STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k návrhu nařízení Evropského parlamentu a Rady o správní spolupráci prostřednictvím systému pro výměnu informací o vnitřním trhu („IMI"), který předkládá Komise

(2012/C 48/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na články 7 a 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([1]),

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů ([2]),

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001,

PŘIJAL TOTO STANOVISKO:

1. ÚVOD

1.1 Konzultace evropského inspektora ochrany údajů

1. Dne 29. srpna 2011 přijala Komise návrh nařízení (dále jen „návrh" nebo „navrhované nařízení") Evropského parlamentu a Rady o správní spolupráci prostřednictvím systému pro výměnu informací o vnitřním trhu (dále jen „IMI") ([3]). Téhož dne byl návrh zaslán evropskému inspektorovi ochrany údajů ke konzultaci.

2. Před přijetím návrhu dostal evropský inspektor ochrany údajů možnost uvést k návrhu neformální připomínky, přičemž ještě dříve se mohl vyjádřit ke sdělení Komise „Lepší správa jednotného trhu prostřednictvím širší správní spolupráce: Strategie pro rozšíření a rozvoj systému pro výměnu informací o vnitřním trhu („IMI")" (dále jen „sdělení o strategii systému IMI") ([4]), které návrhu předcházelo. Mnohé z těchto připomínek byly v návrhu zohledněny, a v důsledku toho byly záruky ochrany údajů v návrhu posíleny.

3. Evropský inspektor ochrany údajů vítá, že jej Komise formálně konzultovala a že v preambuli návrhu je uveden odkaz na toto stanovisko.

1.2 Cíle a oblast působnosti návrhu

4. IMI je nástroj informačních technologií, který příslušným orgánům v členských státech umožňuje vzájemně si vyměňovat informace při použití právních předpisů upravujících vnitřní trh. Díky IMI mohou vnitrostátní, regionální a místní orgány v členských státech EU komunikovat rychle a snadno se svými protějšky v jiných evropských zemích. Zahrnuje to také zpracování příslušných osobních údajů včetně citlivých údajů.

5. Systém IMI byl původně zřízen jako komunikační nástroj pro individuální výměny v rámci směrnice o uznávání odborných kvalifikací ([5]) a směrnice o službách ([6]). IMI pomáhá uživatelům najít příslušný orgán, který je třeba kontaktovat v zahraničí, a komunikovat s takovým orgánem pomocí souboru předem přeložených standardizovaných otázek a odpovědí ([7]).

([1]) Úř. věst. L 281, 23.11.1995, s. 31.
([2]) Úř. věst. L 8, 12.1.2001, s. 1.
([3]) KOM(2011) 522 v konečném znění.
([4]) KOM(2011) 75.
([5]) Směrnice Evropského parlamentu a Rady 2005/36/ES ze dne 7. září 2005 o uznávání odborných kvalifikací (Úř. věst L 255, 30.9.2005, s. 22).
([6]) Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu (Úř. věst. L 376, 27.12.2006, s. 36).
([7]) Pro ilustraci, typická otázka obsahující citlivé údaje by zněla například takto: „Odůvodňuje přiložený dokument zákonným způsobem to, že nedošlo k pozastavení nebo zákazu provádění příslušných profesních činností z důvodu závažného nesprávného počínání při výkonu povolání nebo trestného činu, pokud jde o (migrující výdělečně činnou osobu)?".

6. Systém IMI je však zamýšlen jako pružný horizontální systém, který může podporovat četné oblasti právních předpisů v oblasti vnitřního trhu. Předpokládá se, že jeho použití se bude postupně rozšiřovat s cílem podpořit v budoucnosti další legislativní oblasti.

7. Plánuje se i rozšiřování funkcí systému IMI. Kromě individuálních výměn informací se předpokládají nebo jsou již zavedeny i další funkce, jako jsou „oznamovací postupy, výstražné mechanismy, ujednání o vzájemné pomoci a řešení problémů“ ([8]), jakož i „úložiště informací pro účely jejich budoucího použití subjekty IMI“ ([9]). Mnohé z těchto funkcí, nikoli však všechny, mohou zahrnovat i zpracování osobních údajů.

8. Cílem návrhu je poskytnout jasný právní základ a ucelený rámec ochrany údajů pro systém IMI.

1.3 **Pozadí návrhu: postupný přístup ke stanovení uceleného rámce ochrany údajů pro systém IMI**

9. V průběhu jara 2007 požádala Komise o stanovisko pracovní skupiny pro ochranu údajů zřízené podle článku 29 (dále jen „pracovní skupina zřízená podle článku 29“), které mělo přezkoumat důsledky systému IMI pro ochranu údajů. Pracovní skupina zřízená podle článku 29 vydala své stanovisko dne 20. září 2007 ([10]). Stanovisko doporučilo Komisi, aby zajistila jasnější právní základ a zvláštní opatření k ochraně údajů pro výměnu údajů v rámci systému IMI. Evropský inspektor ochrany údajů se aktivně podílel na práci podskupiny, která se zabývala systémem IMI, a podpořil závěry stanoviska pracovní skupiny zřízené podle článku 29.

10. Následně evropský inspektor ochrany údajů i nadále poskytoval Komisi poradenství ve věci toho, jak pro systém IMI postupně zajistit ucelenější rámec ochrany údajů ([11]). V rámci této spolupráce a od vydání jeho stanoviska k provádění systému IMI dne 22. února 2008 ([12]) evropský inspektor ochrany údajů důsledně hájí potřebu nového právního nástroje v rámci řádného legislativního postupu s cílem vybudovat ucelenější rámec ochrany údajů pro systém IMI a zabezpečit právní jistotu. Návrh takového právního nástroje byl nyní předložen ([13]).

([8]) Viz 10. bod odůvodnění.

([9]) Viz čl. 13 odst. 2.

([10]) Stanovisko pracovní skupiny zřízené podle článku 29 č. 7/2007 k otázkám ochrany údajů týkajícím se systému pro výměnu informací o vnitřním trhu (systém IMI), WP140. K dispozici na adrese http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_cs.pdf

([11]) Klíčové dokumenty týkající se této spolupráce jsou k dispozici na internetové stránce Komise věnované systému IMI na adrese http://ec.europa.eu/internal_market/imi-net/data_protection_en.html, jakož i na internetové stránce evropského inspektora ochrany údajů na adrese http://www.edps.europa.eu

([12]) Stanovisko evropského inspektora ochrany údajů k rozhodnutí Komise 2008/49/ES ze dne 12. prosince 2007 týkajícímu se provádění systému pro výměnu informací o vnitřním trhu (IMI), pokud jde o ochranu osobních údajů (Úř. věst. C 270, 25.10.2008, s. 1).

([13]) Pracovní skupina zřízená podle článku 29 se také hodlá k návrhu vyjádřit. Evropský inspektor ochrany údajů tento vývoj sleduje v příslušné podskupině pracovní skupiny zřízené podle článku 29 a přispěl svými připomínkami.

