

**Mnenje Evropskega ekonomsko-socialnega odbora – Sporočilo Komisije Evropskemu parlamentu in Svetu –
Smernice k uredbi o okviru za prosti pretok neosebni podatkov v Evropski uniji**

(COM(2019) 250 final)

(2020/C 14/18)

Poročevalka: **Laure BATUT**

Zaprosilo	Evropska komisija, 22.7.2019
Pravna podlaga	člen 304 Pogodbe o delovanju Evropske unije
Pristojnost	strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo
Datum sprejetja mnenja strokovne skupine	11.9.2019
Datum sprejetja mnenja na plenarnem zasedanju	25.9.2019
Plenarno zasedanje št.	546
Rezultat glasovanja (za/proti/vzdržani)	162/2/6

1. Priporočila

1.1 EESO priporoča Komisiji, naj:

- preprosto in jasno obvešča o merilih za opredelitev neosebni podatkov in področju uporabe uredbe o prostem pretoku neosebni podatkov, da bi odpravili negotovosti in povečali zaupanje,
- obvešča akterje, na katerih področjih se evropski predpisi o podatkih prekrivajo,
- pri spodbujanju prostega pretoka podatkov poskrbi, da se osebni podatki sčasoma ne bodo šteli za neosebne podatke in da bo področje uporabe splošne uredbe o varstvu podatkov ostalo nespremenjeno kljub srednjeročni združitvi obeh uredb z namenom, da bi bolje zaščitili podatke, ne pa povečali trgovanja z njimi,
- spodbuja ustanavljanje in razvoj zvez vseevropskih storitev za računalništvo v oblaku,
- Evropejcem pomaga, da bodo v zelo kratkem času znali uporabljati algoritme, s katerimi je mogoče obdelovati veliko količino neosebni podatkov na enotnem trgu; spodbuja države članice, naj okrepijo vseživljenjsko izobraževanje na področju informacijske tehnologije in umetne inteligence na vseh ravneh (v šolah, na univerzah in v poklicnem življenju),
- spodbuja akterje, naj razvijajo duh odgovornosti, etike in solidarnosti ter naj ne dopustijo, da bi s samoregulacijo in „mirnim“ reševanjem sporov različno razlagali zakonodajna besedila,
- ne zanemari uporabe regulativnega orodja,
- spodbuja sankcije za kršitev samourejanja,
- pripravi načrt za preverjanje, ali je v skladu z uredbo o prostem pretoku neosebni podatkov podjetjem zagotovljena pravna varnost pri prosti uporabi njihovih podatkov,

- opravi pregled stanja v 27 državah članicah in oceni ukrepe nacionalnih kontaktnih točk že po dvanajstih mesecih njihovega delovanja,
- se temeljito posveti svoji vlogi obveščanja, komuniciranja in opozarjanja,
- spodbuja države članice, naj akterje obveščajo o merilih „javne varnosti“,
- spodbuja države članice, naj razširijo svoja območja hrambe podatkov, ki niso prenosljivi,
- pravočasno pregleda politiko konkurence in preveri, ali je prilagojena prostemu pretoku podatkov v sedanjem smislu.

2. Uvod

2.1 EESO je seznanjen z namero Komisije, da bo podjetjem, ki jih zadeva prenos neosebnih podatkov, dajala ustrezne napotke, dokler se deležniki v letu 2020 ne bodo dogovorili o kodeksih ravnanja. Ker so podatki pogosto mešani – lahko so hkrati neosebni in osebni –, se lahko podjetja znajdejo v negotovosti, s katerimi ukrepi bi jih bilo treba zaščititi. Preden pa se obravnavajo točke, na katere je imel EESO pripombe, je treba najprej spomniti na glavna načela veljavnih predpisov.

2.2 Komisija je ugotovila, da je pomanjkanje konkurenčnosti med storitvami računalništva v oblaku v EU in s tem pomanjkanje podatkovne mobilnosti v okviru oligopolov negativno vplivalo na trg podatkov. Države članice morajo v skladu z uredbo o prostem pretoku neosebnih podatkov čim bolj zmanjšati svoje zahteve glede lokalizacije podatkov in razdrobljenost zakonodaje na tem področju, da bi spodbudile rast in sprostile inovacijske zmogljivosti podjetij.

