občanům EU k dispozici, a to zejména z důvodu otevřených a neurčitých definic a četných možných výjimek,

D. vzhledem k tomu, že nová dohoda o PNR poskytuje právní základ pro předávání údajů o cestujících z EU Spojeným státům americkým a tím dává leteckým dopravcům základ pro jejich působení v USA

E. vzhledem k tomu, že má-li být sdílení údajů a informací cenným a spolehlivým nástrojem v boji proti terorismu, je nezbytné zajistit přiměřenou ochranu soukromí a občanských svobod jednotlivých občanů stejně jako kontrolu kvality údajů,

Obecně

1. uznává obtížné podmínky, za kterých jednání o PNR probíhala, a v zásadě také uznává přínos existence jediné dohody o PNR mezi EU a USA namísto uzavírání 27 bilaterálních dohod mezi členskými státy a USA;

2. velmi lituje, že nová dohoda o PNR nebyla podrobena žádné demokratické kontrole, neboť byla na základě požadavků ze strany USA sjednána a schválena bez jakékoli účasti Evropského parlamentu a neposkytuje národním parlamentům dostatek možností, aby ovlivnily mandát k jednání nebo aby navrženou novou dohodu o PNR řádně vyhodnotily či k ní navrhly změny;

3. je znepokojen tím, že trvale chybí právní jistota ohledně důsledků a rozsahu povinností ukládaných leteckým společnostem, stejně jako ohledně právního vztahu mezi novou dohodou PNR a dopisem ministerstva vnitřní bezpečnosti Spojených států;

4. kritizuje skutečnost, že nová dohoda o PNR neposkytuje odpovídající úroveň ochrany údajů PNR, a vyjadřuje politování nad tím, že chybí jasná a přiměřená ustanovení týkající se sdílení informací, jejich uchovávání a dohledu ze strany orgánů pro ochranu údajů; je znepokojen velkým počtem ustanovení, jejichž provádění je ponecháno na ministerstvu vnitřní bezpečnosti Spojených států;

5. vyzývá proto národní parlamenty členských států, aby pečlivě prozkoumaly předkládaný návrh nové dohody o PNR s ohledem na připomínky vznesené v tomto usnesení;

Pokud jde o právní rámec

6. je znepokojen tím, že shromažďování, použití a uchovávání údajů PNR a nakládání s nimi ze strany DHS není založeno na řádné dohodě, ale pouze na nezávazných ujištěních, která mohou být tímto ministerstvem kdykoli jednostranně změněna a která žádné osobě ani straně neposkytují žádná práva ani výhody;

7. vyjadřuje politování nad tím, že v dopise DHS chybí jasné vymezení účelu, neboť se v něm uvádí, že údaje PNR mohou být použity v boji proti terorismu a souvisejícím trestným činům, ale také k mnoha dalším nespecifikovaným účelům, zejména „v zájmu ochrany životně důležitých zájmů osob, jichž se údaje týkají, nebo jiných osob a v rámci jakéhokoli trestního řízení nebo v jiných případech stanovených zákonem“;

8. v zásadě vítá ochotu DHS přejít na systém předávání údajů (PUSH) nejpozději k 1. lednu 2008, ale lituje toho, že tento přechod, s nímž se počítalo již v dohodě o PNR z roku 2004, byl odložen o celé roky, přestože podmínka technické proveditelnosti byla již dávno splněna; domnívá se, že PUSH pro všechny dopravce by měl být nezbytnou podmínkou pro jakékoli předávání údajů PNR; zdůrazňuje, že souběžná existence systémů předávání PUSH a čerpání PULL údajů by mohla vést k narušení hospodářské soutěže mezi dopravci EU;

9. trvá na tom, aby společný pravidelný přezkum ze strany EU a ministerstva vnitřní bezpečnosti Spojených států byl komplexní, probíhal jednou ročně a jeho výsledky byly zveřejňovány; trvá na tom, aby součástí tohoto přezkumu bylo hodnocení účinnosti opatření z hlediska zvýšení bezpečnosti; vyjadřuje politování nad skutečností, že tento přezkum nepředpokládá zapojení Evropského inspektora ochrany údajů nebo jeho vnitrostátních protějšků, jak bylo stanoveno v předchozí dohodě o PNR;

10. trvá na tom, že cestující musí být o použití svých údajů i o svých právech náležitě informováni, zejména o právu obrátit se na soud a právu na informace o tom, na jakém základě je cestující zastaven, a aby tato povinnost spočívala na leteckých společnostech; domnívá se, že odpovědnost za informování cestujících musí převzít DHS a Komise,

a navrhuje, aby bylo všem cestujícím poskytnuto „krátké sdělení pro cesty mezi Evropskou unií a Spojenými státy“, navržené pracovní skupinou zřízenou podle článku 29 (pracovní dokument 132);

11. vyjadřuje politování nad tím, že při jednáních mezi EU a USA nebyla zohledněna směrnice 2004/82 ani dohody o PNR s Austrálií a Kanadou, které zajišťují vyšší standardy ochrany osobních údajů;

12. připomíná, že správní dohoda uzavřená mezi EU a USA nesmí vést ke snížení úrovně ochrany osobních údajů, kterou zajišťují vnitrostátní právní předpisy členských států, a lituje toho, že tato dohoda povede k další nejistotě ohledně povinností leteckých společností EU a základních práv občanů EU;

Ochrana údajů

13. vítá ustanovení, že působnost amerického zákona na ochranu soukromí (Privacy Act) bude po správní stránce rozšířena i na občany EU;

14. lituje, že DHS si vyhrazuje právo zavádět výjimky podle zákona o svobodě informací (Freedom of Information Act);

15. lituje toho, že nová dohoda o PNR nestanovuje přesná kritéria pro definici ochrany osobních údajů poskytovaných DHS, která by odpovídala normám EU;

16. v tomto ohledu lituje toho, že s údaji PNR občanů EU může být nakládáno čistě podle právních předpisů USA, aniž by bylo provedeno posouzení přiměřenosti nebo byly příslušné konkrétní právní předpisy USA jakkoli upřesněny;

17. lituje, že délka uchovávání údajů PNR byla prodloužena z 3,5 na 15 let a že se tato změna zpětně uplatňuje na údaje shromážděné podle předchozích dohod o PNR; ostře kritizuje skutečnost, že po uplynutí patnáctiletého období uchovávání údajů, které se skládá ze sedmiletého „aktivního“ a osmiletého „pasivního“ období, neexistuje záruka, že údaje budou definitivně vymazány;

18. bere na vědomí, že množství datových polí bylo sníženo ze 34 na 19, ale zdůrazňuje, že jde většinou pouze o kosmetickou změnu, neboť datová pole byla často jen sloučena či přejmenována místo toho, aby byla skutečně odstraněna;

19. se znepokojením konstatuje, že pokud jde o citlivé údaje (tj. osobní údaje týkající se rasového nebo etnického původu, politických názorů, náboženského nebo filozofického přesvědčení, členství v odborových organizacích a údaje týkající se zdraví nebo sexuálního života osoby), budou zpřístupněny DHS a mohou být DHS ve výjimečných případech využity;

20. je znepokojen tím, že údaje budou po dobu 7 let uchovávány v „aktivních analytických databázích“, což představuje významné riziko hromadného dokumentování profilů a získávání údajů, jež je neslučitelné se základními evropskými zásadami a představuje postup, který je v Kongresu Spojených států dosud předmětem diskuse;

Sdílení informací

21. lituje, že nová dohoda o PNR neobsahuje přesný výčet orgánů Spojených států, které mají k údajům jmenné evidence cestujících přístup;

22. je znepokojen zamýšleným převodem analytických informací vyplývajících z údajů PNR orgány USA policejním a soudním orgánům členských států a případně Europolu a Eurojustu, mimo rámec specifických soudních postupů nebo policejního vyšetřování, jak je uvedeno v dopise DHS, protože takový převod by měl být povolen pouze v souladu se stávajícími dohodami mezi EU a USA o vzájemné právní pomoci a vydávání;

23. vyjadřuje svůj zásadní nesouhlas s ustanovením, aby byl třetím zemím obecně umožněn přístup k údajům PNR, pokud vyhoví podmínkám stanoveným DHS, a aby byl třetím zemím v nespecifikovaných naléhavých případech výjimečně umožněn přístup k údajům PNR, aniž by byly poskytnuty záruky, že při práci s údaji PNR bude zajištěna úroveň ochrany dat stanovená DHS;

24. lituje toho, že EU souhlasila, že „nebude zasahovat“ ve věci ochrany údajů jmenné evidence cestujících týkajících se občanů EU, které mohou USA sdílet se třetími zeměmi;

25. bere na vědomí, že nová dohoda o PNR umožňuje DHS, aby v souvislosti s konkrétními případy a přiměřeně k charakteru těchto případů poskytovalo údaje PNR jiným vládním orgánům USA; lituje toho, že nová dohoda o PNR vůbec nespecifikuje, které orgány USA mohou mít k údajům PNR přístup, a že účely, které jsou uvedeny v článku 1 dopisu ministerstva vnitřní bezpečnosti Spojených států, jsou definovány velmi široce;

Evropský systém jmenné evidence cestujících

26. bere na vědomí, že nová dohoda o PNR se zmiňuje o možném budoucím systému PNR na úrovni EU nebo nejméně v jednom z jejích členských států, i o ustanovení o tom, že by jakékoli údaje PNR v takovém systému mohly být zpřístupněny DHS;

27. požaduje, aby Komise objasnila současnou situaci ohledně systému PNR v rámci EU a zpřístupnila studii proveditelnosti, kterou se zavázala provést;

28. opakuje obavy vyjádřené pracovní skupinou zřízenou podle článku 29, pokud jde o využití údajů PNR pro účely vymáhání práva, a zejména vyzývá Komisi, aby zdůvodnila:
   a) zda je nutné a účelné shromažďovat údaje PNR při vstupu na území Evropské unie;
   b) přínos shromažďování údajů PNR s ohledem na stávající kontrolní opatření při vstupu do EU přijatá z bezpečnostních důvodů, jako je schengenský systém, vízový informační systém a systém API;
   c) předpokládané využití údajů PNR, zejména zda budou údaje využity k identifikaci jednotlivců za účelem zajištění bezpečnosti letecké dopravy, identifikaci osob, které vstupují na území EU, nebo negativnímu či pozitivnímu dokumentování profilů cestujících;

29. trvá na tom, aby byl Evropský parlament zapojen do všech dalších relevantních kroků podle čl. 71 odst. 1 písm. c a článku 251 Smlouvy o založení Evropského společenství;

30. připomíná, že nová dohoda o PNR bude muset být nakonec přezkoumána i s ohledem na budoucí institucionální reformy EU zmíněné v závěrech ze zasedání Evropské rady v červnu 2007 a v mandátu příští mezivládní konference;

31. má v úmyslu nechat právně posoudit, zda je nová dohoda o PNR v souladu s právními předpisy na úrovni jednotlivých států i EU, a vyzývá pracovní skupinu zřízenou podle článku 29 a evropského inspektora ochrany údajů, aby v tomto ohledu předložili souhrnná stanoviska;

32. pověřuje svého předsedu, aby předal toto usnesení Radě, Komisi, vládám i parlamentům členských států a Kongresu USA.

(1) Přijaté texty, P6_TA(2006)0354 .
(2) Přijaté texty, P6_TA(2007)0039 .
(3) Úř. věst. L 261, 6.8.2004, s. 4.

Poznámka:

[1)] Text Usnesení Evropského parlamentu ze dne 12. července 2007 o dohodě mezi EU a USA o jmenné evidenci cestujících je také k dispozici na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=left&mid=08:02:10&u1=&u2=&t= v rubrice Zahraničí / Evropská unie.

[2)] Na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=top&mid=02:05&u1=&u2=&t=, v rubrice Názory Úřadu / Na aktuální téma, je k dispozici informace o názoru českého Úřadu na návrhy nové dohody k předávání dat PNR do USA.

## Pracovní skupina pro ochranu údajů zřízená podle článku 29

**01611/06/CS**
**WP 126**

# Stanovisko 8/2006 k přezkumu předpisového rámce pro elektronickou komunikaci a služby s důrazem na směrnici o soukromí a elektronických komunikacích

**přijaté dne**

**26. září 2006**

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán ve věci ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Její sekretariát je na Ředitelství C (Občanská spravedlnost, práva a státní občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B 1049 Brusel, Belgie, kancelář č. LX-46 01/43.

Internetová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB
V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na ustanovení článku 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a ustanovení čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

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

**přijala toto stanovisko:**

## 1. Souvislosti

Evropská Komise dne 29. června 2006 přijala sdělení o přezkumu předpisového rámce EU pro sítě a služby elektronických komunikací {SEC (2006) 816} {SEC (2006) 817}. V tomto sdělení podává Komise zprávu o fungování pěti směrnic tvořících předpisový rámec pro sítě a služby elektronických komunikací[1] a objasňuje, jak právní rámec plní své cíle, a určuje oblasti, které je potřeba změnit.

Sdělení je doplněno pracovním dokumentem útvarů Komise {COM (2006) 334 v konečném znění}, v němž jsou navržené změny provedeny. Posouzení dopadů zachycuje širší paletu možností, které byly zváženy před přijetím závěrů uvedených v tomto sdělení. Výše zmíněné dokumenty zahájily formální veřejnou diskuzi o budoucnosti předpisového rámce pro elektronické komunikace, do níž lze přispívat do 27. října 2006.

S přihlédnutím k obdrženým připomínkám Komise následně vypracuje legislativní návrhy změn předpisového rámce. Tento legislativní návrh poté předloží Parlamentu a Radě.

Přezkum zahrnuje také směrnici o soukromí a elektronických komunikacích, která patří ke skupině směrnic o elektronických komunikacích. Pracovní skupina zřízená podle článku 29 by chtěla tímto způsobem přispět k veřejné diskuzi, zejména pokud jde o směrnici o soukromí a elektronických komunikacích.