2. **ANALÝZA NÁVRHU**

2.1 **Obecné názory evropského inspektora ochrany údajů na návrh a hlavní výzvy v oblasti regulace systému IMI**

11. Obecně evropský inspektor ochrany údajů pohlíží na systém IMI kladně. Evropský inspektor ochrany údajů podporuje cíle Komise při budování elektronického systému pro výměnu informací a při regulaci jeho aspektů týkajících se ochrany údajů. Takovýto sladěný systém nejen zvýší účinnost spolupráce, ale může také pomoci zajistit důsledné dodržování použitelných právních předpisů v oblasti ochrany údajů. Lze toho docílit zajištěním jasného rámce, který bude upravovat, jaké informace lze vyměňovat, s kým a za jakých podmínek.

12. Evropský inspektor ochrany údajů rovněž vítá, že Komise pro systém IMI navrhuje horizontální právní nástroj v podobě nařízení Rady a Parlamentu. Je potěšen tím, že návrh komplexně poukazuje na otázky ochrany údajů, které jsou pro systém IMI nejvýznamnější. Jeho připomínky je třeba chápat v tomto kladném kontextu.

13. Evropský inspektor ochrany údajů nicméně upozorňuje, že zřízení jediného centralizovaného elektronického systému pro více oblastí správní spolupráce přináší i rizika. K nim patří především skutečnost, že lze sdílet více údajů a lze je sdílet v širší míře, než je pro účely účinné spolupráce nezbytně nutné, a že údaje včetně potenciálně zastaralých a nepřesných údajů mohou v elektronickém systému zůstávat déle, než je nezbytné. Citlivým problémem je i zabezpečení informačního systému přístupného v 27 členských státech, protože celý systém bude bezpečný jen tak, jak mu to umožní jeho nejslabší článek v celém řetězci.

Hlavní výzvy

14. Pokud jde o právní rámec pro systém IMI, který má být stanoven navrhovaným nařízením, upozorňuje evropský inspektor ochrany údajů na dvě hlavní výzvy:

— na potřebu zajistit jednotnost a přitom respektovat rozmanitost a

— na potřebu vyvážit flexibilitu a právní jistotu.

15. Tyto klíčové hlavní výzvy slouží jako důležité referenční body a do velké míry určují přístup, který evropský inspektor ochrany údajů v tomto stanovisku zaujal.

Jednotnost při respektování rozmanitosti

16. Za prvé, IMI je systém, který je používán ve 27 členských státech. V současné fázi harmonizace evropských právních předpisů existují značné rozdíly mezi vnitrostátními správními postupy i vnitrostátními právními předpisy v oblasti ochrany údajů. Systém IMI je třeba budovat takovým způsobem, aby uživatelé v každém z těchto 27 členských

států byli schopni při výměnách osobních údajů prostřednictvím systému IMI dodržet své vnitrostátní právní předpisy včetně právních předpisů v oblasti ochrany údajů. Současně je třeba subjekty údajů také znovu ujistit, že jejich údaje budou jednotně chráněny bez ohledu na předávání údajů prostřednictvím systému IMI do jiného členského státu. Jednotnost je při souběžném dodržování rozmanitosti klíčovou výzvou pro budování technické i právní infrastruktury pro systém IMI. Je třeba se vyhnout zbytečné složitosti a roztříštěnosti. Operace zpracování údajů v rámci systému IMI musí být transparentní a musí být jasně rozděleny odpovědnosti za přijímání rozhodnutí o návrhu systému, jeho každodenní údržbě a používání a rovněž o dohledu nad ním.

Vyvážení flexibility a právní jistoty

17. Za druhé, na rozdíl od některých jiných rozsáhlých systémů informačních technologií, jako je Schengenský informační systém, Vízový informační systém, celní informační systém nebo systém Eurodac, což jsou všechno systémy zaměřené na spolupráci v konkrétních, jasně definovaných oblastech, je systém IMI horizontální nástroj pro výměnu informací a lze jej využít k usnadnění výměny informací v mnoha různých oblastech politiky. Rovněž se předpokládá, že oblast působnosti systému IMI se bude postupně rozšiřovat na další oblasti politiky, a i funkce systému se mohou měnit tak, aby začlenily dosud nespecifikované druhy správní spolupráce. V důsledku těchto charakteristických rysů systému IMI je obtížnější jasně definovat funkce systému a výměny údajů, které mohou v daném systému probíhat. Tím se ještě zvyšuje náročnost jasného definování vhodných opatření na ochranu údajů.

18. Evropský inspektor ochrany údajů uznává potřebu flexibility a bere na vědomí snahu Komise učinit nařízení „odolným vůči vývoji v budoucnosti". Nemělo by to však vést k nedostatečné jasnosti nebo právní nejistotě z hlediska funkcí systému a opatření na ochranu údajů, která je třeba zavést. Z tohoto důvodu by ve všech případech, kdy to bude možné, měl být návrh konkrétnější a měl by jít dále než jen opakovat hlavní zásady ochrany údajů stanovené ve směrnici 95/46/ES a v nařízení (ES) č. 45/2001 ([14]).

2.2 **Oblast působnosti systému IMI a její předpokládané rozšiřování (články 3 a 4)**

2.2.1 *Úvod*

19. Evropský inspektor ochrany údajů vítá, že návrh jasně definuje současnou oblast působnosti systému IMI, přičemž příloha I uvádí výčet příslušných aktů Unie, na jejichž základě lze vyměňovat informace. Ty zahrnují spolupráci na základě konkrétních ustanovení směrnice o uznávání odborných kvalifikací, směrnice o službách a směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči ([15]).

20. Protože se očekává, že oblast působnosti systému IMI se bude rozšiřovat, uvádí příloha II možné cíle rozšíření. Položky z přílohy II lze přesunout do přílohy I prostřednictvím aktu v přenesené pravomoci, který přijme Komise po posouzení dopadů ([16]).

21. Evropský inspektor ochrany údajů tuto techniku vítá, protože i) jasně vymezuje oblast působnosti systému IMI a ii) zajišťuje transparentnost, přičemž současně iii) umožňuje flexibilitu v případech, kdy bude systém IMI použit pro dodatečné výměny informací v budoucnosti. Rovněž zajišťuje, aby nebylo možné prostřednictvím systému IMI provádět žádnou výměnu informací, aniž by i) byl k dispozici vhodný právní základ ve specifických právních předpisech v oblasti vnitřního trhu, který bude umožňovat nebo povolovat výměnu informací ([17]), a aniž by ii) byl odkaz na takový právní základ uveden v příloze I nařízení.

22. Vzhledem k výše uvedenému stále existují nejistoty ohledně oblasti působnosti systému IMI, pokud jde o oblasti politiky, do nichž se systém IMI může rozšířit, a pokud jde o funkce, které do systému IMI jsou nebo mohou být začleněny.

23. Za prvé nelze vyloučit, že oblast působnosti systému IMI se může rozšířit nad rámec oblastí politiky uvedených ve výčtech v příloze I a příloze II. Může k tomu dojít tehdy, pokud bude použití systému IMI stanoveno pro určité druhy výměn informací nikoli v aktu Komise v přenesené pravomoci, ale v aktu přijatém Parlamentem a Radou v případě, kdy takovou situaci příloha II nepředpokládala ([18]).

([14]) V tomto ohledu viz též naše připomínky v oddíle 2.2 týkající se předpokládaného rozšiřování systému IMI.

([15]) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).

