# VĚSTNÍK
## ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
## 2011

**Částka 60** | **12. prosince 2011** | **Cena 190,- Kč**


## OBSAH

# ÚVOD

Šedesátá částka Věstníku Úřadu pro ochranu osobních údajů je poslední publikovanou částkou v letošním roce. Obsahuje přehled zrušených registrací v období od 26. 9. 2011 do 1. 12. 2011.

Rubriku Stanoviska Úřadu naplňuje stanovisko č. 3/2011 nazvané „Ochrana osobních údajů podnikajících fyzických osob“. Stanovisko řeší otázku ochrany osobních údajů osob samostatně výdělečně činných (OSVČ). Soukromý i profesní život uvedených osob je úzce svázán a u některých informací lze jen obtížně konstatovat, ke které části jejich života se konkrétní informace spíše vztahují. Úřad vydává toto stanovisko proto, aby vyjádřil svůj obecný právní názor k dané problematice a přispěl k odstranění existujících nejasností při aplikaci příslušných právních předpisů. Ve stanovisku Úřad konstatuje, že údaje týkající se určitých nebo určitelných osob, živnostníků či příslušníků svobodných povolání, jsou osobními údaji ve smyslu zákona o ochraně osobních údajů.

Rubrika Sdělení Úřadu přináší dokument Pracovní skupiny pro ochranu údajů podle článku 29 směrnice 95/46/ES (WP29), kterým je Stanovisko č. 6/2010 o úrovni ochrany osobních údajů v Uruguayské východní republice.

# Přehled zrušených registrací

| Číslo registrace | Subjekt | Datum zrušení |
|---|---|---|
| 00001004/004 | MĚSTO PROSTĚJOV | 18.10.2011 |
| 00032346/004 | ARCHIV BEZPEČNOSTNÍCH SLOŽEK | 4.11.2011 |
| 00035316/001 | NAKLADATELSTVÍ C.H. BECK, O.S. | 4.11.2011 |
| 00037494/006 | AUTOCENTRUM JAN ŠMUCLER S.R.O. | 19.10.2011 |
| 00040174/001 | PETR CHRISTOV | 30.11.2011 |

# II. STANOVISKA ÚŘADU

## Stanovisko č. 1/2011

srpen 2011

### Zveřejňování listin s osobními údaji prostřednictvím internetu

#### Úvod

S rozvojem elektronizace veřejné správy se setkává Úřad pro ochranu osobních údajů (dále jen „Úřad“) při své činnosti stále častěji se situacemi, kdy v důsledku realizace zákonných povinností jednotlivých orgánů veřejné správy, které se vztahují ke zveřejňování různého typu informací též způsobem umožňujícím dálkový přístup, dochází k porušování povinností při zpracování osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“). Nejčastěji jde o specifický a právními normami stanovený způsob doručování písemností sloužící k zachování práv účastníků řízení, případně pak obecně o umožnění veřejnosti jednoduchým způsobem získat informace o činnosti (úkonu) konkrétního orgánu veřejné správy.

Nikoli výjimečně přitom dochází k situaci, kdy listiny zveřejněné prostřednictvím elektronické úřední desky (např. podle zákona č. 500/2004 Sb., správní řád) obsahují osobní údaje, které zůstávají za použití internetových vyhledávačů přístupné i určitou dobu po tom, co jsou z elektronické desky po uplynutí zákonem stanovené doby listiny technicky odstraněny. K tomu, aby byla i v prostředí webových stránek dodržena pravidla pro ochranu osobních údajů, je třeba použít některého z běžně dostupných nástrojů[1], který zamezí indexování[2] příslušných webových stránek respektive jejich ukládání do cache[3] internetového vyhledávače.

Toto stanovisko uvádí možný přístup k úpravě webových stránek či webového portálu do stavu souladného s ochranou osobních údajů, přičemž se tato problematika týká zejména institucí, které budují komplexní nástroje pro výkon elektronizované veřejné správy a dostupnost jejich služeb pro občany na internetu. Jednou z podmínek zadávání a tvorby těchto systémů musí být i dále uvedené požadavky na standardizované zpracování osobních údajů.[4]

Indexování, ukládání do cache a archivy webových stránek

V případě indexování stránek je softwarový nástroj (program – robot[5]), který indexaci a cachování stránek provádí, schopen po určité době odstranit záznam o stránce či souboru (včetně otisku z cache), které již na předchozím umístění nenalezne. Webové dokumenty tak zůstávají dohledatelné a přístupné prostřednictvím vyhledávače ještě po dobu, než robot vyhledávače provede jejich reindexaci. Při zobrazení z cache jsou přitom přístupné i stránky či soubory, které již byly odstraněny, pokud je jejich otisk uložen na serveru vyhledávače.

V případě webových archivů, které uchovávají webové stránky trvale, lze nadbytečnému ukládání stránek obsahujících osobní údaje předejít k ochraně osobních údajů ohleduplným nastavením práv pro přístup výše zmiňovaných robotů (viz následující odstavec).

Soulad s požadavky zákona o ochraně osobních údajů

Jsou-li osobní údaje po uplynutí zákonem stanovené doby, po kterou měly být listiny způsobem umožňujícím dálkový přístup zveřejněny, dále přístupné v podstatě neomezenému okruhu osob, je nutné tento stav považovat za porušení povinnosti stanovené v § 13 odst. 1 zákona o ochraně osobních údajů, tedy povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo naho-

[1] Nástroje či návody k zákazu indexování lze najít prostřednictvím obvyklých internetových vyhledávačů např. po zadání klíčových slov „zákaz indexování“ nebo „zákaz přístupu vyhledávačů“.

[2] Indexování probíhá tak, že vyhledávač prochází stránky skrze náhodné odkazy a každou novou nebo aktualizovanou stránku odešle do své databáze, a pokračuje dalším (i náhodným) odkazem ze stránky. (ZICHA O., *Princip vyhledávačů.* http://www.biolib.cz/cz/help/id154/ 27.5.2011)

[3] Označení pro vyrovnávací paměť používanou ve výpočetní technice. Internetové vyhledávače často ukládají indexované webové stránky do své cache a mohou ji i zpřístupnit. (Cache. http://cs.wikipedia.org/wiki/Cache 1.6.2011) Cachování tedy znamená ukládání webových stránek do vyrovnávací paměti internetového vyhledávače.

[4] Lze připomenout, že dle § 5b zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.

[5] Internetový robot je počítačový program, který pro svého majitele opakovaně vykonává nějakou rutinní činnost na internetu – obvykle sbírá data, odesílá a zpracovává požadavky na služby vzdálených serverů. Častým příkladem robota jsou vyhledávací roboti internetových vyhledávačů. Tento typ robotů prochází jednotlivé webové stránky, hledá na nich odkazy na nové stránky, indexuje obsah zpracovávaných stránek a umožňuje jejich následné prohledávání. Podobným příkladem může být robot na kontrolu odkazů. Prochází zadanou množinu stránek (opět následuje odkazy) a hledá na nich odkazy na již neexistující stránky. (Internetový robot. http://cs.wikipedia.org/wiki/Internetový_robot 16.6.2011)

dilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

Úřad má přitom za to, že správným postupem z hlediska ochrany osobních údajů je obecný zákaz indexování listin s osobními údaji, které jsou umisťovány na elektronické úřední desky, což současně znamená i zákaz jejich cachování. Účelem zpřístupnění osobních údajů respektive konkrétních dokumentů uvedeným způsobem totiž není „automatické“ umožnění předat a sdružovat údaje zveřejněné na jednotlivých úředních deskách do úložišť mimo působnost orgánů veřejné správy, ani trvale uchovávat, prohledávat nebo profilovat dokumenty s osobními údaji, u nichž zákon přesně stanovil některé způsoby zpracování, a to včetně doby tohoto zpracování.

Dále je nutno zdůraznit, že v případě odstranění dokumentu z webové stránky přitom nestačí pouhé odstranění odkazů na tento dokument (stránku), ale je nezbytné jej fyzicky z webového serveru odstranit nebo alespoň přesunout do jeho zabezpečené části.

## Závěr

Úřad tedy považuje zákaz indexování webových stránek, resp. listin s osobními údaji za standardní opatření na straně správce osobních údajů, které má zamezit neoprávněným přístupům a přenosům osobních údajů tak, jak vyžaduje § 13 odst. 1 zákona o ochraně osobních údajů.

Současně lze konstatovat, že příslušné nastavení nepochybně volně dostupné nástroje jednoduše umožňují.

Příklad použití dostupných nástrojů k tomu, aby pravidla pro ochranu osobních údajů byla dodržena i v prostředí webových stránek:

1. Pro celé webové stránky zakázat prostřednictvím souboru *robots.txt* přístup robotů.
2. Zakázat přístup robotů pro každou stránku zvlášť pomocí *meta tagu* obsaženého v hlavičce stránky, případně pro vlastní odkazy použít atribut rel=“nofollow“, rel=“noindex“ a rel=“noarchive“, v důsledku čehož je odkaz s tímto parametrem pro robota neviditelný, neprovede indexaci stránky nebo její uložení do cache. Použití těchto atributů přitom většina vyhledávačů (jako např. Google nebo Seznam.cz) respektuje.
3. Problematické stránky (tj. ty obsahující osobní údaje) zařadit na druhou, lépe třetí a další úroveň struktury webových stránek.
4. Minimalizovat počet odkazů na uvedenou stránku.
5. Webové stránky obsahující osobní údaje vždy opatřit označením správce těchto údajů a dobou, kdy byly tyto stránky vytvořeny.

Poznámka: Publikované stanovisko je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Názory Úřadu/Stanoviska.

# Stanovisko č. 2/2011

srpen 2011

## Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy

### Úvod

V souvislosti s řadou smluvních vztahů, zejména tzv. spotřebitelských smluv mezi *dodavatelem a spotřebitelem,* dochází ke zpracování osobních údajů fyzické osoby. V takovém případě je *dodavatel, tj. profesionál (podnikatel) v postavení poskytovatele určité služby nebo zboží,* v postavení správce osobních údajů a spotřebitel, který je fyzickou osobou, v postavení subjektu údajů (dále jen „klient“).

V praktické rovině se lze velmi často setkat s tím, že součástí smluvních ujednání jsou tzv. Všeobecné obchodní podmínky (dále jen „VOP“), kterými si *dodavatel* upravuje formulářovým způsobem podmínky jím uzavíraných smluvních vztahů. Toto stanovisko se zaměřuje především na některé instituty zpracování osobních údajů (souhlas a informační povinnost) používané právě ve VOP, ale shodná východiska platí i pro běžné smlouvy.

### Relevantní právní úprava

V případě smluvního vztahu mezi podnikatelem (správcem osobních údajů) a klientem (subjektem údajů) nepochybně dochází a musí docházet ke zpracování osobních údajů, a to k řadě účelů [viz § 5 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“)].

Tím nejběžnějším a nejzákladnějším účelem zpracování je uzavření a plnění smlouvy a s tím související identifikace smluvních stran. Je logické, že podnikatel potřebuje v řadě případů identifikovat svého klienta tak, aby mohli uzavřít platnou smlouvu a potřebuje znát jeho identifikační údaje, aby mu mohl řádně plnit, tj. doručit zboží, poskytnout službu apod. Ke zpracování osobních údajů za tímto účelem přitom není potřeba souhlasu subjektu údajů, neboť zákon o ochraně osobních údajů tyto případy předpokládá v § 5 odst. 2 písm. b), a nevyžaduje tak nadbytečné udělování souhlasu vedle vlastního uzavření smlouvy.

Lze přitom uvést, že se Úřad pro ochranu osobních údajů (dále jen „Úřad“) nadále setkává s případy, kdy VOP obsahují ustanovení o souhlasu se zpracováním osobních údajů za účelem uzavření a plnění smlouvy a dokonce existencí tohoto souhlasu podmiňují trvání smluvního vztahu; taková ustanovení jsou pro klienta zavádějící a i případné odvolání souhlasu nemění nic na skutečnosti, že podnikatel může dále zpracovávat osobní údaje klienta bez jeho souhlasu. Namísto formulace souhlasu k účelu uzavření a plnění smlouvy je proto žádoucí zaměřit se na důsledné plnění informační povinnosti podle § 11 zákona o ochraně osobních údajů.

### Souhlas ve VOP

Ve VOP se lze dále setkat s dalšími účely zpracování osobních údajů, ke kterým je již souhlas subjektu údajů nezbytný. Těmito účely jsou zejména přímý marketing (s výjimkou postupu podle § 5 odst. 5 zákona o ochraně osobních údajů, respektive použití osobních údajů k nabízení obchodů a služeb, a to buď přímo samotným podnikatelem nebo i jejich předání za tímto účelem jiným subjektům), předání údajů do dlužnických registrů, nahrávání telefonních hovorů na zákaznické lince apod. V takových případech VOP obsahují formulaci o tom, že klient souhlasí se zpracováním osobních údajů za shora uvedeným účelem.

K problematice souhlasu se Úřad vyjádřil ve stanovisku č. 2/2008 (Souhlas se zpracováním osobních údajů). Použití obecných závěrů tohoto stanoviska na problematiku VOP vede především k otázce posouzení dobrovolnosti úkonu klienta ve chvíli, kdy je mu předkládána formulářová smlouva, resp. VOP, obsahující text souhlasu se zpracováním osobních údajů. Podle § 4 písm. n) zákona o ochraně osobních údajů je souhlasem subjektu údajů svobodný a vědomý projev vůle, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. Souhlas se zpracováním osobních údajů je tedy projevem vůle subjektu údajů (jednostranným právním úkonem), a ne dvoustrannou smlouvou mezi správcem a subjektem údajů. Již z tohoto důvodu lze uvést, že zařazení souhlasu se zpracováním osobních údajů do smluvního ujednání je nevhodné a pro subjekt údajů matoucí, neboť s vlastním smluvním ujednáním nemá nic společného. Naopak, subjekt údajů nad rámec vlastního smluvního vztahu souhlasí, aby správce použil jeho osobní údaje za stanoveným účelem. Z toho vyplývá, že souhlas se zpracováním osobních údajů nemůže a nesmí být podmínkou, která by sama o sobě znemožňovala (v případě jeho neudělení) uzavření smluvního vztahu, neboť osobní údaje nemohou být vedle peněz dalším platidlem za poskytnutou službu nebo zboží.

V praktické rovině je proto čistě na vůli klienta, zda s částí VOP, která obsahuje souhlas se zpracováním osobních údajů, vysloví svůj souhlas tím, že smlouvu v předložené podobě uzavře, nebo ne. Projev vůle, znamenající to, že klient nemá v úmyslu poskytnout svůj souhlas se zpracováním osobních údajů, může být zaznamenán několika způsoby. V případě, kdy je uzavírána smlouva písemně, může klient buď konkrétní ustanovení o souhlasu ve VOP přeškrtnout nebo k tomuto ustanovení (nebo na jiné vhodné místo ve smlouvě) dopsat poznámku, ze které by byla jeho vůle zřej-

má (např. „nesouhlasím se zpracováním osobních údajů za účelem marketingu“). Je přitom povinností správce tento projev vůle respektovat a, jak bylo shora uvedeno, nepodmiňovat uzavření smluvního vztahu (tj. vynucovat si) udělením souhlasu. V případě, kdy klient uzavře smlouvu s takto upravenými VOP, znamená to, že souhlas se zpracováním osobních údajů správci neudělil.

V případě, kdy je souhlas ze strany klienta při uzavření smlouvy udělen, nic nebrání subjektu údajů po uzavření smlouvy, pokud dospěje k závěru, že si již nepřeje, aby byly jeho osobní údaje zpracovávány, svůj souhlas odvolat. Již proto je vynucování si souhlasu na straně správců při uzavírání smluv zbytečné.

S ohledem na výše uvedené lze klientům doporučit nechat si potvrdit kopii smlouvy, resp. VOP bez souhlasu, a to především tehdy, pokud se týká VOP, které nejsou neoddělitelně připojeny k vlastní smlouvě.

V případě, kdy je smluvní vztah uzavírán tzv. prostředky komunikace na dálku, tj. především přes internet, závisí otázka způsobu projevu vůle na konkrétním použitém webovém formuláři pro uzavření smlouvy. Je ovšem třeba uvést, že aby byl souhlas svobodný, musí správce umožnit subjektu údajů projevit svoji vůli, tedy uzavřít smluvní vztah bez souhlasu s nesouvisejícím zpracováním osobních údajů. Toho lze dosáhnout např. kolonkou pro poznámku, doplňující informace, vzkaz apod. Jako nezákonně získaný (vynucený), a tedy neplatný souhlas, tak lze popsat ten způsob jeho získání, kdy by k uzavření smlouvy došlo prostředky komunikace na dálku (přes internet), a to vyplněním smluvního formuláře na webových stránkách podnikatele odkazujícího na VOP obsahující souhlas se zpracováním osobních údajů, pokud by současně neobsahoval prostor pro subjekt údajů před „potvrzením a odesláním“ vyplněných údajů vyjádřit svoji vůli.

## Souhlas s předáním osobních údajů třetím subjektům

Dalším problémem, se kterým se Úřad v souvislosti s VOP setkává, je formulace souhlasu s předáváním osobních údajů třetím subjektům a se zpracováním osobních údajů těmito třetími subjekty (nejčastěji za účelem přímého marketingu nebo tzv. úvěrovým registrům). Pokud je totiž udělen souhlas k předání osobních údajů třetímu subjektu, musí z něj jednoznačně vyplývat nejen identifikace tohoto subjektu, ale také účel, za kterým bude osobní údaje zpracovávat.

Tato povinnost vyplývá z § 5 odst. 4 zákona o ochraně osobních údajů, podle kterého musí být subjekt údajů při udělení souhlasu informován mimo jiné o tom, jakému správci a k jakému účelu svůj souhlas uděluje. Tato podmínka znamená, že text souhlasu musí správce označit běžnými identifikačními údaji (názvem nebo jménem a příjmením, sídlem nebo adresou, IČ) tak, aby ho případně mohl subjekt údajů kontaktovat a uplatnit u něj svoje práva. Proto jsou nedostatečné používané formulace VOP obsahující souhlas s předáním osobních údajů dalším subjektům sdruženým se správcem v holdingu, osobám se správcem spolupracujícím, osobám, se kterými má správce uzavřené smlouvy nebo snad dokonce v budoucnu smlouvy uzavře, pokud nejsou současně tyto spolupracující osoby subjektu údajů sděleny jiným způsobem při udělování souhlasu (např. na samostatné listině). V těchto případech totiž subjekt údajů neví, jakému konkrétnímu správci souhlas uděluje, přičemž „bianco“ souhlas zákon neumožňuje. Uvedené také znamená, že pokud se podnikatel rozhodne předat osobní údaje dalšímu subjektu (s výjimkou postupu podle § 5 odst. 6 zákona o ochraně osobních údajů), se kterým v době získávání souhlasu klientů nespolupracoval, musí nejprve oslovit svoje klienty s žádostí o souhlas s tímto předáním a o účelu zpracování u třetího subjektu je informovat.

Řada VOP obsahuje také ustanovení o způsobu jejich změny a způsobu akceptace změny ze strany klienta. Bez výjimky lze hovořit o tom, že souhlas se změnou VOP je konstruován na základě oznámení změny a nečinnosti klienta. Z hlediska zpracování osobních údajů je takto konstruovaná forma souhlasu se zpracováním osobních údajů ve změně VOP v rozporu s § 4 písm. n) zákona o ochraně osobních údajů, neboť nesplňuje podmínku projevu vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů (analogicky viz také § 44 odst. 1 občanského zákoníku - mlčení a nečinnost samy o sobě neznamenají přijetí návrhu). Současně by v tomto případě správce nebyl schopen takový souhlas prokázat (§ 5 odst. 4 věta druhá zákona o ochraně osobních údajů), neboť skutečnost, že subjekt údajů změnu VOP obdržel, že se s ní seznámil a že na ni vědomě nereagoval, není pro správce prokazatelná a plně závisí na postoji subjektu údajů.

## Rozsah zpracovávaných osobních údajů

Dále lze upozornit na povinnost správce podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, tedy povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Z tohoto důvodu je potřeba i u těch zpracování, která jsou prováděna se souhlasem subjektu údajů, řádně stanovit ve formulaci VOP rozsah vyžadovaných osobních údajů tak, aby nezahrnoval údaje zjevně nadbytečné pro daný účel (např. velikost oblečení pro účely marketingu telekomunikačního operátora). K porušení této povinnosti může dojít nejčastěji v případě, kdy je souhlas formulován ke všem osobním údajům uvedeným na kopii občanského průkazu, přičemž zjevně údaje o rodinném stavu, dětech a jejich rodných číslech nebývají pro účely zpracování stanovené správci ve VOP nezbytné. Je třeba přitom zdůraznit, že ani souhlas

subjektu údajů nezbavuje správce odpovědnosti za to, že vyžaduje a shromažďuje a dále uchovává, tedy zpracovává, nadbytečné osobní údaje.

## Informační povinnost

Vzhledem k tomu, že VOP jsou jedním z prvních dokumentů vyměněných mezi správcem a subjektem údajů v rámci jejich vzájemného vztahu, je logické, že jsou používány také ke splnění informační povinnosti podle § 11 zákona o ochraně osobních údajů. Některé z těchto informací jsou přitom součástí souhlasu se zpracováním osobních údajů (§ 5 odst. 4 zákona o ochraně osobních údajů – účel, rozsah, správce, období) a není nutné je znovu v rámci ustanovení s informační povinností opakovat. Pro přehlednost a srozumitelnost poskytované informace o zpracování osobních údajů lze přitom doporučit členit informaci podle § 11 odst. 1 zákona č. 101/2000 Sb. podle jednotlivých účelů zpracování, tj. uzavření a plnění smlouvy, marketing, předání třetím subjektům za účelem marketingu, dlužnické registry atd.

## Závěr

V případě používání VOP pro oblast zpracování osobních údajů je třeba rozlišovat situace, kdy je souhlas se zpracováním osobních údajů nezbytný (marketing, dlužnické registry atd.) a kdy souhlas není potřeba (uzavření a plnění smlouvy, vymáhání pohledávek ze smlouvy). Těmto případům je třeba uzpůsobit formulaci souhlasu a případné plnění informační povinnosti. V případě poskytování souhlasu je třeba umožnit subjektu údajů projevit svoji vůli a tento projev respektovat tak, aby se jednalo o svobodně a dobrovolně udělený souhlas se zpracováním osobních údajů. Jako nejvhodnější způsob lze doporučit samostatně formulované části VOP doplněné o „zaškrtávací“ pole, jehož vyplněním by subjekt údajů souhlas udělil. Pokud je souhlas přímo v textu VOP, musí správce respektovat vyškrtnutí takové části VOP ze strany subjektu údajů. Pro předávání osobních údajů třetím subjektům musí být nejprve subjekt údajů informován o účelu zpracování třetím subjektem a o identifikaci tohoto subjektu.