2.3 S sprejetjem uredbe o prostem pretoku neosebnih podatkov, ki dopolnjuje splošno uredbo o varstvu podatkov, je „prosti pretok peta svoboščina“, ki se uporablja za vse podatke in se vzpostavlja v evropskih besedilih 21. stoletja (kot je to opredelila poslanka Evropskega parlamenta in poročevalka Anna-Maria Corazza Bildt). Če imetniki tega neopredmetenega blaga (če mu lahko tako rečemo) želijo, da se prenese v upravljanje gostujočim ponudnikom storitev v državah, ki niso država članica, v kateri je bilo ustvarjeno in/ali se uporablja (člen 1 uredbe o prostem pretoku neosebnih podatkov), jim mora biti to omogočeno. Tako bodo lahko lažje delovali in bodo bolj konkurenčni.

Uredba o prostem pretoku neosebnih podatkov

2.4 Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta ⁽¹⁾ spodbuja prosti pretok neosebnih podatkov v Uniji, da bi razvili umetno inteligenco, računalništvo v oblaku in analizo velepodatkov. Njen člen 6 določa, da Komisija usmerja, spodbuja in olajšuje gospodarskim subjektom, ki uporabljajo neosebne podatke, pripravo samoregulativnih kodeksov ravnanja na ravni Unije.

2.5 Te smernice, ki so namenjene poklicnim uporabnikom v mikropodjetjih ter malih in srednjih podjetjih, bi jim morale olajšati razumevanje medsebojnega vpliva med to uredbo in splošno uredbo o varstvu podatkov. Komisija v ponazoritev navaja veliko primerov.

2.6 Kodeksi ravnanja, ki se pripravljajo, bi morali biti dokončno oblikovani med novembrom 2019 in majem 2020 (uvodni izjavi 30 in 31, člen 6(1)). V njih bodo upoštevana mnenja vseh strani. V zvezi s tem potekata dve javni posvetovanji, Komisiji pa pomagata dve delovni skupini, ki ju sestavljajo poklicni uporabniki: ena za certificiranje varnosti storitev v oblaku (CSPCERT) in druga za prenos podatkov in zamenjavo ponudnikov storitev v oblaku (SWIPO). Njuni prispevki zajemajo infrastrukturo kot storitev in programsko opremo kot storitev. Komisija bo maja 2020 predlagala, da se panoga spodbudi k pripravi vzorca pogodbenih klavzul, leta 2022 pa bo poročala Evropskemu parlamentu, Svetu in EESO o izvajanju uredbe, zlasti o uporabi „sestavljenih“ ali mešanih podatkov.

3. Splošne ugotovitve

3.1 *Poslanstvo Komisije: uskladitev splošne uredbe o varstvu podatkov in uredbe o prostem pretoku neosebnih podatkov.*

3.1.1 Da bi uskladili uredbi, ki se dopolnjujeta, Komisija pojasnjuje, da 1) so zahteve glede lokalizacije podatkov **zdaj prepovedane**, 2) podatki ostajajo dostopni **pristojnim organom**, 3) podatki postajajo mobilni in se jih zato lahko „prenaša“. Splošna uredba o varstvu podatkov se nanaša na „prenosljivost“, uredba o prostem pretoku neosebnih podatkov pa na „prenos“. Uporabniki lahko svoje podatke prenesejo iz države, v kateri so bili ustvarjeni, in jih nato po zamenjavi ponudnika storitev brez (večjih) omejitev pridobijo, hranijo, obdelujejo in analizirajo. Za razliko od „prenosljivosti“, ki je pravica posameznikov, na katere se nanašajo osebni podatki, se „prenos“ izvaja v skladu s kodeksi ravnanja in s tem v okviru samoregulativnega pristopa.

(¹) ULL 303, 28.11.2018, str. 59.