## 2. Všeobecné připomínky

Hlavní obavy pracovní skupiny zřízené podle článku 29 se týkají zpracování osobních údajů prostřednictvím elektronických komunikací a jejich bezpečnosti, protože při tomto zpracování vzniká v oblasti ochrany údajů celá řada problémů, na které by pracovní skupina zřízená podle článku 29 chtěla v tomto stanovisku upozornit.

[1] Směrnice 19/2002/ES Úř. věst. L 108, 24.4.2002, s. 7, 20/2002/ES Úř. věst. L 108, 24.4.2002, s. 21, 21/2002/ES Úř. věst. L 108, 24.4.2002, s. 33, 22/2002/ES Úř. věst. L 108, 24.4.2002, s. 51, 58/2002/ES Úř. věst. L 201, 31.7.2002, s. 37

Pracovní skupina zřízená podle článku 29 by při hodnocení sdělení s důrazem na směrnici o soukromí a elektronických komunikacích a na možné změny, které by chtěla do směrnice zavést, chtěla odkázat na své stanovisko 7/2000 k návrhu Evropské Komise na směrnici Evropského parlamentu a Rady týkající se zpracování osobních údajů a ochrany soukromí v odvětví elektronických komunikací[2]. Návrhy uvedené v tomto stanovisku nebyly bohužel zohledněny, a proto by je pracovní skupina chtěla uvést ještě shrnout:

(1) V uvedeném stanovisku pracovní skupina zřízená podle článku 29 zdůraznila, že skutečnost, že ustanovení směrnice o soukromí a elektronických komunikacích se týkají pouze ustanovení o veřejně dostupných službách v oblasti elektronických komunikací ve veřejných komunikačních sítích, je politováníhodná, protože soukromé sítě nabývají v každodenním životě na své důležitosti, čímž se zvyšuje riziko jejich zneužití, a to zejména z důvodu, že tyto sítě jsou stále specializovanější (např. sledování chování zaměstnance prostřednictvím provozních údajů). K přezkoumání rozsahu směrnice přispívá i tendence v oblasti služeb, kdy dochází k stále většímu prolínání soukromých a veřejných služeb.

(2) Pracovní skupina upozorňuje, že definice pojmů „elektronické komunikační služby“ a „poskytování elektronických komunikačních sítí“ nejsou stále jasné a oba pojmy by měly být vysvětleny podrobněji, aby se zajistila jasná a jednoznačná interpretace ze strany pracovníků odpovědných za zpracování údajů i ze strany uživatelů. Nejasné definice vznesly celou řadu otázek, jako např.: „Lze internetovou kavárnu považovat za poskytovatele elektronické komunikační sítě?“ Zodpovědět podobné otázky by mělo být jednoduché, avšak není tomu tak vždy.

(3) Dále se pracovní skupina zřízená podle článku 29 ve svém dřívějším stanovisku 7/2000 vyjádřila k bodu odůvodnění 25 směrnice o soukromí a elektronických komunikacích, pokud jde o používání cookies. V bodě odůvodnění 25 je uvedeno, že uživatelé musí mít možnost odmítnout, aby „cookies“ byly ukládány do jejich koncových zařízení. Pracovní skupina zřízená podle článku 29 toto stanovisko plně podporuje. Poslední odstavec bodu odůvodnění 25 však stanoví, že přístup k obsahu určitých webových stránek lze podmínit plně informovaným přijetím „cookie“, což by mohlo být v rozporu s ustanovením, že uživatelé musí mít možnost odmítnout, aby „cookies“ byly ukládány do jejich koncových zařízení. Z tohoto důvodu směrnice vyžaduje vysvětlení nebo přepracování.

## 3. Zvláštní příspěvky k různým odstavcům

*Pracovní dokument útvarů, oddíl 5.8 Zdokonalení donucovacích mechanismů podle stávajícího předpisového rámce*

Tento oddíl se týká potřeby přizpůsobit donucovací mechanismy a pravomoci, které mají příslušné orgány k dispozici k provádění směrnice o soukromí a elektronických komunikacích.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf

Dokument uvádí, že pokuty za neplnění předpisového rámce se ukázaly být nepřiměřené: *pokuty za porušování směrnice o soukromí a elektronických komunikacích jsou příliš nízké a její uplatňování se vymáhá nerovnoměrně.*

Je možné, že rozdíly zjištěné při vymáhání směrnice o soukromí a elektronických komunikacích nejsou zapříčiněny jejími ustanoveními, ale různými způsoby provedení do vnitrostátního práva. Členské státy například přijaly různé výklady čl. 13 odst. 2 a různé horní výše pokut za porušení této směrnice.

V tomto ohledu mohou vyšší a harmonizované pokuty působit účinněji jako odrazující prostředek, avšak samy o sobě neřeší pociťovanou nerovnoměrnost ve vymáhání směrnice. Samotné dostupné pokuty navíc nemusí nezbytně stanovit četnost, kterou se vymáhání práva vykonává. Povaha těchto pravomocí a postupů, jejichž prostřednictvím se vykonávají, mohou být důležitějším faktorem.

V některých členských státech mají orgány na ochranu údajů pouze omezené vyšetřovací pravomoci, např. nemusí mít právo přístupu ke komunikačním údajům potřebným k prokázání porušení směrnice.

Pokud v několika členských státech stávající donucovací pravomoci neumožňují regulačním orgánům přijmout rychlé opatření, mělo by se to řešit. Další obtíž při vymáhání směrnice je skutečnost, že mnoho spammů nespadá do jurisdikce orgánů v rámci EU. To by mělo být vyřešeno úzkou spoluprací mezi regulačními orgány v jiných zemích.

Pokud jde o výslovné právo týkající se opatření vůči spammům, jež je uvedeno v pracovním dokumentu útvarů, není zřejmé, jakým způsobem by se odlišovalo od současného stavu, kdy příslušný orgán může vůči těm, jež porušují stávající směrnici, přijmout donucovaní opatření.

*Pracovní dokument útvarů, oddíl 7 Bezpečnost*

Tento oddíl obsahuje klíčový návrh rozšířit a posílit bezpečností opatření. Opatření uvedená ve směrnici o soukromí a elektronických komunikacích budou sloučena s opatřeními směrnice o univerzální službě a budou tvořit zvláštní kapitolu rámcové směrnice týkající se bezpečnostních opatření.

Posílení bezpečnostních opatření přinese pravděpodobně prospěch spotřebitelům, není však jasné, jaký přínos by mohlo mít vytvoření zvláštní hybridní kapitoly. Lze namítnout, jak je uvedeno v pracovním dokumentu útvarů, že místo zdůraznění důležitosti tohoto problému, vyšle odstranění bezpečnostních opatření ze směrnice o soukromí a elektronických komunikacích signál, že bezpečnost se týká pouze sítí, hospodářské soutěže a provozovatelů sítí, zatímco ve skutečnosti se týká i ochrany základního práva na soukromí, jak je uvedeno ve směrnici o soukromí a elektronických komunikacích.

Pracovní skupina zřízená podle článku 29 by ráda doplnila, že místo chápání „bezpečnosti" v nejširším smyslu slova by se měla věnovat pozornost zvláštním aspektům bezpečnosti – ne pouze „kontinuitě" a „důvěrnosti", ale také „integritě" údajů, a zejména otázkám, které souvisejí s prokazováním totožnosti a anonymitou. Protože nedostatek přiměřených postupů k prokazování totožnosti může vést k vytvoření podvodných schémat a snížit důvěru uživatelů v elektronickou komunikaci, bylo by vhodné přidat do úvodního textu Kapitoly 7 pododdíl „falšování totožnosti". V tomto pododdíle lze uvést, že důvěrnost a včasné vymazání přebytečných osobních údajů přispívají k předcházení krádeže totožnosti.

Avšak pokud jde o otázky totožnosti, musíme mít na paměti, že jednotlivci musí mít v zásadě možnost používat veřejné elektronické služby anonymně. Proto je před provedením každého návrhu nebo změny, které se týkají otázek totožnosti, nutné provést důslednou analýzu přístupu k elektronickým službám, protože svobodná komunikace je velmi důležitá. Mohlo by vyjít najevo, že různé formy podvodů vznikají tím, že poskytovatelé služeb vyžadují identifikaci. V této oblasti by bylo vhodné provést odpovídající šetření.

*Pracovní dokument útvaru, oddíl 7.1 Povinnosti přijmout bezpečnostní opatření a pravomoci vnitrostátního regulačního orgánu stanovit a sledovat technické provádění*

V tomto oddíle se uvádí, že současný rámec poskytuje poskytovatelům služeb při hodnocení vhodnosti jejich vlastních bezpečnostních opatření příliš velký prostor. S ohledem na narůstající bezpečnostní hrozby se v dokumentu navrhuje vyjasnit pojmy uvedené v článku 4 směrnice o soukromí a elektronických komunikacích, aby se zvýšila účinnost bezpečnostních opatření.

Toto vysvětlení bude mít formu nových povinností, jako např.: opatření k řešení bezpečnostních událostí; požadavek na dodržování pokynů vydaných regulačními orgány; smluvní ustanovení informující spotřebitele o opatřeních, která je nutné přijmout v případě porušení bezpečnosti.

Zaprvé, není jasné, jakým jiným způsobem mohou některé z výše uvedených návrhů přispět ke stávajícímu rámci, než že kodifikují to, co již většina regulačních orgánů předpokládá. Není například pravděpodobné, že by regulační orgán potvrdil, že poskytovatel služeb, jehož bezpečnostní opatření neobsahují postupy týkající se bezpečnostních událostí a minimalizují dopad na spotřebitele, plnil povinnosti v souladu se směrnicí o soukromí a elektronických komunikacích.

Zadruhé, otázka, zda poskytovatel služeb dodržuje pokyny regulačního orgánu, by měla již dnes určitým způsobem rozhodovat o tom, zda poskytovatel služeb porušuje článek 4 směrnice o soukromí a elektronických komunikacích. Proto je obtížné určit, do jaké míry povinnost poskytovatele služeb řídit se těmito pokyny, jde dále než rozumný přístup regulačního orgánu ke stávajícím ustanovením.

Zatřetí, není zřejmé, do jaké míry by smluvní ustanovení, která informují spotřebitele o opatřeních, která by mohli v případě porušení bezpečnosti přijmout, byly jen kosmetickými změnami.

Pokud by tato ustanovení měla být závazná, mohly by návrhy představovat i riziko větší regulace nejen pro odvětví, ale i pro regulační orgán. Vzhledem k povaze tohoto odvětví není pro orgán na ochranu údajů možné stanovit bezpečnostní opatření ve formě závazných pokynů. Opatření musí odpovídat povaze odvětví. Mění se příliš rychle na to, aby orgán mohl kontrolovat celé odvětví a samozřejmě existuje velké množství odborníků v oblasti bezpečnosti, kteří jsou pro poskytování konzultací v oblasti bezpečnostních otázek a provádění kontrol vybaveni lepšími znalostmi.

Objasnění a závazné pokyny by měl poskytnout příslušný orgán tohoto odvětví, a ne odborníci v oblasti ochrany údajů. Je také důležité, abychom se vyhnuli těžkopádným nařízením, protože jak je uvedeno v dokumentu pracovních útvarů (poznámka 30), řešení otázek bezpečnosti zasahuje i mimo oblasti nařízení.

*Pracovní dokument útvarů, oddíl 7.2 Oznamování porušení bezpečnosti provozovatelům sítí a poskytovatelům internetových služeb*

V souvislosti s posledně uvedenými komentáři pracovní skupina zřízená podle článku 29 vítá návrh, který požaduje oznamování porušení bezpečnosti; je však třeba připomenout, že toto sdělení nepředpokládá žádné sankce pro případ, kdy provozovatel sítě nebo poskytovatel internetových služeb neinformuje vnitrostátní regulační orgán.

Pracovní skupina zřízená podle článku 29 předvídá i obavy odvětví, že by to mohlo být chápáno jako „zvláštní zacházení" pro jedno odvětví, kdy ostatní takovou oznamovací povinnost nemají. Avšak skupina zřízená podle článku 29 uznává, že tyto požadavky jsou v současné době „horkým tématem" a co je důležitější, jedná se o „mírnější" nařízení s velmi malým dodatečným zatížením pro ty poskytovatele služeb, kteří provádějí příslušná opatření a představují skutečné odstrašující opatření na trhu pro ty, kteří chtějí obcházet právní předpisy.

Na druhé straně je nutné zdůraznit, že žádné porušení bezpečnosti, která se v poslední době objevila ve zpravodajství USA (Choicepoint, LexisNexis, Bank of America, Time Warner atd.), nezahrnovala poskytovatele internetových služeb. Pracovní skupina zřízená podle článku 29 by chtěla navrhnout, aby se oznamovací povinnost týkala také „zprostředkovatelů údajů", bank a ostatních poskytovatelů internetových služeb. I když svojí definicí nepatří přímo mezi poskytovatelé internetových služeb, patří mezi odvětví, která jsou nejvíce ohrožena porušováním bezpečnosti.

Podle návrhu musí poskytovatelé internetových služeb informovat o porušení bezpečnosti pouze poškozené svých zákazníků. Avšak v případě závažného porušení (cílem sdělení není stanovit různé úrovně poškození nebo stanovit, kdy poškození podléhá oznamovací povinnosti) musí být informováni všichni zákazníci poskytovatele internetových služeb, ne pouze „poškození". Tento legislativní návrh by měl být základem pro pravidla ke klasifikaci různých úrovní porušení.

*Poskytovatelé přístupu k infrastruktuře a poskytovatelé služeb*

Sdělení rozlišuje mezi poskytovateli přístupu k infrastruktuře a poskytovateli služeb. V článku 3 stávající směrnice o soukromí a elektronických komunikacích je uvedeno zpracování údajů, na které se nařízení vztahují. Zatímco dříve bylo zřejmé, kdo je poskytovatelem veřejně dostupných služeb v oblasti elektronických komunikací, je vzhledem k vývoji v oblasti elektronické komunikace pro zákazníka obtížnější rozpoznat, kdo ve skutečnosti službu poskytuje. Zákazníci mohou přistupovat ke službám prostřednictvím portálu a služba může zahrnovat několik různých částí.