Poznámka: Publikované stanovisko je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Názory Úřadu/Stanoviska.

# III. SDĚLENÍ ÚŘADU

## Metodické doporučení Ministerstva vnitra a Úřadu pro ochranu osobních údajů k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím

Ministerstvo vnitra a Úřad pro ochranu osobních údajů společně vypracovaly dokument „Metodické doporučení Ministerstva vnitra a Úřadu pro ochranu osobních údajů k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím“.

Jedná se o metodické doporučení k poskytování informací o platech pracovníků ve veřejném sektoru. Podnětem k vytvoření tohoto společného metodického doporučení byl rozsudek Nejvyššího správního soudu z 27. května 2011 ve věci zveřejnění odměny zaměstnance zlínského magistrátu, jehož laická interpretace vedla k vymáhání informací o platu konkrétních zaměstnanců veřejné správy bez ohledu na existující právo na ochranu soukromého života.

Zástupci Ministerstva vnitra, Úřadu pro ochranu osobních údajů, Ministerstva spravedlnosti, Kanceláře veřejného ochránce práv a Otevřené společnosti o.p.s. se setkali v zájmu vytvoření konsenzuální odborné interpretace, o niž se budou moci opírat instituce při poskytování uvedených informací požadovaných dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Cílem společného jednání bylo zformulovat metodické doporučení, které poskytuje povinným subjektům základní orientační návod, určitá vodítka, jimiž by se měly při vyřizování žádostí o poskytnutí informace o výši platu řídit. Obsah metodického doporučení však není právně závazný, protože závazný výklad právních předpisů mohou v konkrétních věcech podávat pouze soudy. Vyřizování žádostí o poskytnutí informací je tak zcela v působnosti a odpovědnosti každého povinného subjektu.

Výsledkem práce odborníků jmenovaných institucí je zmíněné Metodické doporučení Ministerstva vnitra a Úřadu pro ochranu osobních údajů.

Poznámka:
Publikovaný dokument je také umístěn na internetové adrese Úřadu www.uoou.cz v rubrice Na aktuální téma a je k dispozici i na jiných veřejně přístupných internetových adresách.

Přetisk dokumentu zveřejněného MV ČR (s. 3326 – 3334)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

**Metodické doporučení Ministerstva vnitra a Úřadu pro ochranu osobních údajů k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím**

## I. Úvod

Listina základních práv a svobod upravuje jako součást práva jednotlivce na soukromí (čl.7) v čl. 10 odst. 3 právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Současně však tento ústavní zákon v článku 17 garantuje ve skupině politických práv a svobod právo na informace a svobodu projevu. Mezi těmito právy a svobodami tak často a logicky vzniká konflikt, který je vlastní každé demokratické společnosti.

Podle ustanovení § 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění, *poskytne povinný subjekt základní osobní údaje o osobě, jíž poskytl veřejné prostředky,* a to v rozsahu *jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků.*[1] Tyto druhy osobních údajů poskytne povinný subjekt i bez souhlasu této osoby (subjektu osobního údaje), a ustanovení § 8b InfZ proto představuje z hlediska zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, zvláštní právní důvod pro zpracovávání osobních údajů formou poskytnutí podle zákona o svobodném přístupu k informacím [srov. § 5 odst. 2 písm. a) zákona o ochraně osobních údajů a § 4 odst. 1 InfZ].

V praxi bylo sporné, zda ustanovení § 8b InfZ umožňuje poskytnutí informace o výši platu nebo odměny konkrétního zaměstnance povinného subjektu bez jeho souhlasu.[2] Na tuto otázku odpovídal Nejvyšší správní soud v rozsudku *Maděra v. zlínský magistrát* ze dne 27. května 2011, čj. 5 As 57/2010-79. Rozhodl, že údaj o tom, jaké mimořádné odměny dostal vedoucí oddělení informačních systémů magistrátu a jejich důvod, není předmětem ochrany soukromí, neboť výdaje na odměny, včetně platů zaměstnanců v povinných subjektech spadají do rozsahu pojmu *veřejné prostředky*; NSS proto připustil, aby tato informace byla na základě žádosti podané podle zákona o svobodném přístupu k informacím poskytnuta v tomto konkrétním případě i bez souhlasu zaměstnance.[3]

---

[1] Výjimku z této informační povinnosti představuje *poskytování veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotní péče, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření a státní pomoci při obnově území* (§ 8b odst. 2 InfZ).

[2] V tomto metodickém doporučení užíváme pojmy *zaměstnanec* i pro veřejné funkcionáře podle § 5 odst. 1 nového zákoníku práce, když např. starosta či místostarosta pobírají za svou práci pro obec *měsíční odměnu,* která je stanovena nařízením vlády č. 37/2003 Sb., nejsou však obecními zaměstnanci ve smyslu pracovněprávním.

[3] Nejvyšší správní soud pojem *veřejné prostředky* vyložil podle § 2 písm. g) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole). Nejvyšší správní soud se sice zabýval poskytnutí informace o výši mimořádné *odměny* (v soudem posuzované věci se jednalo o poskytnutí informace o výši

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Protože aplikační praxe po vydání tohoto precedentního rozhodnutí nepostupovala při vyřizování žádostí o poskytnutí informace o platech zaměstnanců povinných subjektů jednotně, uskutečnilo se k této otázce dne 23. srpna 2011 jednání mezi zástupci Ministerstva vnitra, Úřadu pro ochranu osobních údajů, Ministerstva spravedlnosti, Kanceláře veřejného ochránce práv a zástupců Otevřené společnosti o.p.s. Cílem uvedeného jednání bylo zformulovat *metodické doporučení Ministerstva vnitra,* které by povinným subjektům poskytlo základní orientační návod pro poskytování této specifické informace.

Smyslem předkládaného metodického doporučení není a ani nemůže být poskytnutí uceleného návodu pro řešení všech potencionálních situací ani poskytnout komplexní právní analýzu celé tak složité problematiky jako je střet práva na informace a práva na ochranu soukromí a osobních údajů. Předkládané doporučení poskytuje povinným subjektům určitá vodítka, jimiž by se měly při vyřizování žádostí o poskytnutí informace o výši platu (mzdě, odměně) řídit. Předkládá se jednak jasný návod pro celou řadu žádostí o informace týkajících se vrcholných činitelů veřejné moci a současně ukazuje možné způsoby i limity pro rozhodovací činnost v případě poskytování informací u veřejných funkcionářů na různých stupních řízení.

Obsah metodického doporučení však **není právně závazný, neboť závazný výklad právních předpisů mohou v konkrétních věcech podávat pouze soudy. Vyřizování žádostí o poskytnutí informací je zcela v působnosti a především odpovědnosti každého povinného subjektu.**

Autoři věří, že tato metodika současně podpoří souběžnou diskusi, jaké další alternativní způsoby informovanosti veřejnosti jsou vhodné a potřebné ke kontrole a zajištění transparentnosti výkonu veřejné správy tak, aby se minimalizoval zásah do soukromého života zaměstnanců veřejné správy a jejich rodinných příslušníků.

Toto metodické doporučení bylo zpracováno Ministerstvem vnitra a Úřadem pro ochranu osobních údajů s využitím podnětů, které vyplynuly z jednání dne 23. srpna 2011 a vyjadřuje společné stanovisko pouze uvedených institucí.

## II. Poskytnutí informace o výši platu a odměny na základě žádosti podle zákona o svobodném přístupu k informacím

### *a. Obecně*

---

mimořádných odměn vedoucího odboru Magistrátu města Zlína), jeho závěry se však vztahují i na poskytnutí informace o výši platu (všech jeho složek), popř. mzdy.
Pro úplnost je nutné připomenout, že dřívější správní judikatura již připustila poskytnutí informace o *důvodech mimořádných odměn* vyplacených konkrétnímu zaměstnanci (rozsudek Krajského soudu v Českých Budějovicích ze dne 15. května 2002, sp. zn. 10 Ca 40/2002).

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Zákon o svobodném přístupu k informacím rozlišuje *poskytování informace* jejich předchozím zveřejněním nebo zpřístupněním na základě individuální žádosti podané fyzickou nebo právnickou osobou (§ 4 odst. 1). Závěry učiněné Nejvyšším správním soudem se týkají poskytnutí informace na základě individuální žádosti a nevyjadřují se nijak k případnému zveřejňování informace o výši platu či odměny, tj. zpřístupnění neurčenému okruhu subjektů (typicky na internetu). Této otázce je proto pro úplnost věnována pozornost v bodě III doporučení.

Rozsudek Nejvyššího správního soudu, jenž se k výkladu § 8b InfZ precedentně vyjádřil, je samozřejmě nutné respektovat, takže informaci o výši platu či odměně konkrétního zaměstnance bude nutné, při splnění níže psaných podmínek, na základě individuální žádosti podané podle zákona o svobodném přístupu k informacím, poskytnout. Nosné důvody (*ratio decidendi*) odůvodnění rozsudku Nejvyššího správního soudu však principiálně nevylučují, aby vydání takové informace bylo při uplatnění *testu proporcionality* v odůvodněných případech odmítnuto. Podmínkou takového postupu však je zohlednění všech okolností konkrétního případu, takže ve vztahu ke konkrétnímu zaměstnanci a konkrétním podmínkám zcela zřetelně převáží nutnost ochrany soukromí a osobních údajů nad právem na informace, resp. nad požadavkem kontroly ze strany veřejnosti (nutnost uplatnit takový postup vyplývá i z § 5 odst. 3 a § 10 zákona o ochraně osobních údajů[4]). Důvody pro neposkytnutí informace však musejí být vždy náležitě uvedeny v rozhodnutí, jímž by byla žádost o informace odmítnuta [5].

K odmítnutí žádosti o informace zpravidla nebude možné přistoupit ve vztahu k veřejným funkcionářům podle § 2 odst. 1 zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů,[6] tj. v případě vrcholných představitelů povinných subjektů, reprezentantů státní (veřejné) moci. Od této kategorie je však třeba odlišovat skupinu zaměstnanců podle § 2 odst. 2 a 3 zákona o střetu zájmů, např. těch, kteří se v rámci své pracovní činnosti podílejí na rozhodování o veřejných prostředcích (typicky o veřejných zakázkách apod.). V podrobnostech vizte dále.

***b. Postup při vyřizování žádosti***

[4] § 5 odst. 3: *Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.* § 10: *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.*

[5] Kupř. může být vhodné vysvětlit, čím se posuzovaný případ skutkově odlišuje od *Maděra v. zlínský magistrát*, takže výsledné právní posouzení je jiné.

[6] Zákon o střetu zájmů ve vztahu k veřejným funkcionářům nastavil z důvodu veřejného zájmu (veřejné kontroly) vyšší míru publicity ve vztahu k těmto osobám a z tohoto důvodu je legitimní, pokud jsou tyto osoby nuceny snést i vyšší míru informovanosti o jejich platech (odměnách). Jejich majetkové poměry jsou veřejné, a proto by nemělo logiku, kdyby nebyly veřejné i jejich příjmové poměry.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Při vyřizování žádosti o poskytnutí informace o výši platu (mzdy, odměny) konkrétního zaměstnance je na prvním místě nutné zvážit, zda tato informace již není informací zveřejněnou, tedy např. zda přesná výše platu již nevyplývá z určitého právního předpisu (ať již pevnou částkou nebo jednoznačnou metodikou výpočtu na základě předem stanovených hledisek).[7] Příkladem může být zákon č. 236/1995 Sb., o platu a dalších náležitostech spojených s výkonem funkce představitelů státní moci a některých státních orgánů a soudců a poslanců Evropského parlamentu, v platném znění nebo zákony o územních samosprávných celcích ve spojení s nařízením vlády č. 37/2003 Sb., o odměnách za výkon funkce členům zastupitelstev, ve znění pozdějších předpisů. Pokud je požadovaná informace oprávněně zveřejněná, poskytne se bez dalšího zkoumání.

Jestliže informace o platu není takto předem přístupná, měl by povinný subjekt při vyřizování žádosti o poskytnutí informace kontaktovat příslušného zaměstnance a umožnit mu, aby se k podané žádosti vyjádřil, tedy aby případně uplatnil všechny argumenty proti zpřístupnění informace o výši jeho platu (mzdě, osobním příplatku, odměně)[8]. Tato povinnost vyplývá z § 20 odst. 4 InfZ, ve spojení se základními zásadami činnosti správních úřadů, především ve spojení s § 4 odst. 4 nového správního řádu.[9] Takovou výzvu lze učinit i neformálně, např. e-mailovou zprávou či telefonicky (se záznamem do spisu). Je však nutno dodržet lhůtu pro poskytnutí informace (15 dnů od doručení žádosti), tedy požádat dožádaného zaměstnance o odpověď v dostatečně krátké lhůtě. Nepodaří-li se zaměstnance kontaktovat (např. jde-li o bývalého zaměstnance) nebo pokud v zadané lhůtě nereaguje, učiní se o tom záznam do spisu. Nedostatek vyjádření dotčeného zaměstnance však není překážkou pro poskytnutí informace. Člověk dotčený poskytnutím osobního údaje má rovněž oprávnění znát identitu osoby, která o poskytnutí tohoto údaje žádá. Žádá-li se o informace o větším množství zaměstnanců, lze uvažovat i o prodloužení lhůty pro poskytnutí informace podle § 14 odst. 7 InfZ (bude-li současně splněn některý z důvodů v tomto ustanovení uvedený, např. komunikace s jinou složkou povinného subjektu, např. s personálním odborem úřadu apod.).

Pokud zaměstnanec s poskytnutím informace souhlasí, přičemž souhlas musí splňovat požadavky § 4 písm. n) zákona o ochraně osobních údajů[10], uplatnění testu proporcionality odpadá. Pokud nesouhlasí, je nutné především zvážit, v jaké pracovní pozici se dotčený zaměstnanec nachází. Jedná-li se o veřejného funkcionáře podle § 2 odst. 1 zákona o střetu zájmů, bude třeba údaj o výši platu (mzdy) nebo odměny

[7] V této souvislosti je nutné podotknout, že výše platu se může odvíjet i od „započitatelných let“. Taková informace, tedy informace např. po jak dlouhou dobu daný zaměstnanec vykonává své zaměstnání, je rovněž přístupná bez jeho souhlasu, a to na základě § 5 odst. 2 písm. f) zákona o ochraně osobních údajů.
[8] Zaměstnanec by měl být informován o možnosti zpřístupnit údaje o jeho platovém ohodnocení ještě před uzavřením pracovní smlouvy (srov. § 31 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů.).
[9] Správní orgán umožní dotčeným osobám uplatňovat jejich práva a oprávněné zájmy.
[10] K tomu podrobněji Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008 „Souhlas se zpracováním osobních údajů“. Dostupné na www.uoou.cz.


v drtivé většině případů poskytnout, neboť v těchto případech lze presumovat, že veřejný zájem na přístupnosti takové informace v podobě veřejné kontroly povinných subjektů převažuje nad ochranou soukromí daného zaměstnance (není vyloučeno, že výjimečně tomu bude jinak, takovou situaci by však musel povinný subjekt adekvátně odůvodnit ve svém rozhodnutí).

Ve vztahu k ostatním zaměstnancům povinných subjektů[11], včetně těch kteří jsou při své pracovní činnosti oprávněni samostatně vykonávat veřejnou moc (zjednodušeně řečeno rozhodovat o právech a povinnostech fyzických a právnických osob), anebo těch, kteří v mezích své pravomoci smí nakládat s veřejnými prostředky v určité výši,[12] podle § 2 odst. 2 a 3 zákona o střetu zájmů, bude nutné *test proporcionality* provést vždy a *ad hoc* uvážit, zda shora popsaný veřejný zájem na zpřístupnění informace převažuje nad právem na soukromí zaměstnance - ochranou osobního údaje o výši jeho platu (mzdy, odměny). Povinný subjekt přitom musí uplatnit kritérium potřebnosti omezení ochrany osobního údaje, kritérium vhodnosti omezení a hledisko vzájemného porovnání obou práv.[13] V případě zaměstnanců, kteří nemají žádnou rozhodovací pravomoc a ani nedisponují s většími objemy veřejných prostředků, bude zpravidla veřejný zájem na zpřístupnění údaje o jejich platu neporovnatelně menší a ochraně tohoto osobního údaje bude možné dát přednost. Na základě mezinárodní komparace (kanadský zákon o poskytnutí platů ve veřejném sektoru z roku 1996[14] a stanovisko britského informačního komisaře[15]) se jako vhodné kritérium jeví celková vyplacená částka, např. trojnásobek průměrné mzdy v národním hospodářství podle § 17 odst. 4 zákona č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů, nebo § 5 odst. 2 zákona č. 118/2000 Sb., o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů,[16] zaokrouhlená na 5 000 Kč nahoru.[17] (Tento prvek by mohl být do budoucna základem zpřesnění právní úpravy poskytování informace o platech, provedené ať již doplněním zákona o svobodném přístupu k informacím či zákona o střetu zájmů).

[11] Velice zjednodušeně lze hovořit o „řadových úřednících", kteří nevykonávají žádnou rozhodovací pravomoc povinného subjektu a za povinný subjekt nejednají v závažných záležitostech navenek.
[12] Jako vhodné hledisko se jeví § 2 odst. 3 písm. a) zákona o střetu zájmů. Kritériem tam je částka dosahující nejméně 250 000 Kč.
[13] srov. nález Ústavního soudu ze dne 9. října 1996, sp. zn. Pl. ÚS 15/96.
[14] Public Sector Salary Disclosure Act, 1996.
[15] When should salaries be disclosed?
[16] K provedení zákona o ochraně zaměstnanců je průměrná mzda v národním hospodářství každoročně vyhlašována vyhláškou MPSV o rozhodné částce pro určení celkové výše mzdových nároků vyplacených jednomu zaměstnanci podle zákona č. 118/2000 Sb., o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů.
[17] V této souvislosti je vhodné zmínit i rozsudek Evropského soudního dvora ve věci Rechnungshof vs. Österreichischer Rundfunk odst. 94 „…čl. 6 odst. 1 písm. c) a čl. 7 písm. c) a e) Směrnice 95/46 nebrání takové vnitrostátní právní úpravě, jakou je úprava dotčená ve věcech v původních řízeních, za předpokladu, že je prokázáno, že široké zveřejnění nejen výše ročních příjmů, pokud převyšují určity strop, osob zaměstnaných subjekty, jež podléhají dohledu Rechnungshof, ale i jmen poživatelů těchto příjmů je nezbytné a vhodné ve zvtahu k cíli řádné správy veřejných prostředků sledovanému ústavodárcem…".

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pokud povinný subjekt informaci o výši platu poskytne, musí se vypořádat též s povinností plynoucí z § 5 odst. 3 InfZ, tedy s povinností zveřejnit způsobem umožňujícím dálkový přístup informaci poskytnutou na základě žádosti.[18] Tuto povinnost lze bez dalšího posuzování splnit pouze u nejvyššího vedení povinného subjektu (ministr, ředitel, předseda apod.). Protože se i na zveřejnění informace podle tohoto ustanovení uplatní pravidlo plynoucí z § 12 InfZ[19] a protože by *zveřejněním* takové informace předem neurčenému okruhu osob došlo k podstatnému a nepřiměřenému zásahu do práva na ochranu osobnosti a osobních údajů (srov. též § 5 odst. 3 a § 10 zákona o ochraně osobních údajů[20]), je vhodné zveřejnit *informaci o poskytnuté informaci* anonymně, tedy uvést, že byla poskytnuta informace o výši platu konkrétního funkcionáře nebo informace o výši platu konkrétního zaměstnance apod. Bude-li mít další osoba zájem o získání takové informace, může žádost podle zákona podat sama.

Přistoupí-li povinný subjekt k odmítnutí žádosti o poskytnutí informace, musí o tom vydat správní rozhodnutí podle § 15 InfZ (výrok rozhodnutí bude odkazovat na § 8a InfZ ve spojení s § 5 odst. 2 zákona o ochraně osobních údajů). V tomto správním rozhodnutí musí náležitě odůvodnit, proč v daném případě převážila nutnost ochrany osobního údaje nad jeho zpřístupněním. Pokud povinný subjekt poskytne údaje anonymní nebo souhrnné, nejedná se ani o částečné vyhovění žádosti (směřovala-li žádost k poskytnutí informace o platu konkrétní osoby či funkcionáře), ale o sdělení doprovodné informace „nad rámec“ původní žádosti. V takovém případě je nutné žádost rozhodnutím odmítnout v plném rozsahu, aby se dalo hovořit o úplném vyřízení žádosti.

Zbývá dodat, že žadatel, jenž získal informaci o výši platu konkrétního pracovníka, může s takovou informací nakládat pouze v souladu s předpisy stanovujícími jejich ochranu (např. občanský zákoník, zákon o ochraně osobních údajů, trestní zákoník).

[18] *Do 15 dnů od poskytnutí informací na žádost povinný subjekt tyto informace zveřejní způsobem umožňujícím dálkový přístup. O informacích, poskytnutých v jiné než elektronické podobě, nebo mimořádně rozsáhlých elektronicky poskytnutých informacích postačí zveřejnit doprovodnou informaci vyjadřující jejich obsah.*

[19] *Všechna omezení práva na informace provede povinný subjekt tak, že poskytne požadované informace včetně doprovodných informací po vyloučení těch informací, u nichž to stanoví zákon. Právo odepřít informaci trvá pouze po dobu, po kterou trvá důvod odepření. V odůvodněných případech povinný subjekt ověří, zda důvod odepření trvá.*

[20] § 5 odst. 3 (*Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.*) § 10 (*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.*)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

**III. Zveřejnění informace o výši platu a odměny způsobem umožňujícím dálkový přístup**

Podle § 5 odst. 7 InfZ může povinný subjekt za podmínek stanovených zákonem o svobodném přístupu k informacím zveřejnit i další informace. Protože zákon o svobodném přístupu k informacím pro zpřístupňování osobních údajů odkazuje na podmínky plynoucí ze zákona o ochraně osobních údajů (srov. § 8a InfZ), je nutné i v tomto případě uplatnit test proporcionality, jenž je ve vztahu k osobním údajům vyjádřen v § 5 odst. 3 a § 10 zákona o ochraně osobních údajů (citaci vizte výše). V této souvislosti lze odkázat především na stanovisko Úřadu pro ochranu osobních údajů, dostupné na http://www.uoou.cz/uoou.aspx?menu=14&loc=328 a s ohledem na jeho obsah lze obecně doporučit, aby povinné subjekty bez souhlasu dotčených osob údaje o výši jejich platů (mezd či odměn) způsobem umožňujícím dálkový přístup (na internetu) pro předem neurčený okruh osob z vlastní iniciativy nezveřejňovaly, neboť takové „plošné“ zveřejnění zasáhne sféru zaměstnance daleko podstatnějším způsobem než její zpřístupnění na základě individuální žádosti konkrétní fyzické nebo právnické osobě.