3.1.2 To je pomembna razlika med uredbama. Prva temelji na **trdem pravu**, druga pa na nezavezujočih instrumentih (**mehko pravu**), za katere je znano, da ponujajo precej manj jamstev. Po mnenju Komisije večina podatkovnih nizov vsebuje osebne in neosebne podatke, ki so **neločljivo povezani**, zato se imenujejo „mešani“ podatki.

3.1.3 EESO pozdravlja te podporne smernice in odobrava izbrane primere ter ne namerava predlagati še drugih. Ugotavlja pa, da Komisija v smernicah za gospodarske subjekte vsebino ponazarja zgolj z različnimi primeri. EESO želi opozoriti Komisijo na kritična področja, ki bi kljub prihodnjim smernicam in kodeksom ravnanja lahko povzročala težavo uporabnikom.

3.2 Pregled načel

3.2.1 Načelo: prosti pretok podatkov

Ovire za prosti pretok neosebnih podatkov niso toliko geografske kot funkcionalne in/ali povezane s sredstvi, ki so podjetjem na voljo za uporabo informacijske tehnologije.

Uredba o prostem pretoku neosebnih podatkov prepoveduje zahteve glede lokalizacije neosebnih podatkov na določenem ozemlju (člen 4). Državam članicam nalaga, da v 24 mesecih od začetka njene uporabe (maj 2021) razveljavijo vse nasprotno določbe.

Uredba dopušča izjeme, povezane z javno varnostjo. Države morajo na spletu objaviti podrobne informacije o svojih nacionalnih zahtevah glede lokalizacije. Evropska komisija lahko poda pripombe in objavi povezave do spletišč, ki so jih ustvarile države članice.

3.2.2 Izjeme od prostega pretoka

— Organi držav članic imajo lahko **dostop do prenesenih podatkov**: uredba o prostem pretoku neosebnih podatkov določa postopek, ki vsakemu nadzornemu organu neke države omogoča, da pridobi podatke, ki se obdelujejo v drugi državi. Določen je tudi postopek sodelovanja med državami (člena 5 in 7). EESO kljub temu zelo skrbi, da bi nekateri podatki (računovodski, finančni, pogodbeni itd.) brez možnosti lokalizacije ušli nadzoru organov držav članic. Zato opozarja Komisijo, naj ne pozabi po potrebi uporabiti regulativnega instrumenta.

— **Enotna kontaktna točka** posamezne države obravnava prošnjo skupaj z nacionalnim nadzornim organom, ki lahko zagotovi podatke, če meni, da je prošnja dopustna, ali pa jih ne zagotovi. Kontaktne točke bi morale v skladu z uredbo o prostem pretoku neosebnih podatkov pomagati akterjem, da se informirano odločijo o svojih prenosih podatkov in izbirajo ponudnike storitev po vsej Uniji ter ob vsej konkurenci.

EESO meni, da smernice ne zadoščajo za odpravo številnih negotovosti, povezanih z izvajanjem tega načela. Težko je namreč oceniti utemeljitev držav, dobronamernost gospodarskih subjektov ali pravilno delovanje kontaktnih točk.

— Prepoved neposrednih ali posrednih zahtev glede lokalizacije podatkov, razen za upravičene primere „javne varnosti“. EESO meni, da pojem „javna varnost“, naveden v uredbi, ni dovolj natančen in da ni jasno, kaj vse zajema, kadar se nanaša na pretok podatkov in trgovanje z njimi. Zahteve glede lokalizacije podatkov so v uredbi o prostem pretoku neosebnih podatkov opredeljene kot „kakršn[a] koli obveznost, prepoved, pogoj, omejitev ali drug[a] zahtev[a], ki je določena v zakonih ali drugih predpisih države članice ali izhaja iz [...] administrativne prakse“⁽²⁾, ki gospodarske subjekte zavezuje, da podatke ohranjajo na določenem ozemlju Unije. Za Sodišče Evropske unije⁽³⁾ (in kot je navedeno v uvodni izjavi 19 uredbe o prostem pretoku neosebnih podatkov) javna varnost „zajema tako notranjo kot zunanjo varnost države članice“ in predpostavlja obstoj „dejanske in dovolj resne grožnje, ki vpliva na enega od temeljnih interesov družbe“. Ta opredelitev se nanaša tudi na genetske podatke, biometrične podatke in podatke o zdravju. Odgovor države članice mora biti sorazmeren.