([16]) Samotný návrh nařízení posouzení dopadů nezmiňuje. Strana 7 důvodové zprávy k návrhu však vysvětluje, že Komise bude oprávněna přesunout položky z přílohy II do přílohy I přijetím aktu v přenesené pravomoci a „[p]o posouzení technické proveditelnosti, nákladové efektivnosti, uživatelské přívětivosti a celkového dopadu na systém, jakož i výsledků případné zkušební fáze".

([17]) To platí s výjimkou pro síť SOLVIT (viz příloha II, oddíl I bod 1), kde jsou k dispozici pouze právně nevynutitelné předpisy, konkrétně doporučení Komise. Z hlediska zpracování údajů může být dle názoru evropského inspektora ochrany údajů v konkrétním případě sítě SOLVIT právním základem zpracování „souhlas" subjektů údajů.

([18]) Může k tomu dojít z podnětu Komise, nelze však také vyloučit, že myšlenka využití systému IMI v konkrétní oblasti politiky může vzniknout později v legislativním procesu a může je navrhnout Parlament nebo Rada. K tomu již v minulosti došlo v případě směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči. Pro takový případ by byla požadována větší jasnost, pokud jde o „postup" pro rozšíření působnosti, který se zřejmě zaměřuje pouze na případ rozšíření prostřednictvím aktů v přenesené pravomoci (viz ustanovení o posouzení dopadů, aktech v přenesené pravomoci, aktualizaci přílohy I).

24. Za druhé, zatímco rozšíření oblasti působnosti do nových oblastí politiky může vyžadovat malou změnu stávajících funkcí systému nebo ani žádnou změnu nevyvolá ([19]), jiná rozšíření mohou vyžadovat nové a odlišné funkce nebo důležité změny stávajících funkcí:

— ačkoli návrh odkazuje na několik stávajících nebo plánovaných funkcí, tyto odkazy často nejsou dostatečně jasné nebo dostatečně podrobné. To v různé míře platí pro odkazy na výstrahy, vnější subjekty, úložiště, ujednání o vzájemné pomoci a řešení problémů ([20]). Pro ilustraci, slovo „výstražné", které odkazuje na klíčovou stávající funkci, je zmíněno jen jednou, v 10. bodě odůvodnění,

— na základě navrhovaného nařízení lze přijmout nové druhy funkcí, které nejsou v návrhu vůbec zmíněny,

— systém IMI tedy byl dosud popisován jako nástroj informačních technologií pro výměnu informací: jinými slovy, komunikační nástroj (viz např. článek 3 návrhu). Některé z funkcí uvedených v návrhu včetně funkce „úložiště informací" však tento rozsah zřejmě překračují. Navrhované rozšíření lhůt pro uchovávání údajů na pět let rovněž naznačuje posun směrem k „databázi". Takový vývoj by zásadně změnil povahu systému IMI ([21]).

2.2.2 *Doporučení*

25. Pro řešení těchto nejistot evropský inspektor ochrany údajů doporučuje dvoucestný přístup. Za prvé navrhuje, aby byly vyjasněny a konkrétněji řešeny funkce, které již lze předpokládat, a za druhé aby byly uplatněny vhodné procesní záruky pro zajištění toho, že při budoucím vývoji systému IMI bude pečlivě zvažována i ochrana údajů.

Vyjasnění funkcí, které již jsou k dispozici nebo je lze předpokládat (např. individuální výměny, výstrahy, úložiště, řešení problémů a vnější subjekty)

26. Evropský inspektor ochrany údajů doporučuje, aby bylo nařízení konkrétnější, pokud jde o funkce, které jsou již známy, jako v případě výměn informací uvedených v přílohách I a II.

27. Například konkrétnější a jasnější opatření by bylo možné stanovit pro začlenění sítě SOLVIT ([22]) do systému IMI (ustanovení týkající se „vnějších subjektů" a „řešení problémů") a pro seznamy odborných kvalifikovaných pracovníků a poskytovatelů služeb (ustanovení o „úložištích").

28. Další vyjasnění by mělo být provedeno ve věci „výstrah", které se již používají podle směrnice o službách a které lze zavést do dalších oblastí politiky. Konkrétně by „výstraha" jako funkce měla být jasně definována v článku 5 (spolu s dalšími funkcemi, jako jsou individuální výměny informací a úložiště). Měla by být vyjasněna i práva přístupu a lhůty pro uchovávání údajů ([23]).

Procesní záruky (posouzení dopadů ochrany údajů a konzultace orgánů ochrany údajů)

29. Je-li záměrem zachovat nařízení „odolné budoucnosti" z hlediska dodatečných funkcí, které by mohly být v dlouhodobějším výhledu nutné, a tudíž umožnit další funkce, dosud v nařízení nedefinované, měly by tento přístup doprovázet vhodné procesní záruky pro zajištění toho, aby byla přijata vhodná ustanovení k provedení nezbytných opatření na ochranu údajů před spuštěním nové funkce. Totéž by platilo pro rozšíření do nových oblastí politiky, pokud bude mít dopad na ochranu údajů.

30. Evropský inspektor ochrany údajů doporučuje jasný mechanismus, který zajistí, že před každým rozšířením funkcí nebo rozšířením působnosti na nové oblasti politiky budou aspekty ochrany údajů pečlivě posouzeny a v případě potřeby budou v architektuře systému zavedena dodatečná ochranná či technická opatření. Konkrétně:

— posouzení dopadů důvodové zprávy zmíněné na straně 7 by mělo být výslovně požadováno v nařízení samotném a mělo by zahrnovat i posouzení dopadů na ochranu údajů, které by se mělo specificky zabývat tím, zda jsou nutné případné změny návrhu systému IMI pro zajištění toho, aby systém nadále obsahoval opatření na ochranu údajů zahrnující i nové oblasti politiky a/nebo funkce,

— nařízení by mělo konkrétně stanovit, že před každým rozšířením působnosti systému IMI je nutná konzultace s evropským inspektorem ochrany údajů a vnitrostátními orgány ochrany údajů. Tato konzultace může probíhat prostřednictvím mechanismu předpokládaného pro koordinovaný dohled v článku 20.

([19]) Například individuální výměny informací podle směrnice o odborných kvalifikacích a směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči se řídí v podstatě stejnou strukturou a lze je přizpůsobit pomocí podobných funkcí s výhradou podobných opatření na ochranu údajů.

([20]) Viz 2., 10., 12., 13. a 15. bod odůvodnění a čl. 5 písm. b), čl. 5 písm. i), čl. 10 odst. 7 a čl. 13 odst. 2.

([21]) Mimochodem, pokud je záměrem, aby systém IMI nahradil/doplnil stávající systémy manipulace se soubory a jejich archivace, a/nebo aby byl systém IMI využíván jako databáze, mělo by to být v článku 3 vyjasněno.

([22]) Viz příloha II oddíl I bod 1.

([23]) Viz oddíly 2.4 a 2.5.5 níže.

31. Tyto procesní záruky (posouzení dopadů na ochranu údajů a konzultace) by měly platit pro rozšíření působnosti jak prostřednictvím aktu Komise v přenesené pravomoci (převedení položky z přílohy II do přílohy I), tak prostřednictvím nařízení Parlamentu a Rady obsahujícího položku dosud neuvedenou v příloze II.