Pokud jde o otázky poskytování informací a udělení souhlasu, nemusí být vždy zcela jasné, kdo nese odpovědnost za informování uživatelů nebo komu se má vyjádřit souhlas. Současně může existovat riziko, že poskytovatelé služby mylně nasměrují uživatele na poskytovatele přístupu nebo sítě, pokud se tento provozovatel stará o zvláštní aspekty služby v technickém slova smyslu.

Pokud vezmeme v úvahu zvláštní postavení poskytovatelů přístupu k infrastruktuře a poskytovatelů služeb, mohlo by být užitečné přezkoumat, zda je nutné zdůraznit ustanovení o zpracování osobních údajů a ochraně soukromí v odvětví elektronické komunikace, aby se předešlo omylům týkajícím se otázky, pro koho jsou tato opatření určena. Proto by legislativní návrh měl poskytnout vysvětlení, a ne vést dalším nesrovnalostem.

## 4. Závěr

Pracovní skupina zřízená podle článkem 29 uvítala možnost konzultovat přezkum balíčku směrnic o elektronických komunikacích, zejména s důrazem na směrnici o soukromí a elektronických komunikacích. Pracovní skupina zřízená podle článku 29 by v prvé řadě chtěla doporučit zlepšení bezpečnostních opatření a zdůraznit, že ochrana uživatelů a posílení jejich důvěry v elektronické komunikace musí být při zlepšování bezpečnosti infrastruktury řádně zváženy.

Pracovní skupina zřízená podle článku 29 také navrhuje, aby se řešily otázky spojené s aplikacemi online. Ty zahrnují bezpečnostní otázky, odpovědnost poskytovatelů a vysvětlení právního postavení a pracovníků odpovědných za zpracování údajů..

Pracovní skupina zřízená podle článku 29 by ráda zdůraznila, že podporuje zlepšení bezpečnostních opatření, nicméně nepodporuje opatření, která vedou nebo by mohla vést k větší kontrole nebo blokování obsahu.

Pracovní skupina si vyhrazuje možnost komentovat budoucí znění směrnice.

V Bruselu dne 26. září 2006

*Za pracovní skupinu*

místopředseda
Jose Luis Piñar Mañas

## Pracovní skupina pro ochranu údajů zřízená podle ČLÁNKU 29

**01613/06/CS**
**WP 127**

# Stanovisko č. 9/2006 o provádění směrnice Rady 2004/82/ES o povinnosti dopravců předávat předběžné údaje o cestujících

**přijaté dne**

**28. září 2006**

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a v článku 15 směrnice 2002/58/ES.

Její sekretariát je na Ředitelství C (Občanská spravedlnost, práva a státní občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B 1049 Brusel, Belgie, kancelář č. LX-46 01/43.

Webová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na ustanovení článku 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a ustanovení čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

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

**přijala toto stanovisko:**

## I. – Provádění směrnice do vnitrostátního práva – potřeba poradenství

Rada dne 29. dubna 2004 přijala směrnici 2004/82/ES o povinnosti leteckých dopravců sdělovat na žádost orgánů zodpovědných za kontrolu vnějších hranic Evropské unie předběžné údaje o cestujících. Směrnice doplňuje ustanovení Schengenské úmluvy, neboť má rovněž za cíl omezení migračních toků a boj proti nedovolenému přistěhovalectví. Členské státy Evropské unie měly směrnici provést do vnitrostátních právních předpisů do 5. září 2006.

Pracovní skupina zřízená podle článku 29 poukazuje na to, že řada členských států nedodržela tento termín a že vnitrostátní předpisy, které by prováděly tuto směrnici, se ještě projednávají. Zatím stále není jasné, zda budou mít všechny členské státy směrnici provedenou do konce roku 2006. Další členské státy mají rozhodnout o praktických opatřeních, která musejí přijmout ohledně provádění směrnice.
Je třeba podotknout, že v zájmu leteckých cestujících i leteckých dopravců by směrnice měla být prováděna co nejdříve jednotným, harmonizovaným způsobem, aby v rámci Evropské unie nebyla používána odlišná nařízení. Ke všem dotčeným osobám letícím do Evropské unie by se mělo přistupovat stejně a všechny by měly požívat stejných práv. Je nutné vyhnout se situacím, kdy je k cestujícím přistupováno různým způsobem.
Pracovní skupina se rovněž domnívá, že ustanovení směrnice by měla být vykládána a prováděna jednotně, zcela v souladu se zásadami ochrany osobních údajů, jak je stanoveno ve směrnici 95/46/ES, a respektováním ochrany osobních údajů jako základního práva, kterého požívají všechny osoby v celé Evropské unii.
S ohledem na tento cíl považovala pracovní skupina za vhodné přijmout několik interpretačních a prováděcích pokynů, které by členským státům pomohly s prováděním směrnice a s rozvojem operativních postupů.

Pracovní skupina zřízená podle článku 29 si je plně vědoma rostoucího významu, který se celosvětově přikládá využívání předběžných informací o cestujících (API) při kontrole cestujících. Rovněž připomíná svůj názor vyjádřený již dříve[1], že je v střednědobém horizontu nezbytné vyvinout ucelenější přístup k výměně osobních údajů o cestujících, aby byla zajištěna bezpečnost letecké dopravy, boj proti nedovolenému přistěhovalectví a dodržování lidských práv na celosvětové úrovni.

[1] Stanovisko 5/2006 k rozsudku Evropského soudního dvora ze dne 30. května 2006 ve spojené věci C – 317/04 a C-318/04 o předávání záznamů o knihování cestujících do USA, WP122, 14. červen 2006.

**II. Zvláštní pokyny k ochraně osobních údajů**

1) Omezení účelu

1a) *Účely zpracování*: Účel sběru údajů je jasně vymezen v čl. 1 odst. 1 směrnice: zlepšení hraničních kontrol a boj proti nedovolenému přistěhovalectví. Za tímto účelem mohou „příslušné vnitrostátní orgány" od dopravců získat údaje, stanovené v čl. 3 odst. 2 směrnice.
Pracovní skupina připomíná, že při provádění směrnice je rozhodující zásada účelového omezení. Proto musejí být účely zpracování jasně stanovené ve vnitrostátních právních předpisech a omezené na informace stanovené ve výše zmíněném článku směrnice.

1b) *Výjimka pro „účely vynucování práva":* Podle čl. 6 poslední věty odst. 1 směrnice mohou členské státy odchylně od výše zmíněné zásady použít údaje rovněž pro „účely vynucování práva" v souladu se svým vnitrostátním právem a s ohledem na ustanovení o ochraně údajů obsažená ve směrnici 95/46/ES. Ve směrnici 2004/82 se však nedefinují účely vynucování práva. Pracovní skupina považuje za nezbytné, aby členské státy uplatňovaly tuto výjimku pouze omezeně a jasně stanovily konkrétní případy, kdy mohou být dané údaje použity pro vynucování práva. Pracovní skupina se zejména domnívá, že údaje mohou být takto použity pouze při vyšetřování závažných zločinů, ve zvláštních případech a po přijetí zvláštních opatření ochrany údajů, aby se předešlo jakémukoli jejich zneužití. Je nezbytné zajistit, aby práva na ochranu údajů byla zaručena rovněž tehdy, když údaje použijí jiné orgány, než pro které byly původně určeny.

1c) *Pouze lety do EU*: Je potřeba zmínit se také o tom, že se směrnice týká pouze letů směřujících do členského státu EU (viz čl. 3 odst. 1), což členským státům nedává právo požadovat od leteckých dopravců sběr a předávání předběžných údajů o cestujících, pokud jde o lety v rámci Evropské unie.

2) Rozsah sběru údajů: minimalizace údajů, jejich význam a přiměřenost

2a) *Kategorie údajů podle směrnice:* Ve směrnici se jasně stanovuje rozsah údajů, které mohou letečtí dopravci sdělovat příslušným vnitrostátním orgánům pro výše zmíněné účely (čl. 3 odst. 2). Tyto údaje by se měly považovat za nezbytné a dostatečné s ohledem na účely směrnice (zlepšení hraničních kontrol a boj proti nedovolenému přistěhovalectví).

2b) D*odatečné povinnosti a/nebo kategorie údajů, včetně biometrických údajů*: V bodě 8 směrnice je stanoveno, že členské státy mohou na požádání zavést dodatečné kategorie údajů pro letecké dopravce. V bodě 9 se odkazuje na možné zahrnutí „biometrických znaků" do informací, které mají dopravci poskytovat, vycházejících rovněž z „technologické inovace"; v této souvislosti je třeba poznamenat, že směrnice neposkytuje žádnou definici biometrických znaků a ponechává na dožadujících orgánech, aby vymezily, které biometrické znaky mají být předávány a kdy dožadující orgány považují takový převod za technicky proveditelný. Podle pracovní skupiny by byl sběr dodatečných údajů, včetně údajů souvisejících se zpátečními letenkami, jak je zmíněno v bodě 8, nepřiměřený s ohledem na uvedené účely; využití biometrických údajů by bylo dokonce ještě nepřiměřenější vzhledem ke skutečnosti, že neexistuje jednoznačné vymezení účelů, ke kterým by byly sbírány a zpracovávány, ani popis biometrických znaků nezbytných a přiměřených

pro tyto účely (viz úvahy o zpracovávání biometrických údajů v dokumentech WP80, WP96 a WP112).

2c) *Mezinárodní souvislosti a normy specifické pro dané odvětví:* Členské státy by rovněž měly zvážit rozsah údajů, které mají dopravci poskytovat s ohledem na mezinárodní normy stanovené příslušnými orgány, např. Mezinárodní organizací pro civilní letectví (ICAO), Světovou celní organizací (WCO) a Mezinárodním sdružením leteckých dopravců (IATA). Tyto subjekty v zájmu dosažení harmonizovaných norem a jednotného přístupu sestavily jasné definice předběžných informací o cestujících (API). Tyto normy byly nedávno znovu potvrzeny Evropskou konferencí pro civilní letectví, na které bylo dne 8. dubna 2006 přijato prohlášení o zásadách pro systémy API, které mají členské státy zohlednit „při zavádění systému API". Zejména je jasně stanoveno, že „údaje API tvoří údaje nalezené ve strojově čitelné zóně cestovního dokladu". V pokynech je doporučeno, aby údaje API nepřesahovaly tyto údaje uvedené v pokynech. Pracovní skupina by ráda zdůraznila, že pokud by členské státy požadovaly všechny údaje o cestujících obsažené ve jmenné evidenci cestujících (PNR) nebo v kontrolních odletových seznamech leteckých dopravců, porušily by směrnici 95/46, neboť v obou případech by dalece překračovaly údaje uvedené v pokynech a v jiných příslušných mezinárodních normách. Dále je třeba zdůraznit, že údaje PNR nejsou nezbytné pro účely hraničních kontrol.

3) Uchovávání údajů

Pracovní skupina by chtěla zdůraznit, že – jak je stanoveno ve směrnici – údaje, které získají orgány hraničních kontrol, mohou být uchovávány déle než 24 hodin jen v případě, že je to nezbytné pro účely vykonávání zákonných funkcí těchto orgánů. Ve směrnici však není stanoveno, jak dlouho mohou být tyto údaje uchovávány, pokud jsou předávány donucovacím orgánům podle výjimky předpokládané v čl. 6 odst. 1.
Výjimka z pravidla, že údaje nemají být uchovávány déle než 24 hodin, může být použita pro uchovávání údajů delší dobu jen ve zvláštních případech, např. pokud nelze zjistit totožnost cestujících nebo pokud cestující nemá správné cestovní doklady. Členské státy by měly zajistit, aby údaje nebyly uchovávány déle, než je nezbytně nutné s ohledem na tyto zvláštní účely.

4) Informování dotčených osob

V čl. 6 odst. 2 směrnice se od leteckých dopravců požaduje, aby informovali cestující v souladu se směrnicí 95/46/ES. Pracovní skupina zřízená podle článku 29 v této souvislosti připomíná, že 30. září 2004 přijala **Stanovisko 97** o informacích pro cestující, které se týká předávání údajů PNR v případě letů mezi Evropskou unií a Spojenými státy americkými, a 25. listopadu 2004 **Stanovisko 100**, které se týká ustanovení o harmonizovanějších informacích. Obě verze mohou posloužit jako vzory pro podrobné a otevřené informování cestujících. Pracovní skupina vyzývá letecké dopravce, aby využívali obou verzí tak, aby byly zcela v souladu s jejich povinnostmi podle směrnice 95/46/ES. Členské státy mají zajistit, aby cestující byli co nejjednotnějším způsobem rovněž informováni o možném dalším předávání jejich údajů donucovacím orgánům ke zvláštním účelům stanoveným ve vnitrostátních právních předpisech.

## III. – Závěr

Pracovní skupina zřízená článkem 29 plně podporuje cíl zastavení nedovoleného přistěhovalectví zlepšením kontrol v případě letů do Evropské unie, jak je stanoveno ve směrnici Rady 2004/82/ES. Pracovní skupina však chce zajistit, aby provádění této směrnice do vnitrostátního práva proběhlo co nejharmonizovaněji a nejjednotněji při zohlednění zásad ochrany údajů zakotvených ve směrnici 95/46/ES, které daná směrnice Rady úmyslně ponechala nezměněné.

Z tohoto důvodu pracovní skupina v tomto stanovisku vypracovala několik interpretačních a prováděcích pokynů, aby se předešlo rozdílným přístupům ze strany členských států, které by mohly vyplývat z nedostatku jasných pokynů v některých ustanoveních příslušné směrnice. Pracovní skupina vyzývá zákonodárce členských států a všechny příslušné vnitrostátní orgány, aby vzali v úvahu tyto pokyny při vytváření a uplatňování vnitrostátních právních předpisů provádějících tuto směrnici.

V Bruselu dne 27. září 2006

*Za pracovní skupinu*
Předseda
Peter SCHAAR

## Pracovní skupina pro ochranu údajů zřízená podle ČLÁNKU 29

**00323/07/CS**
**WP 131**

# Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR)

**přijatý dne 15. února 2007**

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jde o nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Jeho úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát skupiny zajišťuje ředitelství C (Civilní soudnictví, práva a občanství) Generálního ředitelství pro spravedlnost, svobodu a bezpečnost Evropské komise, B-1049 Brusel, Belgie, kancelář č. LX-46 01/43.