⁽²⁾ Uredba (EU) 2018/1807, člen 3(5).

⁽³⁾ Glej sporočilo COM(2019) 250, opombe na dnu strani 11, ter sodbo v zadevah C-331/16 in C-366/16: K. proti Staatssecretaris van Veiligheid en Justitie in H. F. proti Belgische Staat: „42. V zvezi s **pojmom ‚javna varnost‘** iz sodne prakse Sodišča izhaja, da ta pojem **pokriva tako notranjo kot zunanjo varnost države članice** (sodba z dne 23. novembra 2010, Tsakouridis, C-145/09, EU:C:2010:708, točka 43). Notranja varnost je lahko ogrožena zlasti z **neposredno grožnjo za mir in fizično varnost** prebivalstva zadevne države članice (glej v tem smislu sodbo z dne 22. maja 2012, I, C-348/09, EU:C:2012:300, točka 28). Zunanja varnost pa je lahko ogrožena zlasti s **tveganjem resnih motenj v zunanjih odnosih te države članice** ali mirnem sožitju med narodi (glej v tem smislu sodbo z dne 23. novembra 2010, Tsakouridis, C-145/09, EU:C:2010:708, točka 44).“

3.2.3 Glede prostega pretoka in lokalizacije podatkov Odbor meni, da:

- se sprejeta merila lahko razlagajo na različne načine,
- jih lahko pojasni samo sodnik za vsak primer posebej, kar bi lahko škodilo zaupanju, potrebnemu za trgovino, zlasti v primeru občutljivih podatkov; spori, ki izhajajo iz kodeksov ravnanja, bi lahko povečali razdrobljenost,
- je sodstvo veliko počasnejše od digitalne sfere in pretoka podatkov.

EESO meni, da negotovost in zapletenost odvrata mikropodjetja ter mala in srednja podjetja.

3.2.4 EESO obžaluje, da smernice ne določajo ničesar v zvezi s pravnimi spori ali načini preverjanja, kako države članice izpolnjujejo merila javne varnosti in kako bi jih lahko po potrebi kaznovali. Izraža bojazen, da razlage v smernicah niso dovolj, da bi se lahko upravljavci mikropodjetij ter malih in srednjih podjetij izognili vsem pravnim pastem v besedilih, in da zaradi negotovosti ni mogoče občutiti zaupanja in pravne varnosti, ki sta potrebna za razvoj sektorja.

3.2.5 EESO priznava, da ima sporočilo Komisije velik pomen, saj podrobno in od zgoraj navzdol opisuje stanje, ki je nastalo z uredbama, zato je še kako potrebno za mikropodjetja ter mala in srednja podjetja. EESO želi, da bi ukrepe nacionalnih kontaktnih točk in njihovo uporabo spletišča Komisije ocenili že po šestih mesecih njihovega delovanja, tako da bi bilo mogoče hitro sprejeti popravne ukrepe, če bi ugotovili pomanjkanje informacij in komuniciranja.

4. Posebne ugotovitve

4.1 O podatkih

4.1.1 Neosebni podatki načeloma vključujejo vse digitalne podatke, ki ne spadajo v področje osebnih podatkov, kot je opredeljeno v splošni uredbi o varstvu podatkov. Vključujejo lahko podatke o trgovanju, natančne kmetijske podatke, podatke o potrebah po vzdrževanju strojev, vremenske podatke itd.