**Závěr**

Cílem této metodiky je poskytnout návod na postup v případech, kdy je očekáván jednoznačný veřejný zájem na kontrole veřejné moci a za ni odpovědných pracovníků, přičemž je kladen důraz na rovnováhu obou základních práv a jejich vyvažování pomocí principu proporcionality (přiměřenosti zpracování osobních údajů). Přitom se vychází z již poměrně zavedené praxe agendy o střetu zájmů, z dělení na 3 kategorie veřejných zaměstnanců:

1) Veřejné funkcionáře s klíčovou odpovědností a rozsáhlou řídící a rozhodovací pravomocí. Údaje o jejich příjmech mohou být bez zásadních omezení poskytovány a následně předmětem kontroly a veřejné diskuse (analogicky k § 2 odst. 1 zákona o střetu zájmů).

2) Další vysoce postavené úředníky vybavené podstatným oprávněním nebo vlivem ve spojitosti s nakládáním s veřejnými prostředky (analogicky § 2 odst. 2 zákona o střetu zájmů ve spojení s odst. 3 cit. ustanovení), v jejichž případě je potřebné provádět test proporcionality.

3) Nižší úředníky, u nichž není vůbec dán zákonný důvod poskytovat údaje bez jejich souhlasu, neboť ke kontrole veřejných procesů, na nichž se tito úředníci podílejí, v zásadě postačí souhrnné informace (vč. souhrnu částek vynaložených na odměňování) a nikoliv osobní údaje.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

**Příloha:**
**Vymezení pojmu *veřejný funkcionář* podle zákona o střetu zájmů**

§ 2
**Veřejný funkcionář**

(1) Pro účely tohoto zákona se veřejným funkcionářem rozumí
a) poslanec Poslanecké sněmovny Parlamentu České republiky (dále jen „poslanec“),
b) senátor Senátu Parlamentu České republiky (dále jen „senátor“),
c) člen vlády nebo vedoucí jiného ústředního orgánu státní správy, v jehož čele není člen vlády,
d) předseda a inspektor Úřadu pro ochranu osobních údajů,
e) předseda Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví,
f) člen Rady Českého telekomunikačního úřadu,
g) předseda Energetického regulačního úřadu,
h) člen bankovní rady České národní banky,
i) prezident, viceprezident a člen Nejvyššího kontrolního úřadu,
j) veřejný ochránce práv a jeho zástupce,
k) člen Rady pro rozhlasové a televizní vysílání,
l) člen zastupitelstva kraje nebo člen zastupitelstva hlavního města Prahy (dále jen „kraj“), který je pro výkon funkce dlouhodobě uvolněn, a člen zastupitelstva kraje, který před svým zvolením do funkce člena zastupitelstva nebyl v pracovním poměru, ale vykonává funkce ve stejném rozsahu jako člen zastupitelstva kraje, který je pro výkon funkce dlouhodobě uvolněn,
m) člen zastupitelstva obce, městské části nebo městského obvodu územně členěného statutárního města a městské části hlavního města Prahy (dále jen „obec“), který je pro výkon funkce dlouhodobě uvolněn, a člen zastupitelstva obce, který před svým zvolením do funkce člena zastupitelstva nebyl v pracovním poměru, ale vykonává funkce ve stejném rozsahu jako člen zastupitelstva obce, který je pro výkon funkce dlouhodobě uvolněn,
n) starosta obce, místostarosta obce a členové rady obce a kraje, kteří nejsou pro výkon funkce dlouhodobě uvolněni.

(2) Pokud nejde o veřejného funkcionáře podle odstavce 1, rozumí se pro účely tohoto zákona veřejným funkcionářem také
a) ředitel bezpečnostního sboru a vedoucí příslušník bezpečnostního sboru 1. a 2. řídicí úrovně podle zvláštního právního předpisu v bezpečnostním sboru, s výjimkou příslušníků zpravodajských služeb,
b) člen statutárního orgánu, člen řídicího, dozorčího nebo kontrolního orgánu právnické osoby zřízené zákonem, státní příspěvkové organizace, příspěvkové organizace územního samosprávného celku, s výjimkou členů správních rad veřejných vysokých škol a statutárního orgánu nebo členů statutárního orgánu, členů řídicího, dozorčího nebo kontrolního orgánu samosprávných stavovských organizací zřízených zákonem,
c) vedoucí zaměstnanec 2. až 4. stupně řízení podle zvláštního právního předpisu právnické osoby zřízené zákonem, státní příspěvkové organizace, příspěvkové organizace územního samosprávného celku, s výjimkou právnických osob

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

vykonávajících činnost školy nebo školského zařízení,

d) vedoucí organizační složky státu, která je správním úřadem, a vedoucí zaměstnanec 2. až 4. stupně řízení podle zvláštního právního předpisu v organizační složce státu, s výjimkou zpravodajských služeb,
e) vedoucí úředník územního samosprávného celku podílející se na výkonu správních činností zařazený do obecního úřadu, do městského úřadu, do magistrátu statutárního města nebo do magistrátu územně členěného statutárního města, do úřadu městského obvodu nebo úřadu městské části územně členěného statutárního města, do krajského úřadu, do Magistrátu hlavního města Prahy nebo úřadu městské části hlavního města Prahy.

(3) Povinnosti podle tohoto zákona se na osobu uvedenou v odstavci 2, která podává oznámení podle § 9 až 11 a § 12 odst. 2 evidenčnímu orgánu (§ 14 odst. 1), vztahují pouze tehdy, jestliže v rámci výkonu své činnosti

a) nakládá s finančními prostředky orgánu veřejné správy jako příkazce operace ve smyslu zákona o finanční kontrole, pokud hodnota finanční operace přesáhne 250 000 Kč,
b) bezprostředně se podílí na rozhodování při zadávání veřejné zakázky nebo na rozhodování při výkonu práv a povinností zadavatele při realizaci zadávané veřejné zakázky,
c) rozhoduje ve správním řízení, s výjimkou blokového řízení, nebo
d) se podílí na vedení trestního stíhání.

# Rámec pro posouzení dopadů na ochranu soukromí a údajů pro aplikace RFID

Dne 6. dubna 2011 byla podepsána zástupci Evropské komise, zástupci průmyslu, Evropskou agenturou pro bezpečnost sítí a informací, zástupcem evropských kontrolních orgánů v oblasti ochrany soukromí a osobních údajů a dalšími, dobrovolná dohoda, kterou se stanovují pokyny pro všechny evropské společnosti pro řešení otázek týkajících se ochrany údajů v souvislosti s aplikacemi pracujícími s inteligentními etiketami (identifikace na základě rádiové frekvence – RFID) před jejich uvedením na trh.

Dohoda nazvaná „Rámec pro posouzení dopadů na ochranu soukromí a údajů pro aplikace RFID (The Privacy Impact Assessment Framework for FRID, rámec PIA)“ [1] si klade za cíl zajistit soukromí spotřebitelů před tím, než budou inteligentní etikety masově uvedeny na trh.

Tuto dohodu podepsali:

– Neelie Kroes, Evropská komisařka pro digitální agendu, Brusel, Belgie;

– Jacob Kohnstamm, předseda skupiny WP29, Brusel a předseda nizozemského úřadu pro ochranu osobních údajů, Nizozemí;

– Udo Helmbrecht, výkonný ředitel Evropské agentury pro bezpečnost sítí a informací (ENISA), Heraklion, Řecko;

– Heinz Paul Bonn, viceprezident Federální asociace pro informační technologie, telekomunikace a nová media (BITKOM), Berlín, Německo;

– Véronique Corduant, Evropsko-americká obchodní rada (EABC), Brusel, Belgie;

– Miguel A. Lopera, prezident a generální ředitel organizace GS1[2], Brusel, Belgie;

– Jürgen Noack, poradce pro informační technologie, EuroCommerce, Brusel, Belgie;

– Paul Skehan, ředitel European Retail Round Table (ERRT), Brusel, Belgie;

– Eldor Walk, předseda Evropské expertní skupiny pro RFID (EREG), Lampertheim, Německo.

Podle dohody provedou společnosti komplexní posouzení rizik v oblasti ochrany soukromí a přijmou opatření k řešení zjištěných rizik před uvedením nových aplikací s inteligentními etiketami na trh. Posouzení bude zahrnovat i možný vliv vazeb mezi získanými, předanými a jinými údaji na ochranu soukromí. To je zejména důležité v případě citlivých údajů, jako jsou biometrické údaje či údaje o zdravotním stavu.

Pravidla provedení PIA poprvé v Evropě stanoví jasnou metodiku pro posuzování a zmírňování rizik inteligentních etiket pro ochranu soukromí, kterou mohou uplatňovat všechna průmyslová odvětví, jež používají inteligentní etikety (např. doprava, logistika, maloobchodní prodej, prodej vstupenek, bezpečnost a zdravotní péče).

Společnostem poskytne provedení PIA právní jistotu, že jejich způsob používání etiket je v souladu s evropskou legislativou v oblasti ochrany soukromí a nabídne lepší ochranu evropských občanů a spotřebitelů.

Poznámka:

[1] Dohoda „Rámec pro posouzení dopadů na ochranu soukromí a údajů pro aplikace RFID“ je k dispozici na http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm .

[2] GS1 je nezisková organizace zaměřená na vývoj a implementaci globálních standardů a řešení na podporu efektivity dodavatelského řetězce napříč různými sektory.

[3] Publikovaný materiál je také umístěn na internetové adrese Úřadu www.uoou.cz v rubrice Informace ze světa.

Přetisk (s. 3336 – 3359)

# Rámec pro posouzení dopadů na ochranu soukromí a údajů pro aplikace RFID

# 11. února 2011

# OBSAH

# 1. Úvod

Evropská komise (dále jen „Komise“) vydala doporučení ze dne 12. května 2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence (dále jen „doporučení RFID“). Komise v tomto doporučení stanovila požadavek, aby pracovní skupina pro ochranu údajů zřízená podle článku 29 schválila rámec zpracovaný odvětvím pro posouzení dopadů aplikací RFID na osobní údaje a soukromí. Tato posouzení se obecně uvádějí jako posouzení dopadů na ochranu soukromí nebo PIA (*privacy impact assessments*). Uvedený požadavek je řešen tímto rámcem posouzení dopadů aplikací RFID na ochranu soukromí (dále jen „rámec“).

Posuzování dopadů na ochranu soukromí pro aplikace RFID má řadu přínosů. Zahrnuje pomoc pro provozovatele aplikace RFID ve:

- stanovení a dodržování souladu s právními a správními předpisy o ochraně soukromí a údajů;
- řízení rizik pro jeho organizaci a pro uživatele aplikace RFID (týkající se jak dodržování ochrany soukromí a údajů, tak i z hlediska vnímání ze strany veřejnosti a důvěry spotřebitelů); a
- zajištění přínosů aplikací RFID pro veřejnost a současně hodnocení úspěchu v úsilí zaměřeném na ochranu soukromí při navrhování v raných fázích specifikace nebo v procesu vývoje.

Proces PIA je založen na přístupu řízení rizik ochrany soukromí a údajů, který je zaměřen hlavně na provádění doporučení RFID EU a je v souladu s právním rámcem a osvědčenými postupy EU.

Proces PIA je určen k tomu, aby provozovatelům aplikací RFID pomohl určit rizika ochrany soukromí spojená s aplikací RFID, posoudit jejich pravděpodobnost a dokumentovat kroky přijímané k řešení těchto rizik. Tyto případné dopady by se mohly značně lišit v závislosti na existenci nebo neexistenci zpracování osobních údajů pomocí aplikace RFID. Rámec PIA poskytuje provozovatelům aplikací RFID pokyny k metodám posuzování rizik, včetně odpovídajících opatření pro účinné, efektivní a přiměřené zmírnění jakéhokoli pravděpodobného dopadu na ochranu údajů nebo soukromí.

Rámec PIA je dostatečně obecný, aby byl použitelný pro všechny aplikace RFID a aby současně umožnil řešení zvláštností a specifik na odvětvové úrovni nebo na úrovni typu aplikace.

Rámec PIA je součástí rámce zajišťování dalších informací, správy údajů a provozních norem, který poskytuje dobré nástroje správy údajů pro RFID a jiné aplikace. Současný rámec by se mohl použít jako základ ke zpracování šablon pro posuzování dopadů na ochranu soukromí (PIA) vycházejících z odvětví, sektoru a/nebo aplikace. Podobně jako při provádění jakéhokoli teoretického dokumentu si může rámec PIA vyžadovat vysvětlení týkající se používání jeho pojmů a také pokyny k postupům, které by měly být založeny na praktických zkušenostech, jež mohou pomoci v jeho provádění.

## 1.1. Klíčové pojmy

V daném rámci se používá mnoho klíčových pojmů, které si zasluhují popis. ***RFID*** je technologie, která využívá elektromagnetické vlny ke komunikaci s etiketami RFID s možností čtení jedinečných identifikačních čísel etiket RFID nebo případně jiných informací, které jsou na nich uloženy. ***Etikety RFID*** jsou obecně malé a mohou mít mnoho forem, ale často jsou složeny z elektronické paměti, která je čitelná a případně zapsatelná, a z antény. ***Čtecí zařízení RFID*** se používají ke čtení informací na etiketách RFID.

Zpracování informací ***aplikací RFID*** vyvinuté vzájemnou součinností etiket RFID a čtecích zařízení RFID. Tyto aplikace jsou provozovány jedním nebo více ***provozovateli aplikací RFID*** a podporovány záložními systémy a síťovými komunikačními infrastrukturami. Pokud provozovatel aplikace RFID učiní rozhodnutí týkající se sběru nebo využívání osobních údajů, jeho úloha by mohla být podobná jako úloha správce údajů definovaná ve směrnici 95/46/ES a byla by popsána jako fyzická nebo právnická osoba, veřejný orgán, subjekt nebo jiná organizace, která sama nebo společně s jinými určuje účely a prostředky provozování aplikace RFID, jež má dopady, nebo osobní informace.

V souvislosti s technologií RFID se používají tyto pojmy:

- ***Posouzení dopadů na ochranu soukromí (PIA)*** je proces, kterým se vynakládá záměrné a soustavné úsilí zaměřené na posouzení dopadů konkrétní aplikace RFID na ochranu soukromí a údajů s cílem učinit příslušná opatření k zamezení nebo alespoň minimalizování těchto dopadů.
- ***Rámec*** určuje cíle posouzení dopadů aplikací RFID na ochranu soukromí, složky aplikací RFID, které je třeba během PIA vzít v úvahu a společnou strukturu a obsah zpráv o posouzení dopadů aplikace RFID na ochranu soukromí.
- ***Zpráva o posouzení dopadů na ochranu soukromí (PIA)*** je dokument vyplývající z procesu PIA, který je k dispozici příslušným orgánům. Informace o vlastnictví a informace citlivé z hlediska bezpečnosti lze ze zpráv o PIA odstranit dřív, než budou poskytnuty externě (např. příslušným orgánům), pokud nemají výslovně za následek dopady na ochranu soukromí a údajů. Způsob, jakým by se mělo zpřístupnit posouzení dopadů na ochranu soukromí (např. na žádost nebo bez ní), určí členské státy. Zejména lze vzít v úvahu používání zvláštních kategorií údajů a rovněž další faktory jako přítomnost inspektora ochrany údajů.
- ***Vzorová PIA*** lze vypracovat na základě rámce za účelem zajištění odvětvových formátů, formátů založených na aplikaci nebo jiných specifických formátů pro posouzení dopadů na ochranu soukromí a výsledných zpráv o PIA.

Tyto a další pojmy, jako je ***uživatel a fyzická osoba***, jsou pro účely tohoto rámce PIA popsány také v dodatku B: Glosář pojmů. Pojmy ze směrnice 95/46/ES týkající se ochrany údajů jsou začleněny odkazem.

Případné provádění PIA a podávání zpráv o něm doplňuje ostatní povinnosti, které provozovatelé aplikací RFID mohou mít podle příslušných platných právních a správních předpisů a jiných závazných dohod.

## 1.2. Vnitřní postupy

Provozovatelé aplikací RFID by měli mít vlastní vnitřní postupy na podporu provádění posuzování dopadů na ochranu soukromí, jako je:

- *Časové rozvržení procesu PIA*, aby byl dostatek času pro provedení všech potřebných úprav aplikace RFID a pro zpřístupnění zprávy o PIA příslušným orgánům nejpozději šest týdnů před jejím rozesláním.
- *Vnitřní přezkum procesu PIA (včetně počáteční analýzy) a zprávy o PIA* z hlediska souladu s ostatní dokumentací týkající se aplikace RFID, jako je dokumentace systému, dokumentace produktu a příklady balení produktu a zavedení etiket RFID. Vnitřní přezkum by měl poskytnout smyčku zpětné vazby za účelem řešení všech shromážděných dopadů po zavedení aplikace a uvedení v soulad s výsledky z předcházejících posouzení dopadů na ochranu soukromí (PIA).
- *Sestavení podpůrných artefaktů* (které mohou zahrnovat výsledky přezkumu bezpečnosti, návrhy kontrol a kopie oznámení) jako důkaz, že provozovatel aplikace RFID splnil všechny příslušné povinnosti.

- *Určení osob a/nebo funkcí v rámci organizace, které mají oprávnění přijímat příslušná opatření* během procesu PIA (např. uskutečnění počáteční analýzy PIA a vyhotovení zprávy o PIA, podpis zprávy o PIA, uchovávání příslušných dokumentů a rozdělení povinností pro tyto funkce).
- *Zajištění kritérií, jak hodnotit a dokumentovat, zda aplikace je připravena nebo není připravena pro zavedení* v souladu s rámcem a všemi příslušnými šablonami PIA.
- Je zaručeno *zvážení/identifikace zvláštních prvků, které by si vyžádaly novou nebo revidovanou zprávu o PIA.* Kritéria by měla zahrnovat: podstatné změny v aplikaci RFID, jako jsou věcné změny, které překročily rámec původních účelů (např. sekundární účely); druhy zpracovaných informací; využívání informací, které oslabují používané kontroly; nečekané narušení osobních údajů[1] s rozhodujícím dopadem, které nebylo součástí zbytkových rizik aplikace určených prvním posouzením dopadů na ochranu soukromí; stanovení doby pravidelného přezkumu; reakce na významnou nebo závažnou zpětnou vazbu nebo na dotazy vnitřních a vnějších zúčastněných stran; nebo značné změny v technologii s důsledky na ochranu soukromí a údajů pro předmětnou aplikaci RFID. Věcné změny, které by zúžily rozsah sběru nebo používání, by samy o sobě nevyvolaly potřebu revidovaného posouzení dopadů na ochranu soukromí (PIA). Během životnosti aplikace RFID by byla zaručena nová nebo revidovaná zpráva o posouzení dopadů na ochranu soukromí (PIA), změní-li se aplikace RFID v rozsahu popsaném v oddíle Počáteční analýza.
- *Konzultace zúčastněných stran.* Stanoviska a zpětná vazba od příslušných zúčastněných stran týkající se posuzované aplikace RFID by se měly náležitě zohlednit jako součást přezkumu potenciálních otázek a problému PIA. Konzultace by měly být přiměřené míře, rozsahu, povaze a úrovni aplikace RFID. V rámci společností je pro fyzické osoby stanovena odpovědnost za dohled nad ochranou soukromí v organizaci nebo v útvaru a za její zajištění. Tyto fyzické osoby jsou důležitými účastníky v procesu PIA, neboť jsou zapojeny do konkrétních aplikací RFID nebo dohledu nad nimi. Zaměstnanci se znalostmi technických, marketingových a jiných oborů mohou být rovněž potřebnými účastníky v procesu v závislosti na povaze aplikace RFID a jejich vztahu k ní. Provozovatelé RFID mohou mít konzultační mechanismy, s jejichž pomocí mohou externí zúčastněné strany, ať už fyzické osoby, organizace nebo orgány, vzájemné spolupracovat a zajišťovat zpětnou vazbu. Je-li to vhodné, provozovatel RFID by měl použít konzultační mechanismy k získání vstupu od skupin představujících fyzické osoby, jejichž soukromí bude přímo ovlivněno návrhy, např. zaměstnanci a zákazníci provozovatele RFID.

## 2. Proces posuzování dopadů na ochranu soukromí (PIA)

Účelem rámce je poskytnout návod provozovatelům aplikací RFID k provádění PIA pro konkrétní aplikace RFID, jak k tomu vyzývá doporučení, a vymezit společnou organizační strukturu a kategorie obsahu zpráv o PIA, v nichž je třeba dokumentovat výsledky z těchto PIA. Kromě toho, jelikož mnozí provozovatelé aplikací RFID v konkrétních odvětvích mohou uvažovat o stejných nebo podobných aplikacích RFID, rámec poskytuje základ pro zpracování vzorových PIA pro konkrétní aplikace nebo průmyslové sektory. Vzorová PIA mohou těmto sektorům efektivněji pomoci v provádění PIA a zpracování výsledných zpráv o PIA pro tyto podobné aplikace RFID[2]. Protože společné aplikace RFID mohou být nabízeny v řadě členských států, rámec je určen k harmonizaci požadavků na provozovatele aplikací

[1] V tomto případě je použitelná definice uvedená ve směrnici 2009/136/ES, kterou se mění směrnice 2002/58, viz str. 29 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

[2] Měla by se prozkoumat koncepce vzájemného nebo opakovaného uznávání mezi subjekty a sektory pro rozšíření aplikací RFID prověřených dřív.

RFID v souladu s místními právními a správními předpisy, osvědčenými postupy a jinými závaznými dohodami.