32. A v neposlední řadě evropský inspektor ochrany údajů doporučuje, aby nařízení vyjasnilo, zda bude oblast působnosti aktů v přenesené pravomoci, které bude Komise oprávněna přijímat podle článku 23, zahrnovat jakékoli další záležitosti kromě přesunu položek z přílohy II do přílohy I. Bude-li to proveditelné, měla by být Komise v nařízení zmocněna přijímat konkrétní prováděcí akty nebo akty v přenesené pravomoci pro další definování případných dalších funkcí systému nebo řešení případných problémů v oblasti ochrany údajů, které mohou v budoucnosti vzniknout.

2.3 **Úlohy, pravomoci a povinnosti (články 7–9)**

33. Evropský inspektor ochrany údajů vítá, že byla celá kapitola (kapitola II) věnována vyjasnění funkcí a povinností jednotlivých subjektů zapojených do systému IMI. Tato ustanovení by bylo možné dále posílit níže uvedeným způsobem.

34. Článek 9 popisuje povinnosti vyplývající z úlohy Komise jakožto správce. Evropský inspektor ochrany údajů dále doporučuje, aby bylo zařazeno dodatečné ustanovení odkazující na úlohu Komise při zajišťování toho, aby byl systém navržen za použití zásad „ochrany soukromí již od návrhu“, jakož i na její koordinační úlohu v oblasti ochrany údajů.

35. Evropský inspektor ochrany údajů s potěšením zjišťuje, že úkoly koordinátorů IMI uvedené v článku 7 nyní konkrétně zahrnují koordinační úkoly týkající se ochrany údajů, včetně působení ve funkci kontaktní osoby pro Komisi. Doporučuje dále vyjasnit, že tyto koordinační úkoly zahrnují také styky s vnitrostátními orgány ochrany údajů.

2.4 **Přístupová práva (článek 10)**

36. Článek 10 stanoví ochranná opatření ve věci přístupových práv. Evropský inspektor ochrany údajů vítá, že v návaznosti na jeho připomínky byla tato ustanovení významně posílena.

37. S ohledem na horizontální a rozšiřující se povahu systému IMI je důležité zajistit, aby systém zaručoval použití „čínských zdí“ omezujících informace zpracovávané v jedné oblasti politiky pouze na tuto oblast: uživatelé systému IMI by i) měli mít přístup pouze k informacím, které potřebují, a ii) měli by být omezeni pouze na jednu oblast politiky.

38. Pokud se nelze vyhnout tomu, aby byl uživatel systému IMI oprávněn k přístupu k informacím v několika oblastech politiky (k čemuž může docházet například v některých orgánech místní správy), mělo by být minimálním opatřením alespoň to, že systém neumožní kombinování informací pocházejících z různých oblastí politiky. Výjimky, budou-li nutné, by měly být stanoveny v prováděcích právních předpisech nebo v aktu Unie, za přísného dodržení zásady omezení účelu.

39. Tyto zásady jsou nyní vymezeny v textu nařízení, ale bylo by možné je dále posílit a zvýšit jejich operativnost.

40. Pokud jde o přístupová práva Komise, evropský inspektor ochrany údajů vítá, že čl. 9 odst. 2 a 4 a čl. 10 odst. 6 návrhu společně upřesňují, že Komise nebude mít žádný přístup k osobním údajům vyměňovaným mezi členskými státy, kromě případů, kdy je Komise jmenována jako účastník postupu správní spolupráce.

41. Měla by být dále upřesněna i přístupová práva vnějších subjektů a práva přístupu k výstrahám ([24]). Pokud jde o výstrahy, evropský inspektor ochrany údajů doporučuje, aby nařízení stanovilo, že výstrahy by standardně neměly být zasílány všem relevantním příslušným orgánům ve všech členských státech, ale jen orgánům dotčeným, které tyto informace skutečně potřebují. Tím není vyloučeno zasílání výstrah všem členským státům v konkrétních případech nebo v konkrétních oblastech politiky, jestliže jsou dotčeny všechny členské státy. Obdobně rozhodnutí o tom, zda by měla mít k výstrahám přístup Komise, vyžaduje individuální analýzu.

2.5 **Uchovávání osobních údajů (články 13 a 14)**

2.5.1 *Úvod*

42. Článek 13 návrhu prodlužuje délku doby uchování údajů v systému IMI ze současných šesti měsíců (počítaných od uzavření případu) na pět let, přičemž po osmnácti měsících jsou údaje „zablokovány“. Během doby „blokace“ jsou údaje přístupné až po zvláštním postupu vyhledávání, který lze zahájit pouze na žádost subjektu údajů nebo v případě, že jsou dané údaje potřebné „jako důkaz o výměně informací prostřednictvím systému IMI“.

43. V důsledku toho jsou proto údaje v systému IMI uloženy po tři různá období:

— od okamžiku načtení do okamžiku uzavření případu,

— od uzavření případu po dobu osmnácti měsíců ([25]),

— od uplynutí doby osmnácti měsíců, v zablokované podobě, po dobu dalších tří let a šesti měsíců (jinými slovy do uplynutí pěti let od uzavření případu).

([24]) Viz také oddíl 2.2.2.

([25]) Čl. 13 odst. 1 naznačuje, že osmnáct měsíců je „maximální“ lhůta, lze tudíž stanovit i kratší dobu. To by však nemělo vliv na celkovou délku uchování, které by v každém případě trvalo do uplynutí pěti let od uzavření případu.

44. Kromě těchto obecných pravidel čl. 13 odst. 2 umožňuje uchování údajů v „úložišt[i] informací“ po dobu nezbytnou pro tyto účely, a to buď se souhlasem subjektu údajů, nebo „je-li to nutné pro dodržení aktu Unie“. Článek 14 dále stanoví podobný mechanismus blokování pro uchování osobních údajů uživatelů systému IMI po dobu pěti let od data, kdy osoby přestanou být uživateli systému IMI.

45. Nejsou uvedena žádná další konkrétní ustanovení. Proto mají obecná pravidla zřejmě platit nejen pro individuální výměny, ale i pro výstrahy, řešení problémů (jako v síti SOLVIT ([26])) a pro všechny ostatní funkce zahrnující zpracování osobních údajů.

46. Evropský inspektor ochrany údajů má několik obav týkajících se dob uchování údajů, s přihlédnutím k čl. 6 odst. 1 písm. e) směrnice 95/46/ES a čl. 4 odst. 1 písm. e) nařízení (ES) č. 45/2001, které oba stanoví, že osobní údaje nesmí být uchovávány po dobu delší, než je zapotřebí k uskutečnění cílů, pro něž byly údaje shromážděny nebo jsou dále zpracovávány.

2.5.2 *Od načtení do uzavření případu: nutnost včasného uzavření případu*

47. Pokud jde o první období, od načtení informací do uzavření případu, má evropský inspektor ochrany údajů obavy z rizika toho, že některé případy nemusí být nikdy uzavřeny nebo budou uzavřeny až po nepřiměřeně dlouhé době. To může vést k tomu, že některé osobní údaje zůstanou v databázi déle, než je nezbytné, dokonce i natrvalo.