4.1.2 Podatki, ki jih zbirajo javne službe, kot so bolnišnice, službe za socialno pomoč ali davčne službe, so lahko zelo blizu osebnih podatkov pacientov ali davčnih zavezancev. Podjetja, ki jih uporabljajo, morajo poskrbeti, da ne omogočajo identifikacije oseb ali tega, da bi bilo podatke potem, ko postanejo anonimni, mogoče ponovno identificirati. Za mikropodjetja ali mala in srednja podjetja to lahko pomeni, da bi morala izvajati postopke, ki so preveč zamudni in predragi. Ker uredbi (splošna uredba o varstvu podatkov in uredba o prostem pretoku neosebnih podatkov) skupaj zagotavljata prosti pretok vseh podatkov v EU, kadar so „neločljivo povezani“, se pravna zaščita iz splošne uredbe o varstvu podatkov uporablja za vse mešane podatke (uvodna izjava 8 in člen 2(2) Uredbe (EU) 2018/1807). Poleg prve omejitve prostega pretoka neosebnih podatkov, povezanih z javno varnostjo, obstaja tako še omejitev, povezana s samo naravo podatkov. To je osrednje vprašanje, ki ga Komisija obravnava v svojem sporočilu, v katerem večkrat omenja bližino osebnih in neosebnih podatkov: „mešani podatkovni nizi predstavljajo večino podatkovnih nizov“ (točka 2.2), lahko so „neločljivo povezani“ (točka 2.2), „nobena od uredb podjetij ne zavezuje k ločevanju podatkovnih nizov“ (točka 2.2).

4.1.3 Podjetje se mora vprašati, ali so neosebni podatki, ki jih obdeluje, „neločljivo povezani“ z osebnimi podatki, in jih zaščititi, če to ugotovi. Podjetjem ni lahko oblikovati zunanjega upravljanja (*out management*). Splošna opredelitev mešanih podatkov se ne zdi mogoča, prekrivanje med uredbama pa verjetno povzroča prekrivanje tudi z drugimi besedili, ki se nanašajo na zakonodajo o podatkih, na primer v zvezi z intelektualno lastnino: pretok neosebnih podatkov je dovoljen, če pa se ti podatki ponovno uporabijo v nekem delu, zanje ne veljajo več enaka pravila. EESO meni, da so povezave med različnimi besedili zelo krhke. V sodni praksi se je že zahtevalo, da se neločljiva povezanost podatkov preuči glede na „razumno“ merilo. EESO ugotavlja, da Komisija v sporočilu očitno ni mogla navesti vseh možnih primerov, da bi pomagala akterjem, in da je ustvarjeno stanje naklonjeno predvsem velikim podjetjem. EESO priporoča Komisiji, naj poskrbi, da se v praksi osebni podatki sčasoma ne bodo šteli za neosebne podatke in da bo področje uporabe splošne uredbe o varstvu podatkov ostalo nespremenjeno kljub srednjeročni združitvi obeh uredb z namenom, da bi bolje zaščitili podatke, ne pa povečali trgovanja z njimi.

4.2 O prenosljivosti, prenosu, obdelavi in hrambi podatkov

Prenosljivost podatkov je treba po splošni uredbi o varstvu podatkov urediti z uredbo (člen 20), po uredbi o prostem pretoku neosebnih podatkov pa s samoregulacijo. EESO obžaluje, da lahko nastane precejšnja pravna negotovost, ki bi lahko zaradi številnih pravnih tveganj škodovala mikropodjetjem ter malim in srednjim podjetjem. EESO meni, da se lahko neosebni podatki kot blago, ki je seveda neopredmeteno, a v prostem pretoku, uvažajo in izvažajo. V zvezi s tem bi bila zanimiva razprava o njihovem lastništvu. Pri tem je treba poudariti, da dejanska vrednost ni v samih podatkih, temveč v njihovi množičnosti. Zato Odbor meni, da politika konkurence morda ni primerna za to vrsto trga. Sprašuje se, kako bodo nastale razmere povečale produktivnost mikropodjetij ter malih in srednjih podjetij. V sporočilu Komisije to ni pojasnjeno.

4.3 O ponudnikih storitev

4.3.1 EU nima velikih gospodarskih subjektov niti „evropskega“ oblaka, kar EESO že dolgo časa obžaluje. Učinek obsega, za katerega se vsi prizadevajo, je v rokah zelo velikih ameriških računalniških podjetij in nekaterih kitajskih podjetij. Tako se celo velike uprave držav članic nagibajo k temu, da bi jim zaupale in nanje prenesle upravljanje svojih podatkov (primer Francije).

