Povzetek mnenja Evropskega nadzornika za varstvo podatkov o skupnem sporočilu Komisije in visoke predstavnice Evropske unije za zunanje zadeve in varnostno politiko o „Strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor“ in predlogu Komisije o direktivi v zvezi z ukrepi za zagotavljanje visoke splošne ravni varnosti omrežij in informacij po vsej Uniji

(Celotno besedilo tega mnenja je na voljo v angleškem, francoskem in nemškem jeziku na spletni strani ENVP na naslovu http://www.edps.europa.eu)

(2014/C 32/10)

1. **Uvod**

1.1 *Posvetovanje z ENVP*

1. Komisija in visoka predstavnica Evropske unije za zunanje zadeve in varnostno politiko sta 7. februarja 2013 sprejela skupno sporočilo Evropskemu parlamentu, Svetu, Evropskemu socialno-ekonomskemu odboru in Odboru regij z naslovom „Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor“ ([1]) (v nadaljnjem besedilu: skupno sporočilo, strategija za kibernetsko varnost ali strategija).

2. Komisija je istega dne sprejela predlog direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij po vsej Uniji ([2]) (v nadaljnjem besedilu: predlagana direktiva ali predlog). Priporočilo je bilo ENVP poslano v posvetovanje 7. februarja 2013.

3. ENVP je imel že pred sprejetjem skupnega sporočila in predloga možnost Komisiji predložiti neuradne pripombe. Pozdravlja dejstvo, da so bile nekatere pripombe upoštevane v skupnem sporočilu in predlogu.

4. **Sklepne ugotovitve**

74. EDPS veseli, da sta Komisija in visoka predstavnica EU za zunanje zadeve in varnostno politiko predložili celovito strategijo za kibernetsko varnost, dopolnjeno s predlogom direktive o ukrepih za zagotavljanje visoke splošne ravni varnosti omrežij in informacij (v nadaljnjem besedilu: VOI) po vsej EU. Strategija dopolnjuje politične ukrepe, ki jih je EU že oblikovala na področju VOI.

75. ENVP pozdravlja dejstvo, da strategija presega tradicionalni pristop nasprotja med varnostjo in zasebnostjo z določanjem izrecnega priznavanja zasebnosti in varstva podatkov kot temeljnih vrednot, ki bi morale usmerjati politiko kibernetske varnosti v EU in na mednarodni ravni. ENVP ugotavlja, da sta lahko strategija za kibernetsko varnost in predlagana direktiva o VOI ključnega pomena za prispevek k zagotavljanju varstva pravic posameznikov do zasebnosti in varstva podatkov v spletnem okolju. Hkrati pa mora biti zagotovljeno, da ne privedejo do ukrepov, ki bi pomenili nezakonite posege v pravice posameznikov do zasebnosti in varstva podatkov.

76. Veseli ga tudi, da je varstvo podatkov navedeno v več delih strategije in je upoštevano v predlagani direktivi o VOI. Vseeno pa obžaluje, da v strategiji in predlagani direktivi ni bolj poudarjen prispevek sedanje in prihodnje zakonodaje o varstvu podatkov k varnosti in da ni v celoti zagotovljeno, da vse obveznosti, ki izhajajo iz predlagane direktive ali drugih elementov strategije, dopolnjujejo obveznosti varstva podatkov in se med seboj ne prekrivajo ali si nasprotujejo.

77. ENVP poleg tega ugotavlja, da strategija za kibernetsko varnost zaradi pomanjkljivega upoštevanja oziroma neupoštevanja drugih vzporednih pobud Komisije in zakonodajnih postopkov, ki potekajo, kot so reforma varstva podatkov in predlagana uredba o elektronski identifikaciji in skrbniških storitvah, ne zagotavlja zares vsestranskega in celovitega pogleda na kibernetsko varnost v EU in obstaja nevarnost, da

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

se bo ohranil razdrobljen in segmentiran pristop. ENVP tudi navaja, da s predlagano direktivo o VOI tudi še ni omogočen celovit pristop k varnosti v EU in da je verjetno obveznost, določena v zakonodaji o varstvu podatkov, najcelovitejša obveznost glede omrežja in varnosti na podlagi prava EU.

78. ENVP poleg tega obžaluje tudi, da ni ustrezno upoštevana pomembna vloga organov za varstvo podatkov pri izvajanju in uveljavljanju varnostnih obveznosti in krepitvi kibernetske varnosti.