48. Evropský inspektor ochrany údajů chápe, že na praktické úrovni dosáhla Komise pokroku při omezování nevyřízených případů v systému IMI a že je zaveden systém pro individuální výměny, který má sledovat včasné uzavírání případů a periodicky upomínat ty, kdo jsou ve zpoždění. Kromě toho nová změna funkcí systému, která dodržuje přístup „ochrany soukromí již od návrhu“, umožňuje stiskem jediného tlačítka přijmout odpověď a současně daný případ uzavřít. Dříve tato operace vyžadovala dva samostatné kroky, což mohlo vést k určitému počtu „spících“ případů, které zůstaly v systému.

49. Evropský inspektor ochrany údajů tyto snahy na praktické úrovni vítá. Doporučuje však, aby samotný text nařízení stanovil záruky toho, že případy budou v systému IMI uzavírány včas a že spící případy (případy bez jakékoli nedávné aktivity) budou z databáze vymazány.

2.5.3 *Od uzavření případu po dobu osmnácti měsíců: je prodloužení šestiměsíční lhůty odůvodněné?*

50. Evropský inspektor ochrany údajů vyzývá, aby bylo znovu zváženo, zda existuje odpovídající odůvodnění pro prodloužení stávajícího šestiměsíčního období na osmnáct měsíců po uzavření případu, a pokud ano, zda toto odůvodnění platí pouze pro individuální výměny informací nebo i pro jiné druhy funkcí. Systém IMI existuje již několik let a měly by být využity praktické zkušenosti, které se v tomto ohledu nashromáždily.

51. Jestliže systém IMI zůstane nástrojem výměny informací (na rozdíl od systému manipulace se soubory, databáze nebo archivačního systému) a jestliže budou mít příslušné orgány prostředky k tomu, aby v systému vyhledávaly informace, které obdržely (buď elektronicky, nebo v podobě papírového formuláře, v každém případě však takovým způsobem, aby mohly vyhledané informace použít jako důkaz ([27])), není zřejmě vůbec zapotřebí uchovávat údaje v systému IMI po uzavření případu.

52. V individuálních výměnách informací může případná nutnost pokládat návazné otázky i poté, co byla akceptována odpověď, a tudíž byl případ uzavřen, odůvodňovat (přiměřeně krátkou) dobu uchování údajů po uzavření případu. Současná šestiměsíční lhůta se a priori pro tento účel na první pohled jeví jako dostatečně velkorysá.

2.5.4 *Od osmnácti měsíců do pěti let: „zablokované“ údaje*

53. Evropský inspektor ochrany údajů se domnívá, že Komise také neposkytla dostatečné odůvodnění nezbytnosti a přiměřenosti uchovávání „zablokovaných údajů“ po dobu až pěti let.

54. Důvodová zpráva na straně 8 odkazuje na rozhodnutí Soudního dvora ve věci *Rijkeboer* ([28]). Evropský inspektor ochrany údajů doporučuje, aby Komise znovu zvážila důsledky této věci pro uchovávání údajů v systému IMI. Podle jeho názoru věc *Rijkeboer* nevyžaduje, aby byl systém IMI konfigurován pro uchovávání údajů po dobu pěti let po uzavření případu.

55. Evropský inspektor ochrany údajů nepovažuje odkaz na rozsudek ve věci *Rijkeboer* nebo na práva subjektů údajů mít přístup ke svým údajům za dostatečné a přiměřené odůvodnění pro uchovávání údajů v systému IMI po dobu pěti let po uzavření případu. Méně narušující možností, která možná zasluhuje další zvážení, by mohlo být uchovávání pouze „přihlašovacích údajů“ (přesně definovaných tak, aby vylučovaly veškerý obsah, mimo jiné veškeré přílohy nebo citlivé údaje). V této fázi však evropský inspektor ochrany údajů není přesvědčen, že i toto řešení by bylo nezbytné nebo přiměřené.

([26]) Viz příloha II oddíl I bod 1.

([27]) Vyrozuměli jsme, že jsou činěny kroky k zajištění tohoto cíle na praktické úrovni.

([28]) C-553/07 *Rijkeboer* [2009] Sb. rozh. I-3889.

56. Kromě toho je problematická i nedostatečná jasnost ve věci toho, kdo může mít přístup k „zablokovaným údajům“ a pro jaké účely. Prostý odkaz na použití „jako důkaz o výměně informací“ (jako v čl. 13 odst. 3) není dostatečný. Bude-li ustanovení o „zablokování“ zachováno, mělo by být v každém případě lépe upřesněno, kdo může požádat o důkaz o výměně informací a v jaké souvislosti. Byly by i jiné osoby než daný subjekt údajů oprávněny požádat o přístup? Pokud ano, byly by to výhradně příslušné orgány a výhradně pro účely prokázání toho, že došlo k určité výměně informací s konkrétním obsahem (v případě, že takovou výměnu informací zpochybní příslušné orgány, které dané sdělení odeslaly nebo přijaly)? Předpokládají se další možná použití „jako důkaz o výměně informací“ ([29])?

2.5.5 *Výstrahy*

57. Evropský inspektor ochrany údajů doporučuje, aby bylo jasněji rozlišeno mezi výstrahami a úložišti informací. Jedna věc je používat výstrahu jako komunikační nástroj k upozornění příslušných orgánů na konkrétní přestupek nebo podezření a zcela jiná věc je ukládat tuto výstrahu v databázi po prodlouženou, či dokonce nedefinovanou dobu. Ukládání výstražných informací by zvýšilo další obavy a vyžadovalo by zvláštní pravidla a dodatečná opatření na ochranu údajů.

58. Proto evropský inspektor ochrany údajů doporučuje, aby nařízení jako implicitní pravidlo stanovilo, že i) pro výstrahy by mělo platit šestiměsíční období uchování údajů (není-li stanoveno jinak ve vertikálních právních předpisech a s výhradou odpovídajících ochranných opatření), a především, že ii) toto období by se mělo počítat od okamžiku odeslání výstrahy.

59. Alternativně evropský inspektor ochrany údajů doporučuje, aby byla v navrhovaném nařízení ve věci výstrah konkrétně stanovena podrobná ochranná opatření. Pokud by byl uplatněn tento druhý přístup, je evropský inspektor ochrany údajů připraven být Komisi a zákonodárcům v tomto ohledu nápomocen dalším poradenstvím.

2.6 **Zvláštní kategorie údajů (článek 15)**

60. Evropský inspektor ochrany údajů vítá rozlišení mezi osobními údaji uvedenými v čl. 8 odst. 1 směrnice 95/46/ES na jedné straně a osobními údaji uvedenými v čl. 8 odst. 5 na straně druhé. Rovněž vítá, že nařízení jasně specifikuje, že zvláštní kategorie údajů lze zpracovávat pouze na základě konkrétního důvodu uvedeného v článku 8 směrnice 95/46/ES.

61. V této souvislosti má evropský inspektor ochrany údajů za to, že systém IMI bude zpracovávat značné množství citlivých údajů spadajících do oblasti působnosti čl. 8 odst. 2 směrnice 95/46/ES. Systém IMI byl skutečně od samého svého počátku, kdy byl poprvé uveden do provozu na podporu správní spolupráce podle směrnic o službách a uznávání odborných kvalifikací, určen ke zpracování takových údajů, zejména údajů týkajících se porušení trestněprávních předpisů a správních předpisů, která mohou mít vliv na právo odborně kvalifikovaného pracovníka nebo poskytovatele služeb vykonávat práci/poskytovat služby v jiném členském státě.

