Shrnutí stanoviska evropského inspektora ochrany údajů ke společnému sdělení Komise a vysoké představitelky Evropské unie pro zahraniční věci a bezpečnostní politiku nazvanému „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“ a k návrhu Komise na směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

(Úplné znění tohoto stanoviska je k dispozici v angličtině, francouzštině a němčině na webových stránkách evropského inspektora ochrany údajů na adrese http://www.edps.europa.eu)

(2014/C 32/10)

1. **Úvod**

1.1 *Konzultace evropského inspektora ochrany údajů*

1. Dne 7. února 2013 přijaly Komise a vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů nazvané „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“ ([1]) (dále jen „společné sdělení“, „strategie pro kybernetickou bezpečnost“ nebo „strategie“).

2. Ve stejný den přijala Komise návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii ([2]) (dále jen „navrhovaná směrnice“ nebo „návrh“). Tento návrh byl zaslán dne 7. února 2013 evropskému inspektorovi ochrany údajů ke konzultaci.

3. Před přijetím společného sdělení a návrhu bylo evropskému inspektorovi ochrany údajů umožněno předat Komisi neformální připomínky. Vítá skutečnost, že některé z jeho připomínek jsou ve společném sdělení a návrhu zohledněny.

4. **Závěry**

74. Evropský inspektor ochrany údajů vítá skutečnost, že Komise a vysoká představitelka EU pro zahraniční věci a bezpečnostní politiku již předložily komplexní strategii kybernetické bezpečnosti doplněnou o návrh směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (směrnice NIS). Strategie doplňuje politická opatření, která již byla v oblasti bezpečnosti sítí a informací Evropskou unií vypracována.

75. Evropský inspektor ochrany údajů vítá skutečnost, že strategie překonává tradiční přístup, který proti sobě staví bezpečnost a soukromí, tím, že umožňuje výslovné uznání soukromí a ochrany údajů jako základních hodnot, kterými by se měla řídit politika kybernetické bezpečnosti v EU i ve světě. Evropský inspektor ochrany údajů konstatuje, že strategie kybernetické bezpečnosti a navrhovaná směrnice o bezpečnosti sítí a informací mohou zásadním způsobem přispět k zajištění ochrany práv jednotlivce v oblasti soukromí a ochrany údajů v internetovém prostředí. Současně musí být zajištěno, že nepovedou k opatřením, která by představovala nezákonný zásah do práv jednotlivce v oblasti soukromí a ochrany údajů.

76. Evropský inspektor ochrany údajů (EIOÚ) rovněž vítá, že ochrana údajů je ve strategii uvedena na několika místech a je zohledněna v navrhované směrnici o bezpečnosti sítí a informací. Evropský inspektor ochrany údajů však lituje, že strategie a navrhovaná směrnice nezdůrazňují více přínos stávajících a nových právních předpisů na ochranu údajů pro bezpečnost a nedokáží plně zajistit, aby všechny povinnosti vyplývající z navrhované směrnice nebo jiných prvků strategie byly v souladu s povinnostmi v oblasti ochrany údajů a vzájemně se nepřekrývaly ani si neodporovaly.

77. Kromě toho evropský inspektor ochrany údajů konstatuje, že vzhledem k tomu, že nebyly dostatečně zváženy a plně zohledněny jiné souběžné iniciativy Komise a probíhající legislativní postupy, jako je reforma ochrany údajů a návrh nařízení o elektronické identifikaci a důvěryhodných službách, neposkytuje strategie kybernetické bezpečnosti opravdu komplexní a ucelený pohled na kybernetickou bezpečnost v EU a je zde riziko, že povede k roztříštěnosti a k na sobě nezávislým přístupům v jednotlivých oblastech. Evropský

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

inspektor ochrany údajů rovněž konstatuje, že ani navrhovaná směrnice o bezpečnosti sítí a informací zatím neumožňuje komplexní přístup k bezpečnosti v EU a že povinnosti stanovené právními předpisy na ochranu údajů jsou pravděpodobně nejucelenějšími povinnostmi v oblasti sítí a bezpečnosti, jež právo EU stanoví.

78. Evropský inspektor ochrany údajů rovněž lituje, že není dostatečně zohledněna ani významná úloha, kterou mají orgány pro ochranu údajů při provádění a prosazování povinností týkajících se bezpečnosti a při posilování kybernetické bezpečnosti.

