

EVROPSKI NADZORNIK ZA VARSTVO PODATKOV

Mnenje Evropskega nadzornika za varstvo podatkov o predlogu sklepa Sveta o stališču Unije v Skupnem odboru za carinsko sodelovanje EU-Japonska glede medsebojnega priznavanja programov o pooblaščenih gospodarskih subjektih v Evropski uniji in na Japonskem

(2010/C 190/02)

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 člena 8 Listine,

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

ob upoštevanju 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⁾ ter zlasti člena 41 uredbe –

SPREJEL NASLEDNJE MNENJE:

I. UVOD

1. Komisija je 19. februarja 2010 sprejela predlog sklepa Sveta o stališču Unije v Skupnem odboru za carinsko sodelovanje EU-Japonska glede medsebojnega priznavanja programov o pooblaščenih gospodarskih subjektih v Evropski uniji in na Japonskem⁽³⁾.

2. Evropski nadzornik za varstvo podatkov (ENVP) ni bil zaprosen za mnenje, kot to zahteva člen 28(2) Uredbe (ES) št. 45/2001. To mnenje zato temelji na členu 41(2) iste uredbe. ENVP priporoča, da se sklicevanje na to mnenje vključi v preambulo sklepa.

3. ENVP je ugotovil nekaj pomanjkljivosti in nejasnosti v zvezi z varstvom osebnih podatkov. Po opisu okvira in ozadja predloga v poglavju III bodo te pripombe razvite v poglavju IV.

II. POSVETOVANJE Z ENVP

4. ENVP je izdal strateški dokument, v katerem je opisana njegova svetovalna vloga: ENVP kot svetovalec institucijam Skupnosti v zvezi s predlogi za zakonodajo in povezane dokumente⁽⁴⁾. Ta svetovalna vloga temelji na členih 28(2) in 41 Uredbe (ES) št. 45/2001. Poleg tega je v uvodni izjavi 17 uredbe navedeno, da „učinkovitost varstva posameznikov pri obdelavi osebnih podatkov v Uniji predpostavlja doslednost ustreznih pravil in postopkov, ki veljajo za dejavnosti iz različnih pravnih kontekstov“. Dejansko je treba doslednost šteti za nepogrešljiv element za doseg visoke ravni varstva podatkov na evropski ravni, kar vključuje tudi zunanje delovanje Unije.

5. Evropska komisija priznava to široko odgovornost ENVP in ustaljena praksa je, da se Komisija z ENVP posvetuje o vseh ustreznih predlogih v zvezi z zakonodajnimi in nezakonodajnimi instrumenti. Področje uporabe svetovalne naloge ENVP obsega „zadeve v zvezi z obdelavo osebnih podatkov“. To pomeni, da je treba opraviti posvetovanje o vsej zakonodaji, ki vsebuje določbe o obdelavi osebnih podatkov ali določbe, ki vplivajo (ali lahko vplivajo) na tako obdelavo. Isto velja za vse instrumente, ki spadajo v zunanje pristojnosti Unije.

⁽¹⁾ UL L 281, 23.11.1995, str. 31.

⁽²⁾ UL L 8, 12.1.2001, str. 1.

⁽³⁾ COM(2010) 55 konč.

⁽⁴⁾ Strateški dokument je na voljo na naslovu: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/05-03-18_PP_EDPSadvisor_EN.pdf

6. V strateškem dokumentu je opisan tudi časovni okvir posvetovanja. Posvetovanje v zgodnji fazi zakonodajnega postopka omogoča ENVP, da deluje učinkovito in predlaga spremembe besedila. Pristojna služba Komisije pred sprejetjem uradnega predloga po potrebi evropskemu nadzorniku za varstvo podatkov pošlje to neuradno posvetovanje o osnutku besedila. Drugi korak po sprejetju predloga je uradno posvetovanje. Mnenje ENVP se v tej fazi objavi v Uradnem listu (serija C).

7. Kot je bilo navedeno zgoraj, ENVP v zvezi s tem predlogom ni prejel niti osnutka predloga niti predloga za posvetovanje po sprejetju osnutka. ENVP je še zlasti razočaran zaradi tega poteka dogodkov, ker bi njegovo sodelovanje zagotovilo idealno priložnost dodati vrednost predlogu, kot je pojasnjeno v nadaljevanju.

III. OKVIR IN OZADJE PREDLOGA

8. Namen predloga je medsebojno priznavanje programov o pooblaščenih gospodarskih subjektih (*Authorised Economic Operator*, AEO) Unije in Japonske kot združljivih in enakovrednih, pri čemer se medsebojno sprejmejo ustrezni dodeljeni statusi AEO.