62. Kromě toho bude v systému IMI pravděpodobně zpracováváno značné množství citlivých údajů podle čl. 8 odst. 1 (zejména údajů týkajících se zdravotního stavu), jakmile se systém IMI rozšíří a zahrne modul pro síť SOLVIT ([30]). A v neposlední řadě nelze vyloučit, že prostřednictvím systému IMI bude v budoucnosti rovněž možné dle potřeby nebo systematicky shromažďovat další citlivé údaje.

2.7 **Zabezpečení (článek 16 a 16. bod odůvodnění)**

63. Evropský inspektor ochrany údajů s potěšením zjišťuje, že článek 16 výslovně zmiňuje povinnost Komise dodržovat svá vlastní vnitřní pravidla přijatá Komisí podle článku 22 nařízení (ES) č. 45/2001 a přijmout a průběžně aktualizovat bezpečnostní plán pro systém IMI.

64. S cílem tato ustanovení dále posílit evropský inspektor ochrany údajů doporučuje, aby nařízení požadovalo posouzení rizik a přezkum bezpečnostního plánu před každým rozšířením systému IMI do nové oblasti politiky nebo před přidáním nové funkce s dopadem na osobní údaje ([31]).

65. Kromě toho evropský inspektor ochrany údajů rovněž konstatuje, že článek 16 a 16. bod odůvodnění odkazují pouze na povinnosti Komise a úlohu dohledu evropského inspektora ochrany údajů. Tento odkaz může být zavádějící. Ačkoli je pravda, že Komise je provozovatelem systému a jako taková odpovídá za převážnou část udržování zabezpečení v systému IMI, mají i příslušné orgány své povinnosti, které pak podléhají dohledu vnitrostátních orgánů ochrany údajů. Proto by článek 16 a 16. bod odůvodnění měly odkazovat i na povinnosti v oblasti zabezpečení týkající se ostatních subjektů v systému IMI podle směrnice 95/46/ES a na pravomoci dohledu vnitrostátních orgánů ochrany údajů.

2.8 **Informace poskytované subjektům údajů a transparentnost (článek 17)**

2.8.1 *Informace poskytované v členských státech*

66. Pokud jde o čl. 17 odst. 1, evropský inspektor ochrany údajů doporučuje, aby konkrétnější ustanovení v nařízení zajistila, že subjekty údajů budou plně informovány o zpracování jejich údajů v systému IMI. S přihlédnutím k tomu, že systém IMI využívá více příslušných orgánů včetně mnoha malých orgánů místní správy bez dostatečných zdrojů, důrazně se doporučuje, aby bylo informování koordinováno na celostátní úrovni.

([29]) Ačkoli uchovávání údajů představuje poměrně menší riziko pro ochranu soukromí, evropský inspektor ochrany údajů se přesto domnívá, že uchovávání osobních údajů uživatelů systému IMI po dobu pěti let poté, co již nemají do systému IMI přístup, není dostatečně zdůvodněno.

([30]) Viz příloha II oddíl I bod 1.

([31]) Viz také oddíl 12 věnovaný doporučením týkajícím se auditů.

2.8.2 *Informace poskytované Komisí*

67. Čl. 17 odst. 2 písm. a) vyžaduje, aby Komise uváděla oznámení o ochraně osobních údajů týkající se jejích vlastních činností při zpracování údajů podle článků 10 a 11 nařízení (ES) č. 45/2001. Kromě toho čl. 17 odst. 2 písm. b) požaduje, aby Komise rovněž poskytovala informace týkající se „aspektů ochrany údajů u postupů správní spolupráce v systému IMI podle článku 12". A konečně, čl. 17 odst. 2 písm. c) vyžaduje, aby Komise poskytovala informace „o výjimkách nebo omezení práv subjektů údajů uvedených v článku 19".

68. Evropského inspektora ochrany údajů těší tato ustanovení, která pomáhají přispívat k transparentnosti operací zpracování údajů v systému IMI. Jak bylo uvedeno v oddíle 2.1 výše, v případě systému informačních technologií využívaného v 27 různých členských státech má zásadní význam zajištění jednotnosti ve věci provozu systému, uplatňovaných opatření na ochranu údajů a informací poskytovaných subjektům údajů ([32]).

69. S ohledem na výše uvedené by měla být ustanovení čl. 17 odst. 2 dále posílena. Komise jako provozovatel systému má nejlepší postavení k tomu, aby se chopila aktivní úlohy při poskytování první „vrstvy" oznámení o ochraně údajů a jiných relevantních informací pro subjekty údajů na své mnohojazyčné internetové stránce, také „jménem" příslušných orgánů, tedy aby zajišťovala informace požadované podle článků 10 či 11 směrnice 95/46/ES. Potom by často stačilo, aby oznámení poskytovaná příslušnými orgány v členských státech prostě odkazovala na oznámení poskytované Komisí a pouze je dle potřeby doplňovala s cílem zajistit dodržování případných konkrétních dalších informací, které výslovně požadují vnitrostátní právní předpisy.

70. Kromě toho by čl. 17 odst. 2 písm. b) měl vyjasňovat, že informace poskytnuté Komisí budou komplexně zahrnovat veškeré oblasti politiky, veškeré druhy postupů správní spolupráce a veškeré funkce v systému IMI a konkrétně obsáhnou i kategorie údajů, které lze zpracovávat. To by mělo zahrnovat i zveřejnění souborů otázek používaných v individuální spolupráci na internetové stránce systému IMI, jak tomu v současné době v praxi je.

2.9 **Právo na přístup, opravu a vymazání (článek 18)**

71. Evropský inspektor ochrany údajů by znovu rád odkázal, jak je uvedeno v oddíle 2.1 výše, na to, že zajištění jednotnosti ve věci provozu systému a uplatňovaných opatření na ochranu údajů má zásadní význam. Z toho důvodu by evropský inspektor ochrany údajů dále upřesnil ustanovení o právu na přístup, opravu a vymazání.

72. Článek 18 by měl specifikovat, na koho by se měly subjekty údajů obrátit se žádostí o přístup. To by mělo jasné, pokud jde o přístup k údajům během různých období:

— před uzavřením případu,

— po uzavření případu, ale před uplynutím doby uchovávání údajů v délce osmnácti měsíců,

— a konečně v době, kdy jsou údaje „zablokovány".

73. Nařízení by rovněž mělo požadovat, aby příslušné orgány ve věci žádostí o přístup dle potřeby spolupracovaly. Oprava a vymazání by měly být provedeny „co nejdříve, nejpozději však do 60 dnů", nikoli jen „do 60 dnů". Měl by být uveden odkaz i na možnost vybudování modulu ochrany údajů a možnost řešení vytvořených podle zásady ochrany soukromí již od návrhu pro spolupráci mezi orgány ve věci přístupových práv, jakož i na „oprávnění subjektů údajů", například tím, že by jim byl poskytnut přímý přístup k jejich údajům v případech, kdy to je relevantní a proveditelné.

2.10 **Dohled (článek 20)**

74. V posledních letech byl vypracován model „koordinovaného dohledu". Tento model dohledu, který nyní funguje v systému Eurodac a v částech celního informačního systému, byl rovněž přijat pro Vízový informační systém (VIS) a pro druhou generaci Schengenského informačního systému (SIS-II).