Internetová stránka: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

## SHRNUTÍ

V tomto pracovním dokumentu o **zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (electronic health records, EHR)** poskytuje pracovní skupina zřízená podle článku 29 vodítko k výkladu právního rámce ochrany údajů použitelného pro systémy EHR a vysvětluje některé obecné zásady. Pracovní dokument obsahuje rovněž orientační informace o požadavcích na ochranu údajů při budování systémů EHR a o příslušných ochranných opatřeních.

Pracovní skupina zřízená podle článku 29 nejprve zkoumá **obecný právní rámec ochrany údajů** pro systémy EHR. Přitom připomíná obecný zákaz zpracování osobních údajů týkajících se zdraví uvedený v čl. 8 odst. 1 směrnice o ochraně údajů 95/46/ES a poté se zabývá možným použitím odchylek v čl. 8 odst. 2, 3 a 4 této směrnice v souvislosti se systémy EHR, přičemž zdůrazňuje nutnost úzkého výkladu těchto odchylek.

Dále pracovní skupina zřízená podle článku 29 uvažuje o **vhodném právním rámci pro systémy EHR** a vydává **doporučení k jedenácti oblastem**, v nichž se zvláštní ochranná opatření v rámci systémů EHR jeví jako zvláště potřebná, aby byla pacientům a dalším osobám zaručena práva na ochranu údajů. Jedná se o tyto oblasti:

1. dodržování práva na sebeurčení,
2. identifikace a autentizace pacientů a zdravotníků,
3. oprávnění pro přístup k EHR pro čtení a zápis,
4. využití EHR pro jiné účely,
5. organizační struktura systému EHR,
6. kategorie údajů uložených v EHR a způsoby jejich prezentace,
7. mezinárodní předávání lékařských záznamů,
8. zabezpečení údajů,
9. transparentnost,
10. otázky odpovědnosti,
11. kontrolní mechanismy pro zpracování údajů v EHR.

Pracovní skupina zřízená podle článku 29 vyzývá lékařský stav, všechny zdravotníky, všechny zúčastněné osoby a instituce i širokou veřejnost, aby k tomuto pracovnímu dokumentu podávali připomínky.

## OBSAH

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[1], a zvláště na článek 29 a čl. 30 odst. 1 písm. b) této směrnice,

s ohledem na jednací řád pracovní skupiny[2], a zvláště na články 12 a 14 tohoto jednacího řádu,

PŘIJALA TENTO PRACOVNÍ DOKUMENT:

# I. Úvod

Účelem tohoto pracovního dokumentu pracovní skupiny zřízené podle článku 29 je poskytnout vodítko k výkladu právního rámce ochrany údajů použitelného pro systémy elektronických zdravotních záznamů (EHR) a stanovit některé obecné zásady. Dalším cílem tohoto stanoviska je popsat předběžné podmínky vybudování celostátního systému EHR z hlediska ochrany údajů, jakož i příslušná ochranná opatření.

Náklady na systémy veřejného zdravotnictví dramaticky rostou a vlády volají po nových strategiích pro řešení tohoto problému. „Elektronický zdravotní záznam“ (EHR) je jednou z často navrhovaných odpovědí. V této oblasti se používají termíny „elektronický lékařský záznam“ (electronic medical record, EMR), „elektronický záznam o pacientovi“ (electronic patient record, EPR), „elektronický zdravotní záznam“ (electronic health record, EHR), „počítačový záznam o pacientovi“ (computer-based patient record, CPR) atd. Tyto termíny lze používat zaměnitelně.

Pro účely tohoto pracovního dokumentu se „elektronickým zdravotním záznamem“ (dále jen „EHR“) rozumí:

> *„komplexní lékařský záznam nebo podobná dokumentace o minulém a současném stavu tělesného a duševního zdraví fyzické osoby v elektronické podobě, který zajišťuje snadnou dostupnost těchto údajů pro léčbu a jiné s ní úzce související účely[3]“.*

Tradičně byla dokumentace o léčebných epizodách k dispozici u různých zdravotníků, ale nebyla spojována do jediného souboru záznamů. Naproti tomu koncepce „EHR“ směřuje ke shromáždění stávající dokumentace o lékařské péči týkající se určité osoby z různých zdrojů a z různých časových období. Záznamy tak budou poskytovat co nejúplnější informace o minulém a současném zdravotním stavu dané osoby, a to po značně dlouhou dobu, případně i po celý život této osoby (*„od kolébky do hrobu“*). Poté, co budou údaje v EHR shromážděny, budou k dispozici v elektronické podobě všem zdravotníkům a institucím s příslušným oprávněním, kdekoli a kdykoli budou tyto informace zapotřebí.

Tvrdí se, že EHR je vhodným prostředkem pro:

---

1 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. L 281 23.11.1995, s. 31 (dále jen „směrnice“), dostupná na adrese: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

2 Přijatý pracovní skupinou na jejím třetím zasedání dne 11. září 1996.

3 „Léčbou a s ní úzce souvisejícími účely“ se míní účely uvedené v čl. 8 odst. 3 směrnice.

- zlepšení kvality léčby díky lepším informacím o pacientovi;
- zvýšení nákladové efektivity lékařských výkonů, které zabrání dalšímu rychlému růstu schodků zdravotnických rozpočtů;
- získání údajů nezbytných pro kontrolu kvality, statistiku a plánování ve veřejném zdravotnictví, což by mělo rozpočty veřejného zdravotnictví rovněž příznivě ovlivnit.

Z odpovědí na dotazník, který byl v roce 2005 rozeslán evropským orgánům dozoru nad ochranou údajů, vyplynulo, že celostátní systémy EHR jsou ve většině členských států aktuálním a naléhavým tématem. Míra realizace příslušných projektů se však výrazně liší – zatímco ve většině členských států se o EHR diskutuje, některé jiné již systémy EHR alespoň zčásti vybudovaly.

Vzhledem k tomu, že zdravotní péče je v rostoucí míře poskytována také přeshraničně, Evropská komise ve svém sdělení „*Elektronické zdravotnictví – zlepšení zdravotní péče pro evropské občany: Akční plán pro evropský prostor elektronického zdravotnictví*[4]“ zdůraznila význam služeb elektronického zdravotnictví a interoperability elektronických zdravotních záznamů. Kromě toho Evropské společenství financuje relevantní projekty, které se týkají například elektronických záznamů o pacientech nebo identifikátorů pacientů (např. evropský průkaz zdravotního pojištění). Při provádění takovýchto programů má Evropská komise povinnost společně s členskými státy zajistit dodržování všech příslušných právních předpisů upravujících ochranu osobních údajů, případně rovněž vytvoření mechanismů, které zabezpečí důvěrnost a bezpečnost těchto údajů[5].

**Systémy EHR mají potenciál dosáhnout vyšší kvality a lepšího zabezpečení lékařských informací než tradiční formy lékařské dokumentace. Nicméně z hlediska ochrany údajů je nutné zdůraznit skutečnost, že tyto systémy mají kromě toho také nejen potenciál zpracovávat více osobních údajů (např. v nových souvislostech nebo prostřednictvím seskupování), ale také potenciál snadněji zpřístupňovat údaje o pacientovi širšímu okruhu příjemců než doposud.**

Je rovněž třeba poznamenat, že elektronické informace o zdraví v systému EHR – kromě toho, že jsou přístupné zdravotníkům – mohou obecně vyvolávat také zájem třetích stran, jako jsou pojišťovny či donucovací orgány. Tím, že shromažďují stávající lékařské informace o jednotlivci z různých zdrojů, a tak umožňují snadnější a širší přístup k těmto citlivým informacím, vytvářejí systémy EHR nový rizikový scénář z pohledu ochrany osobních údajů, protože mění celé měřítko možného zneužití lékařských informací o fyzických osobách. Tento nový rizikový scénář sice bude u většiny projektů zcela naplněn teprve v budoucnosti, až budou realizovány v plném rozsahu, ale uvedená nebezpečí je nutné si uvědomit již nyní, kdy je většina stávajících modelů uplatňována jen omezeným nebo dílčím způsobem (např. pouze u základního souboru lékařských údajů nebo u nemocnic v určitém regionu), protože jejich všeobecné uplatnění je jen otázkou času.

# II. Rámec ochrany údajů pro elektronické zdravotní záznamy

Při jakémkoli zpracování osobních údajů v systémech EHR musejí být plně dodržována pravidla ochrany osobních údajů. Pracovní skupina by ráda zdůraznila, že na využívání EHR se vztahuje rámec stanovený ve 2. bodu odůvodnění směrnice, kde je uvedeno, že *„systémy zpracování údajů slouží lidem; že musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob, zejména právo na soukromí,*

[4] KOM(2004) 356 v konečném znění.

[5] Viz např. čl. 5 odst. 5 rozhodnutí 1786/2002/ES.

*a přispívat k hospodářskému a sociálnímu pokroku, k rozvoji obchodu, jakož i dobrých životních podmínek jednotlivců"*.

Základní právo na ochranu osobních údajů je v podstatě založeno na článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod a na článku 8 Listiny základních práv EU[6]. Přesnější pravidla jsou stanovena především ve směrnici ES o ochraně údajů 95/46/ES, ve směrnici 2002/58/ES o soukromí a elektronických komunikacích[7] a ve vnitrostátních právních předpisech členských států, kterými se tyto směrnice provádějí.

Každé zpracování osobních údajů v EHR musí také odpovídat pravidlům stanoveným v Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat Rady Evropy (ETS č. 108) a v Dodatkovém protokolu k Úmluvě č. 108 o orgánech dozoru a toku dat přes hranice (ETS č. 181).

V souvislosti s EHR by pracovní skupina ráda upozornila zvláště na doporučení Rady Evropy č. R(97) 5 o ochraně zdravotních údajů (13. únor 1997). Odkazujeme rovněž na doporučení obsažená v „Pracovním dokumentu o dostupnosti elektronických zdravotních záznamů prostřednictvím internetu" (Working Document on Online Availability of Electronic Health Records) Mezinárodní pracovní skupiny pro ochranu dat v telekomunikacích[8].

## 1. Obecné zásady

Správci údajů, kteří sbírají údaje v souvislosti s použitím EHR, tedy musejí dodržovat všechny obecné zásady ochrany údajů, zejména tyto zásady:

- zásada omezeného použití (zásada účelovosti): tato zásada, která je částečně zakotvena mimo jiné v čl. 6 odst. 1 písm. b) směrnice, zakazuje další zpracování údajů neslučitelné s účely, pro které byly údaje shromážděny;
- zásada kvality údajů: tato zásada, obsažená ve směrnici, vyžaduje, aby osobní údaje byly podstatné a nepřesahovaly míru s ohledem na účely, pro které jsou shromažďovány. Nesmějí se tedy sbírat žádné nepodstatné údaje a pokud byly sebrány, musejí být zlikvidovány (čl. 6 odst. 1 písm. c)). Zásada také vyžaduje, aby údaje byly přesné a aktualizované;
- zásada omezené doby uchovávání: tato zásada vyžaduje, aby osobní údaje byly uchovávány po dobu ne delší, než je nezbytné pro uskutečnění cílů, pro které byly shromážděny nebo dále zpracovány;
- požadavky na informování: podle článku 10 směrnice musejí správci údajů, kteří zpracovávají informace v systémech EHR, subjektům údajů poskytnout určité informace, například informace o totožnosti správce, o účelech zpracování, o příjemcích údajů a o existenci práva na přístup k údajům;
- právo subjektu údajů na přístup k údajům: článek 12 směrnice dává subjektům údajů možnost kontrolovat přesnost údajů a zajistit, aby byly aktualizovány. Tato práva se v plném rozsahu vztahují na shromažďování osobních údajů v systémech EHR;

---

6 Právo na ochranu osobních údajů není absolutní a může být omezeno, vyžaduje-li to konkrétní veřejný zájem. Nicméně tyto cíle ve veřejném zájmu mohou zásah do ochrany osobních údajů ospravedlnit pouze v případech, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných a není to nepřiměřené sledovaným cílům (čl. 8 odst. 2 Evropské úmluvy o ochraně lidských práv a základních svobod).

7 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. L 201, 31.7.2002, s. 37–47).

8 Přijat na jejím 39. zasedání ve Washingtonu D.C. ve dnech 6.–7. dubna 2006 (http://www.berlin-privacy-group.org).

- povinnosti související s bezpečností: článek 17 směrnice správcům údajů ukládá povinnost přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení a neoprávněnému sdělování. Tato opatření mohou být organizační nebo technická.

### 2. Zvláštní ochrana citlivých osobních údajů

Pokud se ovšem zpracování osobních údajů týká zdraví člověka, je zvláště citlivé, a tudíž vyžaduje zvláštní ochranu.

Definice osobních údajů uvedená v čl. 2 písm. a) směrnice 95/46/ES zní takto:

*„Osobními údaji (*se rozumí*) veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.“*

Zvláštní kategorie údajů jsou v čl. 8 odst. 1 směrnice definovány takto:

*„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.“*

Například uvedení skutečnosti, že si určitá osoba poranila nohu a pracuje na poloviční úvazek ze zdravotních důvodů, představuje osobní údaj týkající se zdraví ve smyslu čl. 8 odst. 1 směrnice.[9] Tato definice zahrnuje také osobní údaje, které mají jasnou a těsnou souvislost s popisem zdravotního stavu osoby; „osobními údaji o zdraví“ tak jsou nepochybně údaje o užívání léků, konzumaci alkoholu či drog, jakož i genetické údaje, zvláště jsou-li součástí zdravotních záznamů. Také veškeré další údaje, např. administrativní údaje (číslo sociálního pojištění, datum přijetí do nemocnice apod.), obsažené v lékařské dokumentaci týkající se léčby pacienta je třeba považovat za citlivé – kdyby neměly význam v souvislosti s léčbou pacienta, nebyly by a neměly by být do této dokumentace zařazovány.

