

Stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie Európskemu parlamentu a Rade o priestore slobody, bezpečnosti a spravodlivosti pre občanov

(2009/C 276/02)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 286,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov, a najmä na jeho článok 41,

PRIJAL TOTO STANOVISKO:

I. ÚVOD

1. Komisia 10. júna 2009 prijala oznámenie Európskemu parlamentu a Rade o priestore slobody, bezpečnosti a spravodlivosti pre občanov⁽¹⁾. V súlade s článkom 41 nariadenia (ES) č. 45/2001 predkladá EDPS toto stanovisko.
2. Komisia pred prijatím oznámenia neformálne konzultovala jeho obsah s EDPS listom z 19. mája 2009. EDPS reagoval na túto konzultáciu 20. mája 2009 zaslaním neformálnych pripomienok, ktorých účelom bolo vylepšiť znenie oznámenia. EDPS aktívne prispel aj k listu zo 14. januára 2009, ktorý vypracovala pracovná skupina pre policajnú a justičnú spoluprácu o viacročnom programe v oblasti slobody, bezpečnosti a spravodlivosti⁽²⁾.
3. V oznámení (bode 1) sa zdôrazňuje, že „Únia musí prijať nový viacročný program, ktorý na základe dosiahnutého pokroku a získaných skúseností o súčasných slabých stránkach, ponúkne v budúcnosti ambiciózne riešenia. Tento

nový program by mal vymedziť priority na nasledujúcich päť rokov“. Tento viacročný program (známy už aj ako „Štokholmský program“) nadviaže na programy z Tampere a Haagu, ktoré boli dôležitými politickými impulzmi pre vytváranie priestoru slobody, bezpečnosti a spravodlivosti.

4. Oznámenie má tvoriť základ tohto nového viacročného programu. EDPS v tejto súvislosti poznamenáva, že aj napriek tomu, že viacročné programy nie sú záväznými nástrojmi, významne ovplyvňujú tvorbu politiky inštitúciami v dotknutých oblastiach, keďže mnohé z konkrétnych legislatívnych aj nelegislatívnych krokov vyplynú práve z uvedeného programu.
5. Samotné oznámenie sa musí vnímať z tejto perspektívy. Predstavuje ďalší krok v diskusii, ktorá sa viac-menej začala na základe dvoch správ, ktoré v júni 2008 predložili tzv. poradné skupiny pre otázky budúcnosti zriadené predsedníctvom Rady, aby predkladali návrhy: ide o správu „Sloboda, bezpečnosť, súkromie – európske vnútorné veci v otvorenom svete“⁽³⁾ a „Navrhované riešenia programu EÚ pre budúcnosť spravodlivosti“⁽⁴⁾.

II. HLAVNÝ OBSAH STANOVISKA

6. Toto stanovisko nie je len reakciou na oznámenie, ale predstavuje aj príspevok EDPS k všeobecnejšej diskusii o budúcnosti priestoru slobody, bezpečnosti a spravodlivosti, ktorej výsledkom musí byť nový strategický pracovný program (Štokholmský program), ako to oznámilo švédske predsedníctvo EÚ⁽⁵⁾. Toto stanovisko sa zaoberá aj niektorými dôsledkami možného nadobudnutia platnosti Lisabonskej zmluvy.
7. V časti III sú špecifikované hlavné hľadiská stanoviska a v časti IV sa nachádza všeobecné posúdenie oznámenia.
8. Časť V je venovaná otázke ako reagovať na potrebu nepretržitého dodržiavania ochrany súkromia a osobných údajov v súvislosti s narastajúcou výmenou osobných údajov. Pozornosť je upriamená na bod 2.3. oznámenia o ochrane osobných údajov a súkromia a vo všeobecnosti na potrebu ďalších legislatívnych a nelegislatívnych opatrení s cieľom zlepšiť rámec ochrany údajov.

⁽¹⁾ KOM(2009) 262 v konečnom znení („oznámenie“).

⁽²⁾ Zatiaľ neuverejnené. Pracovná skupina pre policajnú a justičnú spoluprácu (WPPP) bola zriadená na konferencii európskych komisárov pre ochranu údajov, aby pripravila ich pozície v oblasti presadzovania práva a aby v ich mene konala v naliehavých záležitostiach.

⁽³⁾ Dokument Rady č. 11657/08. Ďalej len „správa o vnútorných veciach“.

⁽⁴⁾ Dokument Rady č. 11549/08 (ďalej len „správa o oblasti spravodlivosti“).

⁽⁵⁾ Pracovný program vlády počas predsedníctva v EÚ, <http://www.regeringen.se>

9. V časti VI sa hovorí o potrebách a možnostiach uchovávaní a výmeny informácií a prístupu k nim ako prostriedkoch na presadzovanie práva alebo, ako sa uvádza v oznámení, na zabezpečenie „Európy, ktorá chráni“. Bod 4 oznámenia obsahuje niekoľko cieľov súvisiacich s tokom informácií a technologickými nástrojmi, najmä v bodoch 4.1.2. (Kontrola informácií), 4.1.3. (Mobilizácia potrebných technologických nástrojov) a 4.2.3.2. (Informačné systémy). Zriadenie európskeho informačného modelu (uvedené v odseku 4.1.2.) je možné považovať za najodvážnejší návrh v tomto kontexte. V stanovisku EDPS sa tento návrh podrobne analyzuje.
10. Časť VII sa v krátkosti dotýka osobitnej témy v rámci priestoru slobody, bezpečnosti a spravodlivosti súvisiacej s ochranou údajov, a to prístupu k spravodlivosti a elektronickej justícii.
- ### III. HLADISKÁ STANOVISKA
11. Potreba ochrany základných práv je v tomto stanovisku hlavným východiskovým bodom analýzy oznámenia a vo všeobecnosti budúcnosti priestoru slobody, bezpečnosti a spravodlivosti v podobe, ktorú mu dá nový viacročný program. Stanovisko ďalej vychádza z príspevkov EDPS k tvorbe politiky EÚ v tejto oblasti, najmä v súvislosti s jeho úlohou poradcu. EDPS doteraz prijal viac ako tridsať stanovísk a pripomienok k iniciatívam vyplývajúcim z Haagskeho programu, ktoré je možné nájsť na webovej stránke EDPS.
12. EDPS pri posudzovaní oznámenia zohľadňuje najmä štyri hľadiská, ktoré sú relevantné pre budúcnosť priestoru slobody, bezpečnosti a spravodlivosti. Všetky tieto hľadiská zohrávajú kľúčovú úlohu aj v oznámení.
13. Prvým hľadiskom je exponenciálny rast digitálnych informácií o občanoch, čo je výsledkom vyvíjajúcich sa informačných a komunikačných technológií⁽⁶⁾. Spoločnosť sa vyvíja smerom k spoločnosti, ktorá sa často nazýva aj ako „monitorovaná spoločnosť“, v ktorej každá operácia a skoro každý pohyb občanov môže vytvoriť digitálny záznam. Takzvané „internet vecí“ a „inteligentné prostredie“ sa rýchlo vyvíjajú prostredníctvom používania rádiových frekvenčných identifikačných značiek [RFID (Radio Frequency Identification) tag]. V čoraz väčšej miere sa používajú digitalizované znaky ľudského tela (biometrické údaje). To všetko vedie k čoraz prepojenejšiemu svetu, v ktorom orga-
- nizácie zabezpečujúce verejnú bezpečnosť môžu mať prístup k obrovskému množstvu potenciálne užitočných informácií, čo môže priamo ovplyvniť život dotknutých osôb.
14. Druhým hľadiskom je internacionalizácia. Na jednej strane nie je v digitálnej ére výmena informácií obmedzovaná vonkajšími hranicami Európskej únie, no na strane druhej existuje zväčšujúca sa potreba medzinárodnej spolupráce v širokej škále činností EÚ v oblasti slobody, bezpečnosti a spravodlivosti: boj proti terorizmu, policajná a justičná spolupráca, spravodlivosť v občianskych veciach a kontrola hraníc sú len niekoľkými príkladmi.
15. Tretím hľadiskom je používanie údajov na účely presadzovania práva: dôsledkom nedávnych hrozieb pre spoločnosť, či už súvisiacich s terorizmom alebo nie, sú (požiadavky na) väčšie možnosti pre orgány presadzovania práva zhromažďovať, uchovávať a vymieňať osobné údaje. V mnohých prípadoch sa na tom aktívne spolupodieľajú súkromné subjekty, ako o tom okrem iného svedčí smernica o uchovávaní údajov⁽⁷⁾ a rôzne nástroje súvisiace s osobným záznamom o cestujúcom (PNR)⁽⁸⁾.
16. Štvrtým hľadiskom je voľný pohyb. Postupné vytváranie priestoru slobody, bezpečnosti a spravodlivosti si vyžaduje, aby sa naďalej odstraňovali vnútorné hranice a možné prekážky, ktoré by bránili voľnému pohybu v danej oblasti. Nové nástroje v tejto oblasti by v žiadnom prípade nemali opätovne zavádzať žiadne prekážky. Voľný pohyb v tejto súvislosti pozostáva z voľného pohybu osôb na jednej strane a z voľného pohybu (osobných) údajov na strane druhej.
17. Štyri uvedené hľadiská preukazujú, že kontext, v ktorom sa informácie používajú, sa rýchle mení. V tejto súvislosti nemôžu existovať pochybnosti o dôležitosti silného mechanizmu na ochranu základných práv občanov, predovšetkým ochranu súkromia a údajov. Práve z týchto dôvodov si EDPS zvolil potrebu ochrany za hlavný východiskový bod svojej analýzy, ako sa už uviedlo v bode 11.