9. Carinski odnosi med EU in Japonsko temeljijo na Sporazumu o sodelovanju in medsebojni upravni pomoči v carinskih zadevah (Sporazum) ⁽¹⁾, ki je začel veljati 1. februarja 2008. V skladu s Sporazumom carinsko sodelovanje vključuje vse zadeve v zvezi z uporabo carinske zakonodaje. Sporazum tudi poziva Unijo in Japonsko, da si prizadevata za sodelovanje, da bi razvijali dejavnosti za omogočanje lažje blagovne menjave na področju carin v skladu z mednarodnimi standardi ⁽²⁾. Medsebojno priznavanje programov o pooblaščenih gospodarskih subjektih (AEO) in varnostnih ukrepov krepi varnost celotne dobavne verige in pospešuje trgovino.

10. Predlog med drugim določa, da carinski organi ohranjajo združljivost sistemov in vsak carinski organ zagotovi primerljive ugodnosti gospodarskim subjektom s statusom AEO. V njem je poleg tega navedeno, da morajo carinski organi okrepiti komunikacijo in izmenjevati informacije. V predlogu so naštetne podrobnosti, ki jih je treba izmenjevati v zvezi s subjekti AEO.

IV. ANALIZA PREDLOGA

IV.1 Uporaba zakonodaje o varstvu osebnih podatkov

11. Člen IV Priloge k predlogu se nanaša na izmenjavo informacij in komunikacijo. V njem je določeno, da se informacije in povezani podatki, zlasti o udeležencih programov, izmenjujejo sistematično po elektronskem mediju. Navedene so podrobnosti, ki se izmenjujejo o gospodarskih subjektih, pooblaščenih v sklopu programov o AEO, vključno z na primer imenom gospodarskega subjekta s statusom AEO, naslovom zadevnega gospodarskega subjekta itd.

12. Ureditev za subjekte AEO je opredeljena v členu 5(a) Uredbe (ES) št. 648/2005 Evropskega parlamenta in Sveta ⁽³⁾. Določeno je, da „1. (...). Pooblaščen gospodarski subjekt je upravičen do olajšav pri carinskih kontrolah v zvezi z varstvom in varnostjo in/ali poenostavitve, predvidenih v carinskih predpisih. (...)“.

13. „Gospodarski subjekt“ je v členu 1(12) Uredbe Komisije (ES) št. 1875/2006 ⁽⁴⁾ opredeljen kot „oseba, ki je v okviru svojega poslovanja udeležena v dejavnostih, ki jih ureja carinska zakonodaja“. Gospodarski subjekt je zato lahko fizična ali pravna oseba. Pojem „gospodarski subjekt“ vključuje subjekte AEO iz odstavka 9. Zato je mogoče šteti informacije o nekaterih subjektih AEO za „osebne podatke“, kot je opredeljeno v členu 2(a) Uredbe (ES) št. 45/2001 in Direktive 95/46/ES, vsaj informacije tistih subjektov AEO, ki so fizične osebe. Celotna informacija o subjektih AEO, ki so pravne osebe, je mogoče v nekaterih primerih šteti za osebne podatke. V teh primerih je odločilni dejavnik dejstvo, ali se informacije „nanašajo na“ „določljivo“ fizično osebo ⁽⁵⁾. Zato ni nobenega dvoma, da se v okviru zadevnega predloga lahko izmenjujejo osebni podatki.

14. Osebne podatke bodo obdelali carinski organi. V členu I(2) Priloge k predlogu je predvideno, da „so carinski organi, opredeljeni v členu 1(c) Sporazuma (...), pristojni za izvajanje tega sklepa“. Referenčna opredelitev je, da „„carinski organ“ pomeni (...), v Skupnosti (...) pristojne službe Komisije Evropskih skupnosti, pristojne za carinske zadeve, in carinske organe držav članic Skupnosti“. Zato se bosta v sedanjem okviru uporabljali Uredba (ES) št. 45/2001 in Direktiva 95/46/ES ⁽⁶⁾. Uredba (ES) št. 45/2001 se uporablja za obdelavo, ki jo opravlja Komisija, Direktiva 95/46/ES pa za obdelavo, ki jo opravljajo nacionalni carinski organi.

⁽³⁾ UL L 117, 4.5.2005, str. 13.

⁽⁴⁾ UL L 360, 19.12.2006, str. 64.

⁽⁵⁾ Glej Delovna skupina za varstvo podatkov iz člena 29, Mnenje št. 4/2007 o pojmu osebnih podatkov, WP 136, na voljo na naslovu: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf, zlasti strani 23 in 24.