**V důsledku toho zastávají členové pracovní skupiny stanovisko, že všechny údaje v lékařské dokumentaci, v elektronických zdravotních záznamech a v systémech EHR by měly být považovány za „citlivé osobní údaje“.** Proto se na ně vztahují nejen všechna obecná pravidla ochrany osobních údajů obsažená ve směrnici, ale navíc také zvláštní pravidla pro ochranu údajů uvedená v článku 8 směrnice, která se týkají zpracování citlivých informací.

### 3. Obecný zákaz zpracování osobních údajů týkajících se zdraví – s odchylkami

V čl. 8 odst. 1 směrnice o ochraně údajů 95/46/ES je obecně zakázáno zpracování osobních údajů týkajících se zdraví. Stejný zákaz je obsažen v článku 6 Úmluvy Rady Evropy č. 108.

Tato zvláštní ochrana podle čl. 8 odst. 1 doplňuje ostatní ustanovení směrnice, zejména článek 6 o zásadách pro kvalitu údajů a článek 7 o zásadách pro oprávněné zpracování údajů.

Avšak vzhledem tomu, jak důležité je využití informací o pacientovi pro jeho správnou léčbu, existují výjimky z tohoto obecného zákazu zpracování lékařských údajů.

---

[9] Evropský soudní dvůr, rozsudek ze dne 6. listopadu 2003, věc C-101/01 – Bodil Lindqvist.

Směrnice o ochraně údajů stanoví **závazné odchylky** v čl. 8 odst. 2 a 3 a také **volitelnou výjimku** v čl. 8 odst. 4.

Všechny tyto odchylky mají **omezenou** a **vyčerpávající** povahu a je nutné je **vykládat úzce**.

### 4. Čl. 8 odst. 2 písm. a): „výslovný souhlas“

Čl. 8 odst. 2 písm. a) směrnice stanoví:

> *„Odstavec 1 se nepoužije, pokud: a) subjekt údajů udělí výslovný souhlas k takovému zpracování, ledaže právní předpisy členského státu stanoví, že zákaz uvedený v odstavci 1 nelze zrušit udělením souhlasu subjektu údajů.“*

**a)** Zpracování citlivých údajů tedy může být opodstatněno na základě **souhlasu** subjektu údajů.[10] Jak již bylo uvedeno v předchozích pracovních dokumentech pracovní skupiny WP 12[11] a WP 114[12], důležité je, že aby byl platný, musí tento souhlas, bez ohledu na okolnosti, za kterých je udělen, být „*svobodným, výslovným a vědomým projevem vůle subjektu údajů*“, jak je definováno v čl. 2 písm. h) směrnice.

aa) Souhlas musí být udělen svobodně: „svobodným“ souhlasem se rozumí dobrovolné rozhodnutí osoby, která je při plném vědomí, přijaté bez jakéhokoli nátlaku společenského, finančního, psychického či jiného druhu. Za „svobodný“ nelze považovat žádný souhlas daný v situaci zdravotní péče pod hrozbou odepření léčby nebo horší kvality léčby. Souhlas udělený subjektem údajů, který nemá skutečnou možnost volby nebo je postaven před hotovou věc, nelze pokládat za platný.

Pracovní skupina zřízená podle článku 29 zastává názor, že jestliže zdravotník musí zpracovat osobní údaje v systému EHR, protože je to nutný a nevyhnutelný důsledek situace zdravotní péče, je zavádějící, když se toto zpracování snaží legitimizovat získáním souhlasu. Opírat se o souhlas by mělo být možné pouze v případech, kdy má jednotlivý subjekt údajů skutečnou svobodu volby a má možnost svůj souhlas následně odvolat, aniž by ho to poškodilo.[13]

bb) Souhlas musí být výslovný (určitý): „výslovný“ souhlas se musí týkat jasně definované konkrétní situace, v níž se počítá se zpracováním lékařských údajů. „Obecné svolení“ subjektu údajů např. ke sběru jeho lékařských údajů pro EHR a k následnému předávání těchto lékařských údajů z minulosti a z budoucnosti zdravotníkům podílejícím se na léčbě by tedy nepředstavovalo souhlas ve smyslu čl. 2 písm. h) směrnice.

cc) Souhlas musí být vědomý: „vědomým“ souhlasem se rozumí souhlas subjektu údajů založený na uvědomění si a pochopení relevantních skutečností a důsledků určitého jednání. Dotčené osobě musejí být jasným a srozumitelným způsobem

---

[10] Souhlas s podstoupením určité léčby neznamená automaticky udělení „souhlasu“ ve smyslu čl. 2 písm. h) se zpracováním (zejména se sdělováním nebo předáváním) osobních údajů shromážděných v průběhu této léčby.

[11] Pracovní skupina zřízená podle článku 29, „Pracovní dokument: Předávání osobních údajů do třetích zemí: použití článků 25 a 26 směrnice EU o ochraně údajů“ (WP 12, 24. červenec 1998).

[12] Pracovní skupina zřízená podle článku 29, „Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995“ (WP 114, 25. listopad 2005).

[13] Viz též pracovní skupina zřízená podle článku 29, „Stanovisko č. 8/2001 ke zpracování osobních údajů v pracovním poměru“ (WP 48, oddíl 10).

poskytnuty přesné a úplné informace o všech podstatných otázkách, zvláště těch uvedených v článcích 10 a 11 směrnice, jako jsou povaha zpracovávaných údajů, účely zpracování, příjemci, jimž budou údaje případně předány, a práva subjektu údajů. To zahrnuje také vědomí důsledků nesouhlasu s daným zpracováním údajů.

**b)** Na rozdíl od ustanovení článku 7 směrnice musí být souhlas v případě citlivých osobních údajů, a tedy i v případě EHR, **výslovný** (explicitní). Řešení založená na předpokládaném souhlasu (opt-out) požadavek na „výslovný" souhlas splňovat nebudou. V souladu s obecnou definicí, podle níž souhlas předpokládá vyjádření úmyslu, se výslovnost musí týkat především **citlivosti údajů**. Subjekt údajů si musí být vědom, že se vzdává zvláštní ochrany. Souhlas však nemusí být písemný.

**c)** Pracovní skupina zřízená podle článku 29 zaznamenala, že někdy je složité získat souhlas kvůli praktickým problémům, zejména když neexistuje přímý kontakt mezi správcem údajů a subjekty údajů. Bez ohledu na potíže však musí být **správce údajů** schopen ve všech případech dokázat, že zaprvé získal výslovný souhlas každého subjektu údajů a zadruhé že tento výslovný souhlas byl udělen na základě dostatečně přesných informací.

**d)** Opět na rozdíl od článku 7 se v čl. 8 odst. 2 písm. a) uznává, že mohou existovat případy zpracování citlivých údajů, kdy by **ani výslovný souhlas** subjektu údajů neměl rušit zákaz zpracování; členské státy se mohou svobodně rozhodnout, zda a jak takové případy podrobně upraví.

### 5. Čl. 8 odst. 2 písm. c): „životně důležité zájmy subjektu údajů"

Zpracování citlivých osobních údajů může být opodstatněné, pokud je nezbytné k obraně životně důležitých zájmů subjektu údajů nebo jiné osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas.

Zpracování se musí týkat zásadních individuálních zájmů subjektu údajů nebo jiné osoby a v kontextu lékařské péče musí být nezbytné pro život zachraňující léčbu v situaci, kdy subjekt údajů není schopen vyjádřit své úmysly. Tuto výjimku lze tedy využít pouze v malém počtu případů léčby a vůbec jí nelze odůvodňovat zpracování osobních lékařských údajů pro jiné účely než léčbu subjektu údajů, například pro obecný lékařský výzkum, který přinese výsledky až někdy v budoucnu.[14]

Příklad: předpokládejme, že subjekt údajů upadl po nehodě do bezvědomí a nemůže udělit souhlas s nezbytným sdělením informací o alergiích, kterými trpí. V rámci systémů EHR by toto ustanovení zdravotníkům umožnilo získat přístup k informacím uloženým v EHR, které se týkají známých alergií subjektu údajů, protože tyto informace by mohly mít rozhodující význam pro volbu léčebného postupu.

### 6. Čl. 8 odst. 3: „zpracování (lékařských) údajů odbornými zdravotnickými pracovníky"

Čl. 8 odst. 3 umožňuje zpracování citlivých osobních údajů za tří podmínek, které musejí být splněny současně: zpracování citlivých osobních údajů musí být *„nezbytné"*, toto zpracování probíhá *„pro účely zdravotní prevence, lékařských diagnóz, lékařské péče a ošetřování nebo správy zdravotnických služeb"* a dotčené osobní údaje *„zpracovává odborný zdravotnický pracovník, který je na základě vnitrostátního práva nebo právních předpisů přijatých*

[14] Pro výklad obdobného ustanovení v čl. 26 odst. 1 písm. e), které se týká předávání údajů mimo EU, viz pracovní skupina zřízená podle článku 29, „Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995" (WP 114, 25. listopad 2005).

*příslušnými vnitrostátními orgány vázán povinností zachovávat profesní tajemství, nebo jiná osoba rovněž podléhající obdobné povinnosti mlčenlivosti"*.

**a)** Tato odchylka se vztahuje pouze na zpracování osobních údajů za **konkrétním účelem** poskytnutí zdravotnických služeb v oblasti prevence, diagnostiky, léčby nebo následné péče a za účelem řízení těchto zdravotnických služeb, např. pokud jde o fakturaci, účtování nebo statistiku.

Nevztahuje se na další zpracování, které není nezbytné pro bezprostřední poskytování těchto služeb, tedy například na lékařský výzkum, následnou úhradu nákladů ze systému zdravotního pojištění či uplatňování peněžních nároků. Stejně tak do oblasti použití čl. 8 odst. 3 nespadají některá jiná zpracování údajů 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, protože ta jsou uvedena v 34. bodu odůvodnění směrnice jako příklady, v nichž se uplatní čl. 8 odst. 4.

**b)** Kromě toho musí zpracování osobních údajů z důvodů čl. 8 odst. 3 být „**nezbytné**" pro konkrétní účely uvedené v bodu a). Pracovní skupina zdůrazňuje, že v souvislosti s EHR to znamená, že každé vložení osobních údajů do EHR musí být plně opodstatněné; nepostačuje tedy pouhá skutečnost, že je „užitečné" mít tyto osobní údaje v EHR.

**c)** Třetí podmínkou podle čl. 8 odst. 3 je, že zpracování citlivých osobních údajů provádí zdravotnický nebo jiný personál, který je vázán **profesním (lékařským) tajemstvím nebo obdobnou povinností mlčenlivosti.**

> Etický požadavek mlčenlivosti kladený na lékařský stav byl poprvé formulován v „Hippokratově přísaze"[15] a později potvrzen v Ženevské deklaraci Světové lékařské asociace (1948). Tento požadavek chrání informace, které zdravotník shromáždí v průběhu léčby pacienta. Použití těchto informací je povoleno pouze v mezích kontaktu mezi lékařem a pacientem v rámci léčby. Z tohoto důvěrného vztahu jsou vyloučeny všechny třetí strany, dokonce i ostatní zdravotníci, ledaže pacient s předáním svých údajů souhlasil nebo je stanoveno zvláštním zákonem.

Pracovní skupina upozorňuje, že zvláštní povinnost zachovávat profesní tajemství musí být stanovena vnitrostátními právními předpisy členských států nebo příslušnými vnitrostátními profesními organizacemi s pravomocí přijímat pravidla závazná pro příslušníky daného povolání. Součástí těchto vnitrostátních pravidel pro profesní tajemství musejí být také odpovídající účinné postihy za jejich porušení.

Ze směrnice vyplývá, že pokud nastane potřeba, aby tyto citlivé osobní údaje zpracovávali nezdravotničtí pracovníci, musejí být rovněž podrobeni závazným pravidlům, která zajistí přinejmenším rovnocennou úroveň důvěrnosti a ochrany. Tato pravidla musejí obsahovat zvláště povinnost používat údaje pouze pro účely uvedené v čl. 8 odst. 3.

Zdravotníci, kteří mají přímou odpovědnost za léčbu pacientů, všeobecně podléhají zákonné povinnosti uchovávat dokumentaci o jejich léčbě (o zákrocích, předepsaných lécích atd.) v záznamech o pacientech. V souladu s mnoha platnými právními předpisy o povinnosti zdravotníků zachovávat profesní tajemství je vedení a používání záznamů o pacientech tradičně omezeno na přímý dvoustranný vztah mezi pacientem a zdravotníkem či zdravotnickým zařízením, na které se pacient obrátil.

**d)** Jelikož čl. 8 odst. 3 směrnice představuje výjimku z obecného zákazu zpracování citlivých údajů, tuto výjimku je nutné vykládat restriktivně.

[15] „Cokoli, co při léčbě i mimo svou praxi ve styku s lidmi uvidím a uslyším, co nesmí se sdělit, to zamlčím a uchovám v tajnosti." (Zdroj: http://cs.wikipedia.org/wiki/Hippokratova_přísaha).

**e)** Pokud by byla vznesena otázka, zda čl. 8 odst. 3 může sloužit jako *jediný* právní základ pro zpracování osobních údajů v systému EHR, stanoviskem pracovní skupiny zřízené podle článku 29 je, že čl. 8 odst. 3 se může použít pouze v případě zpracování lékařských údajů přísně pro ty lékařské a zdravotnické účely, které jsou v tomto ustanovení uvedeny, a přísně za podmínek, že zpracování je „nezbytné“ a prováděné zdravotníkem nebo jinou osobou vázanou povinností zachovávat profesní tajemství nebo obdobnou povinností mlčenlivosti. Jestliže jde zpracování osobních údajů v EHR jakkoli nad rámec těchto účelů nebo nesplňuje uvedené podmínky, pak čl. 8 odst. 3 nemůže být jediným právním základem pro zpracování těchto osobních údajů.

