Zhrnutie stanoviska európskeho dozorného úradníka pre ochranu údajov k spoločnému oznámeniu Komisie a vysokej predstaviteľky Európskej únie pre zahraničné veci a bezpečnostnú politiku s názvom Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor a k návrhu Komisie na smernicu o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii

(Úplné znenie tohto stanoviska sa nachádza v anglickom, vo francúzskom a v nemeckom jazyku na webovej stránke európskeho dozorného úradníka pre ochranu údajov http://www.edps.europa.eu)

(2014/C 32/10)

1. **Úvod**

1.1. *Konzultácie s európskym dozorným úradníkom pre ochranu údajov*

1. Komisia a vysoká predstaviteľka Európskej únie pre zahraničné veci a bezpečnostnú politiku prijali 7. februára 2013 spoločné oznámenie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor ([1]) (ďalej len „spoločné oznámenie“, „stratégia kybernetickej bezpečnosti“ alebo „stratégia“).

2. V ten istý deň prijala Komisia návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii ([2]) (ďalej len „navrhovaná smernica“ alebo „návrh“). Tento návrh bol 7. februára 2013 odoslaný európskemu dozornému úradníkovi pre ochranu údajov na konzultáciu.

3. Európsky dozorný úradník pre ochranu údajov mal pred prijatím spoločného oznámenia a návrhu príležitosť poskytnúť Komisii svoje neformálne pripomienky. Víta skutočnosť, že niektoré jeho pripomienky boli v spoločnom oznámení a v návrhu zohľadnené.

4. **Závery**

74. Európsky dozorný úradník pre ochranu údajov víta skutočnosť, že Komisia a vysoká predstaviteľka EÚ pre zahraničné veci a bezpečnostnú politiku predložili komplexnú stratégiu kybernetickej bezpečnosti doplnenú o návrh smernice o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii. Stratégia dopĺňa politické opatrenia, ktoré EÚ v oblasti bezpečnosti sietí a informácií už vypracovala.

75. Európsky dozorný úradník pre ochranu údajov víta skutočnosť, že v rámci tejto stratégie sa súkromie a ochrana osobných údajov výslovne uznávajú ako základné hodnoty, ktorými by sa mala riadiť politika kybernetickej bezpečnosti v EÚ aj na medzinárodnej úrovni, čím sa prekračuje tradičný prístup spočívajúci v protiklade súkromia a bezpečnosti. Európsky dozorný úradník pre ochranu údajov poznamenáva, že stratégia kybernetickej bezpečnosti a navrhovaná smernica o bezpečnosti sietí a informácií môžu významne prispieť k zaisteniu ochrany práv jednotlivcov na súkromie a ochranu osobných údajov v online prostredí. Zároveň sa musí zabezpečiť, aby neviedli k opatreniam, ktoré by predstavovali protiprávne zasahovanie do práv jednotlivcov na súkromie a ochranu osobných údajov.

76. Európsky dozorný úradník pre ochranu údajov víta aj to, že ochrana údajov sa spomína vo viacerých častiach stratégie a zohľadňuje sa v navrhovanej smernici o bezpečnosti sietí a informácií. Európsky dozorný úradník pre ochranu údajov však s poľutovaním konštatuje, že stratégia a navrhovaná smernica dôraznejšie nevyzdvihujú príspevok súčasných a pripravovaných právnych predpisov o ochrane údajov k bezpečnosti a v plnej miere nezaisťujú, aby sa povinnosti vyplývajúce z navrhovanej smernice alebo iných prvkov stratégie vzájomne dopĺňali s povinnosťami vyplývajúcimi z ochrany údajov, neprekrývali sa, ani neboli vo vzájomnom rozpore.