⁽⁶⁾ Správa o vnútorných veciach v tejto súvislosti hovorí dokonca o „digitálnom tsunami“.

⁽⁷⁾ Smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES, Ú. v. EÚ L 105, 13.4.2006, s. 54.

⁽⁸⁾ Pozri napr. Dohodu medzi Európskou úniou a Spojenými štátmi americkými o spracovaní a postupovaní údajov z osobného záznamu o cestujúcom (PNR) leteckými dopravcami Ministerstvu vnútornej bezpečnosti Spojených štátov amerických (DHS) (Dohoda PNR z roku 2007), Ú. v. EÚ L 204, 4.8.2007, s. 18, a návrh rámcového rozhodnutia Rady o využívaní osobných záznamov o cestujúcich (PNR) na účely presadzovania práva, KOM(2007) 654 v konečnom znení.

IV. VŠEOBECNÉ POSÚDENIE

18. V oznámení a Štokholmskom programe sú vymedzené plány EÚ na najbližších päť rokov, ktorých účinky môžu byť aj dlhodobejšie. EDPS poznamenáva, že oznámenie je napísané v takzvanom „lisabonskom neutrálnom“ štýle. EDPS plne chápe prečo sa Komisia rozhodla k oznámeniu pristupovať týmto spôsobom, avšak zároveň s poľutovaním konštatuje, že sa v oznámení plne nevyužili ďalšie možnosti, ktoré ponúka Lisabonská zmluva. V tomto stanovisku sa na hľadisko Lisabonskej zmluvy kladie väčší dôraz.

19. Oznámenie vychádza z výsledkov činností EÚ pri vytváraní priestoru slobody, bezpečnosti a spravodlivosti dosiahnutých v posledných rokoch. Tieto výsledky je možné charakterizovať ako ovplyvnené udalosťami, zamerané na opatrenia, ktoré rozširujú právomoci orgánov presadzovania práva a narušajúce súkromie občanov. Je tomu tak predovšetkým v prípade oblastí, v ktorých sa intenzívne používajú a vymieňajú osobné údaje a ktoré sú z tohto dôvodu významné, pokiaľ ide o ochranu údajov. Výsledky boli ovplyvnené udalosťami, keďže vonkajšie udalosti, ako napr. útoky z 11. septembra a bombové útoky v Madride a Londýne, boli silnými impulzmi pre legislatívnu činnosť. Príkladom môže byť prenos údajov o cestujúcich do Spojených štátov, ktorý je dôsledkom útokov z 11. septembra⁽⁹⁾, zatiaľ čo bombové útoky v Londýne viedli k prijatiu smernice o uchovávaní údajov 2006/24/ES⁽¹⁰⁾. Dôraz sa kládol na opatrenia narušajúce súkromie, keďže zákonodarca EÚ sa zamerával na opatrenia, ktoré zjednodušujú používanie údajov a ich výmenu, zatiaľ čo opatrenia zamerané na zabezpečenie ochrany osobných údajov sa prerokovávali s menšou naliehavosťou. Hlavným ochranným opatrením, ktoré sa prijalo po rokovaniach v rámci Rady, ktoré trvali tri roky, je rámcové rozhodnutie Rady 2008/977/SVV o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach⁽¹¹⁾. Výsledkom je rámcové rozhodnutie Rady, ktoré nie je plne uspokojivé (pozri body 29 a 30).

20. Skúsenosti z nedávnych rokov poukazujú na to, že je potrebné zvážiť dôsledky, ktoré vyplynú pre orgány presadzovania práva a európskych občanov z nových nástrojov, ešte pred ich prijatím. V rámci tohto zváženia by sa mali riadne zohľadniť náklady na ochranu súkromia a účinnosť nástrojov pri presadzovaní práva, a to po prvýkrát pri

navrhnutí a prerokovaní nových nástrojov, a tiež po tom, ako sa tieto nástroje zavedú, prostredníctvom pravidelných revízií. Je tiež dôležité, aby sa toto zväzovanie uskutočnilo predtým, ako sa v novom viacročnom programe stanovia hlavné iniciatívy pre blízku budúcnosť.

21. EDPS je rád, že sa v oznámení ochrana základných práv a najmä ochrana osobných údajov považuje za jednu z kľúčových otázok priestoru slobody, bezpečnosti a spravodlivosti v budúcnosti. V bode 2 oznámenia sa EÚ hodnotí ako jedinečná oblasť, v ktorej existuje ochrana základných práv založená na spoločných hodnotách. Je tiež dobré, že sa pristúpenie k Európskemu dohovoru o ľudských právach uvádza ako priorita, priam ako najvyššia priorita uvedená v oznámení. Uvedené pristúpenie je významným krokom vpred pri zabezpečovaní harmonického a jednotného systému ochrany základných práv. V neposlednom rade sa ochrane údajov v oznámení prisúdilo významné miesto.

22. Toto zameranie oznámenia preukazuje silný zámer zabezpečiť ochranu práv občanov a prostredníctvom nej zaistiť vyrovnanjší prístup. Vlády potrebujú primerané nástroje na zaručenie bezpečnosti občanov, avšak v rámci našej európskej spoločnosti musia plne dodržiavať základné práva občanov. Aby bol priestor slobody, bezpečnosti a spravodlivosti naozaj pre občanov⁽¹²⁾, Európska únia musí zachovať túto rovnováhu.

23. Podľa názoru EDPS oznámenie berie potrebu tejto rovnováhy, ako aj potrebu ochrany osobných údajov vážne do úvahy. Uznáva sa v ňom, že je potrebné zmeniť dôraz. Je to veľmi dôležité, keďže politiky v oblasti slobody, bezpečnosti a spravodlivosti by nemali viesť k postupnému prechodu na monitorovanú spoločnosť. EDPS očakáva, že Rada bude k tejto otázke v Štokholmskom programe pristupovať rovnako, aj prostredníctvom uznania smerovaní uvedených v bode 25 nižšie.

24. Dôležitosť tohto prístupu je o to väčšia, že priestor slobody, bezpečnosti a spravodlivosti je priestorom, ktorý „formuje životné podmienky občanov, najmä súkromný priestor ich vlastnej zodpovednosti a osobnej a spoločenskej bezpečnosti, ktorý je chránený základnými právami“, ako to nedávno zdôraznil ústavný súd Nemecka v rozhodnutí z 30. júna 2009 týkajúcom sa Lisabonskej zmluvy⁽¹³⁾.

⁽⁹⁾ Dohoda PNR z roku 2007 uvedená v predchádzajúcej poznámke pod čiarou a dohody, ktoré jej predchádzali.

⁽¹⁰⁾ Smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES, Ú. v. EÚ L 105, 13.4.2006, s. 54. Aj keď je právnym základom článok 95 Zmluvy o ES, smernica bola priamou reakciou na bombové útoky v Londýne.

⁽¹¹⁾ Rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach, Ú. v. EÚ L 350, 30.12.2008, s. 60.

⁽¹²⁾ Pozri názov oznámenia.

⁽¹³⁾ Tlačová správa spolkového ústavného súdu Nemecka č. 72/2009 z 30. júna 2009, ods. 2 písm. c).

25. EDPS zdôrazňuje, že v takomto priestore:

- by sa informácie mali vymieňať medzi orgánmi členských štátov a v prípade potreby aj medzi relevantnými európskymi orgánmi alebo databázami na základe primeraných a účinných mechanizmov, ktoré plne dodržiavajú základné práva občanov a zabezpečujú vzájomnú dôveru.
- To si vyžaduje nielen dostupnosť informácií v kombinácii so vzájomným uznaním právnych systémov členských štátov (a EÚ), ale aj harmonizáciu noriem ochrany informácií, napríklad, avšak nie výlučne, prostredníctvom spoločného rámca ochrany údajov.
- Tieto spoločné normy by sa nemali uplatňovať len na situácie s cezhraničným rozmerom. Vzájomná dôvera môže existovať iba vtedy, ak sú normy pevné a ak sa vždy dodržiavajú, a to bez rizika, že sa prestanú uplatňovať, keď nebude alebo už viac nebude zrejмый cezhraničný rozmer. Navyše nemôžu rozdiely medzi „vnútornými“ a „cezhraničnými“ údajmi, najmä v prípadoch používania informácií, spolu v praxi fungovať⁽¹⁴⁾.