Pracovní skupina je ovšem nucena upozornit na to, že systémy EHR i při splnění všech těchto nezbytných předpokladů vytvářejí nový rizikový scénář, na který je třeba reagovat dodatečnými novými ochrannými opatřeními – systémy EHR totiž poskytují přímý přístup k souboru stávající dokumentace o léčbě určité osoby získané z různých zdrojů (např. nemocnice a zdravotníci) za celý život této osoby. Tyto systémy tudíž překračují tradiční hranice přímého vztahu mezi jednotlivým pacientem a zdravotníkem nebo zdravotnickým zařízením. Uchovávání lékařských informací v EHR tak jde nad rámec tradičních způsobů vedení a používání lékařské dokumentace o pacientech. Z technického hlediska existence mnoha přístupových bodů v otevřené síti, jako je internet, zvyšuje nebezpečí neoprávněného přístupu k údajům o pacientovi. V okamžiku, kdy jsou elektronické zdravotní záznamy zpřístupněny on-line, nemusí pro ochranu práv pacienta na soukromí stačit, že jsou zachovány zákonné požadavky na důvěrnost, které jsou vhodné v tradičním prostředí papírových záznamů. Plně rozvinuté systémy EHR tedy mají tendenci otevírat a usnadňovat přístup k lékařským informacím a citlivým osobním údajům. Systémy EHR představují vážnou výzvu, pokud jde o to zajistit, že přístup k informacím bude omezen pouze na příslušné zdravotníky a na legitimní účely související s péčí o subjekt údajů. V jejich rámci se zpracování citlivých osobních údajů stává složitější otázkou a to má přímé důsledky pro práva jednotlivců. Z hlediska ochrany citlivých osobních údajů je proto nutné systémy EHR považovat za nový rizikový scénář.

Hlavním a tradičním ochranným opatřením uvedeným v čl. 8 odst. 3 je – vedle omezení účelu a přísného požadavku na nezbytnost – povinnost lékařů zachovávat důvěrnost lékařských údajů o pacientech. V prostředí EHR již toto opatření nemusí být zcela relevantní, protože jedním z cílů EHR je poskytnout přístup k lékařské dokumentaci pro účely léčby zdravotníkům, kteří se na dřívější léčbě zdokumentované v lékařských záznamech nepodíleli.

Pracovní skupina zřízená podle článku 29 proto není přesvědčena, že samotná povinnost zachovávat profesní tajemství představuje dostatečnou ochranu v prostředí EHR, a to ani v případě, že je zpracování údajů odůvodněno čl. 8 odst. 3. Vzhledem k existenci nového rizikového scénáře jsou pro zajištění dostatečné ochrany osobních údajů v souvislosti s EHR nutná dodatečná a případně nová ochranná opatření nad rámec těch, které vyžaduje čl. 8 odst. 3.

### 7. Čl. 8 odst. 4: výjimky z důvodu významného veřejného zájmu

Řada ustanovení směrnice obsahuje značnou míru pružnosti, aby bylo dosaženo vhodné rovnováhy mezi ochranou práv subjektu údajů na jedné straně a legitimními zájmy správců údajů a třetích stran, jakož i případným veřejným zájmem, na straně druhé.

Čl. 8 odst. 4 směrnice dává členským státům další možnost, jak se odchýlit od zákazu zpracovávat údaje citlivých kategorií:

*„Jsou-li poskytnuta vhodná ochranná opatření, mohou členské státy stanovit z důvodu významného veřejného zájmu i jiné výjimky, než jaké jsou stanoveny v odstavci 2 buď prostřednictvím vnitrostátních právních předpisů, nebo rozhodnutím orgánu dozoru.“*

34. bod odůvodnění zní:

*(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 – a vědecký výzkum a veřejné statistiky; že jim nicméně přísluší, aby poskytly vhodná a zvláštní ochranná opatření na ochranu základních práv a soukromí jednotlivců;“*

a) Z toho vyplývá, že pokud má členský stát v úmyslu využít tuto možnost, daná výjimka musí být obsažena v právním ustanovení nebo v rozhodnutí orgánu dozoru (zvláštní právní základ).

b) Zpracování citlivých osobních údajů musí být v tomto případě opodstatněné z důvodu **významného veřejného zájmu**. V 34. bodu odůvodnění směrnice jsou uvedeny příklady oblastí, v nichž se mohou případy „významného veřejného zájmu“ vyskytovat především. Patří k nim zdravotnictví a sociální zabezpečení, kde jde o zajištění kvality a rentability postupů používaných pro vyřizování nároků na plnění a služby v rámci systému zdravotního pojištění.

U každého případu musí členský stát demonstrovat existenci významného veřejného zájmu v celém rozsahu zpracování, na které se vztahuje výjimka, a dané zpracování musí být nezbytné vzhledem k tomuto významnému veřejnému zájmu. Každé takové opatření musí být přiměřené, tj. nesmějí být k dispozici jiná opatření, která by ochranu osobních údajů narušovala v menší míře.

Každý zásah do práva na soukromý a rodinný život může být navíc legitimní jedině tehdy, je-li v souladu s článkem 8 Evropské úmluvy o lidských právech čteným ve světle judikatury Štrasburského soudu, tj. musí se provádět „*v souladu se zákonem*“ a musí to být „*nezbytné v demokratické společnosti*“ za účelem veřejného zájmu. Ve štrasburské judikatuře se opakovaně konstatuje, že v právním předpisu, kterým se zásah stanoví, „*musí být dostatečně přesně uveden rozsah a způsob výkonu každé takové pravomoci svěřené příslušným orgánům s ohledem na legitimní cíl dotyčného opatření, aby byl jednotlivec dostatečně ochráněn před svévolnými zásahy*“.

c) Členské státy mají povinnost zavést vhodná a zvláštní ochranná opatření s cílem ochránit v této souvislosti základní práva a soukromí jednotlivců.

d) Každé použití čl. 8 odst. 4 členským státem musí být v souladu s čl. 8 odst. 6 směrnice oznámeno Komisi.

V souvislosti s EHR pracovní skupina zřízená podle článku 29 poznamenává, že argumenty pro zavádění systémů EHR (srov. oddíl I tohoto dokumentu) mohou zakládat „významný veřejný zájem“. V některých členských státech je „právo na ochranu zdraví“ zakotveno v ústavě. Tím je zdůrazněna důležitost přikládaná všem vhodným prostředkům k zajištění „ochrany zdraví“. V takových právních prostředích by systém EHR nepochybně byl založen na „významném veřejném zájmu“, protože jde o nástroj, jehož základním účelem je zaručit přiměřenou lékařskou pomoc pro pacienty.

Ustanovení čl. 8 odst. 4 směrnice proto může sloužit jako právní základ systémů EHR za předpokladu, že jsou splněny všechny podmínky v něm uvedené. Zejména musejí být stanovena vhodná opatření na ochranu osobních údajů v systému EHR.

Těmito možnými ochrannými opatřeními a vhodným právním rámcem pro systémy EHR se pracovní skupina zabývá v následujícím oddílu.

# III. Úvahy o vhodném právním rámci pro systémy EHR

Pracovní skupina zřízená podle článku 29 dále podrobně pojednává o oblastech, kde se zvláštní ochranná opatření[16] v rámci systémů EHR jeví jako zvláště potřebná, mají-li být zaručena práva pacientů na ochranu údajů. Vzhledem k dopadu systémů EHR a zvláštní potřebě transparentnosti těchto systémů by tato ochranná opatření měla být pokud možno stanovena v samostatném komplexním právním rámci.

## 1. Dodržování práva na sebeurčení

I když systém EHR není zcela postaven na souhlasu jakožto právním základu (čl. 8 odst. 2), sebeurčení pacienta ohledně doby a způsobu použití jeho údajů by mělo hrát významnou úlohu důležitého ochranného opatření.[17]

**a)** Úloha „svolení“ v kontextu vhodných ochranných opatření je odlišná od „souhlasu“ podle čl. 8 odst. 2 směrnice, a toto svolení tedy nemusí splňovat všechny požadavky čl. 8 odst. 2: např. zatímco **souhlas jako právní základ** pro zpracování zdravotních údajů musí být vždy „výslovný“ podle čl. 8 odst. 2, **svolení jako ochranné opatření** nemusí mít nutně podobu rozhodnutí poskytnout údaje v systému předpokládaného nesouhlasu (opt-in), ale v závislosti na situaci může být možnost sebeurčení poskytnuta také ve formě práva odmítnout v systému předpokládaného souhlasu (opt-out).

**b)** Vzhledem k tomu, že různé druhy zdravotních informací mají různý potenciál působit škodu, jednotlivé kategorie použití by měly být odlišeny **různou měrou možnosti uplatnit sebeurčení**:

V právních předpisech, kterými se zavádí systém EHR, by mělo být stanoveno pravidlo, že vkládání údajů do EHR a přístup k těmto údajům by měly podléhat systému stupňovaných požadavků na souhlas (zejména při zpracování údajů, které mohou být zvláště škodlivé, např. údajů o psychiatrické léčbě, potratech apod.[18]) a možností vyslovit nesouhlas pro údaje narušující soukromí v menší míře.[19] Tím by bylo možné zaručit potřebnou míru ochrany na jedné straně a nezbytnou praktičnost a pružnost na straně druhé.

**c)** Pokud si to **pacient** přeje, měl by mít v zásadě vždy **možnost zabránit sdělení** svých lékařských údajů, které v průběhu léčby zadokumentoval určitý zdravotník, jiným zdravotníkům.

---

[16] V této části dokumentu nejsou opakovány obecné požadavky směrnice 95/46/ES pro zákonné zpracování osobních údajů, protože ty platí v každém případě. Tento dokument rozpracovává pouze dodatečné zvláštní požadavky na zpracování lékařských údajů v systémech EHR, které se jeví jako nezbytné pro vyvážení zvláštního rizikového scénáře pro soukromí, jenž je důsledkem systémů EHR.

[17] V některých jurisdikcích neexistuje pouze základní právo na ochranu údajů, ale také ústavní právo na optimální ochranu zdraví – v důsledku této povinnosti zajistit optimální léčbu některé členské státy stanovily, že zdravotníci musejí mít povinně přístup k údajům dostupným prostřednictvím systému EHR. To se zdá přijatelné za předpokladu, že je potřebné rovnováhy dosaženo posílením ostatních ochranných opatření, jako jsou podrobné předpisy týkající se mj. podmínek zákonného přístupu a – závažných – důsledků v případě zneužití přístupových práv.

[18] Je možné využít zvláštních funkcí, jako jsou elektronické „zapečetěné obálky“, které nelze otevřít bez spolupráce subjektu údajů.

[19] Řešení založená na předpokládaném souhlasu však mohou účinně fungovat jako „vhodné ochranné opatření“ pouze v případě, že budou pacienti dostávat dostatečné informace.

Zvážit je třeba také otázku, jak by se mělo postupovat v případech, kdy je odepřen přístup k informacím v EHR. Jde o to, zda by odepření mělo být skryto tak, aby bylo nezjistitelné, nebo zda by měla být (možná jen v některých případech) zobrazována zpráva sdělující, že existují další informace, které jsou však dostupné jen při splnění zvláštních požadavků.

**d)** Platí-li předpoklad, že k účasti v systému EHR nemůže být nikdo nucen, měla by být v právních předpisech zavádějících tento systém upravena otázka **možného úplného vystoupení ze systému EHR**. Nutné je nastavit pravidla ohledně toho, zda by vystoupení znamenalo povinnost údaje v systému EHR zcela vymazat, nebo jen znemožnit k nim další přístup; tuto volbu by bylo rovněž možné ponechat na subjektech údajů.

### 2. Identifikace a autentizace pacientů a zdravotníků

**a) Spolehlivá identifikace[20] pacientů** v systémech EHR má zásadní význam. Pokud by se vinou nesprávné identifikace pacienta použily zdravotní údaje o jiné osobě, mělo by to v mnoha případech škodlivé následky.

K náležité elektronické identifikaci pacientů a také k jejich **autentizaci[21] za účelem přístupu k vlastním údajům v EHR** by mohly významně přispět zdravotní průkazy na bázi čipových karet.

**b)** Zvláštní citlivost zdravotních údajů navíc vyžaduje, aby k nim byl znemožněn přístup neoprávněným osobám. Spolehlivá kontrola přístupu závisí na spolehlivé identifikaci[22] a autentizaci. Proto je nezbytné **uživatele jedinečně identifikovat a jejich identitu náležitě ověřovat autentizací**.[23]

Jelikož jednou z hlavních výhod systémů EHR je jejich přístupnost prostřednictvím elektronické komunikace bez ohledu na čas a místo, bude nutné zavést rutinní postupy pro spolehlivou elektronickou identifikaci a autentizaci. Přinejmenším v dlouhodobějším horizontu by se mělo počítat s autentizací pomocí elektronických podpisů – které oprávnění uživatelé dostávají spolu s řádnou úřední identifikací např. na zvláštní čipové kartě – aby se předešlo známým rizikům spojeným s autentizací pomocí hesla.

Pro zdravotníky bude třeba vyvinout systém identifikace a autentizace, který nebude ověřovat pouze totožnost, ale také **roli, ve které zdravotník s elektronickým systémem pracuje**, tj. například jako psychiatr nebo jako zdravotní sestra.

### 3. Oprávnění pro přístup k EHR pro čtení a zápis

**a)** Obecná ochranná opatření pro přístup:

Údaje v systémech EHR jsou důvěrnými lékařskými záznamy. **Základní zásadou** týkající se přístupu k EHR proto musí být, že – kromě samotného pacienta – **mohou mít přístup pouze zdravotníci** či oprávnění pracovníci zdravotnických zařízení, **kteří se v současnosti podílejí**

---

[20] „Identifikací“ se rozumí popis osoby pomocí identifikátorů, jako jsou jméno, datum narození, adresa atd.; v daném kontextu musí být tento popis úředně potvrzen prostřednictvím rodného listu, cestovního pasu, zdravotní karty apod.

[21] „Autentizací“ se rozumí důkaz o tom, že osoba, která tvrdí, že má určitou totožnost, skutečně je osobou s touto totožností. To se obvykle provádí předložením úředního dokladu totožnosti s fotografií (např. cestovního pasu) a v elektronickém světě pak použitím elektronického podpisu.

[22] „Spolehlivá identifikace“ by neměla využívat identifikačních čísel, která se bez zvláštních ochranných opatření používají v jiných souvislostech, protože je třeba zabránit snadné propojitelnosti databází (viz čl. 8 odst. 7 směrnice).