4.3.2 EESO meni, da bi morali Evropejci ustvariti partnerske ekosisteme in zagotoviti prenos podatkov med platformami. Komisija bi lahko poleg tega, kar predlaga v sporočilu, pomagala mikropodjetjem ter malim in srednjim podjetjem pri razvoju ustreznih virov, kot je to storila za storitve splošnega pomena v okviru projekta vseevropske zveze storitev za računalništvo v oblaku iz leta 2018 za opravljanje storitev splošnega gospodarskega in negospodarskega pomena (storitev na zahtevo, *FaaS – Function as a service*) in kot to načrtuje pri mreži vozlišč za digitalne inovacije (*A network of Digital Innovation Hubs*, web/Commission/DIHs/januar 2019).

4.4 Varnost podatkov ⁽⁴⁾

4.4.1 Na notranji ravni nacionalni gospodarski subjekti ⁽⁵⁾ preverijo naravo svojih podatkov, ki jih bodo prenesli, in jih zavarujejo. Zahteva glede lokalizacije je ustrezala varnostnim predpisom, ki jih je bilo mogoče preveriti v skladu z nacionalno zakonodajo. Kljub splošni uredbi o varstvu podatkov in uredbi o prostem pretoku neosebni podatkov standardi glede računalniške varnosti niso enaki v vseh državah EU. Odbor meni, da bi bilo treba v zvezi s tem prek nacionalnih kontaktnih točk in v različnih jezikih zagotoviti zanesljive informacije mikropodjetjem ter malim in srednjim podjetjem, pa tudi zasebnim in javnim službam.

Na zunanji ravni EESO ni prepričan, da lahko podjetja zunaj EU spoštujejo kodekse ravnanja in pridobijo podatke potem, ko jih njihovi imetniki nadalje prenesejo, in izraža bojazen, da bo sčasoma težko ločiti posamezne odgovornosti.

Priporoča Komisiji, naj pomaga evropskim akterjem, da bodo lahko v zelo kratkem času uporabljali algoritme, ki bodo omogočali obdelavo velikih količin neosebni podatkov na enotnem trgu.

4.4.2 Vprašanje fizične lokacije strežnikov in njihove varnosti se bo še naprej reševalo s trgovinskimi in diplomatskimi pogajanja med posameznimi državami. To vprašanje je bistvenega pomena. Kljub temu, da je upravljanje podatkov v deljeni pristojnosti med državami članicami in EU, bi bilo soočanje z zelo velikimi računalniškimi podjetji in njihovimi referenčnimi državami lahko tvegano, če bi se države članice odločile, da se pogajajo posamezno.

4.4.3 EESO predlaga, naj Komisija pojasni svoje sporočilo o obveznostih ponudnikov storitev v zvezi s hrambo neosebni podatkov, uporabljenimi metodami, fizičnimi lokacijami, načrtovanim ali dovoljenim rokom hrambe in uporabo po obdelavi, saj ti element pogojujejo njihovo varnost in so lahko pomembni za evropska podjetja v svetovni konkurenci.

4.5 O kodeksih ravnanja

4.5.1 Od maja 2019 se akterji, na katere se nanaša uredba o prostem pretoku neosebni podatkov (predvsem uporabniki in ponudniki storitev v oblaku), spodbujajo, naj svoj kodeks ravnanja pripravijo v 12 mesecih. Po mnenju Komisije bi bilo treba upoštevati najboljše prakse, pristope k certifikacijskim shemam in komunikacijske načrte. Delovni skupini SWIPO in CSPCERT bosta prispevali strokovno znanje.