⁽⁶⁾ Člen 3(1) Uredbe (ES) št. 45/2001 in Direktive 95/46/ES.

⁽¹⁾ UL L 62, 6.3.2008, str. 24.

⁽²⁾ Člen 4 Sporazuma.

IV.2 Mednarodni prenos osebnih podatkov

15. V direktivi in uredbi so predvidena podobna pravila v zvezi s čezmejnimi pretokom osebnih podatkov v členih 25–26 oziroma 9. V njih je opredeljeno načelo, da osebnih podatkov ni mogoče prenašati iz države članice v tretjo državo, razen če tretja država zagotovi ustrezno raven zaščite (ali razen če se sprejmejo ustrezni zaščitni ukrepi ali če se uporablja ena od predvidenih izjem).

Izjava o ustreznosti v predlogu

16. Obrazložitevni memorandum vključuje točko o varstvu podatkov (točka 11). V točki 11 je navedeno, da je japonska ureditev varstva podatkov ustrezna v smislu člena 9 Uredbe (ES) št. 45/2001. Člen 9 obravnava ureditev, ki jo je treba upoštevati pri prenosu osebnih podatkov prejemnikom, ki niso institucije in organi Skupnosti, za katere ne velja Direktiva 95/46/ES, kot drži za tretje države, kot je Japonska.

17. V členu 9(1) uredbe je določeno, da se „(o)sebni podatki prenesejo prejemnikom, ki niso institucije in organi Skupnosti in ki niso zavezani nacionalni zakonodaji, sprejeti skladno z Direktivo 95/46/ES, samo, če se zagotovi ustrezna raven varstva v državi prejemnika ali znotraj mednarodne organizacije prejemnika in če se podatki prenesejo samo zato, da se omogoči izvedba nalog, za katere je pristojen upravljavec“.

18. V členu 9(2) je določeno, da se ocena ravni varstva, ki jo nudi tretja država ali mednarodna organizacija, ovrednoti glede na „vse okoliščine postopka prenosa podatkov ali niza postopkov prenosa podatkov“. Poleg tega vključuje primere vidikov, ki jih je treba upoštevati pri vrednotenju: „(...) posebno pozornost je treba nameniti naravi podatkov, namenu in trajanju predlaganega postopka ali postopkov obdelave, tretji državi prejemnici ali mednarodni organizaciji prejemnici, pravni ureditvi, tako splošni kot sektorski, ki velja v zadevni tretji državi ali mednarodni organizaciji, ter strokovnim predpisom in varnostnim ukrepom, ki se uporabljajo v tisti tretji državi ali mednarodni organizaciji“. Ta seznam ni izčrpen in pomembni so lahko tudi drugi elementi glede na dejanski primer.

19. Člen 9 uredbe je treba razlagati ob upoštevanju členov 25 in 26 Direktive 95/46/ES. V členu 25(6) direktive je določeno, da „Komisija lahko v skladu s postopkom iz člena 31(2) ugotovi, da tretja država zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena zaradi svoje domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela, (...)“. Zato je treba upoštevati postopek iz

člena 31(2) direktive – postopek komitologije – za izjavo, da je tretja država „ustrezna“.

20. V okviru tega predloga ta postopek ni bil upoštevan, zato izjava iz točke 11 o ustreznosti japonske ureditve varstva podatkov krši člen 25(6) direktive. ENVP zato močno priporoča, da se ta izjava črta.

21. ENVP priznava, da člen IV(5) Priloge k predlogu določa, da „carinski organi zagotavljajo varstvo podatkov v skladu s Sporazumom, zlasti s členom 16 Sporazuma“. Člen 16 obravnava „izmenjavo informacij in zaupnost“ in v drugemu odstavku tega člena je navedeno, da „se osebni podatki lahko izmenjujejo le, če se pogodbenica, ki bi jih prejela, zaveže, da jih bo varovala na način, ki je vsaj enakovreden tistemu, ki ga v takih primerih uporablja pogodbenica, ki bi podatke posredovala. Pogodbenica, ki bi posredovala podatke, ne postavlja nobenih zahtev, ki bi bile strožje od tistih, ki veljajo pod njeno jurisdikcijo“.