[23] První pokusy s EHR, které se chystají ve Francii, jsou založeny na vytvoření zvláštního identifikátoru; zatím není jisté, zda tento systém zůstane zachován v konečné podobě EHR.

**na léčbě** pacienta. Mezi pacientem a zdravotníkem, který požaduje přístup k jeho EHR, musí existovat vztah založený na skutečné, v přítomnosti probíhající léčbě.

Dále se zdá, že je nutné upravit, které kategorie a úrovně zdravotníků a zdravotnických zařízení budou mít přístup k údajům v EHR (ambulantní lékaři, nemocniční lékaři, lékárníci, zdravotní sestry, chiropraktici? psychologové? rodinní terapeuti? atd.).

Ochranu údajů by bylo možné dále posílit zavedením **modulárních přístupových práv**, tedy vytvořením kategorií lékařských údajů v systému EHR s tím, že přístup k určitým kategoriím údajů budou mít jen určité kategorie zdravotníků či zdravotnických zařízení.[24] Možné výhody modulární struktury EHR jsou podrobněji popsány v bodu 6.

**b)** Zvláštní ochranná opatření pro přístup – s účastí pacienta:

Pokud je to možné a proveditelné, tj. je-li pacient přítomen a schopen se rozhodovat, **měl by pacient dostat možnost zabránit přístupu ke svým údajům v EHR, jestliže si to přeje.** K tomu je třeba, aby byl předem informován o tom, kdo, kdy a proč bude požadovat přístup k jeho údajům, a o možných důsledcích nepovolení přístupu. Musejí se též vypracovat postupy, které zamezí nepatřičnému psychickému nátlaku na pacienta, aby souhlasil s požadavky na přístup ke svým údajům.

Jestliže se vyžaduje **důkaz o souhlasu pacienta** s přístupem k údajům v jeho EHR, je nezbytné mít pro tento důkaz spolehlivé nástroje, jako je elektronická kontrola průkazu pacienta nebo – jsou-li takové nástroje již všeobecně dostupné – elektronický podpis pacienta apod. Předložení takového důkazu musí být elektronicky zdokumentováno pro účely možného auditu.

Měla by být vypracována pravidla stanovující, zda by měl mít subjekt údajů možnost požadovat, aby do jeho záznamů nebyly vloženy určité údaje. Možným způsobem řešení této otázky by mohly být také „zapečetěné obálky“, které nelze otevřít bez výslovného souhlasu subjektu údajů.

**c)** Přístup subjektů údajů k údajům v jejich EHR

Otázka, zda by měli pacienti získat **přímý (elektronický) přístup pro čtení** ke svým EHR, závisí na tom, zda je to v rámci lékařské péče proveditelné. Právo na přístup k údajům stanovené v souvislosti s ochranou údajů, např. v článku 12 směrnice 95/46/ES, nemusí vždy nutně znamenat *přímý* přístup. Přímý přístup by nicméně mohl podstatně přispět k důvěře v systém EHR. Z hlediska ochrany údajů by nezbytnou podmínkou přímého přístupu byla bezpečná elektronická identifikace a autentizace, která v přístupu zabrání neoprávněným osobám.

V předpisech o systému EHR by měla být vyřešena také otázka, zda by měli **údaje do svých EHR vkládat** sami **pacienti**, nebo zda by je za ně měli vkládat zdravotníci. Možné problémy s odpovědností za přesnost by s největší pravděpodobností odstranila dostatečná transparentnost rutinních postupů protokolování, zajišťující známost autorů jednotlivých položek v EHR. Zvážit lze rovněž možnost omezit přístup pro zápis pouze na zvláštní modul EHR.

V této souvislosti je nutné vzít v potaz schopnosti a zvláštní potřeby chronicky nemocných a starších občanů, jakož i zdravotně postižených.

[24] Například první úroveň přístupu k údajům o psychiatrické léčbě může být omezena na psychiatry; nebo může být vytvořen zvláštní lékový modul přístupný i lékárníkům, kteří nemají přístup k ostatním částem systému EHR.

## 4. Využití EHR pro jiné účely

Přijetí systémů EHR ze strany občanů bude záviset na jejich **důvěře v důvěrnost systému.**

Odůvodnění oprávněného přístupu k údajům v EHR by mělo odpovídat hlavnímu účelu každého systému EHR, kterým je úspěšnost léčby daná lepší informovaností. **Pracovní skupina zastává stanovisko, že přístup k lékařským údajům v EHR pro jiné účely než ty, které jsou uvedeny v čl. 8 odst. 3, by měl být v zásadě zakázán.**

To například vylučuje poskytnutí přístupu k EHR lékařům, kteří jednají jako znalci pro třetí strany např. pro soukromé pojišťovny, v rámci soudních sporů, pro účely přiznání podpory na odchod do důchodu, pro zaměstnavatele subjektu údajů apod. Kromě toho by měly být navrženy disciplinární předpisy pro zdravotníky, které by účinně působily proti porušování těchto pravidel.

Měla by být přijata zvláštní opatření bránící tomu, aby byli pacienti nezákonně přesvědčováni ke sdělení údajů ze svých EHR, např. na žádost možného budoucího zaměstnavatele nebo soukromé pojišťovny. Zásadní význam má vzdělávání pacientů, jež by zajistilo, že nebudou vyhovovat žádostem o údaje, které by podle právních předpisů o ochraně údajů byly nezákonné. Rovněž může být nutné použít technické prostředky, např. zvláštní požadavky pro pořizování úplných výtisků EHR apod.

Zpracování údajů v EHR pro účely **vědeckého lékařského výzkumu a veřejné statistiky** může být povoleno ve formě výjimky z výše uvedeného pravidla za předpokladu, že každá taková výjimka je v souladu se směrnicí (srov. čl. 8 odst. 4 a odpovídající 34. bod odůvodnění) – tj. je stanovena zákonem pro předem určené konkrétní účely a za zvláštních podmínek, které zaručují přiměřenost („vhodná a zvláštní ochranná opatření“) s cílem chránit základní práva a soukromí jednotlivců.

Kromě toho by se údaje ze systémů EHR měly pro jiné účely (např. statistika nebo hodnocení kvality) používat pouze v anonymizované podobě, nebo alespoň s bezpečnou pseudonymizací[25], kdykoli je to možné a proveditelné.

## 5. Organizační struktura systému EHR

V kontextu diskuzí o různých možnostech organizace uchovávání údajů v systému EHR jsou obvykle zmiňovány tyto hlavní alternativy:

- EHR jako systém poskytující přístup k lékařským záznamům uchovávaným zdravotníky, kteří mají povinnost vést záznamy o léčení svých pacientů – to se často označuje jako **„decentralizované úložiště“**;
- EHR jako jednotný systém uchovávání údajů, do kterého lékaři musejí předávat svou dokumentaci – toto se často označuje jako **„centralizované úložiště“**;
- třetí možností by mohlo být učinit subjekt údajů „pánem“ jeho vlastních lékařských záznamů tak, že mu bude nabídnuto **úložiště lékařských údajů o pacientech v podobě zvláštní elektronické služby pod kontrolou pacienta**, případně i včetně pravomoci rozhodovat o tom, které údaje budou do EHR vkládány.[26]

[25] Pseudonymizací se rozumí převod identifikátorů (jako jsou jména, data narození atd.) na jiná označení pokud možno pomocí šifrování, aby příjemce informací nemohl určit totožnost subjektu údajů.

[26] Tomu odpovídá v současnosti zaváděný francouzský model. Poskytovatelé služby se označují jako hostitelé („hébergeurs“) a jejich postavení je upraveno vyhláškou, ke které předem zaujal stanovisko úřad CNIL. Jedná se o složitý předpis, který se zabývá především otázkami akreditace těchto poskytovatelů a bezpečnosti systému.

**a)** Třetí alternativa **(úložiště pod kontrolou subjektu údajů)** se sice jeví jako nejlepší řešení z hlediska sebeurčení, ale pokud o tom, které údaje se mají v EHR uchovávat, rozhoduje pouze subjekt údajů, a do systémů není zabudován žádný odborný medicínský korektiv, může nastat problém s kvalitou dokumentace co do přesnosti a úplnosti.

**b)** V případě modelu **„decentralizovaného úložiště"**, který se stává „systémem" teprve vytvořením příslušných vyhledávacích cest, by zůstala zachována stávající struktura dokumentace se zdravotními údaji u různých poskytovatelů zdravotní péče. Míra, do jaké lze údaje o pacientech ukládat do takovéhoto systému, závisí na kvalitě systému vyhledávání.

V tomto organizačním modelu **zdravotník či zdravotnické zařízení zůstává „správcem"** dokumentace (přesněji té části EHR, kterou sám vytvořil). Vzhledem ke složité systémové architektuře tohoto modelu by mohlo být nezbytné jmenovat jeden ústřední orgán s odpovědností za řízení a sledování celého systému a za zajištění slučitelnosti jeho provozu s ochranou údajů. Mohlo by být rovněž užitečné, kdyby se subjekty údajů mohly se svými problémy v oblasti ochrany údajů obracet na ústřední orgán a nemusely hledat mezi mnoha správci.

**c)** Předpokládá se, že hlavní výhodou systému takzvaného **„centralizovaného" úložiště** by bylo lepší technické zabezpečení a vyšší dostupnost (24hodinový přístup), což nelze tak snadno zaručit, pokud jde systém EHR nad rámec nemocnic. Celý systém by měl jediného správce nezávislého na zdravotnících a zdravotnických zařízeních, kteří svou dokumentaci (po částech nebo jako celek) zaslali do centrálního systému.

Z hlediska ochrany údajů by se proti tomuto druhu systémů dalo namítat s ohledem na větší potenciál ke zneužití centralizovaného úložiště údajů. Bylo by ovšem možné naplánovat zvláštní opatření a bezpečnostní prvky (např. šifrované úložiště), které by bezpečnostní rizika spojená s centrálně uchovávanými údaji alespoň do značné míry vyvážily. Odpovědnost za důvěrnost systému je zde nicméně odebrána lékařům, což může ovlivnit stupeň důvěry pacientů v takový systém.

Míra, v jaké by pacient mohl ovlivňovat obsah svého EHR a sdělování v něm obsažených údajů, by v obou případech – u decentralizovaného i centralizovaného úložiště – závisela na zvláštní koncepci systému (viz bod 3 písm. b)).

## 6. Kategorie údajů uložených v EHR a způsoby jejich prezentace

Základní idea „systému EHR" spočívá v tom, že se o určité osobě shromáždí všechny zdravotní údaje, o nichž se předpokládá, že mají význam pro její dlouhodobý zdravotní stav, aby byly v případě budoucí léčby k dispozici komplexní a podstatné informace, a pacienti tak měli větší naději na úspěšnou léčbu.

Pracovní skupina soudí, že z toho mohou vyplývat tyto hlavní problémy:

**a) „Úplnost" zdravotní dokumentace** není prakticky dosažitelná a ani žádoucí: **do EHR by se měly vkládat pouze *podstatné* informace.** Jednou z nejobtížnějších otázek při budování systému EHR proto bude rozhodnutí o tom, které kategorie lékařských údajů by se měly v EHR shromažďovat a jak dlouho by se měly uchovávat.[27] Tato otázka sice musí být zodpovězena především odborníky z řad lékařů, ale má také rozměr ochrany údajů. Podle zásad podstatnosti a přiměřenosti sběru údajů musí být každý soubor údajů omezen jen na údaje, které jsou podstatné a nepřesahující míru s ohledem na stanovený účel zpracování (čl. 6 odst. 1 písm. c) směrnice). Legitimita systémů EHR bude tedy záviset také na nalezení

[27] Některé kategorie údajů jsou důležité po celý život pacienta (např. o alergiích), ale jiné mají velký význam jen krátkou dobu (např. o neslučitelnosti některých druhů léčby).

vhodného řešení, pokud jde o volbu „správných“ kategorií údajů a „správné“ délky doby uchovávání informací v EHR.

**b) Pokud jde o prezentaci údajů v EHR,** z toho, že je možné rozlišovat mezi různými kategoriemi zdravotních údajů, které vyžadují zcela různé úrovně důvěrnosti, lze vyvodit, že může být obecně užitečné vytvořit v rámci systému EHR různé **datové moduly** s různými podmínkami přístupu: „očkovací datový modul“ by měl být kdykoli přístupný subjektu údajů a přístup k němu by mohl mít také poměrně široký okruh pracovníků ve zdravotnictví; „lékový datový modul“ by mohl v případě souhlasu pacienta zahrnovat zvláštní přístup pro lékárníky[28]; k „akutnímu datovému modulu“ by mohl existovat přístup pomocí zvláštních technických prostředků atd. Smysl by zřejmě mělo také vytvoření speciální modulů pro „systémy kontrol“ (recall systems); tyto moduly by sloužily k automatickému upomínání pacienta na nezbytná očkování, zdravotní prohlídky a kontroly v rekonvalescenci.

Rovněž zvláště citlivé údaje by bylo možné lépe chránit jejich uchováváním v samostatných modulech s obzvláště přísnými podmínkami přístupu. To by se týkalo například údajů o psychiatrické léčbě, HIV nebo potratech. Místo toho, aby byly z EHR vynechány – což by mohlo ohrozit úspěšnost budoucí léčby – měla by se do systému zabudovat zvláštní omezení pro přístup k těmto údajům, včetně výslovného souhlasu pacienta a speciálních technických překážek (např. ve formě „zapečetěných obálek“).

**c)** Při navrhování struktury záznamů EHR by se měly vzít v úvahu také opakující se **zvláštní požadavky na informace**. Příkladem může být situace, kdy vnitrostátní právní předpisy dávají soukromým pojišťovnám právo získávat některé (omezené) informace týkající se zdravotních záznamů, je-li to nutné v souvislosti s plněním jejich smluvních závazků vůči pojištěným pacientům. Poskytnutí přístupu k EHR pacienta soukromým pojišťovnám se jeví jako nepřijatelné. Řešením proto může být vytvoření zvláštního standardizovaného „souboru dokumentace“, který v případě potřeby uspokojí oprávněný zájem pojistitele na získání informací a může být (elektronicky) přenášen do příslušné soukromé pojišťovny, pokud to pacient povolí.