Rámec se zabývá procesem posuzování dopadů aplikací RFID na ochranu soukromí před zavedením a specifikuje rozsah výsledných zpráv o PIA.[3]

Provozovatelé aplikací RFID musí zpracovat posouzení dopadů na ochranu soukromí pro každou aplikaci RFID, kterou provozují. Zavedou-li několik souvisejících aplikací RFID (eventuálně ve stejném kontextu nebo ve stejných prostorech), mohou sestavit jednu zprávu o PIA, pokud hranice nebo rozdíly aplikací jsou výslovně popsány ve zprávě o PIA. Jestliže provozovatelé aplikací RFID opětovně použijí jednu aplikaci RFID stejným způsobem pro mnohočetné produkty, služby nebo procesy, mohou sestavit jednu zprávu o PIA pro všechny produkty, služby nebo procesy, které jsou podobné (například výrobce automobilů, který zavede tytéž mechanismy proti krádežím ve všech vozidlech a za stejných provozních podmínek). Případné provádění PIA a podávání zpráv o nich doplňuje ostatní povinnosti, které provozovatelé aplikací RFID mohou mít podle příslušných konkrétních zákonů, nařízení a jiných závazných dohod.

Proces PIA má dvě fáze:

1. **Fáze počáteční analýzy:** provozovatel aplikace RFID bude postupovat podle kroků popsaných v tomto oddíle s cílem určit:

   a) zda se vyžaduje posouzení dopadů jeho aplikace RFID na ochranu soukromí nebo ne; a

   b) zda je zaručeno posouzení dopadů na ochranu soukromí v plném nebo malém rozsahu.

2. **Fáze posouzení rizik:** popisuje kritéria a prvky posouzení dopadů na ochranu soukromí v plném nebo malém rozsahu.

## 2.1. Fáze počáteční analýzy

Jako nezbytný předpoklad posouzení dopadů na ochranu soukromí pro konkrétní aplikaci musí každá organizace pochopit, jak se má tento proces uskutečnit na základě povahy a citlivosti údajů, kterými se zabývá, povahy a druhu zpracování nebo správy informací, které používá, a druhu předmětné aplikace RFID. Těm organizacím, které už mají zavedeny procesy posouzení rizik ochrany soukromí pro jiné aplikace, by klasifikační kritéria a kroky procesu měly pomoci zmapovat jejich existující procesy PIA podle tohoto rámce.

Aby provozovatel aplikace RFID uskutečnil počáteční posouzení, musí projít rozhodovacím stromem znázorněným na obrázku 1. To provozovateli aplikace RFID pomůže určit, zda a v jaké míře je posouzení dopadů na ochranu soukromí pro danou aplikaci RFID nutné.

Výsledná úroveň ve fázi počáteční analýzy pomáhá určit úroveň podrobností potřebnou v posouzení rizik (např. zda má být PIA v plném nebo malém rozsahu).

Tato počáteční analýza musí být dokumentována a dána k dispozici orgánům pro ochranu údajů na jejich žádost. Návod na dokumentaci viz příloha I.

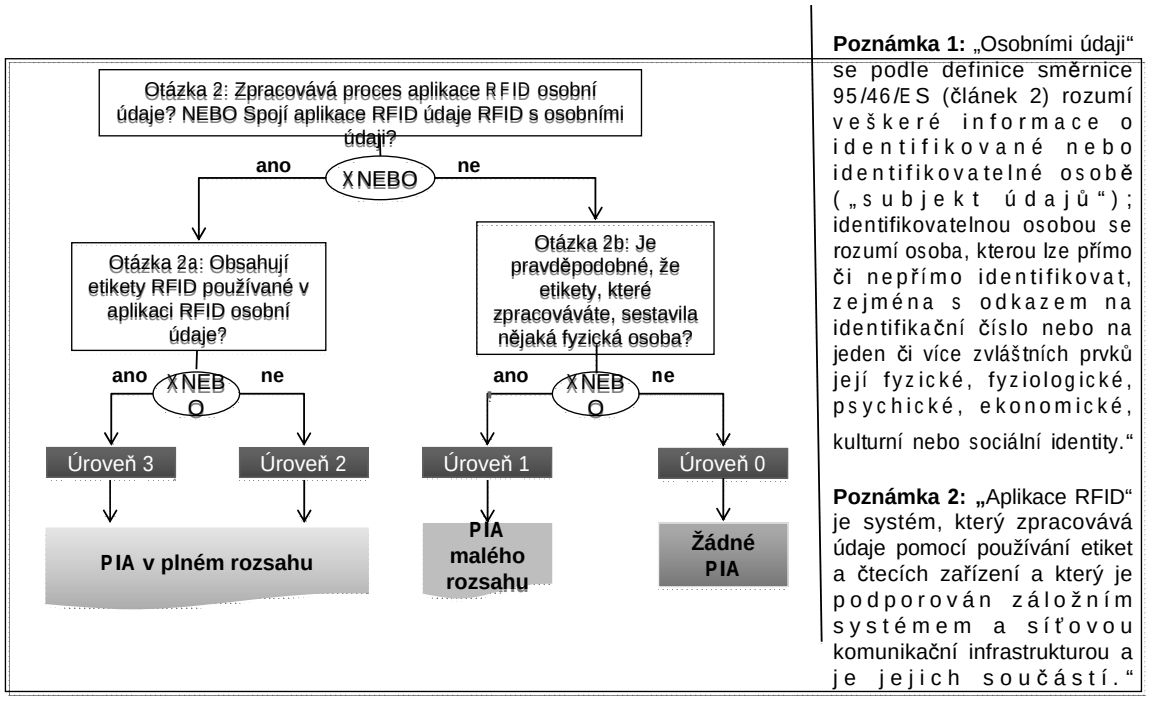
[3] Bod 5 písm. a) doporučení Evropské komise z května 2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence, K(2009) 3200 v konečném znění.

## Posouzení dopadů na ochranu soukromí (PIA) v plném rozsahu

Posouzení dopadů na ochranu soukromí (PIA) v plném rozsahu je nutné u aplikací, které jsou ve fáze počáteční analýzy v oddíle 2.1 určené jako úroveň 2 nebo úroveň 3. Příklady aplikací, u nichž je nutné posouzení dopadů na ochranu soukromí v plném rozsahu, zahrnují aplikace, které zpracovávají osobní informace (úroveň 2), nebo když etiketa RFID obsahuje osobní údaje (úroveň 3). Ačkoli jak úroveň 2, tak i úroveň 3, vedou k posouzení dopadů na ochranu soukromí v plném rozsahu, určují různá riziková prostředí a jako takové budou mít rozdílné strategie zmírnění rizik. Například aplikace úrovně 2 mohou mít kontroly na ochranu záložních údajů, zatímco aplikace úrovně 3 mohou mít kontroly na ochranu jak záložních údajů, tak i údajů etiket. Odvětví může tyto úrovně dále propracovat a na základě dalších zkušenosti posoudit, jak ovlivňují proces PIA. Protože aplikace zpracovává osobní údaje, je nutné velmi podrobné posouzení rizik (v plném rozsahu), aby se zajistilo, že zmírnění rizik bude dobře zpracováno. Provozovateli aplikace RFID to pomůže určit příslušná rizika a připravit odpovídající kontroly. Provozovatelé by měli v této souvislosti rovněž zvážit, zda je pravděpodobné, že použití informací z etiket RFID překročí rámec původního účelu nebo kontextu chápaného fyzickou osobou, zejména když by mohly být použity ke zpracování osobních údajů nebo propojení s nimi, a zda je zaručena nová analýza PIA, nebo by měly být použity jiné kontroly zmírnění rizik.

## Posouzení dopadů na ochranu soukromí (PIA) v malém rozsahu

Posouzení dopadů na ochranu soukromí (PIA) v malém rozsahu dodržuje stejný postup jako PIA v plném rozsahu, ale s ohledem na nižší profil rizika je PIA malého rozsahu více omezeno co do rámce a úrovně podrobností v šetření i ve zprávě než PIA v plném rozsahu. Posouzení dopadů na ochranu soukromí v malém rozsahu jsou důležitá pro aplikace úrovně 1. Zatímco PIA v malém rozsahu dodržuje podobný postup jako PIA v plném rozsahu, neboť související rizika aplikace úrovně 1 jsou nižší než úrovně 2 nebo 3, potřebné kontroly a odpovídající dokumentace ve zprávě o PIA jsou zjednodušené.




**Poznámka 1:** „Osobními údaji" se podle definice směrnice 95/46/ES (článek 2) 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."

**Poznámka 2: „**Aplikace RFID" je systém, který zpracovává údaje pomocí používání etiket a čtecích zařízení a který je podporován záložním systémem a síťovou komunikační infrastrukturou a je jejich součástí."

**Obrázek 1: Rozhodovací strom, zda se má uskutečnit PIA a na jaké úrovni podrobností**

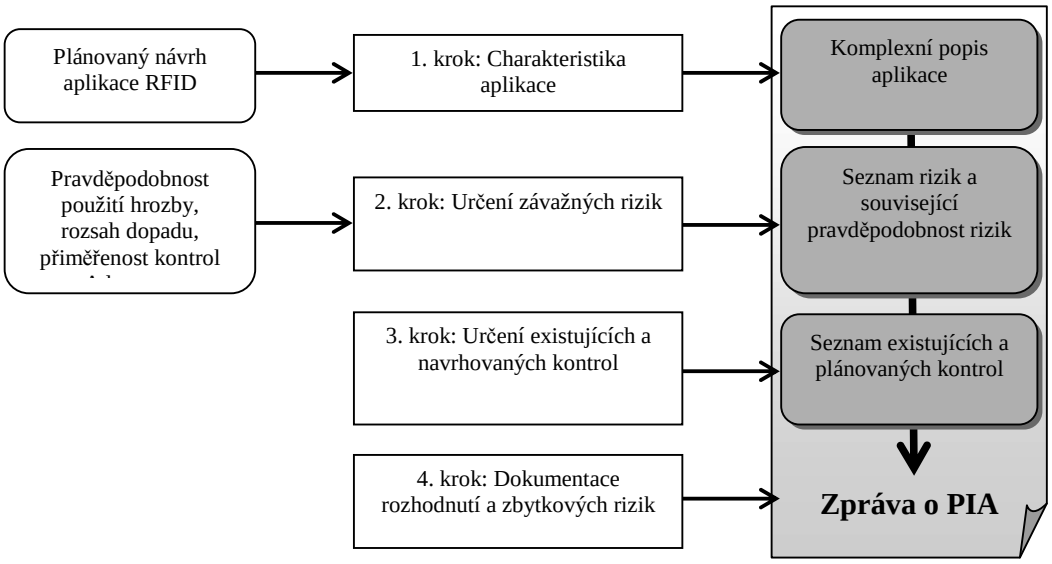
## 2.2. Fáze posouzení rizik:

Cílem posouzení rizik je určit rizika ochrany soukromí způsobených aplikací RFID – v ideálním případě v raném stadiu vývoje systému – a dokumentovat, jak jsou tato rizika *aktivně* zmírňována pomocí technických a organizačních kontrol. PIA takto hraje důležitou úlohu v dodržování ochrany soukromí a právních požadavků na ni (směrnice 95/46) a je opatřením, kterým posuzujeme efektivnost postupů zmírňování rizika. Aby se ušetřil čas a náklady, doporučuje se důkladně projít touto fází posouzení rizika dřív, než budou přijata konečná rozhodnutí o architektuře aplikace RFID, aby technické strategie zmírňování rizika ochrany soukromí mohly být začleněny do návrhu systému a aby nemusely být později dodatečně doplňovány.

V procesu posuzování rizika se zpravidla zvažují především rizika aplikace RFID z hlediska pravděpodobnosti jejich výskytu a rozsahu jejich důsledků. Provozovatelům aplikací RFID se doporučuje využít cíle ochrany soukromí ze směrnice EU jako výchozí bod pro jejich posouzení rizik (viz příloha II). Rizika ochrany soukromí mohou být vysoká, neboť provádění aplikací RFID by mohlo být vystaveno zlovolným útokům, nebo proto, že neexistují organizační kontroly či kontroly prostředí soukromí. Rizika soukromí mohou být rovněž malá, jednoduše z toho důvodu, že jejich výskyt není v daném prostředí nebo organizaci pravděpodobný, nebo proto, že aplikace RFID je už pro ochranu soukromí velmi příznivě konfigurována. Proces PIA se snaží vzít v úvahu veškerá potenciální rizika a pak zvažovat jejich rozsah, pravděpodobnost a možné zmírnění. Výsledkem tohoto zvažování je určení těch rizik ochrany soukromí, která jsou už skutečně důležitá pro zavedení RFID v organizaci a která musí být zmírněna pomocí účinných kontrol.

Proces PIA (znázorněný na obrázku 2) vyžaduje, aby každý provozovatel aplikace RFID:

1. popsal aplikaci RFID;
2. určil a uvedl, jak by posuzovaná aplikace RFID mohla ohrozit ochranu soukromí, a odhadl rozsah a pravděpodobnost těchto rizik;
3. dokumentoval současné a navržené technické a organizační kontroly za účelem zmírnění určených rizik; a
4. dokumentoval rozhodnutí (výsledky analýzy) týkající se aplikace.



**1. krok: Charakteristika aplikace**

Charakteristika aplikace by měla poskytnout komplexní a úplný obraz aplikace, jejího okolí a hranic systému. Popsán je návrh aplikace, její bezprostřední rozhraní s jinými systémy a toky informací. Diagramy toků údajů, které znázorňují zpracování primárních a sekundárních údajů, se doporučují pro zviditelnění toků informací. Struktury údajů musí být také dokumentovány, aby mohla být analyzována potenciální spojení. Příloha I shrnuje prvky, které charakterizují aplikaci RFID pro účely provedení PIA.

Kromě toho se doporučují informace týkající se provozního a strategického prostředí aplikace. Může to zahrnovat bezprostřední a dlouhodobé poslání systému, strany zúčastněné na sběru informací, funkční požadavky, všechny potenciální uživatele a popis architektury aplikace RFID a toků údajů (zejména rozhraní s vnějšími systémy, které mohou zpracovávat osobní údaje).

**2. krok: Určení rizik**

Cílem tohoto kroku je určit podmínky, které mohou ohrozit nebo vystavit nebezpečí osobní údaje, s využitím směrnice EU jako návodu pro důležité charakteristické znaky cílů ochrany soukromí. Rizika se mohou vztahovat na složky aplikací RFID, jejich provozovatele (sběr, ukládání a infrastruktura zpracování) a sdílení údajů a prostředí zpracování, v němž jsou začleněny.

Seznam potenciálních rizik ochrany soukromí je uveden v příloze III. Slouží jako návod pro soustavné určování potenciálních rizik, které ohrožují cíle směrnice EU (příloha II).

Kromě určování rizik vyžaduje PIA jejich relativní kvantifikaci. Provozovatel aplikace RFID by měl tak, jak je to uvedeno v zásadách proporcionality a za přiměřených podmínek, zvážit *pravděpodobnost* výskytu rizik. Rizika se mohou vyskytnout v rámci dané konkrétní aplikace RFID i mimo ni, přichází-li to v úvahu. Tato rizika lze odvodit z pravděpodobného použití i z možného zneužití informací, zejména pokud etikety RFID používané v rámci aplikace RFID zůstanou funkční, když už jsou ve vlastnictví fyzických osob.

Posouzení rizik si vyžaduje hodnocení příslušných rizik z hlediska ochrany soukromí; provozovatel RFID by měl zvážit:

1. závažnost rizika a pravděpodobnost jeho výskytu;
2. rozsah dopadu, pokud by se riziko vyskytlo.

Výslednou úroveň rizika pak lze klasifikovat jako nízkou, střední nebo vysokou.

Riziko, které vyvolalo hlavní předmět diskuse, spočívá v tom, že etikety RFID by bylo možné využít pro vytváření profilu a/nebo sledování fyzických osob. V tomto případě by informace etikety RFID – zejména jejího identifikátoru (identifikátorů) – byly využity k opětovné identifikaci konkrétní fyzické osoby. Maloobchodníci, kteří předali etikety RFID spotřebitelům, aniž by je automaticky deaktivovali nebo odstranili při výstupní kontrole, *mohou* neúmyslně toto riziko umožnit. Klíčovou otázkou je však to, zda uvedené riziko je pravděpodobné a zda se skutečně projeví jako *podstatné* nebo ne. Podle bodu 11 doporučení RFID by měli maloobchodníci v okamžiku prodeje deaktivovat nebo odstranit etikety používané v jejich aplikaci, ledaže spotřebitelé poté, co byli informováni o politice v souladu s tímto rámcem,

udělí souhlas se zachováním funkčnosti etiket. Maloobchodníci nemusí deaktivovat nebo odstranit etikety, pokud zpráva o PIA dospěje k závěru, že etikety, které jsou používány v maloobchodní aplikaci a které by zůstaly po prodeji funkční, nepředstavují pravděpodobnou hrozbu pro soukromí nebo ochranu osobních údajů podle ustanovení bodu 12 téhož doporučení. Deaktivací etiket se rozumí proces, který zastaví vzájemnou součinnost etikety s jejím okolím, jež nevyžaduje aktivní účast spotřebitele.

Vzory specifické pro určité odvětví, které se časem zpracují na základě tohoto rámce a pro použití v různých odvětvích, mohou určování rizik uvádět podrobněji.

**3. krok: Určování a doporučení kontrol**

Cílem tohoto kroku je analyzovat kontroly, které byly zavedeny nebo jsou plánovány pro zavedení, aby byla minimalizována, zmírněna nebo odstraněna určená rizika pro soukromí.

Kontroly jsou buď technické, nebo netechnické povahy. Technické kontroly jsou začleněny do aplikace pomocí výběrů architektury nebo technicky vymahatelných politik, např. standardní nastavení, mechanismy ověřování a metody šifrování. Na druhé straně netechnické kontroly jsou kontroly řízení a provozní kontroly, např. provozní postupy. Kontroly lze klasifikovat jako preventivní nebo detekční. První zabraňují snahám o porušení a druhé upozorňují na porušení nebo na pokusy o porušení.

Mohou existovat rovněž „přirozené“ kontroly vytvořené prostředím. Například nejsou-li nainstalována žádná čtecí zařízení, která by mohla provádět sledování předmětů nebo fyzických osob (tj. jelikož pro to není obchodní důvod), pak přirozeně neexistuje ani (pravděpodobné) riziko.

Určená rizika a s nimi spojené úrovně rizik by měly být vodítkem pro rozhodnutí, které z určených kontrol jsou důležité a tudíž musí být realizovány. Dokumentace PIA by měla vysvětlit, jak kontroly souvisí s konkrétními riziky a měla by podrobněji rozvést, jak toto zmírnění rizika povede k jeho přijatelné úrovni.

Příklady kontrol jsou uvedeny v příloze IV.

**4. krok: Dokumentace rozhodnutí a zbytkových rizik**

Jakmile je posouzení rizik dokončeno, konečné rozhodnutí o aplikaci by mělo být dokumentováno ve zprávě o PIA spolu se všemi dalšími poznámkami týkajícími se rizik, kontrol a zbytkových rizik.

- Aplikace RFID je schválená pro činnost, jakmile je dokončen proces PIA se souvisejícími určenými a náležitě zmírněnými riziky, aby se zajistilo, že nezůstanou žádná závažná zbytková rizika, s cílem splnit požadavky souladu, a s příslušnými vnitřními přezkumy a schváleními.

- Není-li aplikace RFID schválená pro činnost v jejím existujícím stavu, další zvažování si vyžádá zpracování plánu konkrétních nápravných opatření a musí být provedeno nové posouzení dopadů na ochranu soukromí, aby se určilo, zda aplikace dosáhla stavu schopného schválení.

Rozhodnutí by mělo být spojeno s těmito informacemi:

- jméno osoby, která podepisuje rozhodnutí;
- titul osoby;
- datum rozhodnutí.

**Zpráva o posouzení dopadů na ochranu soukromí (PIA)**

Posouzení dopadů na ochranu soukromí jsou vnitřní procesy obsahující citlivé informace, které mohou mít důsledky pro bezpečnost, a také potenciálně důvěrné informace a informace společnosti o vlastnictví týkající se produktů a procesů. To znamená, že zpráva o PIA by měla zpravidla zahrnovat:

1. popis aplikace RFID tak, jak je uveden v PŘÍLOZE I;

2. dokumentaci čtyř kroků popsaných výše.

Podepsaná zpráva o PIA, která obsahuje schválené rozhodnutí, by měla být poskytnuta určenému pracovníkovi společnosti odpovídajícímu za bezpečnost osobních údajů / ochranu v souladu s vnitřními postupy provozovatele aplikace RFID. Tato zpráva se poskytuje správcům údajů, aniž jsou dotčeny povinnosti stanovené ve směrnici 95/46/ES, zejména samostatná povinnost zaslat oznámení příslušnému orgánu tak, jak je to popsáno v oddíle IX směrnice 95/46/ES.

## 3. Závěrečné ustanovení

Rámec posuzování dopadů na ochranu soukromí (PIA) vstoupí v platnost nejpozději 6 měsíců po uveřejnění a schválení pracovní skupinou pro ochranu údajů zřízenou podle článku 29. Na aplikace RFID zavedené před vstupem rámce PIA v platnost se rámec PIA bude vztahovat, pouze pokud budou splněny podmínky pro dokumentování nového nebo revidovaného posouzení dopadů na ochranu soukromí v souladu s rámcem PIA.