22. ENVP želi poudariti, da se – kot je opisano zgoraj – sistem, ki ga je treba analizirati glede ravni varstva, nanaša na „ustreznost“ in ne na „enakovrednost“ (prim. sedanje mednarodne zaveze Unije)⁽¹⁾. V vsakem primeru se zdi, da je člen 16 deklarativen, saj v Sporazumu niso zagotovljeni dokazi o obstoju dejanske „enakovrednosti“. Poleg tega se ne sklicuje na nobeno opravljeno analizo „ustreznosti“ ali celo „enakovrednosti“. Zato te izjave v členu 16 ni mogoče šteti za odločilen element vrednotenja ustreznosti in ne more biti podlaga za izjavo iz točke 5(1) obrazložitenega memoranduma.

Širši vidik zaradi posebnosti primera

23. Treba je opozoriti, da lahko Evropska komisija, organi za varstvo podatkov in upravljavci podatkov vrednotijo raven varstva v neki državi na različnih ravneh in z različnimi pravnimi učinki. Opredelitev ustreznosti, ki jo opravi Evropska komisija na podlagi člena 25(6) Direktive 95/46/ES, je za države članice zavezujoča. To velja tudi za institucije in organe Evropske unije v skladu s členom 9(5) uredbe. Če take odločitve ni, se vrednotenje ustreznosti zaupa organom za varstvo podatkov v številnih državah članicah, v drugih pa upravljavcem podatkov pod

⁽¹⁾ Glej člen XIV sporazuma GATS: „V skladu z zahtevo, da se tovrstni ukrepi ne uporabljajo na način, ki bi pomenil samovoljno ali neupravičeno diskriminacijo med državami, v katerih prevladujejo enake razmere ali prikrito omejevanje trgovine s storitvami, se nobena določba v tem sporazumu ne razlaga tako, da članici preprečuje sprejemanje ali izvajanje ukrepov, ki: (...) (c) so potrebni za zagotovitev skladnosti z zakoni ali predpisi, ki niso v neskladju z določbami tega sporazuma, vključno s tistimi, ki se nanašajo na: (...) (ii) varovanje zasebnosti posameznikov v zvezi z obdelavo in razširjanjem osebnih podatkov ter varovanje zaupnosti dokumentacije in računov posameznikov; (...)“.

- nadzorom organov za varstvo podatkov. Člen 9 uredbe jasno sledi temu zadnjemu modelu.
24. To pomeni, da tudi če država kot celota ni bila razglašena za „ustrezno“ v skladu s postopkom iz člena 25(6) direktive, lahko upravljavec šteje, da je pravna ureditev varstva podatkov, ki se uporablja za poseben prenos ali poseben niz prenosov, „ustrezna“ (v spodaj opisanem okviru).
25. Glede na člen 9(2) uredbe (in člen 25(2) direktive) mora upravljavec oceniti vse okoliščine, povezane s postopkom prenosa ali z nizom postopkov prenosa podatkov. Analizo je treba opraviti in concreto, ob upoštevanju posebnih značilnosti (jamstev in/ali tveganj) zadevnega prenosa ali niza prenosov. Ta ocena bi se končala s sklepom glede obstoječe ravni varstva v zvezi s posebnim prenosom ali nizom prenosov in bila omejena na namene, ki jih upoštevajo upravljavec podatkov in prejemniki v ciljni državi. V tem primeru upravljavec prevzame odgovornost za preverjanje, ali obstajajo razmere za ustreznost. Ko upravljavec podatkov opravi analizo, je njegov sklep predmet nadzora organa za varstvo podatkov.
26. V točki 11 obrazložitvenega memoranduma je navedeno, da je japonska ureditev, ki je bila obravnavana, japonski carinski zakon (člen 108–2), zakon o mednarodni pomoči pri preiskavah in drugih povezanih zadevah (člena 1 in 3), nacionalni zakon o javni službi (člen 100), zakon o varstvu osebnih podatkov, ki jih uporabljajo upravni organi (člen 8), in zakon o dostopu do podatkov, ki jih uporabljajo upravni organi (člen 5).
27. ENVP nima dokazov, da je bila ta ureditev ocenjena na podlagi delovnega dokumenta Delovne skupine iz člena 29 (WP12) o „Prenosih podatkov v tretje države: uporaba členov 25 in 26 direktive EU o varstvu podatkov“ in ob upoštevanju načel, opredeljenih v tem delovnem dokumentu ⁽¹⁾.
28. Poleg tega je treba upoštevati, da metoda ustreznosti pomeni, da je treba upoštevati črko in dejansko uporabo zakona (objektivni in funkcionalni pristop). Zato obravnava te pravne ureditve *same po sebi* ni zadosten dokaz za izvajanje njenih pravil v praksi.
29. To pomeni, da je treba preveriti učinkovitost in uporabo teh pravil v praksi, preden je mogoče opredeliti, ali se učinkovito zagotavlja ustrezna raven varstva za zadevni postopek prenosa podatkov ali niza postopkov prenosa podatkov, v tem primeru za izmenjavo informacij v okviru programov AEO.
30. Glede na navedeno morajo upravljavci (v tem primeru službe Evropske komisije, pristojne za carinske zadeve, in carinski organi držav članic Unije) opraviti oceno, da preverijo, ali ciljna država (v tem primeru Japonska) učinkovito zagotavlja ustrezno raven za zadevne posebne prenose, ki je omejena na posebne namene in prejemnike v tej državi ⁽²⁾ (to je izmenjavo podatkov za izvajanje programov AEO). Vendar taka ocena ni bila opravljena.
31. V predlogu bi se lahko upošteval ta pristop kot nadomestna možnost za postopek za „ustreznost“ Japonske, kot je opisano zgoraj.