77. Európsky dozorný úradník pre ochranu údajov ďalej poznamenáva, že stratégia kybernetickej bezpečnosti nezabezpečuje skutočne komplexný a holistický pohľad na kybernetickú bezpečnosť v EÚ a hrozí riziko, že pretrvá roztrieštený a rozčlenený prístup, pretože nezvažuje a v plnej miere nezohľadňuje ďalšie paralelné iniciatívy Komisie a prebiehajúce legislatívne postupy, ako sú reforma ochrany údajov a navrhované nariadenie o elektronickej identifikácii a dôveryhodných službách. Európsky dozorný úradník pre ochranu

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

údajov tiež konštatuje, že navrhovaná smernica o bezpečnosti sietí a informácií zatiaľ neumožňuje ani komplexný prístup k bezpečnosti v EÚ a že záväzok stanovený v právnych predpisoch o ochrane údajov je pravdepodobne najkomplexnejším záväzkom v oblasti sietí a bezpečnosti v rámci práva EÚ.

78. Európsky dozorný úradník pre ochranu údajov tiež vyjadruje poľutovanie nad skutočnosťou, že pri vykonávaní a presadzovaní záväzkov v oblasti bezpečnosti a pri zvyšovaní úrovne kybernetickej bezpečnosti nie je náležite zvážená ani dôležitá úloha orgánov na ochranu údajov.

79. Pokiaľ ide o stratégiu kybernetickej bezpečnosti, Európsky dozorný úradník pre ochranu údajov zdôrazňuje, že:

— Veľmi dôležité je jasné vymedzenie pojmov „kybernetická odolnosť“, „kybernetická kriminalita“ a „kybernetická obrana“, pretože tieto pojmy sa používajú ako odôvodnenie určitých osobitných opatrení, ktoré by mohli spôsobiť zasahovanie do základných práv vrátane práv na súkromie a ochranu údajov. Vymedzenia pojmu „kybernetická kriminalita“, ktoré sú uvedené v stratégii a v dohovore o počítačovej kriminalite, sú však stále veľmi široké. Namiesto extenzívneho vymedzenia pojmu sa odporúča skôr jasné a *obmedzujúce* vymedzenie pojmu „kybernetickej kriminality“.

— Právne predpisy o ochrane údajov by sa mali uplatňovať na všetky činnosti uvedené v stratégii vždy, keď sa týkajú opatrení, ktoré si vyžadujú spracovanie osobných údajov. Aj keď sa právne predpisy o ochrane údajov v častiach týkajúcich sa kybernetickej kriminality a kybernetickej obrany osobitne neuvádzajú, európsky dozorný úradník pre ochranu údajov zdôrazňuje, že mnohé opatrenia plánované v týchto oblastiach by zahŕňali spracovanie osobných údajov, a preto by patrili do rozsahu pôsobnosti platných právnych predpisov o ochrane údajov. Pripomína tiež, že mnohé opatrenia spočívajú vo vytváraní mechanizmov koordinácie, ktoré si v súvislosti s rôznymi formami výmeny osobných údajov budú vyžadovať uplatňovanie príslušných záruk na ochranu údajov.

— V kontexte kybernetickej bezpečnosti zohrávajú dôležitú úlohu orgány na ochranu údajov. Orgány na ochranu údajov ako ochrancovia práv jednotlivcov na súkromie a ochranu údajov sa aktívne zapájajú do offline aj online ochrany ich osobných údajov. Vo svojej funkcii dozorných orgánov by sa preto mali náležite angažovať v súvislosti s vykonávacími opatreniami, ktoré zahŕňajú spracovanie osobných údajov [ako napríklad začatie pilotného projektu EÚ v oblasti boja proti botnetom a škodlivému softvéru (malware)]. Pri vykonávaní ich úloh by s nimi mali spolupracovať aj iné subjekty pôsobiace v oblasti kybernetickej bezpečnosti, napríklad pri výmene najlepších postupov a opatreniach na zvyšovanie informovanosti. Do konferencie na vysokej úrovni, ktorej usporiadanie sa plánuje v roku 2014 s cieľom posúdiť pokrok dosiahnutý pri vykonávaní stratégie, by mal byť náležite zapojený aj európsky dozorný úradník pre ochranu údajov a vnútroštátne orgány na ochranu údajov.