## **PŘÍLOHA I –** *Charakteristika popisu aplikace RFID*

Provozovatel aplikace RFID případně zahrne do zprávy o PIA informace uvedené níže.

| | |
|---|---|
| **Provozovatel aplikace RFID** | • Název a sídlo právnické osoby<br>• Osoba nebo úřad odpovědné za včasnost PIA<br>• Kontaktní místo(a) a metoda šetření za účelem styku s provozovatelem |
| **Přehled o aplikacích RFID** | • Název aplikace RFID<br>• Účel(y) aplikace(í) RFID<br>• Základní scénáře používání aplikace RFID<br>• Složky aplikace RFID a použitá technologie (tj. frekvence apod.)<br>• Zeměpisný rozsah aplikace RFID<br>• Typy uživatelů/fyzických osob, na něž má aplikace RFID dopad<br>• Přístup a kontrola fyzických osob |
| **Číslo zprávy o PIA** | • Číslo verze zprávy o PIA (rozlišující nové PIA nebo pouze menší změny)<br>• Datum poslední změny provedené ve zprávě o PIA |
| **Zpracování údajů RFID** | • Seznam typů zpracovaných datových prvků<br>• Výskyt citlivých informací ve zpracovávaných údajích, např. zdravotní stav |
| **Ukládání údajů RFID** | • Seznam typů uložených datových prvků<br>• Doba uložení |
| **Interní přenos údajů RFID (je-li to vhodné)** | • Popis diagramů toků údajů vnitřních činností zahrnujících údaje RFID<br>• Účel(y) přenosu osobních údajů |
| **Externí přenos údajů RFID (je-li to vhodné)** | • Typ příjemce(ů) údajů<br>• Účel(y) přenosu nebo přístupu obecně<br>• Zjištěné a/nebo zjistitelné osobní údaje (úroveň osobních údajů) zahrnutých do přenosu<br>• Přenosy mimo Evropský hospodářský prostor (EHP) |

## **PŘÍLOHA II –** *Cíle ochrany soukromí*

V současné době je do směrnice 95/46/ES zahrnuto 9 cílů ochrany soukromí. Proces PIA byl zpracován s přihlédnutím k těmto cílům a souvisejícím rizikům RFID. Tato příloha shrnuje uvedené cíle ochrany soukromí. Ačkoli všechny cíle jsou důležitými prvky souladu organizace, v mnoha případech bude v posuzované aplikaci RFID přicházet v úvahu pouze podskupina těchto požadavků.Úlohou těchto cílů je tedy spíše poskytnout informace pro vytvoření a zpracování procesu PIA než činnost jakéhokoli konkrétního posuzování dopadů na ochranu soukromí.

| **Popis cíle ochrany soukromí**<br>(převzato z příslušné směrnice (směrnic) EU o ochraně soukromí a aktualizováno; v daném případě směrnice 95/46/ES) | |
|---|---|
| Ochrana kvality osobních údajů | Vyhnutí se údajům a jejich minimalizace, specifikace a omezení účelu a kvalita údajů a transparentnost jsou klíčové cíle, které je nutné zajistit. |
| Legitimita zpracování osobních údajů | Legitimita zpracování osobních údajů musí být zajištěna zpracováním údajů na základě souhlasu, smlouvy, právního závazku apod. |
| Legitimita zpracování *citlivých* osobních údajů | Legitimita zpracování citlivých osobních údajů musí být zajištěna zpracováním údajů na základě výslovného souhlasu, zvláštního právního základu apod. |
| Soulad s právem subjektu údajů na informovanost | Musí se zajistit, aby subjekt údajů byl včas informován o sběru jeho údajů |
| Soulad s právem subjektu údajů na přístup k údajům a jejich opravu a vymazání | Musí se zajistit, aby přání subjektu údajů mít přístup ke svým údajům, opravit je, vymazat a zablokovat, bylo včas splněno. |
| Soulad s právem subjektu údajů na vznesení námitek | Musí se zajistit, aby údaje subjektu údajů nebyly dál zpracovávány, má-li proti tomu námitky. Musí být zajištěna zejména transparentnost automatických rozhodnutí ve vztahu k fyzickým osobám. |
| Ochrana důvěrnosti a bezpečnosti zpracování | Zamezení neoprávněnému přístupu, vedení protokolu o zpracování údajů, bezpečnost sítě a přenosu a zamezení náhodné ztrátě údajů jsou klíčové cíle, které musí být zajištěny. |
| Soulad s požadavky oznamování | Oznámení o zpracování údajů, kontrola souladu předem a dokumentace jsou klíčové cíle, které musí být zajištěny. |
| Soulad s požadavky na uchovávání údajů | Údaje by se měly uchovávat po minimální dobu v souladu s účelem uchovávání nebo jinými právními požadavky. |

## **PŘÍLOHA III –** *Rizika ochrany soukromí*

Tento oddíl uvádí seznam případných rizik ochrany soukromí týkajících se používání posuzované aplikace RFID. Doporučuje se, aby – zejména u PIA v plném rozsahu – byla soustavně určována rizika pomocí standardních postupů posuzování rizik, které by zahrnovalo hrozby pro aplikaci RFID a její zranitelnost.

Níže uvedená tabulka uvádí příklady rizik, které mohou ovlivnit schopnost subjektu plnit cíle ochrany soukromí popsané v příloze II. Provozovatelé aplikací RFID mohou použít tento seznam jako výchozí bod; ne všechna tato rizika se však mohou vztahovat na veškeré aplikace RFID. Provozovatelé RFID by se měli jednou nebo více kontrolami ujistit, že každé určené riziko bylo náležitě zmírněno z hlediska pravděpodobnosti jeho výskytu a rozsahu dopadu. Provozovatelé aplikací RFID budou možná muset spojit kontroly nebo rozšířit existující kontroly na základě zvláštních prvků, kromě jiného včetně používané technologie, povahy jejich provádění, typu informací a příslušných politik.

| Riziko ochrany soukromí | Popis a příklad |
|---|---|
| Nespecifikovaný a neomezený účel | Účel sběru údajů nebyl specifikován a dokumentován, nebo se využívá více údajů, než je nutné pro specifikovaný účel.<br><br>Příklad: Neexistuje dokumentace účelů, na které se používají údaje RFID, a/nebo využívání údajů RFID pro všechny druhy proveditelné analýzy. |
| Sběr, který překračuje účel | Údaje se sbírají v identifikovatelné formě, která překračuje rámec rozsahu specifikovaného v účelu.<br><br>Příklad: Informace o platebních kartách RFID se používají nejenom za účelem zpracování transakcí, ale také pro vytváření profilů fyzických osob. |
| Neúplné informace nebo nedostatek transparentnosti | Informace poskytnuté subjektu údajů o účelu a použití údajů nejsou úplné, zpracování údajů není uskutečněno transparentně, nebo informace nejsou poskytnuty včas.<br><br>Příklad: Informace RFID dostupné pro spotřebitele, které postrádají jasné informace o tom, jak se údaje RFID zpracovávají a používají, o totožnosti provozovatele nebo o právech uživatelů. |
| Spojení, které překračuje účel | Osobní údaje jsou spojovány v rozsahu, který není nutný ke splnění specifikovaného účelu.<br><br>Příklad: Informace platebních karet RFID se spojují s osobními údaji získanými od třetí strany. |
| Chybějící politiky nebo mechanismy pro vymazání | Údaje se uchovávají déle, než je to nutné ke splnění specifikovaného účelu.<br><br>Příklad: Osobní údaje se sbírají jako součást aplikace a ukládají se déle, než je to povoleno |

| | |
|---|---|
| | právními předpisy. |
| Zrušení výslovného souhlasu | Souhlas byl získán pod hrozbou znevýhodnění.<br><br>Příklad: Nelze vrátit/vyměnit/použít zákonné záruky na produkty, když je etiketa RFID deaktivována nebo odstraněna. |
| Tajný sběr údajů provozovatelem RFID | Některé údaje se tajně zaznamenávají, takže nejsou subjektu údajů známy, např. profily pohybu.<br><br>Příklad: Informace o spotřebiteli se načítají během chůze před obchody nebo v nákupním středisku a žádné logo nebo symbol jej neupozorňuje na čtení RFID. |
| Neschopnost poskytnout přístup | Neexistuje způsob, jak by subjekt údajů mohl dát podnět k opravě nebo vymazání údajů o sobě.<br><br>Příklad: Zaměstnavatel nemůže dát zaměstnanci úplný obraz o tom, co se o něm ukládá na základě přístupu RFID a zpracovávání údajů. |
| Zamezení námitkám | Neexistují technické nebo provozní prostředky k tomu, aby bylo možné vyhovět námitkám subjektu údajů.<br><br>Příklad: Návštěvník nemocnice se nemůže vyhnout čtení citlivých osobních informací na etiketách (tj. na lécích). |
| Nedostatek transparentnosti jednotlivých automatických rozhodnutí | Používají se jednotlivá automatická rozhodnutí na základě osobních aspektů , ale subjekty údajů nejsou informovány o logice rozhodování.<br><br>Příklad: Provozovatel RFID čte všechny etikety, které nosí fyzická osoba, aniž by to spotřebitelům oznámil, včetně etiket poskytnutých jiným subjektem, a určuje, jaký druh marketingového sdělení by měla fyzická osoba na základě etiket obdržet. |
| Nedostatečné řízení práv přístupu | Práva přístupu nejsou zrušena, když už nejsou nutná.<br><br>Příklad: Díky kartě RFID má bývalý praktikant přístup k částem podniku, ke kterým by ho neměl mít. |
| Nedostatečný mechanismus ověřování | Není zamezeno podezřelému množství pokusů o identifikaci a ověření.<br><br>Příklad: Osobní údaje obsažené na etiketách nejsou standardně chráněny heslem nebo jiným mechanismem ověření. |
| Neoprávněné zpracovávání údajů | Zpracování osobních údajů není založeno na souhlasu, smlouvě, právním závazku apod.<br><br>Příklad: Provozovatel RFID sdílí shromážděné informace s třetí stranou bez oznámení nebo |

| | |
|---|---|
| | souhlasu, jak je to jinak právně povoleno. |
| Nedostatečný mechanismus vedení protokolu | Zavedený mechanismus vedení protokolu není dostatečný. Nezaznamenává administrativní procesy.<br><br>Příklad: Nezaznamenává se, kdo měl přístup k údajům karty RFID zaměstnance. |
| Nekontrolovatelné shromažďování údajů z etiket RFID | Riziko, že etikety RFID by mohly být použity k pravidelnému vytváření profilu a/nebo sledování fyzických osob.<br><br>Příklad: Maloobchodník čte všechny etikety, které vidí. |

## **PŘÍLOHA IV –** *Seznam příkladů kontrol aplikací RFID a opatření ke zmírnění rizik*

**Tento oddíl uvádí seznam příkladů potenciálních kontrol, které mohou provozovateli aplikace RFID pomoci určit vhodné strategie ke zmírnění rizika.** Rizika určená jako důležitá pro provozovatele aplikace RFID ve 2. kroku procesu rizika PIA lze zmírnit pomocí jedné nebo několika strategií ke zmírnění rizik, z nichž některé jsou uvedeny v této příloze IV. Cílem je, aby provozovatel aplikace RFID určil a zavedl kontroly potřebné ke zmírnění závažných rizik ochrany soukromí tím, že projde procesem PIA.

Potenciální kontrolní mechanismy zahrnují:

- postupy správy aplikací RFID;
- přístup a kontrolu fyzických osob;
- opatření na ochranu systému (včetně bezpečnostních kontrol);
- ochranu etiket;
- opatření odpovědnosti.

Tyto postupy jsou doplňkové k existujícímu právnímu rámci ochrany údajů Evropské unie a nemají nahrazovat nebo měnit jeho oblast působnosti.

### Postupy správy aplikací RFID

Postupy správy mohou zahrnovat:

- postupy řízení provozovatelem aplikace RFID;
- nakládání s politikami pro údaje RFID a jejich odstranění;
- politiky týkající se zákonného zpracovávání osobních informací;
- ustanovení zavedená pro minimalizaci údajů v zacházení s údaji RFID, je-li to možné;
- zpracovávání nebo ukládání informací z etiket, které nepatří provozovateli RFID;
- postupy řízení bezpečnosti.

### Zajištění přístupu a kontroly fyzických osob

- poskytování informací o účelech zpracovávání a kategoriích příslušných osobních údajů;
- popis, jak vznést námitky proti zpracování osobních údajů nebo zrušit souhlas;
- stanovení postupu, jak požádat o opravu nebo vymazání neúplných nebo nepřesných osobních údajů.

## Ochrana systému

V tomto oddíle zprávy o PIA by měla být dokumentována také **ochrana systému** s ohledem na příslušnou ochranu soukromí a osobních údajů. Koncepce ochrany systému se vztahují na záložní systémy a komunikační infrastrukturu, pokud se týkají aplikace RFID. Používají-li se, mělo by se uznat, že záložní systémy jsou často složité a mohou podléhat vlastnímu posouzení dopadů na ochranu soukromí. Tato analýza se možná bude muset přezkoumat s cílem zajistit, že vezme v úvahu informace takové povahy, které používá aplikace RFID. Pokud takové posouzení dopadů na ochranu soukromí neexistuje, mělo by se přihlédnout k těmto složkám záložního systému:

- kontroly přístupu týkající se druhu osobních údajů a funkčnosti zavedených systémů;
- kontroly a politiky zavedené pro zajištění, že provozovatel nespojí osobní údaje v aplikaci RFID způsobem, který je v rozporu se zprávou o PIA;
- zda jsou zavedena příslušná opatření pro ochranu důvěrnosti, integrity a dostupnosti osobních údajů v systémech a v komunikační infrastruktuře;
- politiky pro uchovávání a vymazání osobních údajů;
- existence a provádění kontrol bezpečnosti informací, např.:
    - opatření, která řeší bezpečnost sítí a přenos údajů RFID;
    - opatření, která usnadňují dostupnost údajů RFID pomocí vhodného zálohování a obnovy.

## Ochrana etiket RFID

Měly by být uvedeny kontroly **ochrany etiket RFID** týkající se soukromí a osobních údajů. Jsou důležité zejména pro aplikace RFID, které používají etikety RFID obsahující osobní údaje.

Tyto kontroly ochrany zahrnují:

- kontrolu přístupu k funkčnosti a informacím, včetně ověření čtecích a zapisovacích zařízení a základních procesů, a oprávnění jednat na základě etikety RFID;
- metody pro zajištění/řešení důvěrnosti informací (např. pomocí šifrování celé etikety RFID nebo vybraných polí);
- metody pro zajištění/řešení integrity informací;
- uchovávání informací po počátečném sběru (např. doba uchovávání, postupy pro odstranění údajů na konci doby uchovávání nebo vymazání informací na etiketě RFID, postupy pro uchování nebo vymazání vybraných polí);
- porušení odolnosti samotné etikety RFID;
- deaktivaci nebo odstranění, je-li vyžadováno nebo jinak stanoveno.

Zmírnění rizik může zahrnovat kontroly založené na uživatelích, které řeší situace, kdy se může jednat o různé potřeby nebo citlivost týkající se ochrany soukromí. Deaktivace nebo odstranění jsou v současné době dvě nejběžnější formy zmírnění rizik konečného uživatele/spotřebitele. Mohou být za určitých okolností vyžadovány zákonem, jako součást analýzy PIA nebo jako volba spotřebitele po prodeji za účelem zvýšení důvěrnosti. Kromě toho doporučení ES o ochraně soukromí a údajů RFID pro aplikace RFID doporučuje určité metodiky a osvědčené postupy související s prováděním deaktivace nebo odstraňování v maloobchodě.[4]

## Opatření odpovědnosti

Tato opatření jsou určena k řešení procesní ochrany údajů v oblasti odpovědnosti. Pomocí těchto opatření se zvyšuje vnější povědomí o aplikacích RFID.

- Zajištění snadné dostupnosti komplexní **informační politiky**, která zahrnuje:
    - totožnost a adresu provozovatele aplikace RFID;
    - účel aplikace RFID;
    - typy údajů zpracovávaných aplikací RFID, zejména pokud se zpracovávají osobní údaje;
    - zda umístění etiket RFID bude monitorováno, když je bude mít v držení fyzická osoba;
    - případné pravděpodobné dopady na ochranu soukromí a údajů týkající se používání etiket RFID v aplikaci RFID a opatření, která jsou k dispozici pro zmírnění těchto dopadů.
- Zajištění stručných, přesných a snadno pochopitelných **oznámení** o výskytu čtecích zařízení RFID, které zahrnuje:
    - totožnost provozovatele aplikace RFID;
    - kontaktní místo pro fyzické osoby, kde získají informační politiku.
- Zaznamenání, zda a jak jsou k dispozici **mechanismy odškodnění:**
    - odpovědná právnická osoba (odpovědné právnické osoby) provozovatele aplikace RFID (může být jedna pro každou jurisdikci nebo provozní oblast);
    - kontaktní místo(a) určené osoby nebo úřadu odpovědných za přezkum posouzení a další vhodnosti technických a organizačních opatření k zajištění ochrany osobních údajů a soukromí;
    - metody šetření (např. metody, kterými lze kontaktovat provozovatele aplikace RFID za účelem položení otázek, předložení žádosti, podání stížnosti nebo výkonu práva);

[4] Bod 12/13 doporučení ES ze dne 12. května 2009. {SEK(2009) 585}: *Každá metoda deaktivace nebo odstranění by měla být provedena zdarma buď neprodleně, nebo později, aniž by byly omezeny či zrušeny právní povinností maloobchodníka nebo výrobce vůči spotřebiteli.*

- metody vznesení námitky proti zpracování, uplatnění práv přístupu k osobním údajům (včetně vymazání a opravy osobních údajů), zrušení souhlasu nebo změna kontrol a jiné možnosti týkající se zpracování osobních údajů, jsou-li vyžadovány nebo jinak stanoveny;

- jiné metody odškodnění, jsou-li vyžadovány nebo jinak stanoveny.

## Dodatek A: Odkazy

Tento oddíl uvádí odkazy na oficiální dokumenty, s jejichž pomocí byl rámec vypracován.

- „Doporučení Komise o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence“, Komise Evropských společenství, 12. května 2009, K(2009) 3200, k dispozici na http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

- „Doprovodný pracovní dokument útvarů Komise k doporučení Komise o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence“, shrnutí posouzení dopadů, Komise Evropských společenství, 12. května 2009, SEK(2009) 586, k dispozici na http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

- „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“, Úřední věstník Evropských společenství, 23. listopadu 1995, L 281/31, k dispozici na http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

- „Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)“, Úřední věstník Evropských společenství, 31. července 2002, L 201/37, k dispozici na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

- „Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele“, Úřední věstník Evropské unie, 18. prosince 2009, L 337/11, k dispozici na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

- „Stanovisko č. 4/2007 k pojmu osobní údaje“ pracovní skupiny pro ochranu údajů zřízené podle článku 29, 20. června 2007, 01248/07/EN WP 136, k dispozici na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

- „Příručka pro posuzování dopadů na ochranu soukromí“, k dispozici na http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

- „Stav provádění směrnice 95/46 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů", k dispozici na http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

- „Pracovní dokument o otázkách ochrany údajů týkajících se technologie RFID“, pracovní skupina pro ochranu údajů zřízená podle článku 29, 19. ledna 2005, 10107/05/EN WP 105, k dispozici na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

## Dodatek B: Glosář pojmů

V tomto rámci se používá řada termínů, které se týkají pojmů ochrany soukromí a údajů a aplikace technologie RFID v širších souvislostech. Pro účely tohoto rámce by se v souvislosti s ochranou soukromí a údajů měly používat definice stanovené ve směrnici 95/46/ES.

Technologie RFID a její aplikace se týkají tyto definice, které jsou relevantní pro rámec:

**Fyzická osoba.** Fyzická osoba, která je v součinnosti s jednou nebo více složkami aplikace RFID, nebo je do nich jinak zapojena (např. záložní systém, komunikační infrastruktura, etiketa RFID), ale která neprovozuje aplikaci RFID ani nevykonává jednu z jejich funkcí. Z tohoto hlediska se fyzická osoba odlišuje od uživatele. Fyzická osoba nemusí být přímo zapojena do funkce aplikace RFID – může například pouze vlastnit předmět s etiketou RFID.

**Bezpečnost informací.** Zachovávání důvěrnosti, integrity a dostupnosti informací.

**Monitorování.** Činnost vykonávaná za účelem zjištění, pozorování, reprodukování nebo zaznamenání místa, pohybu, činností nebo stavu fyzické osoby.

**Osobní údaje.** Veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjekt údajů“); identifikovatelnou osobou je 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.

**Aplikace RFID.** Aplikace, která zpracovává údaje pomocí etiket a čtecích zařízení a která je podporována záložním systémem a síťovou komunikační infrastrukturou.

**Provozovatel aplikace RFID.** Fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo jiný subjekt, který sám či společně s ostatními stanoví účel a způsoby provozování aplikace, včetně správců osobních údajů používajících aplikaci RFID.

**Identifikace na základě rádiové frekvence (RFID).** Využívání elektromagnetických vln nebo magnetického pole v části spektra rádiových frekvencí ke komunikaci s etiketou prostřednictvím různých modulačních a kódovacích systémů za účelem jednoznačného přečtení identity etikety rádiové frekvence nebo jiných údajů, které jsou na ní uloženy.

**Čtecí zařízení RFID.** Pevné nebo přenosné zařízení k zachycování a identifikaci údajů pomocí vysokofrekvenčních elektromagnetických vln nebo magnetického pole ke stimulaci a vyvolání odezvy modulovaných dat z etikety nebo skupiny etiket.

**Etiketa RFID nebo „etiketa“.** Zařízení RFID, které je schopné vytvářet rádiový signál, nebo zařízení RFID, jež opětovně spojuje, zpětně rozptyluje nebo odráží (podle druhu zařízení) a moduluje nosný signál přijatý ze čtecího nebo zapisovacího zařízení.

**Informace etikety RFID nebo informace na etiketě RFID.** Informace obsažené na etiketě RFID a předávané, když je etiketa RFID snímaná čtecím zařízením RFID.

**Uživatel.** Konkrétní uživatel aplikace RFID, tj. osoba (nebo jiný subjekt, např. právnická osoba), která je v přímé součinnosti s jednou nebo více složkami aplikace RFID (např.

záložní systém, komunikační infrastruktura, etiketa RFID) pro účely provozování aplikace RFID nebo vykonávání jedné z jejich funkcí.

**PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29**

**00664/11/CS**
**WP 181**

# Stanovisko č. 10/2011 k návrhu směrnice Evropského parlamentu a Rady o používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

**Přijato dne 5. dubna 2011**

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

Sekretariát zajišťuje ředitelství C (základní práva a občanství Unie) Evropské komise, generální ředitelství pro spravedlnost, B-1049 Brusel, Belgie, kancelář č. MO-59 06/036.

Internetové stránky: http://ec.europa.eu/justice/policies/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 článek 29 a čl. 30 odst. 1 písm. a) a čl. 30 odst. 3 uvedené směrnice, čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, s ohledem na svůj jednací řád,

přijala toto stanovisko.

**1. Úvod**

Dne 2. února 2011 Evropská komise zveřejnila návrh směrnice o používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Pracovní skupina vydala stanovisko k předchozímu návrhu EU o jmenné evidenci cestujících (návrh rámcového rozhodnutí Rady o používání jmenné evidence cestujících pro účely vynucování práva), který Komise předložila dne 6. listopadu 2007[1]. Pracovní skupina se již dříve v několika stanoviscích obšírně vyjadřovala k různým dohodám o jmenné evidenci cestujících mezi EU a třetími zeměmi a rovněž k přístupu Komise vymezenému ve sdělení ze dne 21. září 2010[2]. Kromě toho pracovní skupina znovu vyjádřila obavy ohledně záležitostí jmenné evidence cestujících v různých dopisech určených panu komisaři Barrotovi, paní komisařce Malmströmové, panu generálnímu řediteli Faullovi a výboru LIBE Evropského parlamentu.