79. Co se týče strategie kybernetické bezpečnosti, evropský inspektor ochrany údajů zdůrazňuje následující:

— Zvláště důležitá je jasná definice pojmů „kybernetická odolnost“, „kyberkriminalita“ a „kybernetická obrana“, protože tyto termíny se používají pro zdůvodnění určitých zvláštních opatření, která by mohla způsobit zásah do základních práv včetně práva na soukromí a ochranu údajů. Avšak definice pojmu „kyberkriminalita“ uvedená ve strategii a v Úmluvě o kyberkriminalitě je stále velmi široká. Bylo by vhodné, aby definice pojmu „kyberkriminalita“ byla jasná a *restriktivní*, a nikoli příliš široká.

— Právní předpisy na ochranu údajů by se měly vztahovat na všechna opatření strategie, která se týkají zpracování osobních údajů. Přestože právní předpisy na ochranu údajů nejsou v oddílech týkajících se kyberkriminality a kybernetické obrany výslovně uvedeny, evropský inspektor ochrany údajů zdůrazňuje, že mnohé z činností plánovaných v těchto oblastech by zahrnovaly zpracovávání osobních údajů, a spadaly by proto do oblasti působnosti platných právních předpisů na ochranu údajů. EIOÚ také poznamenává, že řada opatření spočívá ve vytvoření koordinačních mechanismů, což bude vyžadovat uplatnění odpovídajících záruk na ochranu údajů, pokud jde o postupy pro výměnu osobních údajů.

— Orgány pro ochranu údajů hrají v kontextu kybernetické bezpečnosti důležitou roli. Jako ochránci práv jednotlivců na ochranu soukromí a osobních údajů jsou orgány pro ochranu údajů aktivně zapojeny do ochrany jejich osobních údajů jak v režimu offline, tak i online. Měly by proto v rámci své pravomoci orgánu dohledu být odpovídajícím způsobem zapojeny do provádění opatření, která se týkají zpracování osobních údajů (např. zahájení pilotního projektu EU týkajícího se boje proti botnetům a malwaru). Ostatní subjekty v oblasti kybernetické bezpečnosti by s nimi měly rovněž spolupracovat při plnění svých úkolů, například při výměně osvědčených postupů a zvyšování povědomí. Evropský inspektor ochrany údajů a vnitrostátní orgány pro ochranu údajů by se měli odpovídajícím způsobem zúčastnit konference na vysoké úrovni, která bude svolána v roce 2014 za účelem posouzení pokroku při provádění strategie.

80. Pokud jde o navrhovanou směrnici o bezpečnosti sítí a informací, evropský inspektor ochrany údajů zákonodárcům doporučuje:

— Zajistit v čl. 3 odst. 8 větší jasnost a právní jistotu definice hospodářských subjektů, které spadají do oblasti působnosti návrhu, a sestavit vyčerpávající seznam, který by zahrnoval všechny příslušné zúčastněné strany s cílem zajistit plně harmonizovaný a integrovaný přístup k bezpečnosti v rámci EU.

— Ujasnit v čl. 1 odst. 2 písm. c), že se navrhovaná směrnice vztahuje na instituce a orgány EU, a zahrnout do čl. 1 odst. 5 návrhu odkaz na nařízení (ES) č. 45/2001.

— Uznat horizontální úlohu tohoto návrhu, pokud jde o bezpečnost, tím, že se v článku 1 výslovně stanoví, že by se měl použít, aniž by byla dotčena stávající nebo budoucí podrobnější pravidla v konkrétních oblastech (jako jsou např. pravidla, která se mají vztahovat na poskytovatele důvěryhodných služeb v navrhovaném nařízení o elektronické identifikaci).

— Doplnit bod odůvodnění vysvětlující nutnost zakotvit zásady ochrany údajů již od návrhu a standardního nastavení ochrany údajů již v počáteční fázi návrhu mechanismů stanovených v navrhované směrnici a v průběhu celého životního cyklu všech dotčených procesů, postupů, organizací, technik a infrastruktur a zohlednit přitom navrhované nařízení o ochraně údajů.

— Objasnit definici „sítě a informačních systémů“ v čl. 3 odst. 1 a definici „incidentu“ v čl. 3 odst. 4 a nahradit v čl. 5 odst. 2 povinnost vypracovat „plán posouzení rizik“ povinností „zřídit a udržovat rámec pro řízení rizik“.

— Upřesnit v čl. 1 odst. 6, že zpracování osobních údajů podle článku čl. 7 písm. e) směrnice 95/46/ES by bylo odůvodněné, pouze pokud by bylo nezbytné pro dosažení cílů veřejného zájmu, které sleduje navrhovaná směrnice. Je však třeba zajistit řádné dodržování zásady nezbytnosti a proporcionality tak, aby byly zpracovávány pouze údaje nezbytně nutné pro účely, kterých má být dosaženo.