80. Pokiaľ ide o navrhovanú smernicu o bezpečnosti sietí a informácií, európsky dozorný úradník pre ochranu údajov zákonodarcom odporúča:

— V článku 3 ods. 8 zvýšiť zrozumiteľnosť a istotu v súvislosti s vymedzením pojmu účastníkov trhu, ktorí patria do rozsahu pôsobnosti návrhu, a vypracovať úplný zoznam obsahujúci všetky príslušné zainteresované strany s cieľom zaistiť v EÚ plne harmonizovaný a integrovaný prístup k bezpečnosti.

— V článku 1 ods. 2 písm. c) objasniť, že navrhovaná smernica sa vzťahuje na inštitúcie a orgány EÚ, a do článku 1 ods. 5 návrhu zahrnúť odkaz na nariadenie (ES) č. 45/2001.

— V článku 1 výslovne uviesť, že by sa mal uplatňovať bez toho, aby boli dotknuté súčasné alebo budúce podrobnejšie pravidlá v konkrétnych oblastiach (ako sú napríklad tie, ktoré sa majú v navrhovanom nariadení o elektronickej identifikácii stanoviť pre poskytovateľov dôveryhodných služieb), a uznať tak horizontálnejšiu úlohu tohto návrhu v súvislosti s bezpečnosťou.

— Doplniť odôvodnenie na vysvetlenie potreby začlenenia ochrany údajov už v štádiu návrhu a ako štandard (predvolenú možnosť) od skorého štádia návrhu mechanizmov ustanovených v návrhu a počas celého životného cyklu príslušných procesov, postupov, organizácií, techník a infraštruktúr s ohľadom na navrhované nariadenie o ochrane údajov.

— Objasniť vymedzenie pojmu „siete a informačné systémy“, ktorý sa uvádza v článku 3 ods. 1, pojmu „incident“, ktorý sa uvádza v článku 3 ods. 4, a v článku 5 ods. 2 nahradiť povinnosť ustanoviť „plán na hodnotenie rizika“ vetou „vytvoriť a udržiavať rámec na riadenie rizík“.

— V článku 1 ods. 6 uviesť, že spracovanie osobných údajov by bolo odôvodnené v zmysle článku 7 písm. e) smernice 95/46/ES, pokiaľ je nevyhnutné v záujme plnenia cieľov verejného záujmu sledovaných navrhovanou smernicou. Musí sa však zabezpečiť náležité dodržiavanie zásad nevyhnutnosti a primeranosti, aby sa spracovali len tie údaje, ktoré sú nevyhnutné na dosiahnutie daného účelu.

— V článku 14 uviesť okolnosti, kedy sa požaduje oznámenie, ako aj obsah a formát oznámenia vrátane druhov osobných údajov, ktoré by sa mali oznámiť, a či by sa mali oznámiť, alebo nie, a v akom rozsahu, oznámenie a podporné dokumenty budú obsahovať podrobnosti o osobných údajoch ovplyvnených konkrétnym bezpečnostným incidentom (napríklad adresy IP). Musí sa zohľadniť skutočnosť, že príslušným orgánom pre oblasť bezpečnosti sietí a informácií by sa malo umožniť zhromažďovať a spracúvať osobné údaje v rámci bezpečnostného incidentu len v prípade, ak je to skutočne nevyhnutné. V návrhu by sa mali stanoviť aj vhodné záruky na zaistenie primeranej ochrany údajov spracovaných príslušnými orgánmi pre oblasť bezpečnosti sietí a informácií.