## 7. Mezinárodní předávání lékařských záznamů

Elektronická dostupnost lékařských údajů v systémech EHR může značně rozšířit diagnostické či léčebné možnosti prostřednictvím využití lékařských znalostí, které existují pouze v zahraničních zdravotnických zařízeních. Dodatečná konzultace zahraničních odborníků pro diagnostické účely obvykle nevyžaduje odhalení totožnosti pacienta. Proto by takové údaje měly být do zemí mimo Evropskou unii / Evropský hospodářský prostor předávány pokud možno pouze **v anonymizované či alespoň pseudonymizované podobě**. Tak se lze také vyhnout nutnosti získávat povolení k předání osobních údajů v případech, kdy není k dispozici výslovný souhlas subjektu údajů k tomuto předání[29], protože subjekt údajů není pro příjemce identifikovatelný.

S ohledem na zvýšené riziko hrozící osobním údajům v systému EHR v prostředích bez odpovídající ochrany by pracovní skupina zřízená podle článku 29 chtěla zdůraznit, že jakékoli zpracovávání – a zvláště uchovávání – údajů v EHR by mělo probíhat v jurisdikcích, kde se používá směrnice EU o ochraně údajů nebo jiný dostatečný právní rámec ochrany údajů.

[28] Existence lékového modulu v EHR by měla dvojí výhodu, protože by také umožňovala ošetřujícímu lékaři dozvědět se o všech lécích, které pacient užívá.

[29] V situacích, kdy pacient není fyzicky schopen reagovat na žádost o souhlas (např. je v kómatu), mohou být jeho lékařské údaje podle čl. 26 odst. 1 písm. e) směrnice přesto předány do země nezaručují odpovídající ochranu údajů, jestliže to vyžadují jeho životně důležité zájmy.

Specifickým problémem jsou přeshraniční toky dat během klinických studií – studijní skupina, která pracuje přímo s pacienty, může v některých případech potřebovat přístup k údajům v EHR v jejich původní neanonymní podobě. U každého předání údajů, které jsou výsledkem klinických studií, zadavatelům těchto studií nebo jiným institucím, které se na nich zákonně podílejí, je ovšem nutné jako minimální podmínku požadovat bezpečnou pseudonymizaci, zvláště pokud má zadavatel sídlo v zemi bez odpovídající ochrany údajů.

V této souvislosti je vždy třeba věnovat zvláštní pozornost otázkám zabezpečení údajů, aby se předešlo rizikům jejich neoprávněného sdělování v prostředích, která z hlediska ochrany údajů nemusejí být bezpečná.

## 8. Zabezpečení údajů

Přijatelnost systému zpracování údajů s mimořádným rizikovým potenciálem závisí na přiměřeně vysoké úrovni zabezpečení údajů v rámci celého provozu takového systému. Má-li být systém přijatelný z pohledu ochrany údajů, **přístupu neoprávněných osob se musí bránit tak, aby byl prakticky nemožný**. Dostupnost systému pro oprávněné odborníky v situacích, kdy opravdu potřebují informace, musí být naopak prakticky neomezená, pokud má systém přinést slibované výhody pro léčbu pacientů.

Právní rámec pro budování systému EHR bude muset obsahovat povinnost zavést řadu opatření technické a organizační povahy vhodně zamezujících ztrátě nebo neoprávněným úpravám a zpracování údajů a neoprávněnému přístupu k údajům v tomto systému. Integrita systému musí být zaručena použitím poznatků a nástrojů odpovídajících současnému stavu vývoje informatiky a informačních technologií.

**Technologie zlepšující ochranu soukromí** (**privacy enhancing technologies, PET**)[30] by se měly na podporu ochrany osobních údajů využívat co nejvíce. Údaje by měly být zašifrované nejen při předávání, ale také při jejich uchovávání v systémech EHR. Všechna bezpečnostní opatření by měla být navržena uživatelsky přívětivým způsobem, který pomůže rozšířit jejich využívání. Nezbytné náklady je třeba považovat za investici do slučitelnosti systémů EHR se základními právy, která bude jedním z nejdůležitějších předpokladů úspěšnosti těchto systémů.

Bez ohledu na to, že prvky zabezpečení údajů obsahuje již řada z ochranných opatření, kterými se zabýváme výše, měl by právní rámec týkající se bezpečnostních opatření stanovit zvláště nezbytnost těchto podmínek:

- vývoj spolehlivého a účinného systému elektronické identifikace a autentizace, jakož i nepřetržitě aktualizovaných rejstříků pro kontrolu náležitého oprávnění osob, které mají nebo požadují přístup k systému EHR;
- důkladné protokolování a dokumentování všech kroků v rámci zpracování, které v systému proběhly, především žádostí o přístup pro čtení nebo zápis, spolu s pravidelnými vnitřními kontrolami správnosti oprávnění a návaznými opatřeními;
- účinné mechanismy pro zálohování a zotavení systému, které zabezpečují jeho obsah;
- předcházení neoprávněnému přístupu k údajům v EHR a jejich neoprávněným úpravám v průběhu jejich předávání nebo ukládání záložních kopií, např. pomocí šifrovacích algoritmů;
- jasné a zadokumentované pokyny pro všechny oprávněné pracovníky o tom, jak systémy EHR správně používat a jak se vyhnout bezpečnostním rizikům a porušením bezpečnosti;

[30] Co se týče technologií PET, viz bod 4.3 zprávy Komise „První zpráva o provádění směrnice o ochraně údajů (95/46/ES)“, KOM (2003) 265 v konečném znění.

- jasné rozdělení úkolů a pravomocí jednotlivých kategorií osob, které jsou za systém odpovědné nebo se přinejmenším podílejí na jeho chodu, s cílem vymezit odpovědnost za nedostatky;
- pravidelné interní a externí audity ochrany údajů.

## 9. Transparentnost

Zdá se zřejmé, že EHR má velký potenciál, pokud jde o léčbu, ale v zásadě také pokud jde o možnost zneužití prostřednictvím neoprávněného přístupu. Veřejné mínění i jednotlivci proto budou požadovat zvláštní **transparentnost obsahu a fungování systému EHR**, aby mu mohli důvěřovat. Správce (správci) systému musí podávat **oznámení** orgánům dozoru nad ochranou údajů a současně poskytovat zvláštní **informace, které jsou snadno dostupné a srozumitelné**. K zajištění nezbytné transparentnosti celostátně fungujícího systému (systémů) EHR může napomoci využití internetu jako ideálního nástroje pro distribuci informací.

Cenným příspěvkem k transparentnosti, a tedy i k důvěře v systém mohou být také bezplatné, snadno použitelné, ale zároveň bezpečné přístupové body pro subjekty údajů, které jim umožní kontrolovat obsah jejich záznamů EHR a sdělování údajů z těchto záznamů.

## 10. Otázky odpovědnosti

U každého systému EHR musí být také zaručeno, že **případná narušení soukromí** způsobená uchováváním a předáváním lékařských údajů v tomto systému jsou přiměřeně **vyvážena zákonnou odpovědností za škody** vzniklé např. nesprávným nebo neoprávněným použitím údajů v EHR.

V rámci analýzy možných problémů systémů EHR z hlediska ochrany údajů se lze otázek zákonné odpovědnosti za nesprávné používání těchto systémů pouze dotknout. Podle názoru pracovní skupiny by každý členský stát, který chce zavést systém EHR, měl předem pečlivě provést důkladné odborné občanskoprávní a lékařskoprávní studie a posouzení dopadů za účelem vyjasnění nových otázek zákonné odpovědnosti, které v této souvislosti zřejmě vyvstanou, např. pokud jde o přesnost a úplnost údajů vkládaných do EHR, o míru, do jaké je zdravotník ošetřující pacienta povinen EHR prostudovat, či o důsledky podle právních předpisů o zákonné odpovědnosti, které bude mít nedostupnost systému z technických důvodů apod.

## 11. Kontrolní mechanismy pro zpracování údajů v EHR

Vzhledem ke **zvláštnímu rizikovému scénáři**, který je důsledkem budování systémů EHR, jsou nezbytné **účinné kontrolní mechanismy** pro hodnocení zavedených ochranných opatření. Složitost informací uložených v EHR a velký počet možných uživatelů si mohou vyžádat nové postupy v oblasti přístupových práv subjektů údajů.

**a)** Mělo by být zavedeno **zvláštní rozhodčí řízení pro spory** týkající se správného používání údajů v systémech EHR, přičemž subjekty údajů by měly mít možnost tohoto řízení snadno a bezplatně využít. Jelikož k posouzení tvrzení o nesprávnosti nebo zbytečném zpracování informací v systémech EHR budou obvykle nezbytné specializované lékařské znalosti, orgány dozoru nad ochranou údajů nemusejí být pro vyřizování tohoto druhu stížností nejvhodnější, alespoň ne v prvním stupni. Tam, kde je taková funkce již zřízena, by tímto úkolem mohli být pověřeni veřejní „ochránci práv pacientů“.

**b)** V systému EHR musí být zajištěno, aby subjekt údajů mohl svá práva na přístup vykonávat bez nepřiměřených obtíží. Poskytnutí přístupu je v zásadě povinností správce údajů. **Systémy EHR** však **jsou systémy informačních „poolů"** s mnoha různými správci údajů. V případě takovýchto systémů, na nichž se podílí velký počet správců údajů, **musí být odpovědností vůči subjektům údajů za řádné vyřizování žádostí o přístup pověřena jedna zvláštní instituce**. S ohledem na předvídatelnou složitost plně rozvinutých systémů EHR a nutnost budovat u pacientů důvěru v tyto systémy se jeví jako zásadně důležité, aby pacienti, jejichž údaje jsou v systému EHR zpracovávány, věděli, jak mohou kontaktovat odpovědného partnera, s nímž mohou projednat případné nedostatky systému. Zvláštní ustanovení v tomto smyslu budou muset obsahovat všechny předpisy o systémech EHR.

**c)** V zájmu budování důvěry by bylo možné zavést **zvláštní rutinní postup pro informování subjektu údajů o tom, kdo a kdy získal přístup k údajům v jeho EHR.** Bude-li subjektům údajů pravidelně zasílán protokol s výčtem osob a institucí, které nahlížely do jejich dokumentace, budou pacienti ujištěni, že mají přehled o tom, co se s jejich údaji v systému EHR děje.

**d)** Musejí se provádět **pravidelné interní a externí audity přístupových protokolů z hlediska ochrany údajů**. Dodatečným účinným prostředkem pro kontrolu zákonnosti využívání údajů v EHR by byla již zmíněná výroční zpráva o přístupech zasílaná subjektům údajů. Pravděpodobnost správného využívání údajů v systémech EHR by nepochybně zvýšili úředníci pro ochranu údajů, kteří by působili v nemocnicích zapojených do těchto systémů.

# IV. ZÁVĚR

Každý jednotlivec, a tedy i každý pacient má právo na soukromí, a proto může důvodně očekávat, že všichni zdravotníci budou přísně zachovávat důvěrnost a ochranu jeho osobních informací. Toto očekávání je oprávněné také v případě systémů elektronických zdravotních záznamů (EHR).

Pracovní skupina zřízená podle článku 29 sepsala tento pracovní dokument s cílem poskytnout vodítko k výkladu právního rámce ochrany údajů použitelného pro systémy elektronických zdravotních záznamů (EHR) a stanovit některé obecné zásady. Dalším cílem pracovního dokumentu je popsat předběžné podmínky vybudování celostátního systému EHR z hlediska ochrany údajů, jakož i příslušná ochranná opatření, a přispět k jednotnému používání vnitrostátních opatření přijatých podle směrnice 95/46/ES.

Pracovní skupina zdůrazňuje, že zřizování a provoz systémů EHR musí probíhat plně v souladu se zásadami ochrany osobních údajů stanovenými ve směrnici 95/46/ES. Skupina soudí, že dodržování těchto zásad pomáhá všem osobám a institucím, které se podílejí na zajišťování řádného fungování těchto systémů. Kromě toho pracovní skupina podtrhuje, že je nutné, aby systémy EHR byly zakládány a provozovány uvnitř solidního právního rámce ochranných opatření určených k ochraně osobních údajů, a to bez ohledu na právní základ těchto systémů.

Pracovní skupina zřízená podle článku 29 vyzývá lékařský stav, všechny ostatní zdravotníky a osoby a instituce, které se podílejí na poskytování zdravotnických služeb, jakož i širokou veřejnost, aby k tomuto pracovnímu dokumentu podávali připomínky.[31]

---

[31] Připomínky k tomuto pracovnímu dokumentu je třeba zasílat na adresu: Secretariat of the Article 29 Working Party

European Commission, Directorate-General Justice, Freedom and Security

Vzhledem k pokračujícímu vývoji v této oblasti se může ukázat jako nezbytné, aby pracovní skupina vykonala další práce, vydala další poznámky nebo podnikla návazné kroky.

V Bruselu dne 15. února 2007

*Za pracovní skupinu*
*Peter SCHAAR*
*předseda*

Unit C.5 – Protection of personal data

Office: LX 46 1/43

B - 1049 Brussels

E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu ; Fax: +32-2-299 80 94

Všechny připomínky od veřejného i soukromého sektoru budou zveřejněny na internetových stránkách pracovní skupiny zřízené podle článku 29, pokud respondent výslovně neuvede, že si přeje zachovat důvěrnost určitých informací.

# Věstník Úřadu pro ochranu osobních údajů

**Vydavatel:** Úřad pro ochranu osobních údajů
**Adresa redakce:** Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7
**Redakce:** Miluše Nejedlá, tel.: 234 665 232, fax: 234 665 505
e-mail: posta@uoou.cz
internetová adresa: www.uoou.cz

**Administrace:** Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, www.sevt.cz, e-mail: sevt@sevt.cz. – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 450 Kč – Vychází podle potřeby – **Tiskne**: sprint servis, Lovosická 31, Praha 9.

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

**ISSN 1213-3442**