4.5.2 Komisija se sklicuje na to, kar je bilo storjeno za splošno uredbi o varstvu podatkov (sporočilo, str. 19). Ta se opira na mnenje Evropskega odbora za varstvo podatkov ⁽⁶⁾, kar bi lahko storili tudi za uredbi o prostem pretoku neosebni podatkov. Združenja predstavnikov različnih gospodarskih panog lahko pripravijo svoj kodeks ravnanja, pri čemer morajo pristojnim organom dokazati, da njihov osnutek nacionalnega ali nadnacionalnega kodeksa izpolnjuje posebne zahteve panoge, olajšuje izvajanje uredbe in vzpostavlja učinkovite mehanizme za nadzor nad spoštovanjem kodeksa.

⁽⁴⁾ UL C 227, 28.6.2018, str. 86.

⁽⁵⁾ UL C 218, 23.7.2011, str. 130.

⁽⁶⁾ Evropski odbor za varstvo podatkov, smernice 1/2019 za kodekse ravnanja, 12. 2. 2019, https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12019-codes-conduct-and-monitoring-bodies-under_sl.

4.5.3 Še preden je začela veljati splošna uredba o varstvu podatkov, so glavni ponudniki infrastrukture na zahtevo (*IaaS*) in programske opreme na zahtevo (*SaaS*) pripravili svoje kodekse ravnanja, v katerih so opredelili načine izvajanja in tako odpravili nejasnosti, na katere so opozarjali poklicni uporabniki (⁽⁷⁾); vključili so tudi mala in srednja podjetja, saj so menili, da se številna med njimi raje odločijo za samopotrjevanje kot za zelo drago certificiranje.

4.5.4 EESO pri uredbi o prostem pretoku neosebni podatkov podpira sektorski pristop, če se ne zdi primerno, da bi uporabili rešitev, ki bi bila enaka za vse. V splošni uredbi o varstvu podatkov je naveden neizčrpen seznam postavk, ki jih morajo zajemati kodeksi ravnanja (člen 40(2)), zlasti kar zadeva poštene in pregledne postopke, varnost prenosa podatkov in reševanje sporov. Akterje bi bilo treba v njihovem lastnem interesu in da bi okrepili zaupanje potrošnikov v evropski pristop, spodbujati, da bi na tem gradili in razvijali duh odgovornosti, etike in solidarnosti, zlasti prek smernic, ki se nanašajo na umetno inteligenco. Odbor med drugim želi poudariti, da priporoča Komisiji, naj ne dopusti, da bi s samoregulacijo in „mirnim“reševanjem sporov različno razlagali besedila. Narediti bi bilo treba vse za konsolidacijo teh besedil, s čimer bi se oblikovala pravila, ki bi veljala za vse, kar bi Komisija navedla v svojih načrtih za obveščanje in komuniciranje.

5. O oceni

Komisija bo redno ocenjevala učinek prostega pretoka, izvajanje uredbe, odpravo omejevalnih ukrepov držav članic in učinkovitost kodeksov ravnanja. EESO meni, da bi bilo treba povabiti tudi predstavnike civilne družbe, da bi izrazili svoje stališče o tem (⁽⁸⁾). Da bi se družba kot celota počutila varno in bi imela zaupanje v te nove digitalne prakse, morajo tako Unija kot države članice odpraviti negotovosti glede prava, ki se uporablja, zaupnosti, hrambe in obnovitve podatkov brez izgube, jamstev izvedljivosti in dobronamernosti akterjev ter finančnih jamstev. Neločljiva povezanost podatkov, ki so hkrati osebni in neosebni, vzbuja zaskrbljenost in EESO se sprašuje, ali je glede na velik delež teh podatkov v primerjavi z vsemi podatki samoregulacija resnično edina rešitev. Priporoča, da se pravila iz splošne uredbe o varstvu podatkov srednjeročno uporabljajo za vse podatke in vse podatkovne tokove, razen za „prave“neosebne podatke.

V Bruslju, 25. septembra 2019

Predsednik
Evropskega ekonomsko-socialnega odbora
Luca JAHIER

⁽⁷⁾ CISPE – *Cloud Infrastructure Services Providers in Europe* (ponudniki infrastrukturnih storitev v oblaku v Evropi).

⁽⁸⁾ UL C 487, 28.12.2016, str. 92; UL C 62, 15.2.2019, str. 292.