— V článku 14 objasniť, že oznamovanie incidentov podľa článku 14 ods. 2 by sa malo uplatňovať bez toho, aby bola dotknutá povinnosť oznamovania narušenia osobných údajov podľa príslušných právnych predpisov o ochrane údajov. V návrhu by sa mali vysvetliť hlavné aspekty spolupráce príslušných orgánov pre oblasť bezpečnosti sietí a informácií s orgánmi na ochranu údajov v prípadoch, keď sa bezpečnostný incident týka porušenia ochrany osobných údajov.

— Zmeniť článok 14 ods. 8 tak, aby sa vylúčenie mikropodnikov z rozsahu pôsobnosti oznámenia nevzťahovalo na tých prevádzkovateľov, ktorí zohrávajú rozhodujúcu úlohu pri poskytovaní služieb informačnej spoločnosti, napríklad z hľadiska charakteru informácií, ktoré spracúvajú (napríklad biometrické údaje alebo citlivé údaje).

— Doplniť do návrhu ustanovenia upravujúce ďalšiu výmenu osobných údajov príslušnými orgánmi pre oblasť bezpečnosti sietí a informácií s ďalšími príjemcami, aby sa i) príjemcom sprístupnili len tie osobné údaje, ktorých spracovanie je nevyhnutné na vykonávanie ich úloh v súlade s príslušným právnym základom. a ii) aby sa tieto informácie obmedzili na to, čo je nevyhnutné na plnenie ich úloh. Zvážiť by sa malo aj to, ako subjekty poskytujúce údaje do siete na výmenu informácií zabezpečujú súlad so zásadou obmedzenia účelu.

— Špecifikovať časové obmedzenie uchovávania osobných údajov na účely stanovené v navrhovanej smernici, najmä čo sa týka uchovávania údajov príslušnými orgánmi pre oblasť bezpečnosti sietí a informácií a v rámci bezpečnej infraštruktúry siete spolupráce.

— Pripomenúť príslušným orgánom pre oblasť bezpečnosti sietí a informácií ich povinnosť poskytovať dotknutým osobám príslušné informácie o spracovaní osobných údajov, napríklad zverejnením politiky v oblasti ochrany súkromia na ich webovej stránke.

— Doplniť ustanovenie o úrovni bezpečnosti, ktorú majú príslušné orgány pre oblasť bezpečnosti sietí a informácií spĺňať v súvislosti so zhromažďovanými, spracovanými a vymieňanými informáciami. Pokiaľ ide o ochranu osobných údajov príslušnými orgánmi pre oblasť bezpečnosti sietí a informácií, osobitne by sa mal zahrnúť odkaz na bezpečnostné požiadavky uvedené v článku 17 smernice 95/46/ES.

— V článku 9 ods. 2 objasniť, že kritériá pre účasť členských štátov v bezpečnom systéme výmeny informácií by mali zabezpečiť, aby všetci účastníci systému výmeny informácií zaručovali vo všetkých krokoch spracovania vysokú úroveň bezpečnosti a odolnosti. Tieto kritériá by mali zahŕňať príslušné opatrenia na zabezpečenie dôvernosti a bezpečnosti v súlade s článkami 16 a 17 smernice 95/46/ES a článkami 21 a 22 nariadenia (ES) č. 45/2001. Komisii by mali tieto kritériá ukladať výslovnú povinnosť, aby sa podieľala na bezpečnom systéme výmeny informácií vo funkcii kontrolóra.

— V článku 9 doplniť opis úloh a zodpovedností Komisie a členských štátov pri vytvorení, prevádzkovaní a údržbe bezpečného systému výmeny informácií a stanoviť, že tento systém by sa mal navrhovať v súlade so zásadami ochrany údajov už v štádiu návrhu, ako štandard (predvolená možnosť), a zásadou bezpečnosti už v štádiu návrhu.

— V článku 13 doplniť, že akýkoľvek prenos osobných údajov príjemcom so sídlom mimo územia EÚ by sa mal uskutočniť v súlade s článkami 25 a 26 smernice 95/46/ES a článkom 9 nariadenia (ES) č. 45/2001.

V Bruseli 14. júna 2013

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov