Mnenje evropskega nadzornika za varstvo podatkov o predlogu uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA)

(2011/C 101/04)

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 16 Pogodbe,

ob upoštevanju Listine Evropske unije o temeljnih pravicah in zlasti členov 7 in 8 Listine,

ob upoštevanju Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ([1]),

ob upoštevanju prošnje za mnenje v skladu s členom 28(2) Uredbe (ES) št. 45/2001 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov ([2]) –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

Opis predloga

1. Komisija je 30. septembra 2010 sprejela predlog uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA) ([3]).

2. Agencija ENISA je bila ustanovljena marca 2004 z Uredbo (ES) št. 460/2004 ([4]) za začetno petletno obdobje. Z Uredbo (ES) št. 1007/2008 ([5]) iz leta 2008 je bil njen mandat podaljšan do marca 2012.

3. Člen 1(1) Uredbe (ES) št. 460/2004 določa, da se agencija ustanovi zato, da se zagotovi visoka in učinkovita raven varnosti omrežij in informacij v Uniji ter se prispeva k nemotenemu delovanju notranjega trga.

4. Komisija želi s svojim predlogom posodobiti agencijo, okrepiti njene pristojnosti in ji zagotoviti nov petletni mandat, da se tako omogoči njeno neprekinjeno delovanje tudi po marcu 2012 ([6]).

5. Pravna podlaga predloga uredbe je člen 114 PDEU ([7]), s katerim je Uniji podeljena pristojnost sprejeti ukrepe za vzpostavitev ali zagotovitev delovanja notranjega trga. Člen 114 PDEU je nasledil člen 95 nekdanje Pogodbe ES, na katerem so temeljile predhodne uredbe o agenciji ENISA ([8]).

6. V obrazložitvenem memorandumu k predlogu je pojasnjeno, da je od začetka veljavnosti Lizbonske pogodbe pristojnost glede preprečevanja kriminala in boja proti njemu deljena. S tem je agencija ENISA dobila priložnost, da deluje kot platforma za vidike varnosti omrežij in informacij (NIS) v boju proti kibernetskemu kriminalu ter da izmenjuje mnenja in najboljše prakse z organi za kibernetsko obrambo, organi pregona in organi za varstvo podatkov.

7. Komisija je med več možnostmi izbrala predlog o razširitvi trenutnih nalog agencije ENISA ter vključitvi organov pregona in organov za varstvo podatkov kot enakopravnih članov v stalno interesno skupino agencije. Nov seznam nalog ne vključuje operativnih nalog, ampak so z njim posodobljene in na novo opredeljene sedanje naloge.

Posvetovanje z evropskim nadzornikom za varstvo podatkov (ENVP)

8. Predlog je bil 1. oktobra 2010 v skladu s členom 28(2) Uredbe (ES) št. 45/2001 poslan ENVP v posvetovanje. ENVP pozdravlja odločitev, da je bil v zvezi s tem zaprošen za mnenje, in priporoča, da se sklic na to posvetovanje vključi v uvodne izjave predloga, tako kot je to običajno v zakonodajnih besedilih, v zvezi s katerimi je bil zaprošen za mnenje v skladu z Uredbo (ES) št. 45/2001.

9. ENVP je bil za neuradno mnenje zaprošen še pred sprejetjem predloga, pri čemer je predložil več neuradnih pripomb. Vendar v končni različici predloga ni bila upoštevana nobena od teh pripomb.

Splošna ocena

10. ENVP poudarja, da je varnost obdelave podatkov bistven vidik varstva podatkov ([9]). V zvezi s tem pozdravlja namen predloga, to je krepitev pristojnosti agencije, da bi ta lahko učinkoviteje izvajala svoje sedanje naloge in odgovornosti

([1]) UL L 281, 23.11.1995, str. 31.
([2]) UL L 8, 12.1.2001, str. 1.
([3]) COM(2010) 521 konč.
([4]) UL L 77, 13.3.2004, str. 1.
([5]) UL L 293, 31.10.2008, str. 1.
([6]) Komisija je – da bi preprečila pravno praznino, če se zakonodajni postopek v Evropskem parlamentu in Svetu ne bi končal do izteka sedanjega mandata – 30. septembra 2010 sprejela drugi predlog o spremembi Uredbe (ES) št. 460/2004, s katerim bi le podaljšala rok za iztek sedanjega mandata za 18 mesecev. Glej COM(2010) 520 konč.

([7]) Glej zgoraj.
([8]) Sodišče je 2. maja 2006 zavrnilo tožbo za razglasitev ničnosti predhodne Uredbe (ES) št. 460/2004, s katero se je izpodbijala pravna podlaga te uredbe (C-217/04).
([9]) Varnostne zahteve so vključene v člena 22 in 35 Uredbe (ES) št. 45/2001, člena 16 in 17 Direktive 95/46/ES ter člena 4 in 5 Direktive 2002/58/ES.

ter hkrati razširila svoje področje delovanja. ENVP pozdravlja vključitev organov za varstvo podatkov in organov pregona kot enakopravnih akterjev. Po njegovem mnenju je mogoče s podaljšanjem mandata agencije ENISA na evropski ravni spodbuditi profesionalno in poenostavljeno upravljanje varnostnih ukrepov za informacijske sisteme.

11. Splošna ocena predloga je pozitivna. Vendar je predlog uredbe z več vidikov nejasen ali nepopoln, kar zbuja zaskrbljenost glede varstva podatkov. Ti vidiki bodo pojasnjeni in obravnavani v naslednjem poglavju tega mnenja.

II. **PRIPOMBE IN PRIPOROČILA**

Razširjene naloge, ki jih bo izvajala agencija ENISA, niso dovolj jasne

12. Razširjene naloge agencije glede vključitve organov pregona in organov za varstvo podatkov so v členu 3 predloga opredeljene zelo splošno. Obrazložitveni memorandum je glede tega bolj nedvoumen. Agencija ENISA je v njem opredeljena kot vmesnik pri komunikaciji z organi pregona na področju kibernetskega kriminala in izvajalka neoperativnih nalog pri boju proti takemu kriminalu. Vendar te naloge niso bile vključene v člen 3 ali pa so v njem omenjene le zelo splošno.

13. Da bi se izognili kakršni koli pravni negotovosti, je treba s predlogom uredbe jasno in nedvoumno opredeliti naloge agencije ENISA. Kot je bilo že navedeno, je varnost obdelave podatkov bistven vidik varstva podatkov. Agencija ENISA bo postala na tem področju še pomembnejša. Državljanom, institucijam in organom bi moralo biti jasno, v kake dejavnosti bi lahko bila vključena. Ta razsežnost je še pomembnejša, če naj bi razširjene naloge agencije ENISA obsegale tudi obdelavo osebnih podatkov (glej točke od 17 do 20 spodaj).

14. Člen 3(1)(k) predloga določa, da agencija opravlja kakršne koli druge naloge, ki so bile nanjo prenesene z drugimi pravnimi akti Unije. ENVP je zaskrbljen zaradi tako odprte postavke, saj bi lahko zaradi nje nastala vrzel, ki bi lahko vplivala na povezanost pravnega instrumenta, to pa bi lahko vodilo do nenadzorovane širitve obsega dejavnosti agencije.

15. Ena od nalog iz člena 3(1)(k) predloga je vključena v Direktivo 2002/58/ES ([1]). Ta določa, da se Komisija pri vseh tehničnih izvedbenih ukrepih, ki se uporabljajo za obvestila o kršitvah varstva podatkov, posvetuje z agencijo. ENVP priporoča, da se ta dejavnost agencije podrobneje opiše in se omeji na varnostno področje. Glede na vpliv, ki bi ga lahko imela agencija ENISA na razvoj politike na tem področju, bi morala biti ta dejavnost v predlogu uredbe jasneje opredeljena in bi morala zasesti pomembnejše mesto.

16. ENVP nadalje priporoča, da se ob upoštevanju posebne naloge agencije ENISA iz člena 3(1)(c) trenutnega predloga, to je podpore državam članicam ter evropskim institucijam in organom v prizadevanjih, da zbirajo, analizirajo in razširjajo podatke o varnosti omrežij in informacij, v uvodno izjavo 21 vključi sklic na Direktivo 1999/5/ES ([2]). Tako bi spodbudili spodbujevalne dejavnosti, ki jih izvaja agencija ENISA za zagotovitev najboljših praks in tehnologij glede varnosti omrežij in informacij (NIS), saj bodo tako bolje prikazane možnosti konstruktivnih interakcij med agencijo in organi za standardizacijo.

Treba bi bilo razjasniti, ali bo agencija obdelovala osebne podatke

17. V predlogu ni navedeno, ali bi lahko naloge, podeljene agenciji, vključevale obdelavo osebnih podatkov. Predlog torej ne vsebuje posebne pravne podlage za obdelavo osebnih podatkov v smislu člena 5 Uredbe (ES) št. 45/2001.

18. Vendar bi lahko nekatere naloge, podeljene agenciji, (vsaj v neki meri) vključevale obdelavo osebnih podatkov. Ni na primer izključena možnost, da bi lahko analiza varnostnih incidentov in kršitev varstva podatkov ali izvajanje neoperativnih nalog v boju proti kibernetskemu kriminalu vključevali zbiranje in analizo osebnih podatkov.

19. Uvodna izjava 9 predloga se sklicuje na določbe Direktive 2002/21/ES ([3]), v kateri je določeno, da o morebitnih kršitvah varnosti agencijo po potrebi obvestijo tudi nacionalni regulativni organi. ENVP priporoča, da se v predlogu natančneje opredeli, katera obvestila naj bi se poslala agenciji ENISA in kako naj bi ta nanje odgovorila. V predlogu bi bilo treba obravnavati tudi vidike obdelave osebnih podatkov, ki bi lahko nastali zaradi analize zadevnih obvestil (če obstajajo).

([1]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

([2]) Direktiva 1999/5/ES Evropskega parlamenta in Sveta z dne 9. marca 1999 o radijski opremi in telekomunikacijski terminalski opremi ter medsebojnem priznavanju skladnosti te opreme (UL L 91, 7.4.1999, str. 10) in zlasti člen 3(3)(c) te direktive.

([3]) Direktiva Evropskega parlamenta in Sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL L 108, 24.4.2002, str. 33).

20. ENVP zakonodajalca poziva, naj razjasni, ali bodo dejavnosti agencije ENISA, navedene v členu 3, vključevale obdelavo osebnih podatkov, in če je tako, katere so take dejavnosti.

Treba bi bilo opredeliti notranje varnostne predpise za agencijo ENISA

21. Čeprav agencija ENISA pomembno vpliva na razpravo o varnosti omrežij in informacij v Evropi, predlog skoraj ne obravnava vzpostavitve varnostnih ukrepov za samo agencijo (če so ti povezani z obdelavo osebnih podatkov ali ne).

22. Po mnenju ENVP bo lahko agencija še učinkoviteje spodbujala dobre prakse, kar zadeva varnost obdelave podatkov, če bo take varnostne ukrepe najprej sama strogo izvajala. To bo pripomoglo k temu, da se agencija prizna ne le kot strokovni center, temveč tudi kot referenčna točka pri praktičnem izvajanju najboljših razpoložljivih tehnologij na področju varnosti. Torej bi bilo treba prizadevanja za odličnost pri izvajanju varnostnih praks vključiti v uredbo, s katero so urejeni delovni postopki agencije. ENVP zato predlaga, naj se v predlog vključi taka določba, na primer v obliki zahteve, da agencija uporablja najboljše razpoložljive tehnologije, to je najučinkovitejše in najnaprednejše varnostne postopke ter z njimi povezane metode dela.

23. Agencija bo lahko s takim pristopom svetovala o praktični ustreznosti posameznih tehnologij za zagotavljanje zahtevanih varnostnih ukrepov. Dalje, pri uveljavljanju najboljših razpoložljivih tehnologij bi bilo treba dati prednost tistim, s katerimi se zagotovi varnost in se hkrati čim bolj omeji vpliv na zasebnost. Treba bi bilo izbrati tehnologije, ki se bolje skladajo s konceptom „vgrajene zasebnosti“.

24. ENVP tudi ob manj velikopoteznem pristopu priporoča, da se v uredbo vključijo vsaj naslednje zahteve: (i) oblikovanje notranje varnostne politike na podlagi celostne ocene tveganja, pri čemer se upoštevajo mednarodni standardi in najboljše prakse držav članic; (ii) imenovanje uradne osebe za varnost, pristojne za izvajanje politike, ki bo razpolagala z ustreznimi viri in pooblastili; (iii) odobritev te politike, potem ko se podrobno preučijo preostalo tveganje in nadzorni ukrepi, ki jih predlaga upravni odbor; ter (iv) periodični pregled politike z jasno navedbo izbranega časovnega okvira pogostnosti in ciljev pregleda.

Treba je bolje opredeliti kanale za sodelovanje z organi za varstvo podatkov (vključno z ENVP) in delovno skupino iz člena 29

25. Kot je bilo že navedeno, ENVP pozdravlja podaljšanje mandata agencije in verjame, da lahko organom za varstvo podatkov obstoj agencije močno koristi (kakor lahko tudi agenciji koristi strokovno znanje teh organov). Ob upoštevanju naravnega in logičnega prepletanja varnosti in varstva podatkov je treba zagotoviti tesno sodelovanje agencije z organi za varstvo podatkov.

26. Uvodni izjavi 24 in 25 se sklicujeta na predlog direktive EU o kibernetskem kriminalu ter omenjata, da mora agencija navezati stike z organi pregona in organi za zaščito zasebnosti, kar zadeva vidike varnosti informacij v boju proti kibernetskemu kriminalu ([1]).

27. S predlogom je treba določiti tudi konkretne kanale in mehanizme sodelovanja, s katerimi se (i) zagotovi *skladnost* dejavnosti agencije z dejavnostmi organov za varstvo podatkov ter (ii) omogoči *tesno sodelovanje* med agencijo in organi za varstvo podatkov.

28. Kar zadeva *skladnost*, je v uvodni izjavi 27 izrecno navedeno, da ne sme priti do nasprotij med nalogami agencije in organov za varstvo podatkov v državah članicah. ENVP pozdravlja to navedbo, vendar hkrati opozarja, da nista nikjer omenjena niti ENVP niti delovna skupina iz člena 29. Zato priporoča, da zakonodajalec v predlog vključi še podobno določbo o nevmešavanju v zvezi z navedenima subjektoma. Tako bo ustvarjeno jasnejše delovno okolje za vse strani, hkrati pa bi bilo treba opredeliti še kanale in mehanizme sodelovanja, s katerimi se agenciji omogoči podpora različnim organom za varstvo podatkov in delovni skupini iz člena 29.

29. Na podlagi navedenega ENVP, kar zadeva *tesno sodelovanje*, pozdravlja vključitev predstavnikov organov za varstvo podatkov v stalno interesno skupino, ki bo agenciji svetovala o izvajanju njenih dejavnosti. Glede tega svetuje, naj se izrecno navede, da take predstavnike nacionalnih organov za varstvo podatkov imenuje agencija na podlagi predloga delovne skupine iz člena 29. Dobro bi bilo, da se doda še določba o udeležbi ENVP na sestankih, na katerih naj bi se obravnavala vprašanja, pomembna za sodelovanje z njim. Dalje, ENVP priporoča, da agencija (na predlog stalne interesne skupine in po odobritvi upravnega odbora) ustanovi *ad hoc* delovne skupine za različna vprašanja, v okviru katerih se varstvo podatkov in varnost prekrivata, da bi tako opredelili okvir zadevnega prizadevanja za tesno sodelovanje.

([1]) Predlog direktive Evropskega parlamenta in Sveta o napadih na informacijske sisteme in razveljavitvi Okvirnega sklepa Sveta 2005/222/PNZ (COM(2010) 517 konč.).

30. Nazadnje, da bi se izognili morebitnim nesporazumom, ENVP priporoča, da se namesto izraza „organi za zaščito zasebnosti“ uporabi izraz „organi za varstvo podatkov“ ter da se razjasni, kateri so ti organi, in sicer z vključitvijo sklica na člen 28 Direktive 95/46/ES in ENVP, kot je opredeljen v poglavju V Uredbe (ES) št. 45/2001.

Ni jasno, kateri upravičenci lahko pri agenciji ENISA vložijo zahtevek za podporo

31. ENVP je ugotovil, da predlog uredbe vključuje neskladje, kar zadeva vprašanje, kdo lahko pri agenciji ENISA vloži zahtevek za podporo. Iz uvodnih izjav 7, 15, 16, 18 in 36 predloga izhaja, da lahko agencija ENISA zagotavlja podporo organom držav članic in Uniji kot celoti. Vendar so v členu 2(1) navedene le Komisija in države članice, medtem ko je v členu 14 določeno, da lahko zahtevke za podporo vložijo le: (i) Evropski parlament, (ii) Svet, (iii) Komisija (iv) in vsi pristojni organi, ki jih imenuje država članica, s čimer so izključene nekatere institucije, organi, agencije in uradi Unije.

32. Člen 3 predloga je bolj specifičen in predvideva različne vrste podpore za različne upravičence, in sicer: (i) zbiranje in analizo podatkov o varnosti informacij (v primeru držav članic ter evropskih institucij in organov); (ii) analizo stanja varnosti omrežij in informacij v Evropi (v primeru držav članic in evropskih institucij); (iii) spodbudo uporabi dobrih praks za obvladovanje tveganj in varnost (v vsej Uniji in državah članicah); (iv) razvoj odkrivanja na področju varnosti omrežij in informacij (v evropskih institucijah in organih) ter (v) sodelovanje pri dialogu in sodelovanju s tretjimi državami (v primeru Unije).

33. ENVP zakonodajalca poziva, naj to neskladje odpravi in uskladi navedene določbe. Glede tega priporoča, da se člen 14 spremeni tako, da bo vključeval vse institucije, organe, urade in agencije Unije ter da bo v njem jasno navedeno, kakšno vrsto pomoči lahko zahtevajo različni subjekti v Uniji (če je zakonodajalec predvidel tako razlikovanje). Hkrati bi bilo dobro, da bi lahko zahtevek za podporo agencije vložili tudi nekateri javni in zasebni subjekti, če bi iz njega jasno izhajalo, da bi zahtevana podpora lahko imela evropske razsežnosti in bi bila v skladu s cilji agencije.

Naloge upravnega odbora

34. Z obrazložitvenim memorandumom so določene okrepljene pristojnosti upravnega odbora pri nadzoru. ENVP pozdravlja tako povečano vlogo in priporoča, da se med naloge upravnega odbora vključi več vidikov, povezanih z varstvom podatkov. ENVP poleg tega priporoča, da se v Uredbi nedvoumno opredeli, kdo lahko: (i) določi ukrepe, na podlagi katerih agencija uporablja Uredbo (ES) št. 45/2001, vključno z ukrepi v zvezi z imenovanjem uradne osebe za varstvo podatkov; (ii) odobri varnostno politiko in z njo povezane periodične preglede ter (iii) določi protokol sodelovanja z organi za varstvo podatkov in organi pregona.