Toto stanovisko je určeno těm, kdo se podílejí na diskusi a vývoji nejnovějšího návrhu, tedy Komisi, pracovní skupině Rady GENVAL a Evropskému parlamentu.

**2. Nezbytnost a proporcionalita**

K návrhu z roku 2011 je přiloženo posouzení dopadů, které má podrobněji zdůvodnit návrh a jeho ustanovení. Pracovní skupina se domnívá, že boj proti terorismu a organizované trestné činnosti je nezbytný a legitimní a že osobní údaje, zejména některé údaje o cestujících, by mohly být cenné při posuzování rizik a prevenci terorismu a organizované trestné činnosti a boji proti nim. V případě evropského systému jmenné evidence cestujících však musí být omezení základních práv a svobod řádně zdůvodněno a musí být jasně prokázána jeho nezbytnost, aby bylo možné nastolit správnou rovnováhu mezi požadavky na ochranu veřejné bezpečnosti a omezením práv na soukromí.

Pracovní skupina soustavně zpochybňuje nezbytnost a přiměřenost systémů jmenné evidence cestujících a činí tak i v případě návrhu z roku 2011. Třebaže oceňujeme, jak je posouzení dopadů podrobné, domníváme se, že neobsahuje patřičné hodnocení používání jmenné evidence cestujících a nijak neprokazuje, že to, co návrh obsahuje, je nezbytné. Návrh by měl jasně uvádět, zda cíl spočívá v boji proti závažné (nadnárodní) trestné činnosti, která zahrnuje i terorismus, nebo zda je cílem pouze boj proti terorismu a trestné činnosti, která s ním souvisí.
Kapitola 3.2 posouzení dopadů s názvem „Dodržování základních práv“ pouze uvádí, že byl použit kontrolní seznam základních práv, ale neobsahuje žádné další informace o tomto

[1] WP 145 – společné stanovisko s Pracovní skupinou pro policii a spravedlnost.
[2] Stanoviska pracovní skupiny WP 103 (Kanada), WP 138 (Spojené státy), WP 151 (Spojené státy – informace pro cestující) a WP 178 (globální přístup Komise).

posouzení, které by jeho závěry odůvodňovaly. Kromě toho tato kapitola obsahuje tautologické zdůvodnění zásahu do práv na soukromí podle článku 8 Evropské úmluvy o lidských právech a článků 7 a 8 Listiny základních práv Evropské unie. Právním předpokladem zásahu do těchto práv je, že je „nezbytný v zájmu národní bezpečnosti, veřejné bezpečnosti nebo hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných“ a je „nezbytný v demokratické společnosti“ a probíhá „při dodržení zásady proporcionality“. Skutečnost, že účelem návrhu je předcházet terorismu a závažné trestné činnosti, neznamená, že návrh tyto požadavky jednoznačně splňuje; nezbytnost a přiměřenost je stále třeba prokázat. Komise ve vlastním přehledu o systémech správy informací[3] uvádí:

> „Nutnost
> Zásah do práva jednotlivce na soukromí ze strany veřejného orgánu může být nutný v zájmu vnitrostátní bezpečnosti, veřejného pořádku nebo předcházení trestné činnosti. Judikatura Evropského soudního dvora pro lidská práva stanovuje tři podmínky, za kterých je takové omezení oprávněné: pokud je zákonné, sleduje legitimní cíl a je v demokratické společnosti nutné. Zásah do práva na soukromí je považován za nutný, pokud reaguje na naléhavou sociální potřebu, je přiměřený sledovanému cíli a důvody, kterými veřejný orgán zásah zdůvodňuje, jsou významné a dostatečné. V případě všech budoucích návrhů politik Komise posoudí očekávaný dopad konkrétní iniciativy na právo jednotlivce na soukromí a ochranu osobních údajů a vysvětlí, proč je takový dopad nutný a proč je navrhované řešení přiměřené legitimním cílům zachování vnitřní bezpečnosti v Evropské unii, předcházení trestné činnosti či řízení migrace.“

Pracovní skupina se nedomnívá, že Komise splnila své závazky, které učinila výše v souvislosti s návrhem EU o jmenné evidenci cestujících. Argumenty ohledně nutnosti a přiměřenosti mají řadu dalších aspektů; zabývá se jimi následující text.

### 2.1. Posílená bezpečnost

Návrh a posouzení dopadů uvádějí, že systém EU pro jmennou evidenci cestujících by zaručil bezpečnost a zabránil by mezerám vzniklým v důsledku zrušení kontrol na vnitřních hranicích na základě Schengenské úmluvy. Takový cíl by byl legitimní, pokud by byl řádně zdůvodněn, pracovní skupina však dosud nezaznamenala žádné uspokojivé důkazy o tom, že by zpracování údajů ze jmenné evidence cestujících ve všech členských státech zabránilo vzniku bezpečnostních mezer, jež vznikají v důsledku zpracování těchto údajů pouze v několika členských státech.

Na úrovni EU jsou již zavedeny systémy a nástroje, které vyvažují zrušení hraničních kontrol mezi zeměmi schengenského prostoru a vycházejí z tzv. schengenského acquis, a pokud tedy bezpečnostní mezery přetrvávají, měla by být prvním krokem analýza řádného fungování stávajících systémů.

---

[3] Přehled o správě informací v prostoru svobody, bezpečnosti a práva, KOM(2010) 385 v konečném znění.

### 2.2. Stávající systémy, nástroje a spolupráce

Přehled Komise o správě informací v prostoru svobody, bezpečnosti a práva nevyhodnotil účinnost různých stávajících systémů ani nezvážil, zda společně zajišťují vhodné nástroje pro boj proti terorismu a organizované trestné činnosti, a pokud nikoli, kde by mohly existovat mezery. Pracovní skupina má za to, že je nutné takovéto hodnocení provést, než budou uložena další obdobná opatření, jako např. systém EU pro jmennou evidenci cestujících. Návrh jmenné evidence cestujících povede k tomu, že se závazky dopravců budou překrývat, že budou shromažďovány údaje, které jsou již dostupné prostřednictvím jiných systémů, a představuje vážnou hrozbu rozšiřování funkcí na neplánované účely. Například směrnice API ukládá dopravcům povinnost předem předávat informace o cestujících a údaje nejsou používány pouze při hraničních kontrolách, ale lze je použít také pro účely vynucování práva. Navzdory tomu, že Komisi na tuto záležitost několikrát upozornila, pracovní skupina dosud nezaznamenala řádné vyhodnocení účinnosti směrnice API a jejího vnitrostátního provádění a pochybuje o tom, zda bude tato směrnice nadále potřeba, pokud bude v celé EU zaveden systém jmenné evidence cestujících.

Pracovní skupina klade otázku, zda veškeré formy policejní a soudní spolupráce, které jsou zavedeny v EU a mají bránit trestné činnosti a stíhat ji (zahrnují i boj proti terorismu a závažné trestné činnosti), nejsou pro účel, jemuž má sloužit návrh EU týkající se jmenné evidence cestujících, odpovídajícími nástroji. V posouzení dopadů není tato analýza provedena.

Pracovní skupina uznává, že některé členské státy, které nepatří do schengenského prostoru, nemohou některé zavedené nástroje a systémy používat, což může mít dopad na ověření potřebnosti pro tyto země. Uvedené členské státy však mohou uplatňovat směrnici API, což také činí, a mělo by být zváženo, zda by nezbytné informace pro dané účely nebylo ve skutečnosti možné získat lepším využitím stávajících systémů a zlepšenou spoluprácí mezi těmito a ostatními členskými státy. Rovněž je třeba poznamenat, že skutečnost, že by údaje ze jmenné evidence cestujících byly použity jako zpravodajský nástroj, jak uvádí posouzení dopadů, rovněž zvyšuje úroveň požadavků na opatření na ochranu údajů.

### 2.3. Přiměřenost

Podle návrhu bude shromažďováno značné množství osobních informací o všech cestujících, kteří přilétají do EU a odlétají z ní, bez ohledu na to, zda se jedná o podezřelé osoby, či nikoli. Shromažďování a zpracování údajů ze jmenné evidence cestujících pro účely boje proti terorismu a závažné trestné činnosti by nemělo umožnit hromadné sledování všech cestujících a dohled nad nimi. Pracovní skupina se domnívá, že návrh shromažďovat a uchovávat údaje o všech cestujících na všech letech je nepřiměřený, a tudíž není v souladu s článkem 8 Listiny základních práv. Jak bylo zmíněno výše, posouzení dopadů neobsahuje v tomto ohledu přesvědčivé důkazy. Návrhy na úrovni EU by měly být konkrétní a cílené a měly by řešit určitou otázku a v této souvislosti by měl každý návrh klást důraz na rizika, která představuje terorismus a závažná trestná činnost.

Pracovní skupina má vážné pochybnosti o přiměřenosti systematického vyhodnocování všech cestujících podle určitých předem stanovených kritérií a neupřesněných „příslušných databází“. Není jasné, jak mají být tato předem stanovená kritéria a příslušné databáze definovány, zda budou údaje ze jmenné evidence cestujících použity k vytváření či aktualizaci kritérií a do jaké míry budou všechny vyhovující kombinace automaticky podrobeny

dodatečnému šetření. Pracovní skupina by rovněž ráda připomněla, že v některých členských státech jsou obdobné metody dohledu výhradně ústavní, a tudíž jsou policii k dispozici na základě soudního povolení a za určitých okolností, např. při konkrétní hrozbě. Navrhovaný systém jmenné evidence cestujících by z této mimořádné metody učinil běžný nástroj policejní práce.

Zavedená opatření, která nemohou zajistit ochranu práv a svobod cestujících, jsou přiměřená pouze tehdy, jsou-li zaváděna jako přechodná opatření při konkrétní hrozbě, což není případ tohoto návrhu. Narušení soukromí cestujících musí být úměrné přínosům pro boj proti terorismu a závažné trestné činnosti. Pracovní skupina dosud neobdržela žádné statistiky, z nichž by byl patrný poměr mezi počtem nevinných cestujících, o nichž byly shromážděny údaje ze jmenné evidence cestujících, a výsledky vynucování práva, které z těchto údajů ze jmenné evidence cestujících vzešly.

Souhrnně lze konstatovat, že pracovní skupina má stále za to, že nebyla prokázána potřebnost systému a že navrhovaná opatření nejsou v souladu se zásadou proporcionality. Navzdory tomu se pracovní skupina domnívá, že je konstruktivní vyjádřit se také k dalším aspektům navrhované směrnice, které jsou popsány níže.

**3. Účely**

Navrhovaná směrnice stanoví dva obecné účely zpracování se čtyřmi konkrétními činnostmi. Údaje ze jmenné evidence cestujících lze zpracovat pouze za účelem:

– prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti posuzováním cestujících před příletem nebo odletem prostřednictvím jejich porovnání s příslušnými databázemi (účel 1, činnost 1) a reakcí na žádosti příslušných orgánů v konkrétních případech (účel 1, činnost 2), a

– prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné nadnárodní trestné činnosti posuzováním cestujících před příletem nebo odletem podle stanovených kritérií (účel 2, činnost 3) a analýzou údajů ze jmenné evidence cestujících s cílem aktualizovat kritéria nebo vytvořit kritéria nová (účel 2, činnost 4).

Není jasné, co tyto účely obnášejí v praxi. Účel 1, činnost 1 zřejmě znamená porovnávání se seznamy podezřelých, s databází SIS a jinými databázemi EU a vnitrostátními databázemi. Účel 1, činnost 2 zřejmě znamená sdílení informací o jednotlivých případech na konkrétní žádost. Účel 2, činnost 3 podle všeho znamená porovnávání údajů ze jmenné evidence cestujících s profily u konkrétních trestných činů; a účel 2, činnost 4 podle všeho znamená používání údajů ze jmenné evidence cestujících k vývoji těchto profilů.

Základní zásada ochrany údajů spočívá v tom, že tyto účely a činnosti jsou jednoznačně definovány. Rovněž by měly být konkrétněji definovány „příslušné databáze“, případně tím, že budou rovněž doplněny do seznamu příslušných orgánů, který bude muset každý členský stát poskytnout Komisi. V každém případě by měly být použity databáze vytvořené pro tytéž účely, totiž pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Kromě toho musí prováděcí právní předpisy obsahovat jasná ustanovení, pokud jde o omezení používání těchto databází. Pracovní skupina rovněž připomíná, že je důležité zaručit, aby kritéria posuzování používaná členskými státy k analýze údajů byla konkrétní, nezbytná, odůvodněná a aby byla pravidelně podrobována přezkumu.

### 3.1. Definice

Návrh definuje „teroristické trestné činy“ jako trestné činy podle vnitrostátního práva uvedené v článcích 1 až 4 rámcového rozhodnutí Rady 2002/475/SVV. „Závažná trestná činnost“ a „závažná nadnárodní trestná činnost“ jsou definovány jako trestné činy podle vnitrostátního práva uvedené v čl. 2 odst. 2 rámcového rozhodnutí 2002/584/SVV. Pracovní skupina zdůrazňuje význam konkrétních definic v této oblasti. Definice závažné trestné činnosti je však poměrně široká; zpochybňujeme nezbytnost a přiměřenost používání údajů ze jmenné evidence cestujících v souvislosti s některými z těchto trestných činností.

V souvislosti s tím 12. bod odůvodnění návrhu uvádí, že členské státy smí vyjmout méně závažné trestné činy, pokud by to nebylo přiměřené, rozhodnutí je však na každém členském státě. Tím pravděpodobně vznikne situace, kdy budou určité trestné činy do definice v jednom členském státě začleněny, v dalším nikoli. Není jasné, kdo o přiměřenosti rozhoduje a zda má být toto rozhodnutí oznámeno Komisi, kdo by mohl odpovídat za zaručení soudržnosti a za správné uplatňování zásady proporcionality.

Obavy pracovní skupiny ohledně možné široké definice závažné trestné činnosti mají rovněž význam z hlediska navrhovaných ustanovení směrnice, která se týkají sdílení údajů s jinými orgány jak v EU, tak mimo ni.

## 4. Uchovávání údajů

Navržené doby uchovávání údajů jsou ve srovnání s předchozím návrhem a různými dohodami o jmenné evidenci údajů na úrovni EU jednoznačně kratší. Pracovní skupina se nicméně domnívá, že návrh uchovávat údaje po dobu pěti let je nepřiměřený, třebaže jsou maskovány. V souvislosti se systémy jmenné evidence údajů vždy vzbuzovala obavu skutečnost, že všechny údaje o všech cestujících jsou uchovávány stejně dlouho a že tato doba uchovávání údajů je sama o sobě nepřiměřená. Pracovní skupina dosud nezaznamenala žádné uspokojivé důkazy, že je třeba uchovávat údaje o všech cestujících a že je nutné je uchovávat po dobu pěti let.

### 4.1. Maskování údajů

Ačkoli návrh uvádí, že údaje budou po 30 dnech maskovány a obecně budou k dispozici pouze určitým pracovníkům složky pro informace o cestujících, kteří jsou pověřeni vývojem profilů a cestovních modelů, bylo by možné zachovat plný přístup ke všem údajům po celou dobu uchovávání údajů. I když je maskování pokusem o minimalizaci údajů a kontrolu přístupu, což jsou důležité zásady ochrany údajů, pracovní skupina stále zpochybňuje, proč jsou potřebné všechny údaje o všech cestujících, a domnívá se, že údaje o cestujících, kteří nejsou podezřelí, by měly být vymazány.

Pokud zákonodárce rozhodne, že údaje budou po omezenou dobu uchovány, měly by být údaje chráněny tak, aby nebyly odhaleny údaje o totožnosti. Tato ochrana by měla být zajištěna nejpozději při příletu. Přístup ke chráněným údajům za účelem získání údajů o totožnosti by měl podléhat soudnímu rozhodnutí při konkrétním vyšetřování, a to pro jednotlivé případy zvlášť.

Pracovní skupina by rovněž ráda důrazně poukázala na potřebu přesného jazyka, který není matoucí ani zavádějící. Návrh zmiňuje jak maskování, tak anonymizaci údajů. Nejedná se

o totéž a je zřejmé, že v návrhu jde o maskování, nikoli o anonymizaci, jelikož údaje o totožnosti jednotlivce lze stále snadno získat. Návrh by neměl být záměrně ani jinak matoucí a zavádějící, ani by neměl slibovat, co nelze splnit.

**5. Práva jednotlivce na ochranu údajů**

Návrh obsahuje ustanovení, která se týkají konkrétně ochrany údajů. Pracovní skupina se domnívá, že je nezbytné, aby každý návrh na úrovni EU, který má dopad na práva a svobody jednotlivců, obsahoval ustanovení o právech jednotlivce na přístup, opravu, náhradu škody a soudní přezkum. Avšak práva obsažená v tomto návrhu jsou práva uvedená v rámcovém rozhodnutí 2008/977/SVV, nikoli ve směrnici 95/46/ES. V důsledku toho jsou tato práva omezenější. Není jasné, zda se práva vztahují pouze na údaje předávané jinému orgánu nebo zda zahrnují údaje v držení vnitrostátního orgánu. V některých členských státech, které v současné době používají údaje ze jmenné evidence cestujících, mají jednotlivci práva na přístup, opravu a soudní přezkum na základě vnitrostátních právních předpisů, kterými se provádí směrnice 95/46; pokud návrh směrnice o jmenné evidenci cestujících vstoupí v platnost, budou tato práva omezena.

Rovněž hrozí, že v důsledku vytváření profilu dojde k diskriminaci, neboť tento systém se zaměřuje na cestující v letecké dopravě jako na skupinu. Cestujícím nejsou sděleny žádné informace o kritériích, na jejichž základě jsou posuzováni, a tím je ovlivněn výkon práv osob, jichž se vytváření profilu přímo týká.

Pracovní skupina připomíná, že je důležité začlenit do návrhů na úrovni EU, které mají dopad na práva a svobody jednotlivců, odpovídající opatření na ochranu údajů, např. pravidla týkající se důvěrnosti a bezpečnostních prohlídek, povinnosti informovat jednotlivce, zákazu předávání údajů soukromým subjektům a pravidlo, že rozhodnutí by neměla být prováděna pouze na základě automatického zpracování. Pracovní skupina rovněž zdůrazňuje, že je důležité začlenit do návrhu vnitrostátní orgány dozoru, které mají určitou úlohu při provádění právních předpisů EU na vnitrostátní úrovni.

Pokud jde o citlivé údaje, návrh uvádí, že filtrování a vymazávání těchto údajů by měla provádět složka pro informace o cestujících. Pracovní skupina ve svých stanoviscích k různým dohodám o jmenné evidenci cestujících na úrovni EU v této souvislosti vždy podporovala zákaz zpracování citlivých údajů a důrazně opakuje svůj dlouhodobý názor, že filtrování údajů by měl provádět dopravce před tím, než jsou údaje předány přijímajícímu orgánu.

Pracovní skupina zdůrazňuje, že je důležité zajistit, aby návrhy na úrovni EU, které mají dopad na práva a svobody jednotlivců, obsahovaly požadavky na sledování a přezkum, např. u zpracování přihlašovacích údajů a žádostí o údaje, aby mohly vnitrostátní orgány pro ochranu údajů ověřovat zákonnost zpracování a vlastního sledování a zaručit náležitou integritu a bezpečnost údajů. Je však důležité pochopit, jak takové systémy budou fungovat v praxi a jak bude účinné přihlašování a dokumentování vyhovovat výše popsaným zásadám minimalizace údajů.

**6. Prvky údajů**

Na rozdíl od předběžných informací o cestujících nejsou údaje ze jmenné evidence ověřovány, a tudíž jsou méně spolehlivé. Prvky údajů, které jsou uvedeny v příloze tohoto

návrhu, představují stejných 19 prvků jako v dohodách o jmenné evidenci cestujících, které byly uzavřeny mezi EU a Spojenými státy a mezi EU a Kanadou. Pracovní skupina znovu opakuje svůj postoj, že neexistují uspokojivé důkazy, z nichž by vyplývalo, která pole se ukázala jako nezbytná, a tudíž je takový seznam nepřiměřený. Kategorie jsou obecné a řada z nich obsahuje další dílčí soubory údajů. I přes zákaz zpracování citlivých osobních údajů je v seznam prvků údajů obsaženo pole „obecné poznámky“, které by mohlo zahrnovat všechny druhy informací, např. objednávky jídel, žádosti o zvláštní služby atd. Pracovní skupina dosud neobdržela uspokojivé důkazy, z nichž by bylo zřejmé, které prvky údajů ze jmenné evidence cestujících se ukázaly jako nezbytné nebo byly úspěšně použity pro vynucování práva. Kromě toho ne všichni dopravci údaje ze jmenné evidence cestujících shromažďují.

**7. Příslušné orgány a další předávání údajů**

Návrh uvádí, že členské státy musí oznámit seznam svých příslušných orgánů Komisi do dvanácti měsíců po vstupu směrnice v platnost a že tento seznam bude zveřejněn v Úředním věstníku. Pracovní skupina podporuje opatření zajišťující transparentnost, díky nimž lze jednoznačně poznat, kdo je oprávněn přijímat a zpracovávat údaje. Nejsou však jasné úlohy (kontrolor/zpracovatel) přidělené příslušným orgánům a složkám pro informace o cestujících.

Pracovní skupina znovu vyjadřuje obavy týkající se široké definice závažné trestné činnosti, a to zejména ve vztahu k dalšímu předávání údajů jak v EU, tak mimo ni.

**8. Přezkum a reciprocita**

Podle návrhu bude směrnice přezkoumána do čtyř let po vstupu v platnost. Do dvou let po vstupu směrnice v platnost bude proveden zvláštní přezkum možného rozšíření oblasti působnosti směrnice na lety na území EU. Pracovní skupina zdůrazňuje, že je třeba, aby postupy EU v oblasti legislativního přezkumu obsahovaly jasná kritéria, na jejichž základě lze při přezkumu posoudit potřebnost a účinnost systému. Pracovní skupina rovněž znovu zdůrazňuje, že je důležité zapojit do každého přezkumu vnitrostátní orgány pro ochranu údajů, zejména proto, že je tak stanoveno v rámci jiných nástrojů na úrovni EU, např. v dohodách o jmenné evidenci cestujících mezi EU a třetími zeměmi.

Pracovní skupina podotýká, že při vývoji návrhů EU je důležité zvážit dopad možných požadavků na reciprocitu. Evropský model jmenné evidence cestujících by mohl vést k tomu, že obdobné požadavky budou recipročně vznášeny nedemokratickými zeměmi nebo zeměmi, které nezajišťují odpovídající úroveň ochrany základních práv a svobod včetně ochrany osobních údajů a soukromí. Je jasné, že pokud by takové země obdržely údaje ze jmenné evidence cestujících EU, mohlo by to mít pro jednotlivce závažné důsledky.