— Stanovit v článku 14 okolnosti, za jakých je oznámení vyžadováno, jakož i obsah a formu oznámení včetně druhu osobních údajů, které by měly být oznámeny, a zda a do jaké míry budou oznámení a související podklady obsahovat informace o osobních údajích, které se týkají konkrétního bezpečnostního incidentu (např. IP adresy). Je třeba zohlednit skutečnost, že příslušným orgánům pro bezpečnost sítí a informací by mělo být umožněno shromažďovat a zpracovávat osobní údaje v rámci bezpečnostního incidentu, pouze pokud je to nezbytně nutné. V návrhu by měla být rovněž uvedena vhodná ochranná opatření pro zajištění odpovídající ochrany osobních údajů zpracovávaných příslušnými orgány pro bezpečnost sítí a informací.

— Ujasnit v článku 14, že oznamování incidentů podle čl. 14 odst. 2 by se mělo použít, aniž jsou dotčeny oznamovací povinnosti týkající se porušení ochrany osobních údajů podle platných právních předpisů na ochranu údajů. V návrhu by měly být uvedeny hlavní aspekty postupu pro spolupráci příslušných orgánů pro bezpečnost sítí a informací s orgány pro ochranu údajů v případech, kdy bezpečnostní incident zahrnuje porušení ochrany osobních údajů.

— Upravit čl. 14 odst. 8 tak, aby se vynětí mikropodniků z působnosti oznámení nevztahovalo na subjekty, které hrají klíčovou roli v poskytování služeb informační společnosti, například s ohledem na povahu informací, které zpracovávají (např. biometrické údaje nebo citlivé údaje).

— Přidat do návrhu ustanovení upravující další výměnu osobních údajů mezi příslušnými orgány pro bezpečnost sítí a informací a jinými příjemci s cílem zajistit, že i) osobní údaje jsou zpřístupněny pouze v případě, že je jejich zpracování pro plnění úkolů příjemce nezbytné, a to v souladu s příslušným právním základem a ii) zpřístupněné informace jsou omezeny na to, co je pro plnění jejich úkolů nezbytné. Pozornost by měla být věnována tomu, jak subjekty, které poskytují údaje do sítě pro sdílení informací, zajišťují soulad se zásadou omezení účelu.

— Určit časový limit pro uchovávání osobních údajů pro účely stanovené v navrhované směrnici, zejména pokud jde o uchovávání údajů příslušnými orgány pro bezpečnost sítí a informací a také v rámci bezpečné infrastruktury sítě pro spolupráci.

— Připomenout příslušným orgánům pro bezpečnost sítí a informací jejich povinnost poskytovat subjektům údajů příslušné informace o zpracování osobních údajů, například zveřejněním zásad ochrany osobních údajů na jejich internetových stránkách.

— Přidat ustanovení týkající se úrovně bezpečnosti, kterou musí příslušné orgány pro bezpečnost sítí a informací splnit, pokud jde o shromažďované, zpracovávané a vyměňované informace. V souvislosti s ochranou osobních údajů ze strany orgánů pro bezpečnost sítí a informací by měl být výslovně uveden odkaz na bezpečnostní požadavky stanovené v článku 17 směrnice 95/46/ES.

— Vyjasnit v čl. 9 odst. 2, že kritéria pro účast členských států v bezpečném systému pro sdílení informací by měla zajistit, že všichni účastníci systému pro sdílení informací na všech stupních zpracování údajů zaručí vysokou úroveň bezpečnosti a odolnosti. Tato kritéria by měla zahrnovat odpovídající opatření týkající se důvěrnosti a bezpečnosti v souladu s články 16 a 17 směrnice 95/46/ES a články 21 a 22 nařízení (ES) č. 45/2001. Komise by těmito kritérii měla být výslovně vázána vzhledem k tomu, že je do bezpečného systému pro sdílení informací zapojena jako správce.

— Doplnit do článku 9 popis rolí a odpovědností Komise a členských států, pokud jde o nastavení, provoz a údržbu bezpečného systému pro sdílení informací, a stanovit, že návrh systému by měl být proveden v souladu se zásadou ochrany údajů již od návrhu, zásadou standardního nastavení ochrany údajů a zásadou bezpečnosti již od návrhu.

— Doplnit do článku 13, že veškeré předávání osobních údajů příjemcům se sídlem v zemích mimo EU by se mělo uskutečňovat v souladu s články 25 a 26 směrnice 95/46/ES a článkem 9 nařízení (ES) č. 45/2001.

V Bruselu dne 14. června 2013.

Peter HUSTINX

evropský inspektor ochrany údajů