Druge nadomestne možnosti

32. V predlogu bi se lahko tudi proučilo, ali bi lahko upravljavci navedli druge vrste „primernih zaščitnih ukrepov“ v skladu s členi 9(7) uredbe in 26(2) direktive ali če se uporablja katera koli izjema iz členov 9(6) uredbe ali 26(1) direktive ⁽³⁾.

IV.3 Dodatne zahteve zakonodaje o varstvu podatkov

Kakovost podatkov

33. Načelo kakovosti podatkov je opisano v členu 4 uredbe. Poleg drugih zahtev določa, da „morajo biti osebni podatki: (...) (c) primerni, ustrezni in ne pretirani glede na namene, za katere se zbirajo in/ali naprej obdelujejo; (...)“. Zdi se, da kategorije podatkov iz člena IV(4) upoštevajo to načelo.
34. Poleg tega je v členu 4 uredbe navedeno, da „morajo biti osebni podatki: (...) (e) hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, le toliko časa, kolikor je potrebno za namene, za katere so bili podatki zbrani ali za katere se naprej obdelujejo (...)“. Zato bo treba določiti obdobje hrambe osebnih podatkov, ki jih je treba obdelati.

⁽¹⁾ Delovna skupina za varstvo podatkov iz člena 29, delovni dokument „Prenosi osebnih podatkov v tretje države: uporaba členov 25 in 26 direktive EU o varstvu podatkov“, na voljo na naslovu: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf

⁽²⁾ ENVP je podal podobno razlago v okviru zahtevka za posvetovanje, prejetega od urada OLAF, glede „Prenosov osebnih podatkov tretjim državam: ‚ustreznost‘ držav podpisnic Konvencije št. 108 Sveta Evrope (primer 2009–0333)“, na voljo na naslovu: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf

⁽³⁾ V zvezi s členom 26(1) Direktive glej: Delovna skupina za varstvo podatkov iz člena 29, Delovni dokument o skupni razlagi člena 26(1) Direktive 95/46/ES, WP114, na voljo na naslovu: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

Pravice posameznika, na katerega se podatki nanašajo

35. Komisija bo morala predvideti mehanizme za zagotavljanje uresničevanja pravic posameznika, na katerega se podatki nanašajo, kot je pravica do dostopa in popravka (člena 13 in 14 uredbe).

Obveznost predložitve informacij

36. Člena 11 in 12 uredbe določata, da je treba informacije posredovati zadevni osebi in opredeliti njihov časovni okvir. Komisija bo morala vzpostaviti postopek za preverjanje, ali bodo na primer informacije predložene ob zbiranju podatkov (ki ga opravi tretja država) ali jih bo predložila Komisija sama.

V. SKLEPNE UGOTOVITVE IN PRIPOROČILA

37. ENVP je razočaran, da se ni upošteval postopek posvetovanja iz poglavja II.
38. ENVP priporoča, da se črta izjava o ustreznosti japonske ureditve iz točke 11 obrazložitvenega memoranduma, ker ni v skladu z zahtevami Uredbe (ES) št. 45/2001 in

Direktive 95/46/ES. Poleg tega priporoča proučitev različnih možnosti iz uredbe in direktive za zagotavljanje upoštevanja pravil o mednarodnih prenosih.

39. ENVP priporoča tudi, da Komisija:

- opredeli obdobje hrambe za osebne podatke, ki jih je treba obdelati,
- predvidi mehanizme za zagotavljanje uresničevanja pravic posameznika, na katerega se podatki nanašajo,
- oblikuje postopek za zagotavljanje informacij posameznikom, na katere se podatki nanašajo.

V Bruslju, 12. marca 2010

Peter HUSTINX
evropski nadzornik za varstvo podatkov