PRILOGA

Naslednji amandmaji, ki jih je plenarna skupščina zavrnila, so prejeli vsaj četrtino oddanih glasov (člen 59(3) poslovnika):

Točka 4.1.3

Spremeni se tako:

Podjetje se mora vprašati, ali so neosebni podatki, ki jih obdeluje, „neločljivo povezani“ z osebnimi podatki, in jih zaščititi, če to ugotovi. Podjetjem ni lahko oblikovati zunanjega upravljanja (out management). Splošna opredelitev mešanih podatkov se ne zdi mogoča, prekrivanje med uredbama pa verjetno povzroča prekrivanje tudi z drugimi besedili, ki se nanašajo na zakonodajo o podatkih, na primer v zvezi z intelektualno lastnino: pretok neosebnih podatkov je dovoljen, če pa se ti podatki ponovno uporabijo v nekem delu, zanje ne veljajo več enaka pravila. EESO meni, da so povezave med različnimi besedili zelo krhke. V sodni praksi se je že zahtevalo, da se neločljiva povezanost podatkov preuči glede na „razumno“ merilo. EESO ugotavlja, da Komisija v sporočilu očitno ni mogla navesti vseh možnih primerov, da bi pomagala akterjem, in da je ustvarjeno stanje naklonjeno predvsem velikim podjetjem. EESO priporoča Komisiji, naj poskrbi, da se v praksi osebni podatki sčasoma ne bodo šteli za neosebne podatke in da bo področje uporabe splošne uredbe o varstvu podatkov ostalo nespremenjeno ~~kljub srednjeročni združitvi obeh uredb~~ z namenom, da bi bolje zaščitili podatke, ne pa povečali trgovanja z njimi.

Točka 5

Spremeni se tako:

Komisija bo redno ocenjevala učinek prostega pretoka, izvajanje uredbe, odpravo omejevalnih ukrepov držav članic in učinkovitost kodeksov ravnanja. EESO meni, da bi bilo treba povabiti tudi predstavnike civilne družbe, da bi izrazili svoje stališče o tem. Da bi se družba kot celota počutila varno in bi imela zaupanje v te nove digitalne prakse, morajo tako Unija kot države članice odpraviti negotovosti glede prava, ki se uporablja, zaupnosti, hrambe in obnovitve podatkov brez izgube, jamstev izvedljivosti in dobronamernosti akterjev ter finančnih jamstev. Neločljiva povezanost podatkov, ki so hkrati osebni in neosebni, vzbuja zaskrbljenost in EESO se sprašuje, ali je glede na velik delež teh podatkov v primerjavi z vsemi podatki samoregulacija resnično edina rešitev. ~~Priporoča, da se pravila iz splošne uredbe o varstvu podatkov srednjeročno uporabljajo za vse podatke in vse podatkovne tokove, razen za „prave“ neosebne podatke.~~

Točka 1.1, tretja alineja:

Spremeni se tako:

EESO priporoča Komisiji, naj:

[...];

— pri spodbujanju prostega pretoka podatkov poskrbi, da se osebni podatki sčasoma ne bodo šteli za neosebne podatke in da bo področje uporabe splošne uredbe o varstvu podatkov ostalo nespremenjeno ~~kljub srednjeročni združitvi obeh uredb~~ z namenom, da bi bolje zaščitili podatke, ne pa povečali trgovanja z njimi;

[...].

Obrazložitev

Splošna uredba o varstvu podatkov in Uredba (EU) 2018/1807 imata različno pravno podlago, in sicer člen 16 PDEU o temeljni pravici posameznika do varstva osebnih podatkov oziroma člen 114 PDEU o približevanju zakonodaje. Ta člena dopuščata EU različen manevrski prostor za ukrepanje na področju zasebnega gospodarstva (kar je razlog za to, da EU v prvem primeru ukrepa z zelo strogo in podrobno uredbo, v drugem primeru pa je izbrala samourejanje kot najprimernejše, sorazmerno sredstvo ukrepanja). Zato ta instrumenta ni mogoče pravno združiti.

Rezultat glasovanja

Za:	54
Proti:	84
Vzdržani:	18