79. Kar zadeva strategijo za kibernetsko varnost ENVP poudarja, da:

— je zlasti pomembna opredelitev pojmov „kibernetska odpornost“, „kibernetska kriminaliteta“ in „kibernetska obramba“, ker se ti pojmi uporabljajo kot utemeljitev nekaterih posebnih ukrepov, ki bi lahko povzročili poseganje v temeljne pravice, vključno s pravicama do zasebnosti in varstva podatkov. Vendar pa so opredelitve „kibernetske kriminalitete“ v strategiji in Konvenciji o kibernetski kriminaliteti še vedno zelo široke. Priporočljivo bi bilo imeti jasno in *ožjo* opredelitev „kibernetske kriminalitete“ namesto preobširne opredelitve,

— zakonodaja o varstvu podatkov naj se uporablja za vse ukrepe strategije, kadar koli zadevajo ukrepe, ki povzročijo obdelavo osebnih podatkov. Čeprav zakonodaja o varstvu podatkov ni posebej navedena v oddelkih, ki se nanašajo na kibernetsko kriminaliteto in kibernetsko obrambo, pa ENVP poudarja, da bi številni ukrepi, načrtovani na teh področjih, vključevali obdelavo osebnih podatkov in spadajo zato v področje uporabe veljavnih zakonov o varstvu podatkov. Ugotavlja tudi, da številni ukrepi zajemajo vzpostavitev mehanizmov za usklajevanje, zaradi katerih bo potrebno izvajanje ustreznih zaščitnih ukrepov za varstvo podatkov, kot načinov izmenjave osebnih podatkov,

— organi za varstvo podatkov imajo pomembno vlogo pri kibernetski varnosti. Kot skrbniki zasebnosti in pravic posameznikov do varstva podatkov dejavno sodelujejo pri varstvu osebnih podatkov v spletnem in nespletnem okolju. Zato bi morali biti v svoji vlogi nadzornih organov ustrezno vključeni v zvezi z izvedbenimi ukrepi, ki vključujejo obdelavo osebnih podatkov (kot je uvedba pilotnega projekta EU boja proti botnetom in zlonamerni programski opremi). Tudi drugi igralci na področju kibernetske varnosti bi morali sodelovati z njimi pri opravljanju nalog, na primer pri izmenjavi najboljših praks in dejavnostih za povečanje ozaveščenosti. ENVP in nacionalni organi za varstvo podatkov naj bodo tudi ustrezno vključeni v konferenco na visoki ravni, ki bo sklicana leta 2014, da se oceni napredek pri izvajanju strategije.

80. Kar zadeva predlagano direktivo o VOI, ENVP svetuje zakonodajalcem, naj:

— v členu 3(8) zagotovijo večjo jasnost in gotovost pri opredelitvi tržnih udeležencev, ki spadajo v področje uporabe predloga, in sestavijo izčrpen seznam, ki bo vključeval vse ustrezne zainteresirane strani, da se v EU zagotovi popolnoma usklajen in celosten pristop k varnosti,

— v členu 1(2)(c) pojasnijo, da se predlagana direktiva uporablja za organe in institucije EU, in naj se v členu 1(5) predloga vključi sklic na Uredbo (ES) št. 45/2001,

— se temu predlogu prizna večja horizontalna vloga v zvezi z varnostjo, s tem, da se v členu 1 izrecno določi, da se mora uporabljati, ne da bi posegal v sedanja ali prihodnja podrobna pravila na posebnih področjih (kot so pravila, ki bodo določena za ponudnike skrbniških storitev v predlagani uredbi o elektronski identifikaciji),

— dodajo uvodno izjavo za pojasnitev potrebe po vključitvi načel varstva podatkov, kot sta vgrajena zasebnost in zasebnost s privzetimi nastavitvami, od zgodnje faze načrtovanja mehanizmov, določenih v predlogu, in vsej življenjski dobi vključenih procesov, postopkov, organizacije, tehnik in infrastruktur, ob upoštevanju predlagane uredbe o varstvu podatkov,

— pojasnijo opredelitve „omrežje in informacijski sistem“ v členu 3(1) in „incident“ v členu 3(4) ter v členu 5(2) nadomestijo obveznost vzpostavitve „načrta ocene tveganja“ z „vzpostavitvijo in vzdrževanjem okvira za obvladovanje tveganja“,

— v členu 1(6) določijo, da bi bila obdelava osebnih podatkov upravičena na podlagi člena 7(e) Direktive 95/46/ES, če je treba izpolniti cilj javnega interesa iz predlagane direktive. Vseeno pa je treba zagotoviti ustrezno upoštevanje načel nujnosti in sorazmernosti, tako da se obdelujejo le podatki, ki so nujno potrebni za doseganje namena,