V. NÁSTROJE NA OCHRANU ÚDAJOV

V.1. Smerom ku komplexnému systému ochrany údajov

26. EDPS schvaľuje strategický prístup, v ktorom sa ochrane údajov v oznámení prisúdilo popredné miesto. Mnoho iniciatív v oblasti slobody, bezpečnosti a spravodlivosti sa totiž spolieha na používanie osobných údajov, a preto je dobrá ochrana údajov pre ich úspech mimoriadne dôležitá. Rešpektovanie súkromia a ochrana údajov nie sú len zákonnou povinnosťou, ktorá na úrovni EÚ získava na dôležitosť, ale predstavujú aj oblasť, ktorá je mimoriadne dôležitá pre európskych občanov, ako o tom svedčia výsledky Eurobarometra⁽¹⁵⁾. Obmedzenie prístupu k osobným údajom je tiež mimoriadne dôležité na zabezpečenie dôvery zo strany agentúr presadzovania práva.
27. V bode 2.3. oznámenia sa uvádza, že je potrebný komplexný systém ochrany údajov, ktorý sa bude týkať všetkých oblastí, v ktorých má EÚ právomoci⁽¹⁶⁾. EDPS plne podporuje tento cieľ, nezávisle od nadobudnutia platnosti Lisabonskej zmluvy. Poznomenáva aj to, že takýto

systém nemusí nevyhnutne znamenať jeden právny rámec uplatniteľný na všetky typy spracovania údajov. V rámci platných zmlúv sú možnosti prijatia jedného, komplexného právneho rámca uplatniteľného na všetky typy spracovania údajov obmedzené vzhľadom na pilierovú štruktúru a skutočnosť, že – prinajmenšom v prvom pilieri – ochrana údajov spracovávaných európskymi inštitúciami sa uskutočňuje na oddelenom právnom základe (článok 286 Zmluvy o ES). EDPS však poukazuje na to, že je možné zaviesť niekoľko zlepšení, a to plným využitím možností, ktoré ponúkajú platné zmluvy, ako to už zdôraznila Komisia vo svojom oznámení „Implementácia Haagskeho programu – ďalšie smerovanie“⁽¹⁷⁾. Po nadobudnutí platnosti Lisabonskej zmluvy článkom 16 Zmluvy o fungovaní Európskej únie sa ustanoví potrebný právny rámec pre jeden komplexný právny rámec uplatniteľný na všetky typy spracovania údajov.

28. EDPS poznamenáva, že je mimoriadne dôležité, aby sa – v každom prípade – zabezpečila jednotnosť právneho rámca ochrany údajov, a to v prípade potreby prostredníctvom harmonizácie a konsolidácie rôznych právnych nástrojov uplatniteľných na priestor slobody, bezpečnosti a spravodlivosti.

V rámci platných zmlúv

29. Prvý krok sa urobil nedávno prijatím rámcového rozhodnutia Rady 2008/977/SVV⁽¹⁸⁾. Tento právny nástroj sa však nemôže klasifikovať ako komplexný rámec v podstate preto, že jeho ustanovenia nemajú všeobecnú pôsobnosť. Neuplatňujú sa na vnútorné situácie, kedy majú osobné údaje pôvod v členskom štáte, ktorý ich používa. Toto obmedzenie bude prirodzene znižovať pridanú hodnotu rámcového rozhodnutia Rady, pokiaľ sa všetky členské štáty nerozhodnú zahrnúť vnútorné situácie do vnútroštátnych vykonávacích právnych predpisov, čo nie je veľmi pravdepodobné.
30. Druhým dôvodom prečo si EDPS myslí, že z dlhodobého hľadiska rámcové rozhodnutie Rady 2008/977/SVV neposkytuje uspokojivý rámec ochrany údajov v oblasti slobody, bezpečnosti a spravodlivosti je skutočnosť, že niekoľko základných ustanovení nie je v súlade so smernicou 95/46/ES. V rámci platných zmlúv by druhým krokom mohlo byť rozšírenie rozsahu pôsobnosti a zosúladenie rámcového rozhodnutia Rady so smernicou 95/46/ES.

31. Ďalší impulz na realizáciu komplexného systému ochrany údajov by mohlo poskytnúť vypracovanie jasnej a dlhodobej vízie. Táto vízia by mohla obsahovať globálny a jednotný prístup k vymedzeniu zhromažďovania a výmeny údajov – ako aj používania existujúcich databáz

⁽¹⁴⁾ EDPS sa tejto poslednej záružke venoval bližšie v stanovisku z 19. decembra 2005 k návrhu rámcového rozhodnutia Rady o ochrane osobných údajov spracovávaných v rámci policajnej a súdnej spolupráce v trestných veciach (KOM(2005) 475 v konečnom znení), Ú. v. EÚ C 47, 25.2.2006, s. 27, ods. 30 – 32.

⁽¹⁵⁾ Ochrana údajov v Európskej únii – „Pohľad občanov“ – analytická správa, Flash Eurobarometer Series 225, január 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

⁽¹⁶⁾ Pozri aj prioritné oblasti činnosti uvedené v oznámení.

⁽¹⁷⁾ KOM(2006) 331 v konečnom znení z 28. júna 2006.

⁽¹⁸⁾ Pozri poznámku pod čiarou č. 11.

– a zároveň záruky ochrany údajov. Táto vízia by mala zabrániť zbytočnému prekrývaniu sa a zdvojovaniu nástrojov (a tým spracovávaniu osobných údajov). Mala by tiež podnietiť jednotnosť politik EÚ v tejto oblasti, ako aj dôveru občanov voči spôsobu, akým orgány verejnej moci zaobchádzajú s údajmi o nich. EDPS odporúča, aby Rada v Štokholmskom programe oznámila potrebu jasnej a dlhodobej vízie.

32. Ďalším odporúčaním EDPS je zhodnotiť a zväziť opatrenia, ktoré sa už v tejto oblasti prijali, ich konkrétnu realizáciu a účinnosť. Toto hodnotenie by malo riadne zohľadniť náklady na ochranu súkromia a účinnosť pri presadzovaní práva. Ak toto hodnotenie preukáže, že niektoré opatrenia neprinášajú plánované výsledky alebo že nie sú primerané na požadované účely, mali by sa zväziť tieto kroky:

— V prvom rade zmena a doplnenie alebo zrušenie opatrení, pokiaľ sa nezdajú byť dostatočne opodstatnené pri dosahovaní konkrétnej pridanej hodnoty pre orgány presadzovania práva a pre európskych občanov.

— V druhom rade posúdenie možností na zlepšenie uplatňovania existujúcich opatrení.

— Až v treťom rade návrh nových legislatívnych opatrení, ak by tieto nové opatrenia mali byť potrebné na požadované účely. Nové nástroje by sa mali prijať iba vtedy, ak budú mať jasnú a konkrétnu pridanú hodnotu pre orgány presadzovania práva a pre európskych občanov.

EDPS odporúča, aby sa v Štokholmskom programe uviedol odkaz na systém na zhodnotenie existujúcich opatrení.

33. V neposlednom rade by sa osobitný dôraz mal klásť na zlepšenie realizácie existujúcich záruk v súlade s oznámením Komisie o pokračovaní pracovného programu pre lepšiu implementáciu smernice o ochrane údajov⁽¹⁹⁾ a návrhmi EDPS uvedenými v stanovisku k uvedenému oznámeniu⁽²⁰⁾. Komisia nanešťastie nemá možnosť začať v treťom pilieri konanie o porušení právnych predpisov.

⁽¹⁹⁾ KOM(2007) 87 v konečnom znení zo 7. marca 2007.

⁽²⁰⁾ Stanovisko z 25. júla 2007, Ú. v. EÚ C 255, 27.10.2007, s. 1, najmä odsek 30.

V rámci Lisabonskej zmluvy

34. Lisabonská zmluva otvára priestor pre skutočný komplexný rámec ochrany údajov. V článku 16 ods. 2 Zmluvy o fungovaní Európskej únie sa od Rady a Európskeho parlamentu vyžaduje, aby stanovili pravidlá vzťahujúce sa na ochranu údajov, ktoré majú dodržiavať inštitúcie, orgány, úrady a agentúry EÚ, členské štáty pri vykonávaní činností, ktoré spadajú do rozsahu práva Unie a súkromné osoby a subjekty.

35. EDPS chápe dôraz v oznámení kladený na komplexný systém ochrany údajov ako ambíciu Komisie navrhnuť právny rámec uplatniteľný na všetky typy spracovateľských činností. Plne schvaľuje túto ambíciu, ktorá posilňuje jednotnosť systému, zabezpečuje právnu istotu, a tým zlepšuje ochranu údajov. Konkrétne by sa tak v budúcnosti dalo predísť ťažkostiam pri hľadaní deliacej čiary medzi piliermi v prípade, kedy sa údaje zhromaždené v súkromnom sektore na komerčné účely neskôr použijú na presadzovanie práva. Táto deliaca čiara medzi piliermi plne neodráža skutočnosť, o čom svedčia aj dôležité rozsudky Súdneho dvora v súvislosti s PNR⁽²¹⁾ a uchovávaním údajov⁽²²⁾.

36. EDPS navrhuje, aby sa zmysel komplexného systému ochrany údajov zdôraznil v Štokholmskom programe. Ten svedčí o tom, že takýto systém nie je len otázkou preferencie, ale aj nevyhnutnosťou z dôvodu meniacich sa praktík pri používaní údajov. EDPS odporúča, aby sa v Štokholmskom programe ako priorita uviedla potreba nového legislatívneho rámca, ktorý okrem iného nahradí rámcové rozhodnutie Rady 2008/977/SVV.

37. EDPS zdôrazňuje, že pojem komplexného systému ochrany údajov založeného na všeobecnom právnom rámci nevyklučuje prijatie dodatočných pravidiel na ochranu údajov pre policajný a justičný sektor. Tieto dodatočné pravidlá by mohli zohľadniť osobitné potreby orgánov presadzovania práva tak, ako to predpokladá Vyhlásenie 21 tvoriace prílohu k Lisabonskej zmluve⁽²³⁾.

V.2. Zopakovanie zásad ochrany údajov

38. V oznámení sa uvádzajú technologické zmeny, ktoré menia spôsob komunikácie medzi jednotlivcami a verejnými a súkromnými subjektmi. To si podľa Komisie vyžaduje zopakovanie niekoľkých základných zásad ochrany údajov.