Uporaba Uredbe (ES) št. 45/2001

35. Čeprav se to zahteva že z Uredbo (ES) št. 45/2001, ENVP predlaga, naj se v člen 27 vključi imenovanje uradne osebe za varstvo podatkov, saj je to zelo pomembno, ta ukrep pa bi moralo spremljati hitro oblikovanje izvedbenih pravil glede obsega pooblastil in nalog, ki naj se zaupajo taki uradni osebi v skladu s členom 24(8) Uredbe (ES) št. 45/2001. Konkretneje, člen 27 bi lahko določal:

1. Za informacije, ki jih obdeluje agencija na podlagi te uredbe, veljajo določbe Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov.

2. Upravni odbor določi ukrepe, na podlagi katerih agencija uporablja Uredbo (ES) št. 45/2001, vključno z ukrepi v zvezi z uradno osebo za varstvo podatkov v agenciji.

36. Če se zahteva posebna pravna podlaga za obdelavo osebnih podatkov, kot je bilo to obravnavano v točkah od 17 do 20 zgoraj, je treba zagotoviti podrobno opredelitev potrebnih in primernih zaščitnih ukrepov, omejitev in pogojev, pod katerimi bi se taki podatki obdelovali.

III. **SKLEPNE UGOTOVITVE**

37. Splošna ocena predloga je pozitivna: ENVP pozdravlja podaljšanje mandata agencije ter razširitev njenih nalog z vključitvijo organov za varstvo podatkov in organov pregona kot enakopravnih akterjev. Po njegovem mnenju je mogoče z neprekinjenim delovanjem agencije na evropski ravni spodbuditi profesionalno in poenostavljeno upravljanje varnostnih ukrepov za informacijske sisteme.

38. Da bi se izognili pravni negotovosti, ENVP priporoča, da se predlog razjasni ob upoštevanju razširitve nalog agencije, še zlasti tistih, ki so povezane z vključitvijo organov pregona in organov za varstvo podatkov. ENVP opozarja še na morebitno vrzel, ki bi lahko nastala, ker je v predlog vključena določba, na podlagi katere je mogoče agenciji s katerim koli drugim pravnim aktom Unije in brez kakršne koli dodatne omejitve dodeliti nove naloge.

39. ENVP zakonodajalca poziva, naj razjasni, ali bodo dejavnosti agencije ENISA vključevale obdelavo osebnih podatkov, in če je tako, katere so take dejavnosti.

40. ENVP priporoča, da se vključijo določbe o vzpostavitvi varnostne politike same agencije, da bi tako okrepili njeno vlogo subjekta, ki omogoča odličnost pri izvajanju varnostnih praks in spodbuja „vgrajeno zasebnost“ z vključevanjem uporabe najboljših razpoložljivih varnostnih tehnologij ob upoštevanju pravic na področju varstva osebnih podatkov.

41. Da bi zagotovili skladnost in tesno sodelovanje, je treba bolje opredeliti kanale za sodelovanje z organi za varstvo podatkov, vključno z ENVP in delovno skupino iz člena 29.

42. ENVP zakonodajalca poziva, naj odpravi nekatera neskladja glede omejitev iz člena 14, kar zadeva možnost, da se vloži zahtevek za podporo agencije. Glede tega zlasti priporoča, da se te omejitve opustijo ter se vsem institucijam, organom, agencijam in uradom Unije omogoči, da vložijo tak zahtevek.

43. Nazadnje, ENVP priporoča, da se v razširjena pooblastila upravnega odbora vključijo nekateri konkretni vidiki, s katerimi bi bilo mogoče okrepiti zagotovilo, da se agencija ravna v skladu z dobrimi praksami, kar zadeva varnost in varstvo podatkov. Med drugim predlaga, naj se vključi imenovanje uradne osebe za varstvo podatkov in naj se odobrijo ukrepi za pravilno uporabo Uredbe (ES) št. 45/2001.

V Bruslju, 20. decembra 2010

Giovanni BUTTARELLI

Pomočnik evropskega nadzornika za varstvo podatkov