— v členu 14 določijo okoliščine, v katerih se zahteva priglasitev incidenta, ter vsebino in obliko priglasitve, vključno z vrsto osebnih podatkov, ki jih je treba priglasiti, ter ali da ali ne in v kakšni meri bodo podrobnosti o osebnih podatkih, ki jih ogrozi posebni varnostni incident (kot so naslovi IP), vključeni v priglasitev in podporno dokumentacijo. Treba je upoštevati, da naj bi bila pristojnim organom za VOI zbiranje in obdelava osebnih podatkov v okviru varnostnega incidenta dovoljena le, če je to nujno potrebno. V predlogu naj bi bili določeni tudi ustrezni zaščitni ukrepi za zagotovitev ustreznega varstva podatkov, ki jih obdelujejo pristojni organi za VOI,

— v členu 14 pojasnijo, da bi se morale prijave o incidentu v skladu s členom 14(2) uporabljati brez vpliva na obveznosti glede obveščanja o kršitvi varnosti osebnih podatkov v skladu z veljavno zakonodajo o varstvu podatkov. V predlogu določijo glavne vidike postopka za sodelovanje med pristojnimi organi za VOI in organi za varstvo podatkov v primerih, pri katerih varnostni incident vključuje kršitev varnosti osebnih podatkov,

— spremenijo člen 14(8) tako, da se izključitev mikro podjetij iz področja uporabe priglasitve ne uporablja za tiste ponudnike, ki so ključni za opravljanje storitev informacijske družbe, npr. glede na naravo informacij, ki jih obdelujejo (tj. biometrični ali občutljivi podatki),

— se v predlogu dodajo določbe, ki urejajo nadaljnjo izmenjavo osebnih podatkov med pristojnimi organi za VOI in drugimi prejemniki, za zagotovitev, da (i) se osebni podatki razkrijejo le prejemnikom, katerih obdelava je nujna za opravljanje nalog v skladu z ustrezno pravno podlago in (ii) da so take informacije omejene na to, kar je nujno potrebno za opravljanje nalog. Upošteva naj se tudi, kako subjekti, ki mreži izmenjave informacij priskrbijo podatke, zagotavljajo skladnost z načelom omejitve namena,

— določijo rok hranjenja osebnih podatkov za namene, določene v predlagani direktivi, zlasti kar zadeva hranjenje pri pristojnih organih za VOI in v varni infrastrukturi mreže za sodelovanje,

— spomnijo pristojne organe za VOI na dolžnost zagotavljanja ustreznih informacij posameznikom, na katere se nanašajo osebni podatki, o obdelavi osebnih podatkov, na primer z objavo politike varovanja zasebnosti na svoji spletni strani,

— dodajo določbo v zvezi z ravnjo varnosti, ki jo morajo upoštevati pristojni organi za VOI v zvezi z zbranimi, obdelanimi in izmenjanimi informacijami. V zvezi z varstvom osebnih podatkov pri pristojnih organih za VOI naj se posebej vključi sklic na varnostne zahteve iz člena 17 Direktive 95/46/ES,

— v členu 9(2) pojasnijo, da bi morala merila za sodelovanje držav članic v varnem sistemu izmenjave informacij zagotoviti, da vsi sodelujoči v tem sistemu jamčijo za visoko raven varnosti in odpornosti v vseh fazah obdelave. Ta merila bi morala vsebovati ustrezne ukrepe zaupnosti in varnosti v skladu s členoma 16 in 17 Direktive 95/46/ES in členoma 21 in 22 Uredbe (ES) št. 45/2001. Komisija naj bo glede sodelovanja kot upravljavka tega varnega sistema izmenjave informacij izrecno zavezana tem merilom,

— v členu 9 dodajo opis vlog in odgovornosti Komisije in držav članic pri vzpostavitvi, delovanju in vzdrževanju varnega sistema izmenjave informacij in določijo, da je treba sistem načrtovati v skladu z načeloma varstva podatkov vgrajene zasebnosti in zasebnosti s privzetimi nastavitvami in

— v členu 13 dodajo, da se morajo vsi prenosi osebnih podatkov prejemnikom v državah zunaj EU izvesti v skladu s členoma 25 in 26 Direktive 95/46/ES in členom 9 Uredbe (ES) št. 45/2001.

V Bruslju, 14. junija 2013

Peter HUSTINX

Evropski nadzornik za varstvo podatkov