**9. Závěr**

Pracovní skupina se domnívá, že potřebnost systému EU pro jmennou evidenci cestujících dosud nebyla prokázána a že navrhovaná opatření nejsou v souladu se zásadou proporcionality, a to zejména proto, že systém plánuje shromažďování a uchovávání všech údajů o všech cestujících na všech letech. Pracovní skupina má rovněž vážné pochybnosti o přiměřenosti systematického vyhodnocování všech cestujících podle předem stanovených kritérií.

Pracovní skupina doporučuje, aby byly nejprve vyhodnoceny stávající systémy a metody spolupráce a způsoby, jak dokáží společně určit mezery v bezpečnosti. Pokud takové mezery existují, měl by další krok spočívat v analýze nejlepšího způsobu, jak tyto mezery překlenout, což nutně neznamená, že by měl být zaveden zcela nový systém. Stávající mechanismy by mohly být důkladněji využity a vylepšeny.

Pokud navrhovaná směrnice vstoupí v platnost, měla by zaručit přiměřená a odpovídající opatření na ochranu údajů. Komise by rovněž měla zvážit, zda by v důsledku toho nebylo možné zrušit některé stávající systémy, např. směrnici API, aby se zabránilo tomu, že se opatření budou překrývat.

Pracovní skupina bude nadále pozorně sledovat další vývoj a vítá každou příležitost k tomu, aby se svými názory seznámila různé strany, které se na přípravě tohoto návrhu podílejí, a aby své názory dále rozvíjela. Pracovní skupina bude rovněž, pokud to bude vhodné a nezbytné, nadále poskytovat svá stanoviska.

V Bruselu dne 5. dubna 2011

*Za pracovní skupinu*
*předseda*
*Jacob KOHNSTAMM*

**PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29**

**00671/11/CS**

**WP 183**

# Stanovisko č. 12/2011 k inteligentnímu měření

**Přijaté dne 4. dubna 2011**

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 (Základní práva a občanství Unie) Evropské komise, Generální ředitelství pro spravedlnost, B-1049 Brusel, Belgie, kancelář MO-59 06/036.

Internetové stránky: http://ec.europa.eu/justice/policies/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 článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád,

**PŘIJALA TENTO DOKUMENT:**

## Úvod a oblast působnosti

Cílem tohoto stanoviska pracovní skupiny zřízené podle článku 29 je objasnit právní rámec, který se vztahuje na fungování technologií inteligentního měření v odvětví energetiky. Záměrem tohoto stanoviska není předložit komplexní přehled všech zvláštních aspektů programů inteligentního měření v jednotlivých členských státech, jelikož rozdíly v jejich současné situaci to neumožňují. Inteligentní měřicí přístroje nabízejí nové funkce, například poskytování podrobných informací o spotřebě energie, možnost odečtu měřicího přístroje na dálku, vývoj nových sazeb a služeb podle energetických profilů a možnost přerušení dodávek energie na dálku.

Ještě větší prostor pro rozvoj a zpracovávání více osobních údajů nabízejí inteligentní sítě. Pracovní skupina nemá v této fázi v úmyslu zahrnout inteligentní sítě do oblasti působnosti tohoto stanoviska. Nevylučuje však další analýzu inteligentních sítí, jakmile bude získána přesnější představa.

Směrnice ES o energetické účinnosti u konečného uživatele a o energetických službách (2006/32/ES) stanoví cíle v oblasti úspor energie, jež mají být přijaty jednotlivými členskými státy. V zájmu dosažení těchto cílů a s výhradou omezených výjimek ukládá článek 13 směrnice členským státům povinnost vybavit spotřebitele měřiči, které přesně zobrazují skutečnou spotřebu energie a skutečnou dobu její spotřeby. Tyto inteligentní měřiče jsou součástí úsilí o naplnění cílů Evropské unie souvisejících s dosažením udržitelných dodávek energie do roku 2020.

Generální ředitelství pro energii zřídilo pracovní skupinu pro inteligentní sítě. Odborná skupina č. 2, která je součástí této pracovní skupiny, si vyžádala pomoc pracovní skupiny zřízené podle článku 29 za účelem získání širší analýzy opatření, která se provádějí na vnitrostátní úrovni. Za tímto účelem byl v roce 2010 orgánům pro dohled nad ochranou údajů zaslán dotazník. V dotazníku bylo položeno šest otázek týkajících se názorů na rozvoj inteligentních sítí (z nichž mnohými se zabývá rovněž toto stanovisko). Další soubor dvanácti otázek se týkal informací o současném stavu zavádění inteligentního měření v členských státech. Členské státy, které odpověděly na těchto šest otázek, poznamenaly, že úroveň bezpečnosti musí být srovnatelná s jinými rozsáhlými operacemi, jako je internetové bankovnictví. Odpovědi na soubor dvanácti otázek prokázaly, že provádění programů k rozvoji inteligentního měření u odběratelů energie z řad domácností představuje v mnoha členských státech EU důležité a naléhavé téma. Inteligentní měření má obzvláštní význam v tom, že může ovlivnit životy téměř všech občanů, jelikož všichni očekávají

poskytování dodávek elektřiny a plynu. Jeho dosah je mimořádně velký a není omezen pouze na subjekty, které se rozhodly podílet na technologickém rozvoji. Cílem je zajistit do roku 2020 pokrytí u 80 % zákazníků[1].

Inteligentní měřicí přístroje umožňují vytváření, předávání a analýzu údajů týkajících se odběratelů v mnohem větším rozsahu, než je to možné s „tradičními“ či „neinteligentními“ měřicími přístroji. Provozovateli sítě (nazývanému rovněž provozovatelem distribuční soustavy), dodavatelům energie a dalším stranám umožňují proto rovněž sestavovat podrobné informace o spotřebě energie a o modelech spotřeby, jakož i přijímat rozhodnutí týkající se jednotlivých odběratelů na základě profilů spotřeby. Ačkoliv se uznává, že tato rozhodnutí mohou často přinést odběratelům prospěch, pokud jde o úspory energie, objevují se rovněž signály, že existuje možnost narušení soukromého života občanů používáním zařízení, která jsou instalována v domácnostech. To znamená taktéž posun v našem základním vztahu s dodavateli energie, jelikož odběratelé tradičně platili jednoduše dodavatelům za dodanou elektřinu a plyn. S příchodem inteligentních měřičů je proces složitější, jelikož subjekt údajů dovolí dodavatelům nahlédnout do svých osobních zvyků.

K široce projednávaným výhodám inteligentního využívání energie patří možnost odběratelů snížit účty změnou svých zvyků, případně používáním energie v jiné době s cílem využít nižších sazeb, jakož i možnost odvětví přesněji předvídat poptávku a snížit náklady na drahé skladování elektřiny. Dosažení cílů v oblasti změny klimatu závisí do jisté míry na uvolnění osobních údajů odběrateli, toho však musí být dosaženo tak, aby všechny strany podílející se na programech k zavedení inteligentních měřicích přístrojů a rozvoji inteligentních sítí zajistily ochranu a dodržování základních práv jednotlivců. Bez této ochrany existuje nejen riziko, že zpracovávání osobních údajů bude v rozporu s vnitrostátními právními předpisy k provedení směrnice 95/46/ES, nýbrž rovněž riziko, že odběratelé tyto programy odmítnou na základě toho, že shromažďování osobních údajů je pro ně nepřijatelné. Takovéto odmítnutí může nastat i tehdy, nedojde-li k porušení právních předpisů. Z hlediska ochrany údajů proto pracovní skupina zřízená podle článku 29 zdůrazňuje, že ačkoliv jsou potenciální přínosy těchto programů dalekosáhlé a značné, mohou vést rovněž k zpracovávání většího objemu osobních údajů, v tomto odvětví dříve nevídaného, a zajistit, aby byly osobní údaje snáze dostupné širšímu okruhu příjemců, než je tomu v současnosti.

Pracovní skupina si je vědoma skutečnosti, že mezi jednotlivými členskými státy existují obrovské rozdíly, kdy v některých členských státech je na základě pověření vlády zavádění velkou měrou dokončeno a v některých členských státech nebyly dosud instalovány žádné měřiče.

Existuje rovněž velký rozdíl v úrovni zapojení orgánů pro ochranu údajů. Pokud tomu tak již není, připomíná pracovní skupina všem subjektům podílejícím se na inteligentním měření význam konzultací s příslušnými orgány pro ochranu údajů.

---

1 Smart meters: controlling your energy bill? *Euractiv.com*, [internet]. K dispozici na adrese: http://www.euractiv.com/en/energy-efficiency/smart-meters-controlling-your-energy-bill-linksdossier-257199 [dostupné od 25. března 2011]
Tento článek odkazuje na mezníky uvedené ve třetím energetickém balíčku, který byl přijat v červnu 2009.

Další rozdíly mezi členskými státy se vyskytují s ohledem na povahu trhu a na to, kdo odpovídá za instalaci měřicích přístrojů. V řadě členských států za to odpovídají podniky veřejných služeb, které jsou ve vlastnictví státu. Jinde existuje konkurenční trh dodavatelů. V některých zemích hrají výraznější úlohu provozovatelé distribučních soustav. V některých členských státech je nahrazení měřicích přístrojů povinné u všech odběratelů. Jsou-li záznamy z měřicího přístroje zaslány provozovatelům distribučních soustav, mohou mít dodavatelé energie právo na přístup k informacím, které potřebují ke správě svých odběratelů a vystavování faktur. Mohou mít přístup rovněž k podrobnějším informacím (např. za účelem poskytování poradenství ohledně úspor energie), avšak pouze se souhlasem odběratele. Provozovatel distribuční soustavy má rovněž právo shromažďovat podrobné informace o spotřebě odběratelů za účelem správy a údržby fyzické sítě.

Existují rovněž rozmanité a složité způsoby komunikace s dalšími místy vstupu a datovými toky, což vyvolává složité problémy v oblasti bezpečnosti, jež vyžadují řešení, která zahrnují všechny tyto záležitosti.

Vzhledem k složitému a odlišnému prostředí je úkol spočívající ve vydání doporučení potenciálně složitý a v této fázi se zdá, že tato doporučení mohou být pouze obecná, nikoli konkrétní. V této fázi se proto jeví jako rozumné a reálné stanovit jednoznačné zadávací podmínky pro tuto analýzu a zaměřit se na vztah mezi právními požadavky stanovenými ve směrnici o ochraně údajů a rámcem inteligentního měření. Bude-li to vhodné, bude případně odkázáno na výzkum, který již uskutečnila skupina odborníků pro inteligentní sítě[2]. Hlavní myšlenky v tomto stanovisku týkající se ochrany soukromí již ve fázi návrhu a bezpečnosti se například shodují s doporučeními skupiny. Nesporné je to, že již dochází k hromadnému zavádění inteligentních měřicích přístrojů, takže je naléhavě nutné, abychom společně pochopili způsob, jakým inteligentní měřicí přístroje zpracovávají osobní údaje, a otázky, které to vyvolává, ačkoliv rozsah této práce není vyčerpávající.

Cílem stanoviska je zabývat se těmito záležitostmi: definice osobních údajů v souvislosti s inteligentním měřením, kontrola údajů a přezkum legitimních důvodů zpracování údajů. Vydaná doporučení budou založena na stávajících poznatcích, je však pravděpodobné, že k vyřešení budoucích záležitostí (např. inteligentní spotřebiče) bude zapotřebí další práce.

---

[2] S cílem usnadnit a podpořit proces zavádění inteligentních sítí v celé EU se Evropská komise rozhodla zřídit pracovní skupinu pro inteligentní sítě. Za tímto účelem byly vytvořeny tři skupiny odborníků, které mají určit doporučení týkající se zavádění inteligentních sítí. Dokumentem použitým při vypracovávání tohoto stanoviska je:
Odborná skupina č. 2 pracovní skupiny pro inteligentní sítě, *Regulatory Recommendations for Data Safety, Data Handling and Data Protection, zpráva vydaná dne 16. února 2011,* [internet]. K dispozici na adrese: < http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf> [zpřístupněno dne 25. března 2011].

**Definice**

K dispozici je řada definic inteligentních měřicích přístrojů a inteligentních sítí. Za účelem zahrnutí záležitostí a priorit, které určila pracovní skupina zřízená podle článku 29, je však užitečné vymezit inteligentní sítě a inteligentní měřicí přístroje takto:

Inteligentní měřicí přístroje jsou instalovány v domácnostech uživatelů veřejné služby a jsou schopny obousměrné komunikace. Informují odběratele o množství spotřebovávané energie a tyto informace mohou být zasílány rovněž dodavatelům energie a jiným určeným stranám. Hlavním znakem inteligentních měřicích přístrojů je to, že zajišťují možnost dálkové komunikace mezi měřicím přístrojem a oprávněnými stranami, jako jsou dodavatelé, provozovatelé sítí a oprávněné třetí strany nebo společnosti poskytující energetické služby. Inteligentní měřicí přístroje mohou zvýšit četnost komunikace mezi odběratelem a ostatními stranami a v důsledku toho i množství údajů o odběrateli, které jsou k dispozici ostatním stranám. Sběr a používání těchto údajů je mnohem širší a pro větší počet účelů, než je tomu u tradičních či „neinteligentních“ měřicích přístrojů, u nichž se provádějí fyzické odpočty, a to relativně méně často.

Z nejabstraktnějšího a nejzákladnějšího hlediska odečítá inteligentní měřicí přístroj údaje, které odrážejí spotřebu energie v dané nemovitost. V určitém okamžiku mohou být tyto odečtené údaje spolu s dalšími informacemi předány mimo nemovitost. V některých modelech budou zaslány přímo do hlavního komunikačního centra, v němž jsou spravovány údaje z inteligentních měřicích přístrojů. Tam k nim mohou mít přístup provozovatelé distribučních soustav, dodavatelé a společnosti poskytující energetické služby.

Zavedení inteligentních měřicích přístrojů je předpokladem inteligentní sítě. *Inteligentní sítí* je inteligentní elektrická síť, která spojuje informace od uživatelů této sítě s cílem naplánovat účinněji a hospodárněji dodávky elektřiny, než to bylo možné v prostředí před zavedením inteligentního měření.

**Uplatňování práva v oblasti ochrany údajů na zpracovávání údajů shromážděných prostřednictvím inteligentních měřicích přístrojů**

Jsou-li v informacích vytvořených a šířených inteligentním měřicím přístrojem obsaženy osobní údaje, pracovní skupina stanoví, že se na toto zpracování vztahuje směrnice 95/46/ES.

Z obecně dostupných informací o této záležitosti a z podrobných diskusí na vnitrostátní úrovni ohledně fungování inteligentních měřicích přístrojů vyplývá, že lze předpokládat zpracovávání těchto druhů údajů:

- jedinečné identifikační číslo inteligentního měřicího přístroje a/nebo jedinečné referenční číslo nemovitosti (i v případě neexistence těchto identifikátorů lze měřicí přístroj identifikovat rovněž podle jedinečného diagramu zatížení),
- metadata vztahující se na konfiguraci inteligentního měřicího přístroje,

- popis předávané zprávy, například zda se jedná o údaje odečtené měřicím přístrojem nebo o výstrahu týkající se neoprávněné manipulace,
- zaznamenání data a času,
- obsah zprávy.

Obsah zprávy bude pravděpodobně zahrnovat tyto druhy informací:

- údaje odečtené z měřicího přístroje. Může se jednat o jedno odečtení či v případě složitější sazby o skupinu odečtení,
- výstrahy. Měřicí přístroj může předat zprávu, která informuje, že k události vedl alarm měřicího přístroje,
- informace na úrovni sítě, jako je napětí, přerušení dodávek energie a kvalita energie,
- grafické znázornění zatížení s různou úrovní podrobnosti.

Údaje mohou být správci zasílány v reálném čase, nebo mohou být uloženy v inteligentním měřicím přístroji. V obou případech se však podle směrnice o ochraně údajů usuzuje, že údaje byly shromážděny správcem.

Tento seznam není ani zdaleka úplný, pracovní skupina však podotýká, že fungování inteligentních měřicích přístrojů (a v širším slova smyslu další rozvoj inteligentních sítí a spotřebičů) znamená zpracovávání osobních údajů, jak je vymezeno v článku 2 směrnice 95/46/ES a jak je pracovní skupina vyložila ve svém stanovisku č. 4/2007. S ohledem na zpracovávání většího množství osobních údajů znamená možnost dálkového řízení spojení a pravděpodobnost vytváření energetických profilů na základě podrobných údajů odečtených měřicím přístrojem, že je naprosto nezbytné věnovat náležitou pozornost základním právům jednotlivců na ochranu soukromí.

Závěr, že jsou zpracovávány osobní údaje, byl vyvozen z těchto důvodů:

1. údaje, které byly vyjmenovány výše jako údaje vytvořené inteligentními měřicími přístroji, jsou ve většině případů spojeny s jedinečnými identifikátory, jako je identifikační číslo měřicího přístroje. U odběratelů energie z řad domácností je tento identifikátor neoddělitelně spojen s osobou, která odpovídá za účet. Jinými slovy, přístroj umožňuje odlišit jednotlivce od ostatních odběratelů;
2. informace shromážděné v souvislosti se službou inteligentního měření se týkají energetického profilu odběratele v rámci spotřeby energie a používají se k přijímání rozhodnutí, která se přímo týkají tohoto jednotlivce. Nejzřejmějším takovým rozhodnutím je určení výše poplatků za dodávky energie, toto však není omezeno na účely vyúčtování;
3. tento názor je dále potvrzen, vezmou-li se v úvahu obecně propagované výhody zavádění inteligentních měřicích přístrojů, jako je snížení celkové spotřeby energie v členských státech. Tohoto cíle může být jednoznačně dosaženo pouze tehdy, sníží-li se spotřeba energie rovněž u jednotlivých odběratelů, a podle dodavatelů energie a energetických sítí je dosažení tohoto cíle do značné míry závislé na shromažďování velkého množství informací o chování těchto odběratelů.

**Definice správce údajů vztahující se na inteligentní měřicí přístroje**

Je stanoveno, že směrnice 95/46/ES ukládá správci údajů povinnosti s ohledem na zpracovávání osobních údajů. Dříve než bude objasněno, jak se tyto povinnosti uplatňují v rámci tohoto stanoviska, je důležité, aby pracovní skupina objasnila svůj názor na to, které právnické osoby spadají do definice správce údajů.

Zavádění inteligentních měřicích přístrojů zapojuje do zpracovávání osobních údajů řadu organizací, včetně například dodavatelů energie, provozovatelů energetických sítí, regulačních orgánů, vládních orgánů, poskytovatelů služeb, kteří jsou třetími stranami, a poskytovatelů komunikačních služeb. Vzhledem k počtu a složitosti vztahů je pravděpodobné, že se při používání příslušných definic objeví problémy, analýza obsažená v tomto stanovisku však odráží přístup, který pracovní skupina zaujala ve svém stanovisku č. 1/2010 k pojmům „správce“ a „zpracovatel“ údajů. Odpovědnosti vyplývající z právních předpisů v oblasti ochrany údajů by proto měly být jednoznačně přiděleny způsobem, který dostatečně zajišťuje dodržování pravidel ochrany údajů v praxi.

**Dodavatelé energie**

V některých členských státech bude právnickou osobou, která nese největší odpovědnost za zpracovávání osobních údajů, dodavatel. Dodavatelé mají smlouvu se subjektem údajů, jež iniciuje zpracovávání, a vzhledem k tomu, že rozhodují o tom, které údaje potřebují k plnění svých funkcí a jak je budou shromažďovat, uchovávat a používat, lze zjevně mít za to, že určují účely, pro něž jsou osobní údaje zpracovávány, a rovněž způsob, jakým jsou tyto údaje zpracovávány. To je poměrně jednoznačně určuje jako správce údajů při zpracovávání osobních údajů vytvořených přístrojem k měření spotřeby energie a pracovní skupina zastává názor, že bez ohledu na větší složitost, která je způsobena inteligentními měřicími přístroji, zůstávají dodavatelé v této souvislosti správci údajů.

**Provozovatelé sítí nebo provozovatelé distribučních soustav**

V jiných modelech bude za instalaci a provozování systému inteligentního měření odpovídat provozovatel distribuční soustavy, který vlastní síť. Provozovatel distribuční soustavy bude odpovídat rovněž za určení způsobu shromažďování, uchovávání a používání údajů. V tomto modelu bude správcem údajů provozovatel distribuční soustavy. Mají-li dodavatelé energie právo na přístup k údajům předávaným měřicími přístroji a používají-li tyto údaje pro vlastní účely (např. vystavování faktur nebo poskytování poradenství odběratelům), pak budou rovněž správci údajů u osobních údajů, které zpracovávají.

**Ostatní strany**

Existuje mnoho dalších stran, které by při plnění své úlohy v rámci programu pro zavádění inteligentních měřicích přístrojů mohly případně zpracovávat osobní údaje. Některé z nich nemusí dokonce vzniknout, dokud se neprojeví úplné účinky přechodu směrem k většímu množství zpracovávaných osobních údajů, takže by nebylo rozumné pokoušet se vypracovat v této fázi konečný seznam. Je rovněž důležité mít na paměti rozdíly mezi jednotlivými členskými státy, pokud jde o modely a koncepce

dodávek. Je však třeba uznat, že nebudou-li všechny strany působit na základě společného chápání toho, jak se uplatňuje definice správce údajů, existuje vyšší riziko, že nebude dosaženo dodržování předpisů a osvědčených postupů. Majíc toto na paměti pracovní skupina připomíná všem stranám tyto důležité body:

1. V některých modelech zavádění je zřízena hlavní komunikační funkce, která odpovídá za řízení předávání údajů mezi měřicím přístrojem a dodavatelem. Je možné, že tato funkce může působit jako zpracovatel údajů, který jedná pouze podle pokynů dodavatelů, jimž posílá údaje a od nichž přijímá údaje. Pokud se však komunikační funkce podílí na rozhodování, zda lze osobní údaje sdělit třetí straně nebo zda lze tyto údaje zpracovávat pro nové účely, pak může komunikační funkce převzít s ohledem na toto zpracování osobních údajů úlohu správce údajů.

2. Důležitými subjekty jsou rovněž energetické regulační orgány. Tyto orgány mohou mít přístup k údajům za účelem tvorby politik a pro výzkumné účely. Jsou-li tyto údaje osobními údaji, pak regulační orgán jednoznačně přebírá úlohu správce údajů.