⁽²¹⁾ Rozsudok Súdneho dvora z 30. mája 2006, Európsky parlament/Rada Európskej únie (C-317/04) a Komisia Európskych spoločenstiev (C-318/04), spojené veci C-317/04 a C-318/04, Zb. [2006], s. I-4721.

⁽²²⁾ Rozsudok Súdneho dvora z 10. februára 2009, Írsko/Európsky parlament a Rada Európskej únie, Vec C-301/06, zatiaľ neuverejnený.

⁽²³⁾ Pozri Vyhlásenie 21 o ochrane osobných údajov v oblasti justičnej spolupráce v trestných veciach a policajnej spolupráce, ktoré tvorí prílohu záverečného aktu medzivládnej konferencie, na ktorej sa prijala Lisabonská zmluva, Ú. v. EÚ C 115, 9.5.2008, s. 345.

39. EDPS víta tieto zámery uvedené v oznámení. Zhodnotenie účinnosti týchto zásad vo svetle technologických zmien je nesmierne užitočné. V prvom rade je dôležité poznamenať, že zopakovanie a opätovné potvrdenie zásad ochrany údajov nemusí vždy priamo súvisieť s technickým rozvojom. Môže byť potrebné aj z dôvodu iných hľadísk stanovených v časti III vyššie, internacionalizácie, zvýšeného používania údajov pri presadzovaní práva a voľnom pohybe.
40. Podľa názoru EDPS sa toto hodnotenie môže tiež zahrnúť do verejnej konzultácie, ktorú oznámila Komisia na konferencii s názvom „Osobné konzultácie, ktorú oznámila Komisia na konferencii s názvom údaje – väčšia miera používania, väčšia ochrana“, ktorá sa uskutočnila 19. a 20. mája 2009. Táto verejná konzultácia by mohla byť hodnotným prínosom⁽²⁴⁾. EDPS navrhuje, aby Rada v texte Štokholmského programu a Komisia vo svojich verejných vyhláseniach týkajúcich sa uvedenej konzultácie zdôraznili prepojenie medzi zámermi oznámenia v bode 2.3. a verejnou konzultáciou o budúcnosti ochrany údajov.
41. Ako príklad toho, čoho by sa mohlo toto hodnotenie týkať, uvádzame tieto body:
- Osobné údaje v priestore slobody, bezpečnosti a spravodlivosti budú mať pravdepodobne osobitne citlivú povahu, ako napr. údaje týkajúce sa odsúdení za trestné činy, policajné údaje a biometrické údaje, ako napr. odtlačky prstov a profily DNA.
 - Ich spracovanie by mohlo mať negatívne dôsledky na dotknuté osoby, najmä ak sa vezmú do úvahy donucovacie právomoci orgánov presadzovania práva. Okrem toho sa monitorovanie a analýza údajov čoraz častejšie vykonávajú automatizovane, celkom často aj bez ľudského zásahu. Technológia umožňuje používanie databáz s osobnými údajmi na všeobecné vyhľadávanie (hlbkové prehľadávanie údajov, vytváranie profilov atď.). Zákonné povinnosti, na ktorých sa spracovanie údajov zakladá, by mali byť jasne stanovené.
 - Základným kameňom práva zabezpečujúceho ochranu údajov je, že sa osobné údaje musia zhromažďovať na konkrétne účely a nesmú sa ďalej používať spôsobmi, ktoré s týmito účelmi nie sú zlučiteľné. Používanie údajov na nezlučiteľné účely by sa malo umožniť, iba ak je tak stanovené zákonom a nevyhnutné pre sledovanie osobitných verejných záujmov, napr. záujmov uvedených v článku 8 ods. 2 Európskeho dohovoru o ľudských právach.
 - Potreba dodržiavať zásadu obmedzenia účelu môže mať dôsledky na súčasné trendy v používaní údajov. Orgány
- presadzovania práva používajú údaje, ktoré zhromaždili súkromné spoločnosti na komerčné účely v odvetví telekomunikácií, dopravy a financií. Navyše sa budujú rozsiahle informačné systémy, napríklad v oblasti imigrácie a kontroly hraníc. Umožňujú sa prepojenia a prístupy k databázam, čím sa rozširuje škála účelov, na ktoré sa osobné údaje pôvodne zhromaždili. Je potrebné zvážiť tieto súčasné trendy, ako aj možné úpravy a/alebo dodatočné záruky tam, kde je to potrebné.
- Popri zásadách ochrany údajov uvedených v oznámení by sa hodnotenie malo venovať aj potrebe transparentnosti spracovania, čím by sa dotknutej osobe umožnilo vykonávanie jej práv. Transparentnosť je mimoriadne ťažkým problémom v oblasti presadzovania práva najmä preto, že by sa v záujme transparentnosti nemalo ohroziť vyšetrovanie.
 - Mali by sa nájsť riešenia pre výmeny s tretími krajinami.
42. Toto hodnotenie by sa ďalej malo zamerať na možnosti zlepšenia účinnosti uplatňovania zásad ochrany údajov. V tejto súvislosti by mohlo byť užitočné sústrediť sa na nástroje, ktoré by mohli rozšíriť zodpovednosť prevádzkovateľov. Tieto nástroje musia umožniť plnú zodpovednosť prevádzkovateľov za správu údajov. „Dobrá správa údajov“ je v tejto súvislosti užitočným pojmom. Zahŕňa všetky právne, technické a organizačné prostriedky, ktorými organizácie zabezpečujú plnú zodpovednosť za spôsob, ktorým sa s údajmi manipuluje, ako napr. plánovanie a kontrolu, používanie vhodnej technológie, primerané zaškolenie zamestnancov, audit súladu s legislatívou a pod.

V.3. Technológie nenarušujúce súkromie

43. EDPS je rád, že sa v bode 2.3. oznámenia uvádza udeľovanie certifikátov o nenarúšaní súkromia. Okrem uvedeného by sa mohol zaviesť odkaz aj na „rešpektovanie súkromia už od návrhu systému“ a potrebu identifikovať „najlepšie dostupné postupy“, ktoré sú v súlade s rámcom ochrany údajov EÚ.
44. Podľa názoru EDPS by „rešpektovanie súkromia už od návrhu systému“ a technológie nenarušujúce súkromie mohli predstavovať užitočné nástroje pre lepšiu ochranu, ako aj na účinnejšie používanie informácií. EDPS navrhuje dve cesty vpred, ktoré sa vzájomne nevyklučujú:
- Zavedenie certifikátov o rešpektovaní súkromia a ochrane údajov⁽²⁵⁾ ako možnosti pre tvorcov a používateľov informačných systémov, či už s podporou financovania z EÚ alebo právnych predpisov EÚ.

⁽²⁴⁾ Pracovná skupina článku 29 pre ochranu údajov, v ktorej pôsobí aj EDPS, sa rozhodla intenzívne sa podieľať na tejto verejnej konzultácii.

⁽²⁵⁾ Príkladom takéhoto systému je európsky systém osvedčení o zachovaní dôverného charakteru informácií (EuroPriSe).

— Zákonná povinnosť pre tvorcov a používateľov informačných systémov používať systémy, ktoré sú v súlade so zásadou rešpektovania súkromia už od návrhu systému. To si môže vyžadovať rozšírenie súčasného rozsahu práva v oblasti ochrany údajov s cieľom zvýšiť zodpovednosť tvorcov za informačné systémy, ktoré vytvoria ⁽²⁶⁾.

EDPS navrhuje, aby sa tieto možné cesty vpred uviedli v Štokholmskom programe.

V.4. Vonkajšie hľadiská

45. Ďalšou témou uvedenou v oznámení je tvorba a presadzovanie medzinárodných noriem na ochranu údajov. V súčasnosti prebieha mnoho činností s cieľom zostaviť realizovateľné normy na globálne použitie, ktoré vykonáva napríklad medzinárodná konferencia komisárov pre ochranu údajov a súkromia. V blízkej budúcnosti môžu tieto činnosti viesť k medzinárodnej dohode. EDPS navrhuje, aby sa v Štokholmskom programe tieto činnosti podporili.
46. V oznámení sa tiež uvádza uzavretie dvojstranných dohôd založených na pokroku, ktorý sa dosiahol spolu so Spojenými štátmi. EDPS je tiež toho názoru, že je potrebný jasný právny rámec na prenos údajov do tretích krajín, a preto uvítal spoločnú prácu orgánov EÚ a USA v rámci kontaktnej skupiny na vysokej úrovni súvisiacu s možným transatlantickým nástrojom na ochranu údajov, pričom vyzýva k väčšej jasnosti a zameraniu na osobitné otázky ⁽²⁷⁾. V tejto súvislosti je tiež zaujímavé spomenúť myšlienky uvedené v správe o vnútorných veciach a týkajúce sa euroatlantického priestoru spolupráce v oblasti slobody, bezpečnosti a spravodlivosti, o ktorom by mala EÚ podľa uvedenej správy rozhodnúť do roku 2014. Vytvorenie tohto priestoru nebude možné bez riadnych záruk ochrany údajov.
47. Podľa EDPS by mali európske normy na ochranu údajov, založené na Dohovore Rady Európy č. 108 na ochranu jednotlivcov pokiaľ ide o automatické spracovanie osobných údajov ⁽²⁸⁾ a judikatúre Európskeho súdneho dvora a Európskeho súdu pre ľudské práva, určiť úroveň ochrany vo všeobecnej dohode so Spojenými štátmi o ochrane

a výmene údajov. Táto všeobecná dohoda by mohla tvoriť základ pre osobitné dohovory o výmene osobných údajov. Táto dohoda je ešte dôležitejšia vo svetle zámeru uvedeného v bode 4.2.1. oznámenia, podľa ktorého musí Európska únia v prípade potreby uzavrieť dohody o policajnej spolupráci.