75. Tento model má tři vrstvy:

— dohled na vnitrostátní úrovni zajišťují vnitrostátní orgány ochrany údajů,

— dohled na úrovni EU zajišťuje evropský inspektor ochrany údajů,

— koordinace je zajištěna prostřednictvím pravidelných setkání a dalších koordinovaných činností za podpory evropského inspektora ochrany údajů, který pro tento koordinační mechanismus zajišťuje služby sekretariátu.

76. Tento model se osvědčil jako úspěšný a efektivní a měl by být v budoucnosti předpokládán pro další informační systémy.

77. Evropský inspektor ochrany údajů vítá, že článek 20 návrhu konkrétně stanoví koordinovaný dohled pro vnitrostátní orgány ochrany údajů a evropského inspektora ochrany údajů na základě (obecně řečeno) modelu zřízeného v nařízeních o systémech VIS a SIS II ([33]).

([32]) Tento přístup k zajištění jednotnosti by měl samozřejmě v případě potřeby a odůvodnění řádně zohledňovat veškeré rozdíly mezi státy.

([33]) Viz nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) (Úř. věst. L 381, 28.12.2006, s. 4) a nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS) (Úř. věst. L 218, 13.8.2008, s. 60).

78. Evropský inspektor ochrany údajů by v určitých bodech posílil ustanovení o koordinovaném dohledu a pro tento účel by podpořil podobná ustanovení, jaká jsou zavedena například v kontextu Vízového informačního systému (články 41–43 nařízení o VIS), Schengenského systému II (články 44–46 nařízení o SIS-II) a jaká se předpokládají pro systém Eurodac ([34]). Zejména by bylo užitečné, kdyby nařízení:

— v čl. 20 odst. 1 a 2 stanovilo a jasněji rozdělilo příslušné úkoly vnitrostátních orgánů ochrany údajů a evropského inspektora ochrany údajů v oblasti dohledu ([35]),

— v čl. 20 odst. 3 upřesnilo, že vnitrostátní orgány ochrany údajů a evropský inspektor ochrany údajů, každý v rozsahu svých pravomocí, „aktivně spolupracují" a „zajišťují koordinovaný dohled nad systémem IMI" (a nikoli jen odkazovalo na koordinovaný dohled, aniž by zmínilo aktivní spolupráci) ([36]), a

— podrobněji upřesňovalo, co může spolupráce zahrnovat, například aby stanovilo požadavek, že vnitrostátní orgány ochrany údajů a evropský inspektor ochrany údajů, „každý v rozsahu svých pravomocí, si vyměňují důležité informace, vzájemně si pomáhají při provádění auditů a inspekcí, posuzují potíže vznikající při výkladu a uplatňování nařízení o systému IMI, zkoumají obtíže s výkonem nezávislého dohledu nebo při výkonu práv subjektů údajů, vypracovávají harmonizované návrhy společných řešení všech obtíží a podle potřeby prosazují informovanost o právech na ochranu údajů" ([37]).

79. S ohledem na výše uvedené, evropský inspektor ochrany údajů si je vědom současných menších rozměrů systému IMI, různé povahy zpracovávaných údajů i toho, že se systém IMI vyvíjí. Proto uznává, že ve věci četnosti setkání a auditů by mohla být žádoucí větší flexibilita. Stručně řečeno, evropský inspektor ochrany údajů doporučuje, aby nařízení stanovilo potřebná minimální pravidla pro zajištění efektivní spolupráce, ale aby nevytvářelo zbytečnou správní zátěž.

80. Čl. 20 odst. 3 návrhu nevyžaduje pravidelná setkání, ale pouze stanoví, že evropský inspektor ochrany údajů může „vnitrostátní orgány dohledu vyzvat, aby se … sešly, je-li to nezbytné". Evropský inspektor ochrany údajů vítá, že tato ustanovení ponechávají na dotčených stranách, aby rozhodly o četnosti a formách setkání a o ostatních procesních podrobnostech týkajících se jejich spolupráce. Tyto podrobnosti lze dohodnout v jednacích řádech, které jsou již v návrhu zmíněny.

81. Pokud jde o pravidelné audity, mohlo by být také efektivnější ponechat na spolupracujících orgánech, aby ve svých jednacích řádech určily, kdy a s jakou četností by se takové audity měly konat. To může záviset na řadě faktorů a může se to i postupně měnit. Proto evropský inspektor ochrany údajů podporuje přístup Komise, který i v tomto ohledu umožňuje větší flexibilitu.

2.11 **Vnitrostátní používání systému IMI**

82. Evropský inspektor ochrany údajů vítá, že návrh poskytuje jasný právní základ vnitrostátního používání systému IMI a že toto používání podléhá několika podmínkám, včetně toho, že musí být konzultován vnitrostátní orgán ochrany údajů a že použití musí být v souladu s vnitrostátními právními předpisy.

2.12 **Výměna informací s třetími zeměmi (článek 22)**

83. Evropský inspektor ochrany údajů vítá požadavky stanovené v čl. 22 odst. 1 v oblasti výměn informací, jakož i skutečnost, že čl. 22 odst. 3 zajišťuje transparentnost rozšíření oblasti působnosti prostřednictvím zveřejnění aktualizovaného seznamu třetích zemí, které systém IMI používají, v Úředním věstníku (čl. 22 odst. 3).

84. Evropský inspektor ochrany údajů dále doporučuje, aby Komise zúžila odkaz na výjimky podle článku 26 směrnice 95/46/ES tak, aby zahrnoval pouze čl. 26 odst. 2. Jinými slovy: příslušné orgány nebo jiné vnější subjekty ve třetí zemi, která nezajišťuje odpovídající ochranu, by neměly mít možnost přímého přístupu k systému IMI, pokud nebudou existovat vhodné smluvní doložky. Tyto doložky by měly být sjednány na úrovni EU.

85. Evropský inspektor ochrany údajů zdůrazňuje, že jiné výjimky, například případ, kdy „předání je nezbytné nebo se stává právně závazným pro zachování důležitého veřejného zájmu nebo pro zjištění, výkon nebo obranu právních nároků před soudem", by neměly být využívány k odůvodnění předávání údajů do třetích zemí pomocí přímého přístupu k systému IMI ([38]).

2.13 **Odpovědnost (článek 26)**

86. V souladu s očekávaným posilováním ujednání pro zvýšení odpovědnosti během přezkumu rámce ochrany údajů EU ([39]) evropský inspektor ochrany údajů doporučuje, aby nařízení stanovilo jasný rámec pro vhodné mechanismy vnitřní kontroly, který zajistí soulad s předpisy v oblasti ochrany údajů a poskytne o něm doklady, přičemž bude obsahovat alespoň níže uvedené prvky.

([34]) Nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 2000 o zřízení systému „Eurodac" pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy (Úř. věst. L 316, 15.12.2000, s. 1), v současné době prochází přepracováním. V této souvislosti jsou zvažována podobná ustanovení, jaká uvádí nařízení o VIS a SIS II.

([35]) Viz například články 41 a 42 nařízení o VIS.

([36]) Viz například čl. 43 odst. 1 nařízení o VIS.