3. Poskytovatelé služeb, kteří jsou třetí stranou (a na něž se často odkazuje jako na společnosti poskytující energetické služby), budou mít při používání údajů vytvořených inteligentními měřicími přístroji stále důležitější úlohu. Jsou-li určité společnosti poskytující energetické služby sděleny osobní údaje za účelem poskytování služby odběrateli či jiné straně, například dodavateli, pak tato společnost přebírá úlohu správce údajů.

**Oprávněnost zpracování a legitimní důvody/účely zpracování**

Jakmile bylo zjištěno, že určitou právnickou osobu je nutno pokládat za správce údajů, pak je důležité objasnit právní požadavky, které správci údajů ukládá směrnice o ochraně údajů. Podle článku 6 směrnice musí být osobní údaje zpracovány korektně a zákonným způsobem. Aby bylo zpracovávání osobních údajů zákonné, musí být splněn jeden či více ze šesti důvodů legitimního zpracování, které jsou stanoveny v článku 7 směrnice.

Pracovní skupina podotýká, že v mnoha členských státech (ne-li ve všech) nebyla dosud zcela objasněna nebo náležitě vymezena přesná povaha účelů zpracování osobních údajů uložených v inteligentním měřicím přístroji či předávaných takovýmto přístrojem. Vzhledem k této skutečnosti pracovní skupina doporučuje, aby byly takovéto účely stanoveny dříve, než je možno tvrdit, že důvody zpracování jsou legitimní. Pracovní skupina rovněž podotýká, že každý zvláštní účel musí být legitimní sám o sobě a že jeden legitimní účel nemůže sloužit k ospravedlnění jiného účelu. Osobní údaje nelze zejména znovu zpracovat pro jiný účel, který není slučitelný s účelem, pro nějž byly tyto údaje shromážděny původně.

Pracovní skupina se domnívá, že v této souvislosti existuje pět možných důvodů zpracování, které mohou správci údajů uplatnit.

**Souhlas**

Je zřejmé, že mnoho účelů, pro něž lze použít osobní údaje, bude souviset se zdokonalenými službami, které jsou poskytovány subjektům údajů, jako jsou sazby podle doby spotřeby nebo poradenství týkající se spotřeby energie. Pokud subjekt údajů souhlasil s touto službou, je pravděpodobné, že poskytovatel služby (dodavatel nebo třetí strana) mohou získat souhlas subjektu údajů se zpracováním jeho osobních údajů.

Pracovní skupina správcům údajů připomíná, že spoléhání se na souhlas bude vyžadovat uvážení skutečnosti, že platný souhlas existuje pouze tehdy, pokud subjekt údajů přijal zcela vědomé rozhodnutí. Souhlas nelze použít jako důvod pro zpracovávání osobních údajů, pokud nebyly subjektu údajů poskytnuty dostatečné informace o zpracování údajů, aby si mohl skutečně vybrat. Zejména v případě, existuje-li řada různých funkcí, musí být souhlas dostatečně rozčleněný, aby odrážel tyto vícenásobné účely, místo jednoho souhlasu, který se používá k ospravedlnění potenciálně odlišných a nesouvisejících různých účelů.

Pracovní skupina doporučuje, aby odvětví vyvinulo účelné a praktické prostředky, jimiž mohou subjekty údajů vyjádřit svůj souhlas. Je důležité mít na paměti, že souhlas musí být svobodný, a proto musí být možné tento souhlas odvolat, takže způsoby získávání souhlasu by měly subjektu údajů umožňovat, aby svůj názor změnil, aniž by to pro něj znamenalo přílišné potíže. Jedním z možných řešení by mohlo být navržení ovládacího panelu pro domácnosti, který umožňuje udělit souhlas pomocí tlačítka. Dostupnost takovéto funkce bude záviset na důmyslnosti návrhu měřicího přístroje a ovládacího panelu, aby bylo zajištěno, že souhlas je i nadále platný.

**Smlouva**

Zpracování může být nezbytné rovněž k plnění smlouvy, jejíž stranou je subjekt údajů, nebo k podniknutí kroků před uzavřením smlouvy na žádost subjektu údajů. Tento právní základ by bylo možno použít k ospravedlnění zpracování osobních údajů pro účely vyúčtování, jelikož bez náležitě sestaveného účtu není možné plnit smlouvu o dodávkách energie.

Pokud jde o vyúčtování, je důležité mít na paměti prvek nutnosti obsažený v této podmínce. Jinými slovy, je-li důvodem zpracování plnění smlouvy, která vyžaduje pouze to, aby byla odběrateli předložena čtvrtletní faktura a aby ji tento uhradil, není nutné, aby za účelem plnění této smlouvy shromažďoval dodavatel údaje častěji. Smlouva by musela obsahovat platné právní ustanovení o častějším odečítání údajů, nebo by se dodavatel musel s ohledem na tyto odečtené údaje spoléhat na jiný právní základ.

**Plnění úkolu, který je prováděn ve veřejném zájmu nebo v souvislosti s výkonem veřejné moci**

V některých členských státech odpovídá provozovatel elektrické sítě za výkonnost fyzické sítě, avšak rovněž za snižování celkové spotřeby elektřiny. Tato spotřeba elektřiny se týká celkové spotřeby i spotřeby v době špičky. Tyto úkoly jsou

prováděny ve veřejném zájmu a ospravedlňují instalaci inteligentních měřicích přístrojů.

**Právní povinnost**

V některých členských státech je provozovatel sítě povinen instalovat inteligentní měřicí přístroje a shromažďovat jejich prostřednictvím údaje u každého nového zařízení[3].

**Oprávněné zájmy**

Podle čl. 7 písm. f) směrnice může být zpracování zákonné pouze tehdy, je-li nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva subjektu údajů.

Hlavním bodem, který je třeba zmínit, je to, že spoléhání se na tento právní základ závisí na přisouzení náležité váhy zájmům a právům subjektů údajů. Může se zdát nesporné, že by oprávněným zájmům správce údajů a celé společnosti sloužila vyšší účinnost při dodávkách a spotřebě energie a že toho lze dosáhnout prostřednictvím osobních údajů shromažďovaných pomocí inteligentních měřicích přístrojů. Samotná skutečnost, že se toto konkrétní použití osobních údajů jeví jako legitimní (a pro mnohé jako žádoucí), neznamená, že je lze použít k ospravedlnění každého prvku zpracování. Jinými slovy, nutnost snižovat spotřebu energie může být sice rozumným cílem veřejné politiky, přesto však nepřevyšuje v každém případě práva a zájmy subjektů údajů.

Ve skutečnosti je zřejmé, že pravděpodobnost, že by správce údajů mohl tuto podmínku použít při zpracovávání údajů, zvýší zahrnutí praktických opatření, jako jsou technologie zvyšující ochranu soukromí a posouzení dopadů na soukromí, k zvýšení bezpečnosti a ochrany údajů zpracovávaných inteligentními měřicími přístroji.

To je obzvláště důležité, pokud zpracovávání z důvodu oprávněných zájmů správce údajů zasahuje podstatně a nepřiměřeně do soukromí nebo má-li zpracování způsobit subjektu údajů neodůvodněnou újmu. K příkladům může patřit vytváření podrobných profilů subjektů údajů, které ve skutečnosti nejsou k dosažení daného účelu zapotřebí, předávání údajů třetím stranám bez vědomí či souhlasu subjektu údajů nebo používání osobních údajů při přijímání rozhodnutí o odpojení na dálku bez náležitého přihlédnutí k ochraně údajů jednotlivce a jiných práv.

Pracovní skupina průmyslovému odvětví rovněž připomíná, že v některých členských státech existuje možnost, aby subjekt údajů vznesl námitky vůči instalaci inteligentního měřicího přístroje, a že v těchto případech převyšuje volba subjektu údajů jakékoli jiné zájmy.

[3] Viz francouzská vyhláška č. 2010-1022 ze dne 31. srpna 2010.

**Další záležitosti týkající se dodržování předpisů, jež vyvolává inteligentní měření**

Vzhledem k dalekosáhlé povaze záležitostí, které vyvolává inteligentní měření, není možné, aby pracovní skupina poskytla úplný seznam bodů, k nimž by bylo možno poskytnout vodítko. Jedná se o novou oblast práce a pracovní skupina očekává, že v souvislosti s tím, jak bude instalováno stále více inteligentních měřicích přístrojů, se objeví nové problémy a řešení v oblasti ochrany údajů. Existují však určité záležitosti obecné povahy, které podle názoru pracovní skupiny odůvodňují důkladné uvážení ze strany všech subjektů působících v této oblasti.

**Ochrana soukromí již ve fázi návrhu**

Pracovní skupina připomíná své stanovisko č. 168, v němž uvedla, že by služby a technologie, které závisí na zpracovávání osobních údajů, měly být navrženy s ochranou soukromí jako standardním nastavením. V tomto ohledu by při zavádění inteligentního měření měla být od začátku zajištěna ochrana soukromí, a to nejen z hlediska bezpečnostních opatření, nýbrž rovněž s ohledem na omezení množství zpracovávaných osobních údajů na nejnižší možnou míru. Některé členské státy přikročily k plánům zavádění, které vyžadují posouzení dopadů na soukromí, a pracovní skupina tento přístup doporučuje.

Inteligentní měřicí přístroje, které jsou v současnosti testovány v některých členských státech, shromažďují řadu údajů v závislosti na druhu smlouvy, kterou zákazník podepsal. Pokud má například zákazník jednoduchou smlouvu, podle níž platí za elektřinu stejnou cenu během celého dne, bude měřicí přístroj shromažďovat jeden údaj denně. Má-li však zákazník smlouvu, podle níž se účtují různé ceny v závislosti na denní době, bude měřicí přístroj shromažďovat každý den deset různých údajů. Na nejzákladnější úrovni by ochrana soukromí již ve fázi návrhu zajišťovala, že údaje z měřicího přístroje jsou předávány pouze tak často, jak je to nezbytné pro fungování systému nebo poskytování služby odběrateli, s níž tento souhlasil.

Jeden druh měřicích přístrojů, který se používá v současnosti, například shromažďuje údaje o spotřebě v reálném čase každých 10 až 60 minut za účelem vytvoření diagramu zatížení. Četnost může provozovatel elektrické sítě nastavit na dálku. Tento diagram zatížení je v měřicím přístroji uložen po dobu 2 měsíců a provozovatel elektrické sítě si jej vyzvedne v případě potřeby. Přijetím přístupu založeného na ochraně soukromí již ve fázi návrhu by bylo možno tento model upravit tak, aby shromažďoval a uchovával údaje pro diagram zatížení pouze na žádost.

Rovněž technické specifikace sítě by měly zajistit, aby shromažďované údaje zůstaly v domácí síti, není-li nutný jejich přenos jinam nebo pokud subjekt údajů nesouhlasil s jejich předáním. Systém by měl být navržen tak, aby bylo zajištěno, že v případě předávání osobních údajů jsou vyfiltrovány nebo odstraněny údaje, které nejsou pro splnění daného účelu předání potřebné. Celkovým cílem by mělo být to, aby byly zpracovávány a předávány co nejmenší možné objemy údajů.

Pracovní skupina rovněž doporučuje navrhnout systémy tak, aby umožňovaly přístup k osobním údajům pouze v rozsahu nezbytném pro plnění úlohy správce údajů. Všechny strany, které mají přístup k osobním údajům, by měly být prověřeny, zda jsou náležitými a příslušnými příjemci osobních údajů, a měly by mít přístup pouze

k osobním údajům, které potřebují pro plnění své úlohy. Nad tento rámec by neměly mít k osobním údajům přístup.

**Uchovávání osobních údajů**

Ve světě před zavedením inteligentního měření vypracovalo odvětví energetiky postupy pro uchovávání osobních údajů pro omezený počet účelů, například vyúčtování. Prostředí inteligentního měření vyvolává nové problémy. Vzhledem k podstatně většímu objemu zpracovávaných údajů je nutno vypracovat politiky a postupy k uchovávání údajů pro nové účely a přezkoumat je s ohledem na stávající účely. Aby bylo zajištěno, že osobní údaje jsou uchovávány pouze po dobu nezbytnou k dosažení stanoveného a zákonného účelu, je nutno dosáhnout jednoznačnějšího pochopení účelů zpracování. To zase správcům umožní prokázat, že osobní údaje jsou uchovávány pouze po nezbytnou dobu. Jedním z účelů, který je zmiňován poměrně často, je například to, že údaje získané z měřicího přístroje umožní poskytovat poradenství ohledně energetické účinnosti. V některých případech může tento druh služby zahrnovat meziroční srovnání a bylo navrženo, že by vhodnou dobou uchovávání osobních údajů za tímto účelem byla lhůta v délce třinácti měsíců. Tato dlouhá doba uchovávání by však byla přijatelná pouze tehdy, pokud subjekt údajů souhlasil s využitím tohoto systému. Při poskytování jiných druhů služeb by se měla vyžadovat mnohem kratší doba uchovávání.

Lze si rovněž představit, že by odběratelé mohli uchovávat mnoho těchto údajů v měřicím přístroji nebo srovnatelném síťovém komunikačním zařízení (jiném než se požaduje pro účely vyúčtování). To by umožnilo, aby subjekt údajů sám rozhodoval o uchovávání údajů. Pokud by tomu tak bylo, je vhodné, aby odběratelé obdrželi systém nápovědy nebo připomínek, který jim bude nápomocen při tomto interním uchovávání údajů.

**Zpracovávání osobních údajů třetími stranami**

Je pravděpodobné, že účast třetích stran / společností poskytujících energetické služby, které zajišťují a podporují zavádění inteligentního měření, bude značná a pracovní skupina se domnívá, že to bude vyžadovat pečlivé zvážení. Vliv a účast třetích stran se budou mezi jednotlivými členskými státy lišit, je však zřejmé, že v případě největšího zasahování do soukromí by zavedení inteligentního měření mohlo vést k obchodování s energetickými profily v zájmu stran, které chtějí obchodovat s energetickými službami.

Postupy, které byly navrženy s cílem pomoci při dodržování předpisů, zahrnují vytvoření hlavního informačního a komunikačního centra, které působí jako kanál pro všechny subjekty, které chtějí získat přístup k údajům odběratelů; kodex, k jehož dodržování se musí všechny strany zavázat, a stanovy, které se vztahují na celé odvětví. Pracovní skupina chce vysvětlit, že čím více zpracování narušuje soukromí, tím přísnější musí být ochranná opatření. Pracovní skupina příslušné regulační orgány důrazně vyzývá, aby přezkoumaly přijatelnost zpracování, které více zasahuje do soukromí.

To vše bude založeno na souhlasu odběratele, přičemž odvětví musí zajistit, aby subjekt údajů mohl tento souhlas udělit vědomě. Pracovní skupina chce objasnit, že je nepřijatelné, aby třetí strany zpracovávaly podrobné údaje o spotřebě energie subjektu údajů bez vědomí a souhlasu tohoto subjektu údajů.

**Bezpečnost**

Jako součást procesu zajišťování ochrany soukromí již ve fázi návrhu určí posouzení rizik pro bezpečnost a ochranu soukromí možná rizika pro bezpečnost údajů. Vzhledem k novosti a rozsáhlým očekáváním, pokud jde o inteligentní síť a související technologie, je úkol spočívající v předjímání bezpečnostních požadavků složitý.

Se zřetelem k těmto skutečnostem toto stanovisko doporučuje, aby v zájmu zmírnění rizika byl tento přístup zajištěn v celém rozsahu, zahrnoval všechny strany a vycházel ze široké škály zkušeností. Bezpečnostní opatření by měla být rovněž navržena spíše v počáteční fázi jako součást architektury sítě než přidávána později.

Pracovní skupina chce objasnit, že aby si byly subjekty údajů jisté, že jejich osobní údaje jsou zpracovávány bezpečně a že je chráněno jejich základní právo na soukromí, je nutno zavést náležitě důkladná ochranná opatření. Tato ochranná opatření se musí vztahovat na celý proces, včetně prvků sítě umístěných v domácnostech, předávání osobních údajů v síti a uchovávání a zpracovávání osobních údajů dodavateli, sítěmi a jinými správci údajů.

Pracovní skupina předpokládá, že inteligentní měřicí přístroje budou mít dlouhou odhadovanou životnost, a proto doporučuje, aby byla ochranná opatření v průběhu času aktualizována a zdokonalována a pravidelně podrobována přezkumu a testování.

Vzhledem k vyššímu množství zpracovávaných osobních údajů je zřejmé, že se zvyšuje rovněž riziko s ohledem na ochranu údajů. Pracovní skupina proto doporučuje, aby technická a organizační ochranná opatření zahrnovala přinejmenším tyto oblasti:

- předcházení neoprávněnému sdělení osobních údajů,
- zachovávání integrity údajů s cílem zabránit nedovoleným úpravám,
- účinné ověřování totožnosti příjemců osobních údajů,
- zamezení tomu, aby byly důležité služby přerušeny kvůli útokům na bezpečnost osobních údajů,
- možnost provádění náležitých auditů osobních údajů, které jsou uchovávány v měřicím přístroji nebo předávány z měřicího přístroje,
- náležité kontroly přístupu a lhůty pro uchovávání údajů,
- agregování údajů, nejsou-li zapotřebí údaje na individuální úrovni.

**Práva jednotlivců, včetně informací poskytovaných subjektům údajů**

Zavádění inteligentních měřicích přístrojů povede k složitým a novým činnostem spojeným se zpracováváním osobních údajů. Většina subjektů údajů nebude mít povědomí o povaze těchto činností a o možném dopadu na jejich soukromí. Pokud

nejsou subjekty údajů informovány o zpracovávání osobních údajů, nemohou samozřejmě přijmout vědomá rozhodnutí v tomto ohledu. Povinnost informovat subjekty údajů o zpracovávání jejich osobních údajů je jednou ze základních zásad směrnice o ochraně údajů. Poskytování těchto informací upravuje článek 10, který vyžaduje, aby správce údajů poskytl subjektu údajů tyto informace:

- totožnost správce údajů a popřípadě jeho zástupce,
- účely zpracování,
- veškeré doplňující informace, které zajišťují, aby bylo zpracování korektní. K těmto informacím patří totožnost příjemců osobních údajů, existence práva na přístup k údajům a práva na jejich opravu.

Správce údajů, který je odpovědný za instalaci a údržbu měřicího přístroje, by měl subjektům údajů objasnit, jaké informace jsou z měřicího přístroje získávány a k čemu jsou používány.

Pokud se na zpracovávání osobních údajů za účelem poskytování služeb subjektům údajů podílejí třetí osoby, musí být o tom subjekty údajů odpovídajícím způsobem informovány. Za určitých okolností může být vhodné umožnit nezávislé kontroly nebo sledování přístupu třetí strany k osobním údajům a používání těchto údajů, aby bylo zajištěno, že subjekty údajů nejsou uváděny v omyl.

**Práva subjektu údajů**

Správci údajů musí dodržovat práva subjektů údajů na přístup a případně na opravu nebo výmaz údajů, které o nich uchovávají. Skutečnost, že nedílnou součástí projektu inteligentního měření je zavedení „domácí sítě“ (kde může odběratel z inteligentního měřicího přístroje získat okamžité informace o svých modelech spotřeby energie a o sazbách), znamená, že je možné zajistit, aby mohly subjekty údajů snadno uplatňovat svá práva pomocí nástrojů, které umožňují přímý přístup k údajům.

Některé technologie však nemusí být s to usnadnit subjektům údajů přístup k jejich údajům. Například jeden z měřicích přístrojů, který se v současnosti testuje v některých členských státech, má pouze malý textový displej. To zákazníkovi neumožní přístup k informacím, které již byly měřicím přístrojem předány, ani zobrazení grafiky, například diagramu zatížení (který je uložen uvnitř měřicího přístroje). Nezdá se proto, že by byl tento displej vhodný pro použití v případě žádosti subjektu údajů o přístup.

**Zpracovávání údajů za účelem předcházení trestné činnosti a jejího vyšetřování**

Směrnice o ochraně údajů upravuje zpracovávání osobních údajů v případě, kdy zpracování přesahuje míru s ohledem na daný účel. Je zřejmé, že podrobný obraz získaný inteligentními měřicími přístroji, který dodavatele informuje o modelech spotřeby energie, umožní určit podezřelé a v některých případech protiprávní činnosti. Pracovní skupina průmyslovému odvětví připomíná, že skutečnost, že existuje tato možnost, neospravedlňuje automaticky rozsáhlé zpracovávání údajů pro tento účel. Je obzvláště důležité zmínit, že pokud osobní údaje souvisí s údajným spácháním trestného činu, považují se tyto osobní údaje za citlivé, a správce údajů by je proto nemohl zpracovávat, pokud se nepoužije čl. 8 odst. 5 směrnice.

**Závěr**

Nástup inteligentního měření, které připravuje půdu pro inteligentní síť, s sebou přináší zcela nový a složitý model vzájemných vztahů, který vyvolává problémy při uplatňování práva v oblasti ochrany údajů. Odpovědi na dotazník generálního ředitelství pro energii prokázaly, že v situaci jednotlivých členských států EU existují velké rozdíly, a to s ohledem na pokrok při zavádění i na smlouvy o dodávkách energie, což situaci dále komplikuje. Co je však naprosto jasné, je to, že inteligentní měření je co do rozsahu obrovské: odhaduje se, že velká většina evropských občanů bude mít do konce tohoto desetiletí v domácnosti instalován inteligentní měřicí přístroj.

Toto stanovisko objasňuje použitelnost práva v oblasti ochrany údajů: bylo prokázáno, že měřicí přístroje zpracovávají osobní údaje, takže se použijí právní předpisy o ochraně údajů.

V tomto stanovisku bylo prokázáno, že inteligentní měření s sebou přináší možnost četných nových způsobů zpracovávání údajů a poskytování služeb odběratelům. Bez ohledu na to, zda je zpracovávání podobné tomu, jaké existovalo v prostředí před zavedením inteligentního měření, nebo zda se jedná o zcela nové zpracovávání, je nutno určit jednoznačně správce údajů a tento si musí být vědom povinností, které vyplývají z právních předpisů týkajících se ochrany údajů, včetně ochrany soukromí již ve fázi návrhu, bezpečnosti a práv subjektu údajů. Subjekty údajů musí být náležitě informovány o způsobu zpracovávání jejich údajů a být si vědomy zásadních rozdílů ve způsobu, jakým jsou jejich údaje zpracovávány, aby v případě, že udělí svůj souhlas, byl tento souhlas platný.

V Bruselu dne 4. dubna 2011

*Za pracovní skupinu*
*předseda*
*Jacob KOHNSTAMM*

# 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 400 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 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**