48. EDPS plne chápe potrebu posilnenia medzinárodnej spolupráce, v niektorých prípadoch aj s krajinami, ktoré nechránia základné práva. Je však ⁽²⁹⁾ nesmierne dôležité zohľadniť skutočnosť, že táto medzinárodná spolupráca pravdepodobne vyústi do značného zvýšenia objemu zhromažďovaných a medzinárodne prenášaných údajov. Je preto nevyhnutné, aby sa zásady spravodlivého a zákonného spracovania – ako aj zásady riadneho postupu vo všeobecnosti – uplatňovali aj na zhromažďovanie a prenos osobných údajov mimo hraníc Únie a aby sa osobné údaje prenášali do tretích krajín alebo medzinárodných organizácií, iba ak dotknuté tretie strany zabezpečia primeranú úroveň ochrany údajov alebo poskytnú iné vhodné záruky.
49. Záverom EDPS odporúča, aby sa v Štokholmskom programe zdôraznil význam všeobecných dohôd so Spojenými štátmi a ďalšími tretími krajinami o ochrane a výmene údajov, ktoré by zaručovali rovnakú úroveň ochrany, aká je garantovaná na území EÚ. V širšej súvislosti EDPS poukazuje na význam aktívneho presadzovania dodržiavania základných práv, najmä ochrany údajov, v súvislosti s tretími krajinami a medzinárodnými organizáciami ⁽³⁰⁾. V Štokholmskom programe by sa ďalej mohlo vo všeobecnosti uviesť, že výmena osobných údajov s tretími krajinami si vyžaduje primeranú úroveň ochrany údajov alebo iné vhodné záruky v týchto tretích krajinách.

VI. POUŽÍVANIE INFORMÁCIÍ

VI.1. Smerom k európskemu informačnému modelu

50. Lepšia výmena informácií je základným cieľom politiky Európskej únie týkajúcej sa priestoru slobody, bezpečnosti a spravodlivosti. V bode 4.1.2. oznámenia sa zdôrazňuje, že bezpečnosť v Európskej únii závisí od výkonných mechanizmov výmeny informácií medzi vnútroštátnymi orgánmi a inými európskymi subjektmi. Tento dôraz na výmenu informácií je logický, nakoľko chýba európsky policajný zbor, európsky systém trestného súdництва a európska

⁽²⁶⁾ Na používateľov informácií sa vzťahujú zákony na ochranu údajov, rovnako ako aj na prevádzkovateľov a spracovateľov údajov.

⁽²⁷⁾ Pozri stanovisko EDPS z 11. novembra 2008 k záverečnej správe kontaktnej skupiny EÚ – USA na vysokej úrovni pre spoločné využívanie informácií a ochranu súkromia a osobných údajov, Ú. v. EÚ C 128, 6.6.2009, s. 1.

⁽²⁸⁾ ETS č. 108, 28.1.1981.

⁽²⁹⁾ Pozri list EDPS z 28. novembra 2005 týkajúci sa oznámenia Komisie o vonkajšom rozmere priestoru slobody, bezpečnosti a spravodlivosti, ktorý je k dispozícii na webovej stránke EDPS.

⁽³⁰⁾ Nedávna judikatúra súvisiaca so zoznamami teroristov potvrdzuje, že sú potrebné záruky – aj vo vzťahoch s Organizáciou Spojených národov – s cieľom zabezpečiť, aby boli protiteroristické opatrenia v súlade s normami EÚ týkajúcimi sa základných práv (spoločné veci C-402/05 P a C-415/05 P, Kadi a Al Barakaat Foundation/Rada, rozsudok z 3. septembra 2008, zatiaľ neuverejnený).

kontrola hraníc. Opatrenia vzťahujúce sa na informácie preto predstavujú významný prínos Európskej únie, ktorý umožňuje orgánom členských štátov účinne čeliť cezhraničnej trestnej činnosti a efektívne chrániť vonkajšie hranice. Neprispiievajú však len k bezpečnosti občanov, ale aj k ich slobode – voľný pohyb osôb sme už spomenuli vyššie ako jedno z hľadísk tohto stanoviska – a k spravodlivosti.

51. Práve z týchto dôvodov sa zásada dostupnosti začlenila do Haagskeho programu. Znamená, že informácie potrebné na boj proti trestnej činnosti by mali bez prekážok pokračovať vnútorné hranice EÚ. Nedávne skúsenosti preukázali, že je ťažké začleniť túto zásadu do legislatívnych opatrení. Rada neakceptovala návrh Komisie na rámcové rozhodnutie Rady o výmene informácií podľa zásady dostupnosti z 12. októbra 2005⁽³¹⁾. Členské štáty neboli pripravené akceptovať dôsledky zásady dostupnosti v plnej miere. Namiesto toho sa prijali obmedzenejšie nástroje⁽³²⁾, ako napr. rozhodnutie Rady 2008/615/SVV z 23. júna 2008 o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti („Prümské rozhodnutie“)⁽³³⁾.

52. Zatiaľ čo zásada dostupnosti predstavovala jadro Haagskeho programu, zdá sa, že Komisia teraz k tejto téme pristupuje opatrnejšie. Plánuje ďalšiu stimuláciu výmeny informácií medzi orgánmi členských štátov prostredníctvom zavedenia európskeho informačného modelu. Švédske predsedníctvo EÚ zmýšľa rovnakým spôsobom⁽³⁴⁾. Predložil návrh stratégie pre výmenu informácií. V Rade sa už začali práce na tomto ambicióznom projekte stratégie Európskej únie pre riadenie informácií, ktorý je úzko prepojený s európskym informačným modelom. EDPS berie tento vývoj na vedomie s obrovským záujmom a zdôrazňuje, že pozornosť by sa v rámci týchto projektov mala venovať prvkom ochrany údajov.

Európsky informačný model a ochrana údajov

53. Na začiatok je vhodné zdôrazniť, že budúcnosť priestoru slobody, bezpečnosti a spravodlivosti by nemala závisieť od technického rozvoja, a to v tom zmysle, že skoro nevyčerpatelne možnosti, ktoré nové technológie ponúkajú, by sa mali vždy posúdiť v súvislosti s relevantnými zásadami ochrany údajov, pričom by sa tieto technológie mali používať, iba ak sú v súlade s uvedenými zásadami.

54. EDPS poznamenáva, že v oznámení sa o informačnom modeli hovorí nielen ako o technickom modeli, ale ako

o modeli so silnou kapacitou strategickej analýzy a zlepšeným zhromažďovaním a spracovávaním operačných informácií. V oznámení sa tiež uznáva, že by sa mali zohľadniť aspekty súvisiace s politikou – ako napríklad kritériá zhromažďovania, vzájomného poskytovania a spracovávania informácií – za súčasného dodržiavania zásad ochrany údajov.

55. Informačné technológie a zákonné podmienky sú – a naďalej budú – rovnako významné. EDPS víta skutočnosť, že oznámenie vychádza z predpokladu, že európsky informačný model sa nesmie zakladať iba na technických parametroch. Je nesmierne dôležité, aby sa informácie zhromažďovali, poskytovali a spracovávali iba na základe konkrétnych bezpečnostných potrieb za súčasného zohľadnenia zásad ochrany údajov. EDPS tiež plne súhlasí s tým, že je potrebné vymedziť monitorovací mechanizmus, ktorý umožní posúdiť fungovanie výmeny informácií. Navrhuje, aby Rada tieto prvky bližšie rozvinula v Štokholmskom programe.

56. EDPS v tejto súvislosti podčiarkuje, že ochrana údajov zameraná na ochranu občanov by sa nemala chápať ako ochrana brániaca účinnej správe údajov. Zabezpečuje totiž dôležité nástroje na zlepšenie uchovávaní, prístupu a výmeny informácií. Právo dotknutej osoby byť informovaný o tom, ktoré informácie, ktoré sa jej týkajú, sú spracovávané, a právo opraviť nesprávne informácie môžu tiež posilniť presnosť údajov v systémoch na správu údajov.

57. Zákony o ochrane údajov majú v zásade tieto dôsledky: ak sú údaje potrebné na osobitný a legitímny účel, môžu sa použiť; ak nie sú potrebné na dobre vymedzený účel, osobné údaje by sa nemali použiť. V prvom prípade je možné prijať aj ďalšie opatrenia na zabezpečenie primeraných záruk.

58. EDPS má však kritické výhrady k rozsahu, v rámci ktorého sa v oznámení uvádza „identifikácia budúcich potrieb“ ako súčasť informačného modelu. Zdôrazňuje, že aj v budúcnosti by sa budovanie informačných systémov malo riadiť zásadou obmedzenia účelu⁽³⁵⁾. Táto zásada je jednou zo základných záruk, ktoré systém ochrany údajov poskytuje občanom: občan musí vopred vedieť na aké účely sa jeho údaje zhromažďujú, ako aj to, že sa tieto údaje použijú iba na daný účel, predovšetkým v budúcnosti. Táto záruka je dokonca zakotvená v článku 8 Charty základných práv Európskej únie. Zásada obmedzenia účelu umožňuje výnimky, ktoré sa vzťahujú predovšetkým na priestor slobody, bezpečnosti a spravodlivosti, avšak tieto výnimky by nemali byť rozhodujúce pre tvorbu systému.