([37]) Viz například čl. 43 odst. 2 nařízení o VIS.

([38]) Podobný přístup byl uplatněn v čl. 22 odst. 2 ve věci Komise jako subjektu IMI.

([39]) Viz oddíl 2.2.4. sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609 v konečném znění. Viz také oddíl 7 stanoviska evropského inspektora ochrany údajů vydaného k tomuto sdělení Komise dne 14. ledna 2011.

87. V této souvislosti evropský inspektor ochrany údajů vítá požadavek v čl. 26 odst. 2 nařízení, podle něhož by Komise měla každé tři roky podávat evropskému inspektorovi ochrany údajů zprávu o aspektech ochrany údajů včetně zabezpečení. Bylo by žádoucí, aby nařízení vyjasnilo, že evropský inspektor ochrany údajů by pak naopak byl povinen sdílet zprávu Komise s vnitrostátními orgány ochrany údajů v rámci koordinovaného dohledu podle článku 20. Také by bylo užitečné objasnit, že zpráva by se ve vztahu ke každé oblasti politiky a každé funkci měla zabývat tím, jak jsou klíčové zásady a aspekty ochrany údajů (např. informace pro subjekty údajů, přístupová práva, zabezpečení) řešeny v praxi.

88. Kromě toho by nařízení mělo upřesnit, že rámec pro mechanismy vnitřní kontroly by měl zahrnovat i posouzení ochrany soukromí (také včetně analýzy bezpečnostních rizik), politiku ochrany údajů (včetně bezpečnostního plánu) přijatou na základě uvedených posouzení, jakož i periodické přezkumy a audity.

2.14 **Ochrana soukromí již od návrhu**

89. Evropský inspektor ochrany údajů vítá, že na tuto zásadu odkazuje 6. bod odůvodnění v nařízení ([40]). Doporučuje, aby kromě tohoto odkazu nařízení zavedlo i konkrétní ochranná opatření podle zásady ochrany soukromí již od návrhu, jako například:

— modul ochrany údajů umožňující subjektům údajů efektivnější výkon jejich práv ([41]),

— jasné oddělení jednotlivých oblastí politiky zařazených do systému IMI („čínské zdi") ([42]),

— zvláštní technická řešení pro omezení kapacit vyhledávání v adresářích, výstražných informacích a jinde s cílem zajistit omezení účelu,

— konkrétní opatření, která zajistí, že případy bez jakékoli aktivity budou uzavřeny ([43]),

— vhodné procesní záruky v kontextu budoucího vývoje ([44]).

3. **ZÁVĚRY**

90. Obecně evropský inspektor ochrany údajů pohlíží na systém IMI kladně. Evropský inspektor ochrany údajů podporuje cíle Komise při budování elektronického systému pro výměnu informací a při regulaci jeho aspektů týkajících se ochrany údajů. Evropský inspektor ochrany údajů rovněž vítá, že Komise pro systém IMI navrhuje horizontální právní nástroj v podobě nařízení Parlamentu a Rady. Je potěšen tím, že návrh komplexně poukazuje na otázky ochrany údajů, které jsou pro systém IMI nejvýznamnější.

91. Pokud jde o právní rámec pro systém IMI, který má být stanoven navrhovaným nařízením, upozorňuje evropský inspektor ochrany údajů na dvě hlavní výzvy:

— na potřebu zajistit jednotnost a přitom respektovat rozmanitost a

— na potřebu vyvážit flexibilitu a právní jistotu.

92. Funkce systému IMI, které již lze předpokládat, by měly být vyjasněny a řešeny konkrétněji.

93. Měly by být uplatněny vhodné procesní záruky pro zajištění toho, že při budoucím vývoji systému IMI bude pečlivě zvažována i ochrana údajů. To by mělo zahrnovat posouzení dopadů a konzultace evropského inspektora ochrany údajů a vnitrostátních orgánů ochrany údajů před každým rozšířením systému IMI o nové oblasti politiky a/nebo nové funkce.

94. Měla by být dále upřesněna přístupová práva vnějších subjektů a práva přístupu k výstrahám.

95. Pokud jde o doby uchovávání údajů:

— nařízení by mělo stanovit záruky toho, že případy budou v systému IMI uzavírány včas a že spící případy (případy bez jakékoli nedávné aktivity) budou z databáze vymazány,

— mělo by být znovu zváženo, zda existuje odpovídající odůvodnění pro prodloužení stávajícího šestiměsíčního období na osmnáct měsíců po uzavření případu,

— Komise neposkytla dostatečné odůvodnění nezbytnosti a přiměřenosti uchovávání „zablokovaných údajů" po dobu až pěti let, a proto by tento návrh měl být znovu zvážen,

— mělo by být jasněji rozlišeno mezi výstrahami a úložišti informací: nařízení by mělo jako implicitní pravidlo stanovit, že i) pro výstrahy by mělo platit šestiměsíční období uchování údajů (není-li stanoveno jinak ve vertikálních právních předpisech a s výhradou odpovídajících ochranných opatření) a že ii) toto období by se mělo počítat od okamžiku odeslání výstrahy.

96. Nařízení by mělo požadovat posouzení rizik a přezkum bezpečnostního plánu před každým rozšířením systému IMI do nové oblasti politiky nebo před přidáním nové funkce s dopadem na osobní údaje.

97. Ustanovení o informacích pro subjekty údajů a přístupových právech by měla být posílena a měla by podporovat jednotnější přístup.

([40]) Tamtéž.
([41]) Viz oddíl 2.9 výše.
([42]) Viz oddíl 2.4 výše.
([43]) Viz oddíl 2.5.2 výše.
([44]) Viz oddíl 2.2.2 výše.

98. Evropský inspektor ochrany údajů by v určitých bodech posílil ustanovení o koordinovaném dohledu a k tomuto účelu by podpořil podobná ustanovení, jaká platí například v kontextu Vízového informačního systému či Schengenského systému II a jaká se předpokládají pro systém Eurodac. Pokud jde o četnost setkání a auditů, evropský inspektor ochrany údajů podporuje návrh v jeho pružném přístupu, který má zajistit, aby nařízení stanovilo potřebná minimální pravidla pro zajištění efektivní spolupráce, aniž by vytvářelo zbytečnou správní zátěž.

99. Nařízení by mělo zajistit, aby příslušné orgány nebo jiné vnější subjekty ve třetí zemi, která nezajišťuje odpovídající ochranu, neměly možnost přímého přístupu k systému IMI, pokud nebudou existovat vhodné smluvní doložky. Tyto doložky by měly být sjednány na úrovni EU.

100. Nařízení by mělo stanovit jasný rámec pro odpovídající mechanismy vnitřní kontroly, který zajistí soulad s předpisy v oblasti ochrany údajů a poskytne o něm doklady, včetně posouzení ochrany soukromí (také včetně analýzy bezpečnostních rizik), politiky ochrany údajů (včetně bezpečnostního plánu) přijaté na základě uvedených posouzení, jakož i periodických přezkumů a auditů.

101. Nařízení by mělo zavést i konkrétní ochranná opatření podle zásady ochrany soukromí již od návrhu.

V Bruselu dne 22. listopadu 2011.

Giovanni BUTTARELLI

zástupce evropského inspektora ochrany údajů