⁽³¹⁾ KOM(2005) 490 v konečnom znení.

⁽³²⁾ Z hľadiska dostupnosti, Prümské rozhodnutie obsahuje ďalekosiahle ustanovenia o používaní biometrických údajov (DNA a odtlačkov prstov).

⁽³³⁾ Ú. v. EÚ L 210, 6.8.2008, s. 1.

⁽³⁴⁾ Pozri pracovný program vlády počas predsedníctva v EÚ citovaný v poznámke pod čiarou č. 5, s. 23.

⁽³⁵⁾ Pozri aj bod 41 vyššie.

Voľba správnej štruktúry

59. Voľba správnej štruktúry na výmenu informácií stojí na začiatku všetkého. Dôležitosť správnych informačných štruktúr je uznaná v oznámení (v bode 4.1.3.), ale nanešťastie iba v súvislosti s interoperabilitou.
60. EDPS zdôrazňuje ďalší aspekt: v rámci európskeho informačného modelu by mali byť požiadavky na ochranu údajov neoddeliteľnou súčasťou celého vývoja systému, pričom by sa nemali považovať iba za nevyhnutnú podmienku na legálnosť systému⁽³⁶⁾. Použiť by sa mali koncepcie „rešpektovania súkromia už od návrhu systému“ a potreby identifikovať „najlepšie dostupné postupy“⁽³⁷⁾ tak, ako sa uvádza v bode 43 vyššie. Európsky informačný model by mal vychádzať z uvedených koncepcií. Konkrétne to znamená, že informačné systémy, ktoré sú navrhnuté na účely zabezpečenia verejnej bezpečnosti, by mali byť vždy vytvorené v súlade so zásadou „rešpektovania súkromia už od návrhu systému“. EDPS odporúča, aby Rada zahrnula tieto prvky do Štokholmského programu.

Interoperabilita systémov

61. EDPS zdôrazňuje, že interoperabilita nie je len technickou záležitosťou, ale má dôsledky aj na ochranu občanov, najmä ochranu údajov. Z hľadiska ochrany údajov má interoperabilita systémov, ak je dobre urobená, jasné výhody v zmysle predchádzania dvojitému uchovávaní. Je však tiež zrejmé, že ak sa prístup k údajom alebo ich výmena technicky umožnia, pohánka fakticky využiť prístup k týmto údajom alebo ich vymieňať je v mnohých prípadoch silná. Inými slovami interoperabilita predstavuje osobitné riziko pri prepojení databáz, ktoré slúžia na rozdielne účely⁽³⁸⁾. Môže ovplyvniť prísne obmedzenia kladené na účely databáz.
62. V skratke to znamená, že samotná skutočnosť, že je technicky možné vymieňať digitálne informácie medzi interoperabilnými databázami alebo zlúčiť takéto databázy, neopodstatňuje udelenie výnimky zo zásady obmedzenia účelu. Interoperabilita by sa mala v konkrétnych prípadoch zakladať na jasnej a opatrnej voľbe politiky. EDPS navrhuje, aby sa tento aspekt bližšie určil v Štokholmskom programe.

⁽³⁶⁾ Pozri „Usmernenia a kritéria pre vývoj, realizáciu a používanie bezpečnostných technológií posilňujúcich ochranu súkromia“, ktoré boli vypracované v rámci projektu PRISE (<http://www.prise.oaw.ac.at>).

⁽³⁷⁾ Najlepšie dostupné postupy znamenajú najúčinnější a najnovší stupeň vývoja činností a metód prevádzky, ktoré preukazujú praktickú vhodnosť určitých postupov pre poskytovanie základu pre aplikácie a systémy ITS, aby boli v súlade s regulačným rámcom EÚ v oblasti ochrany súkromia, údajov a bezpečnostných požiadaviek.

⁽³⁸⁾ Pozri pripomienky EDPS k oznámeniu Komisie o interoperabilite európskych databáz z 10. marca 2006, ktoré sú k dispozícii na http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

VI.2. Používanie informácií zhromaždených na iné účely

63. Oznámenie sa výslovne nevenuje jednej z najdôležitejších tendencií posledných rokov, ktorou je používanie údajov, ktoré boli zhromaždené v súkromnom sektore na komerčné účely, na účely presadzovania práva. Táto tendencia sa netýka len prevádzkových údajov elektronickej komunikácie a údajov o cestujúcich, ktorí letia do (určitých) tretích krajín⁽³⁹⁾, ale zameriava sa aj na finančný sektor. Príkladom je smernica Európskeho parlamentu a Rady 2005/60/ES z 26. októbra 2005 o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu⁽⁴⁰⁾. Ďalší dobre známy a značne diskutovaný príklad sa týka spracovania osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT)⁽⁴¹⁾, a to tých, ktoré sú potrebné na účely programu ministerstva financií Spojených štátov na sledovanie financovania terorizmu.
64. EDPS je toho názoru, že tieto tendencie si v Štokholmskom programe vyžadujú osobitnú pozornosť. Je možné ich chápať ako výnimky zo zásady obmedzenia účelu, pričom často narušajú súkromie, keďže používanie týchto údajov môže mnoho odhaliť o správaní jednotlivcov. V každom prípade, v ktorom sa takéto opatrenia navrhujú, musia existovať silné dôkazy, že takéto súkromie narušajúce opatrenie je nevyhnutné. Ak sa takýto dôkaz predloží, musí sa zabezpečiť, aby boli práva jednotlivcov plne zaručené.
65. Podľa názoru EDPS by sa používanie osobných údajov, ktoré boli zhromaždené na komerčné účely, na účely presadzovania práva malo umožniť iba za dodržania prísnych podmienok, ako napr.:

— Údaje sa musia použiť iba na osobitne vymedzené účely, ako napr. boj proti terorizmu alebo závažnému trestnému činu, ktoré sa budú v jednotlivých prípadoch posudzovať individuálne.

— Údaje sa majú prenášať skôr cez systém zasielania údajov („push“ systém) a nie prostredníctvom prístupu do databáz („pull“ systém)⁽⁴²⁾.

⁽³⁹⁾ Pozri napr. bod 15 vyššie.

⁽⁴⁰⁾ Ú. v. EÚ L 309, 25.11.2005, s. 15.

⁽⁴¹⁾ Pozri stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT), ktoré vypracovala pracovná skupina článku 29.

⁽⁴²⁾ V rámci systému „push“ prevádzkovateľ zasiela („tlačí“) údaje agentúre presadzovania práva na požiadanie. V rámci systému „pull“ má agentúra presadzovania práva prístup do databázy prevádzkovateľa, z ktorej môže čerpať („pull“) informácie. Pri systéme „pull“ je pre prevádzkovateľa oveľa ťažšie opätovne prevziať zodpovednosť.

- Žiadosti o údaje by mali byť primerané, úzko zacielené a v zásade založené na podozreniach voči konkrétnym osobám.
- Malo by sa predchádzať rutinnému vyhľadávaniu, hĺbkovému prehľadávaniu údajov a vytváraniu profilov.
- Akékoľvek použitie údajov na účely presadzovania práva by sa malo zaznamenať, aby mohli dotknutá osoba využívajúca svoje práva, orgány na ochranu údajov a justičné orgány účinne kontrolovať použitie údajov.

VI.3. Informačné systémy a orgány EÚ

Informačné systémy s centralizovaným uchovávaním alebo bez neho ⁽⁴³⁾

66. V posledných rokoch značne vzrástol počet informačných systémov v rámci priestoru bezpečnosti a spravodlivosti založených na práve EÚ. Niekedy sa prijímajú rozhodnutia na vytvorenie systému, ktorý zahŕňa centralizované uchovávanie údajov na európskej úrovni, v iných prípadoch právo predpokladá iba výmenu informácií medzi vnútroštátnymi databázami. Schengenský informačný systém je pravdepodobne najlepším príkladom systému s centralizovaným uchovávaním. Rozhodnutie Rady 2008/615/SVV (Prümské rozhodnutie) ⁽⁴⁴⁾ je z hľadiska ochrany údajov najdôležitejším príkladom systému bez centralizovaného uchovávania, keďže predpokladá rozsiahlu výmenu biometrických údajov medzi orgánmi členských štátov.
67. Oznámenie poukazuje na to, že táto tendencia vytvárania nových systémov bude pokračovať. Prvým príkladom, uvedeným v bode 4.2.2., je informačný systém, ktorý upravuje Európsky informačný systém registrov trestov (ECRIS) tak, aby sa rozšíril aj na štátnych príslušníkov krajín, ktoré nie sú členmi EÚ. Komisia si už objednala štúdiu o európskom zozname odsúdených osôb, ktoré sú štátnymi príslušníkmi tretích krajín (EICTCN), ktorá pravdepodobne povedie k vytvoreniu centralizovanej databázy. Druhým príkladom je výmena informácií o jednotlivcoch z konkurzných registrov v iných členských štátoch v rámci elektronickej justície (bod 3.4.1. oznámenia) bez centralizovaného uchovávania.
68. Decentralizovaný systém by mal z hľadiska ochrany údajov určité výhody. Predchádza sa ním dvojitému uchovávaniu údajov orgánom členského štátu a centralizovaným systémom, pričom zodpovednosť za údaje je jasná, keďže orgán členského štátu je prevádzkovateľom a kontrola justičnými orgánmi a orgánmi na ochranu údajov môže prebiehať na úrovni členského štátu. Tento systém má

však aj slabé stránky, a to v prípadoch, kedy sa údaje vymieňajú s inými jurisdikciami, napríklad pri zabezpečovaní, aby boli informácie v krajine pôvodu a prijímajúcej krajine aktualizované, a pri zabezpečovaní účinnej kontroly na oboch stranách. Ešte zložitejšie je zabezpečiť zodpovednosť za technický systém slúžiaci na výmenu. Tieto slabé stránky je možné prekonať voľbou centralizovaného systému so zodpovednosťou orgánov EÚ aspoň za časti systému (ako napr. technickú infraštruktúru).

69. V tejto súvislosti by bolo užitočné zaviesť hlavné kritériá na voľbu medzi centralizovanými a decentralizovanými systémami, ktoré umožnia jasnú a starostlivú voľbu politiky v konkrétnych prípadoch. Tieto kritériá môžu prispieť k fungovaniu samotných systémov, ako aj k ochrane údajov občanov. EDPS navrhuje, aby sa zámer vypracovať takéto kritériá zahrnul do Štokholmského programu.

Rozsiahle informačné systémy

70. V bode 4.2.3.2. oznámenia sa v krátkosti preberá budúcnosť rozsiahlych informačných systémov s dôrazom na Schengenský informačný systém (SIS) a Vízový informačný systém (VIS).
71. V bode 4.2.3.2. sa tiež uvádza zavedenie systému elektronického registra informácií o vstupoch na územie členských štátov Európskej únie a výstupoch z neho, ako aj programy registrácie cestujúcich. O tomto systéme už skôr informovala Komisia ako o súčasť „legislatívneho balíka v oblasti riadenia hraníc“ v súvislosti s iniciatívou podpredsedu Komisie Frattiniho ⁽⁴⁵⁾. EDPS mal vo svojich predbežných pripomienkach ⁽⁴⁶⁾ celkom kritické výhrady k tomuto návrhu, pretože potreba takéhoto systému narušujúceho súkromie popri existujúcich rozsiahlych systémoch nebola dostatočne preukázaná. EDPS nevidí žiadne ďalšie dôvody preukazujúce potrebu takéhoto systému, a preto navrhuje, aby Rada túto myšlienku v Štokholmskom programe neuviedla.
72. EDPS si v tejto súvislosti želá odkázať na svoje stanoviská k rôznym iniciatívam v oblasti výmeny informácií v EÚ ⁽⁴⁷⁾, v ktorých predstavil mnoho návrhov a pripomienok k aspektom ochrany údajov pri používaní rozsiahlych databáz na úrovni EÚ. Venoval pozornosť okrem iného aj

⁽⁴³⁾ Za centralizované uchovávanie sa v tejto súvislosti považuje uchovávanie na centrálnej európskej úrovni, pričom decentralizované uchovávanie sa uskutočňuje na úrovni členských štátov.

⁽⁴⁴⁾ Pozri poznámku pod čiarou č. 33.

⁽⁴⁵⁾ Oznámenie Komisie Príprava ďalších krokov pre riadenie hraníc v Európskej únii, 13.2.2008, KOM(2008) 69.

⁽⁴⁶⁾ Predbežné pripomienky EPDS k trom oznámeniam Komisie o riadení hraníc [KOM(2008) 69, KOM(2008) 68 a KOM(2008) 67], 3. marec 2008 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

⁽⁴⁷⁾ Predovšetkým: Stanovisko z 23. marca 2005 k návrhu nariadenia Európskeho parlamentu a Rady o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi, Ú. v. EÚ C 181, 23.7.2005, s. 13, a stanovisko z 19. októbra 2005 k trom návrhom týkajúcim sa Schengenského informačného systému druhej generácie (SIS II), Ú. v. EÚ C 91, 19.4.2006, s. 38.

potrebe silných a na mieru šitých záruk, ktoré by sa mali zaviesť, ako aj proporčnosti a nevyhnutnosti posúdení vplyvu uskutočňovaných ešte predtým, než sa akékoľvek opatrenia v tejto oblasti navrhnu alebo prijmú. EDPS sa vždy prikláňa k rovnováhe medzi bezpečnostnými požiadavkami a ochranou súkromia jednotlivcov zaradených v systémoch, ktorá je v súlade s ochranou práv a údajov. Zaujal to isté stanovisko pri vykonávaní dohľadu nad centrálnymi časťami systémov.

73. EDPS ďalej využíva túto príležitosť na zdôraznenie potreby jednotného prístupu k výmene informácií v EÚ ako celku z hľadiska právnej, technickej a dozornej jednotnosti medzi systémami, ktoré sa už v praxi používajú, a systémami, ktoré sa vyvíjajú. V súčasnosti je viac ako kedykoľvek predtým potrebná odvážna a komplexná vízia, ako by mali výmena informácií v EÚ a budúce rozsiahle informačné systémy vyzeráť. Iba na základe tejto vízie bude možné prehodnotiť elektronický register informácií o vstupoch na územie členských štátov a výstupoch z neho.
74. EDPS navrhuje, aby sa v Štokholmskom programe uviedol zámer vypracovať takúto víziu, v ktorej by sa venovala pozornosť aj možnému nadobudnutiu platnosti Lisabonskej zmluvy a jeho dosahov na systémy založené na právnom základe prvého a tretieho piliera.
75. V oznámení sa nakoniec spomína zriadenie novej agentúry, do ktorej právomocí by podľa oznámenia mal patriť aj elektronický register informácií o vstupoch a výstupoch. Komisia medzičasom prijala návrh na zriadenie tejto agentúry⁽⁴⁸⁾. EDPS v zásade podporuje tento návrh, keďže môže dopomôcť k účinnejšiemu fungovaniu týchto systémov vrátane ochrany údajov. Stanovisko k tomuto návrhu predloží v príslušnom čase.

Europol a Eurojust

76. Úloha Europolu sa spomína na niekoľkých miestach v oznámení, ktoré ako prioritnú otázku zdôrazňuje, že Europol musí zohrávať ústrednú úlohu pri koordinácii, výmene informácií a odbornej príprave odborných pracovníkov. Rovnako v bode 4.2.2. oznámenia sa odkazuje na nedávne zmeny v právnom rámci spolupráce medzi Eurojustom a Europolom a oznamuje sa, že budú pokračovať práce na upevňovaní pozície Eurojustu, a to najmä v oblasti vyšetrovania cezhraničnej organizovanej trestnej činnosti. EDPS plne podporuje tieto ciele za predpokladu, že budú primerane zabezpečené záruky ochrany údajov.

⁽⁴⁸⁾ Komisný návrh nariadenia Európskeho parlamentu a Rady z 24. júna 2009, ktorým sa zriaďuje Agentúra na prevádzkové riadenie Schengenského informačného systému (SIS II), Vízového informačného systému (VIS), EURODAC-u a ďalších rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti [KOM(2009) 293/2].

77. EDPS v tejto súvislosti víta nový návrh dohody, ktorý nedávno dosiahli Europol a Eurojust⁽⁴⁹⁾ a ktorého cieľom je zlepšenie a posilnenie vzájomnej spolupráce medzi týmito dvoma orgánmi a zabezpečenie účinnej výmeny informácií medzi nimi. Ide o prácu, v ktorej účinná a efektívna ochrana údajov zohráva dôležitú úlohu.

VI.4. Používanie biometrických údajov

78. EDPS poznamenáva, že sa v oznámení nerieši otázka zvyšujúceho sa používania biometrických údajov v rôznych právnych nástrojoch Európskej únie týkajúcich sa využívania výmeny informácií vrátane nástrojov, ktorými sa zriaďujú rozsiahle informačné systémy. Je to poľutovaniahodné vzhľadom na skutočnosť, že táto záležitosť je mimoriadne dôležitá a citlivá z hľadiska ochrany údajov a súkromia.
79. Aj keď EDPS uznáva všeobecné výhody používania biometrických údajov, neustále zdôrazňuje veľký vplyv používania týchto údajov na práva jednotlivcov, pričom navrhuje zavedenie prísnych bezpečnostných opatrení vzťahujúcich sa na používanie biometrických údajov v každom jednotlivom systéme. Nedávny rozsudok Európskeho súdu pre ľudské práva vo veci *S. and Marper/Spojené kráľovstvo*⁽⁵⁰⁾ je v tejto súvislosti smerodajný, najmä čo sa týka opodstatnenia a obmedzení používania biometrických údajov. Predovšetkým používanie informácií z DNA môže o jednotlivcoch odhaliť citlivé informácie, navyše ak zväzíme, že technické možnosti získavania informácií z DNA sa neustále zväčšujú. Pokiaľ ide o rozsiahle používanie biometrických údajov v informačných systémoch, ďalším problémom sú nepresnosti, ktoré nevyhnutne vznikajú pri zhromažďovaní a porovnávaní biometrických údajov. Zákonodarca EÚ by mal z uvedených dôvodov preukázať zdržanlivosť v používaní týchto údajov.
80. Ďalšou opakujúcou sa otázkou posledných rokov je aj používanie odtlačkov prstov detí a starších osôb, a to z dôvodu sprievodných nedostatkov biometrických systémov v prípade týchto vekových skupín. EDPS požiadal o hĺbkovú štúdiu, aby bolo možné verne určiť presnosť daných systémov⁽⁵¹⁾. V prípade detí navrhuje hranicu 14 rokov, pokiaľ uvedená štúdia nepreukáže inak. EDPS navrhuje, aby sa táto otázka spomenula v Štokholmskom programe.

⁽⁴⁹⁾ Návrh dohody, ktorý schválila Rada a ktorý ešte musia podpísať obe zmluvné strany. Pozri register Rady:

<http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf>
<http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf>

⁽⁵⁰⁾ Spoločné žiadosti 30562/04 a 30566/04, *S. and Marper/Spojené kráľovstvo*, rozsudok zo 4. decembra 2008, ESEP, zatiaľ neuverejnený.

⁽⁵¹⁾ Stanovisko z 26. marca 2008 k návrhu nariadenia, ktorým sa mení a dopĺňa nariadenie Rady (ES) č. 2252/2004 o normách pre bezpečnostné znaky a biometriu v pasoch a cestovných dokladoch vydávaných členskými štátmi, Ú. v. EÚ C 200, 6.8.2008, s. 1.

81. Vzhľadom na uvedené EDPS navrhuje, že by bolo užitočné vypracovať hlavné kritériá vzťahujúce sa na používanie biometrických údajov. Tieto kritériá by mali zabezpečiť, že sa údaje budú používať iba v prípade potreby, primerane a proporčne, a ak zákonodarca preukáže výslovný, konkrétny a legitímny účel ich použitia. Konkrétnejšie, biometrické údaje a najmä údaje o DNA by sa nemali použiť, ak je možné dosiahnuť ten istý výsledok použitím iných, menej citlivých informácií.

VII. PRÍSTUP K SPRAVODLIVOSTI A ELEKTRONICKEJ JUSTÍCI

82. Technológie sa tiež budú používať ako nástroj na lepšiu justičnú spoluprácu. V bode 3.4.1. oznámenia je elektronická justícia predstavená ako systém zabezpečujúci jednoduchší prístup občanov k spravodlivosti. Pozostáva z portálu s informáciami a videokonferenciami ako súčasťami právneho konania. Okrem toho umožňuje online právne konania a predpokladá prepojenie vnútroštátnych registrov, ako napr. konkurzných registrov. EDPS poznamenáva, že sa v oznámení nespomínajú nové iniciatívy súvisiace s elektronickou justíciou, ale sa v ňom konsolidujú už začaté činnosti. EDPS sa spolupodieľa na stanovisku z 19. decembra 2008 k oznámeniu Komisie s názvom Na ceste k európskej stratégii v oblasti elektronickej justície⁽⁵²⁾.

83. Elektronická justícia je ambiciózny projekt, ktorý potrebuje plnú podporu. Môže účinne vylepšiť justičný systém v Európe a súdnu ochranu občanov. Predstavuje dôležitý krok vpred smerom k európskemu priestoru spravodlivosti. S prihliadnutím na toto pozitívne hodnotenie, je vhodné pripomenúť:

— Technologické systémy pre elektronickú justíciu by sa mali budovať v súlade so zásadou „rešpektovanie súkromia už od návrhu systému“. Ako sa už uviedlo vyššie v súvislosti s európskym informačným modelom, voľba správnej štruktúry stojí na začiatku všetkého.

— Prepojenie a interoperabilita systémov by mali dodržiavať zásadu obmedzenia účelu.

— Zodpovednosť jednotlivých aktérov by sa mala presne vymedziť.

— Dôsledky prepojenia vnútroštátnych registrov obsahujúcich citlivé osobné údaje, ako napr. konkurzných registrov, ktoré by z toho vyplynuli pre jednotlivcov, by sa mali vopred zanalyzovať.

VIII. ZÁVERY

84. EDPS schvaľuje dôraz, ktorý sa v oznámení kladie na ochranu základných práv a najmä ochranu osobných údajov ako jednu z kľúčových otázok budúceho priestoru

slobody, bezpečnosti a spravodlivosti. Podľa názoru EDPS sa v oznámení správne presadzuje rovnováha medzi potrebou vhodných nástrojov na zaručenie bezpečnosti občanov a ochranou ich základných práv. V oznámení sa uznáva, že väčší dôraz by sa mal klásť na ochranu osobných údajov.

85. EDPS plne podporuje bod 2.3. oznámenia, v ktorom sa vyzýva na vytvorenie komplexného systému ochrany údajov, ktorý by sa vzťahoval na všetky oblasti právomocí EÚ, bez ohľadu na to, Lisabonská zmluva nadobudne platnosť alebo nie. V tejto súvislosti odporúča:

— oznámiť v Štokholmskom programe potrebu jasnej a dlhodobej vízie týkajúcej sa takéhoto komplexného systému,

— zhodnotiť opatrenia, ktoré sa v tejto oblasti prijali, ich konkrétnu realizáciu a účinnosť za súčasného zohľadnenia nákladov na ochranu súkromia a účinnosti pri presadzovaní práva,

— zahrnúť v Štokholmskom programe ako prioritu potrebu nového legislatívneho rámca, ktorý by okrem iného nahradil rámcové rozhodnutie Rady 2008/977/SVV.

86. EDPS víta zámery Komisie opätovne potvrdiť zásady ochrany údajov, čo musí byť prepojené s verejnou konzultáciou oznámenou Komisiou na konferencii Osobné údaje – väčšia miera používania, väčšia ochrana?, ktorá sa uskutočnila 19. a 20. mája 2009. EDPS v podstate zdôrazňuje význam zásady obmedzenia účelu ako základného kameňa zákonov na ochranu údajov a zamerania sa na možnosti zlepšenia účinnosti uplatňovania zásad ochrany údajov prostredníctvom nástrojov, ktoré by mohli rozšíriť zodpovednosť prevádzkovateľov.

87. Mohli by sa podporovať koncepcie „rešpektovania súkromia už od návrhu systému“ a technológie nenarúšajúce súkromie, a to:

— zavedením certifikátov o rešpektovaní súkromia a ochrane údajov ako možnosti pre tvorcov a používateľov informačných systémov,

— zavedením zákonnej povinnosti pre tvorcov a používateľov informačných systémov používať systémy, ktoré sú v súlade so zásadou rešpektovania súkromia už od návrhu systému.

88. Pokiaľ ide o vonkajšie aspekty ochrany údajov, EDPS odporúča:

— zdôrazniť v Štokholmskom programe význam všeobecných dohôd so Spojenými štátmi a ďalšími tretími krajinami o ochrane a výmene údajov,

⁽⁵²⁾ Stanovisko EDPS z 19. decembra 2008 k oznámeniu Komisie s názvom Na ceste k európskej stratégii v oblasti elektronickej justície, Ú. v. EÚ C 128, 6.6.2009, s. 13.

- aktívne presadzovať dodržiavanie základných práv, najmä ochrany údajov, v súvislosti s tretími krajinami a medzinárodnými organizáciami,
 - uviesť v Štokholmskom programe, že výmena osobných údajov s tretími krajinami si vyžaduje primeranú úroveň ochrany alebo ďalšie vhodné záruky v týchto tretích krajinách.
89. EDPS s obrovským záujmom berie na vedomie vývoj smerujúci k stratégii EÚ pre riadenie informácií a európskemu informačnému modelu a podčiarkuje pozornosť, ktorá by sa v týchto projektoch mala venovať prvkom ochrany údajov, ktoré by sa mali podrobnejšie rozpracovať v Štokholmskom programe. Štruktúra výmeny informácií by sa mala zakladať na „rešpektovaní súkromia už od návrhu systému“ a „najlepších dostupných postupoch“.
90. Samotná skutočnosť, že je technicky možné vymieňať digitálne informácie medzi interoperabilnými databázami alebo zlúčiť takéto databázy neopodstatňuje udelenie výnimky zo zásady obmedzenia účelu. Interoperabilita by sa mala v konkrétnych prípadoch zakladať na jasnej a opatrnej voľbe politiky. EDPS navrhuje, aby sa tento aspekt upresnil v Štokholmskom programe.
91. Používanie osobných údajov, zhromaždených na komerčné účely, na účely presadzovania práva by malo byť podľa EDPS možné iba za splnenia prísnych podmienok, ktoré sú špecifikované v bode 65 tohto stanoviska.
92. Medzi ďalšie návrhy týkajúce sa používania osobných informácií patria:
- Vypracovať hlavné kritériá voľby medzi centralizovanými a decentralizovanými systémami a zahrnúť zámer vypracovať tieto kritériá do Štokholmského programu.
 - Zriadenie elektronického registra informácií o vstupoch na územie členských štátov a výstupoch z nich, ako aj programov registrácie cestujúcich by sa v Štokholmskom programe nemalo uviesť.
 - Podporiť posilnenie Europolu a Eurojustu a novú dohodu, ktorá sa nedávno dosiahla medzi Europolom a Eurojustom.
 - Vypracovať základné kritériá vzťahujúce sa na používanie biometrických údajov, ktoré by zabezpečili, že údaje sa použijú iba v prípade potreby, primerane a proporčne, a ak zákonodarca preukáže výslovný, konkrétny a legitímny účel ich použitia. Údaje z DNA by sa nemali použiť, ak je možné dosiahnuť ten istý výsledok použitím iných, menej citlivých informácií.
93. EDPS podporuje elektronickú justíciu, pričom uviedol niekoľko pripomienok k tomu, ako vylepšiť tento projekt (pozri bod 83).

V Bruseli 10. júla 2009

Peter HUSTINX

Európsky dozorný úradník pre ochranu údajov