16/SL
WP 238

Mnenje št. 1/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU–ZDA

Sprejeto 13. aprila 2016

POVZETEK

Evropska komisija je 29. februarja 2016 objavila sporočilo, tj. osnutek sklepa o ustreznosti in priložena besedila, ki pomenijo nov okvir za čezatlantske izmenjave osebnih podatkov za poslovne namene: zasebnostni ščit EU–ZDA (v nadaljnjem besedilu: zasebnostni ščit), ki naj bi nadomestil prejšnjo odločbo o varnem pristanu ZDA, ki jo je Sodišče Evropske unije (v nadaljnjem besedilu: Sodišče) razveljavilo 6. oktobra 2015 v zadevi Schrems.

Delovna skupina iz člena 29 (v nadaljnjem besedilu: WP29) je v skladu s členom 30(1)(c) Direktive 95/46/ES ocenila te dokumente, da bi podala svoje mnenje glede osnutka sklepa o ustreznosti. WP29 je ocenila komercialne vidike in možna odstopanja od načel zasebnostnega ščita za namene nacionalne varnosti, kazenskega pregona in javnih interesov.

WP29 je upoštevala veljavni pravni okvir EU za varstvo podatkov, kot je določen v Direktivi 95/46/ES, pa tudi temeljne pravice do zasebnega življenja in varstva podatkov, kot so določene v členu 8 Evropske konvencije o človekovih pravicah ter členih 7 in 8 Listine Evropske unije o temeljnih pravicah. Upoštevala je tudi pravico do učinkovitega pravnega sredstva in nepristranskega sodišča iz člena 47 Listine, pa tudi sodno prakso, povezano z različnimi temeljnimi pravicami.

Poleg tega analiza odraža obrazložitev Sodišča v zadevi Schrems v zvezi z mejo proste presoje pri oceni ustreznosti. Preverjanje in nadzor zahtev glede ustreznosti je treba strogo izvajati, ob tem pa upoštevati temeljno pravico do zasebnosti in varstva podatkov ter število posameznikov, na katere bi lahko vplivali prenosi.

Zasebnostni ščit je treba obravnavati v sedanjem mednarodnem okviru, kot se pojavljajo velepodatki in potreba po vse večji varnosti. Obseg in razpon zbiranja in uporabe osebnih podatkov sta se od izdaje prvotne odločbe o varnem pristanu leta 2000 izjemno povečala. Evropski organi za varstvo podatkov odločno podpirajo pomembnost načel, ki jih zagovarjajo.

WP29 predvsem pozdravlja znatne izboljšave, ki jih je prinesel zasebnostni ščit v primerjavi z odločbo o varnem pristanu. Ugotavlja, da so pogajalci obravnavali številne pomanjkljivosti varnega pristana, ki jih je poudarila v svojem dopisu z dne 10. aprila 2014, naslovljenem na podpredsednico Redingovo.

Ker so načela in jamstva, ki jih zagotavlja zasebnostni ščit, določena v sklepu o ustreznosti in njegovih prilogah, je informacije težko najti, včasih pa so tudi neusklajene. To prispeva k splošnemu pomanjkanju jasnosti v zvezi z novim okvirom ter posameznikom, na katere se nanašajo osebni podatki, organizacijam in organom za varstvo podatkov otežuje dostopnost. Podobno tudi uporabljeni jezik ni dovolj jasen. Zato WP29 Komisijo poziva, naj poskrbi, da bo to jasno in razumljivo za uporabnike na obeh straneh Atlantika.

Kar zadeva veljavno pravo, WP29 poudarja, da če se sklep o ustreznosti zasebnostnega ščita sprejme na podlagi Direktive 95/46/ES, mora biti skladen s pravnim okvirom EU za varstvo podatkov, tako glede področja uporabe kot tudi glede terminologije. WP29 meni, da je treba

pregled izvesti kmalu po začetku uporabe Splošne uredbe o varstvu podatkov, s čimer se bo zagotovilo, da se bo v sklepu o ustreznosti in njegovih prilogah upoštevala višja raven varstva podatkov, ki jo zagotavlja ta uredba.

O poslovnih vidikih zasebnostnega ščita

Ključni cilj WP29 je zagotoviti ohranitev v bistvu enakovredne ravni varstva, zagotovljenega posameznikom, kadar se osebni podatki obdelujejo na podlagi določb zasebnostnega ščita. Čeprav WP29 ne pričakuje, da bo zasebnostni ščit zgolj izčrpna kopija pravnega okvira EU, pa meni, da bi moral vključevati vsebino temeljnih načel in s tem zagotavljati „v bistvu enakovredno“ raven varstva.

WP29 ne glede na izboljšave, ki jih ponuja zasebnostni ščit, meni, da nekatera ključna načela glede varstva podatkov, kot so začrtana v evropskem pravu, v osnutku sklepa o ustreznosti in prilogah niso izražena ali pa so bila neustrezno nadomeščena z drugimi pojmi.

Na primer, načelo hrambe podatkov ni izrecno navedeno in ga ni mogoče jasno razlagati na podlagi sedanjega besedila načela neokrnjenosti podatkov in omejitve namena. Poleg tega ni besedila o varstvu, ki bi ga bilo treba zagotoviti proti avtomatiziranim posameznim odločitvam, ki temeljijo zgolj na samodejni obdelavi. Nejasna je tudi uporaba načela omejitve namena za obdelavo podatkov. Za večjo jasnost glede uporabe več pomembnih pojmov WP29 predlaga, naj se EU in ZDA dogovorijo o jasnih opredelitvah, ki bi morale biti del glosarja izrazov, ki bi moral biti vključen v pogosto zastavljena vprašanja o zasebnostnem ščitu.

Ker se bo zasebnostni ščit uporabljal tudi za prenos podatkov zunaj ZDA, WP29 vztraja, da bi morali prenosi tretjemu od subjekta zasebnostnega ščita na prejemnike v tretji državi zagotavljati enako raven varstva glede vseh vidikov ščita (vključno z nacionalno varnostjo) ter ne bi smeli oslabiti načel EU glede varstva podatkov ali povzročiti izogibanja tem načelom. Če je v okviru zasebnostnega ščita predviden prenos tretji državi, bi morala biti vsaka organizacija v zasebnostnem ščitu zavezana, da pred prenosom oceni vse obvezne zahteve nacionalne zakonodaje tretje države, ki se uporablja za uvoznika podatkov. Na splošno WP29 ugotavlja, da prenosi osebnih podatkov iz EU tretjemu niso dovolj izdelani, zlasti kar zadeva njihov obseg, omejitev njihovega namena in jamstva, ki se uporabljajo za prenose posrednikom.

Čeprav WP29 ugotavlja, da so posameznikom za uveljavljanje pravic na voljo dodatne možnosti pravnega varstva, jo skrbi, da se bo novi mehanizem pravnega varstva v praksi izkazal za preveč zapletenega, zahtevnega za uporabo za posameznike iz EU in zato za neučinkovitega. Zato je treba dodatno pojasniti različne postopke pravnega varstva; zlasti se lahko organi EU za varstvo podatkov, če to želijo, štejejo za naravne kontaktne točke za posameznike iz EU v različnih postopkih, saj imajo možnost, da delujejo v njihovem imenu.

Odstopanja zaradi nacionalne varnosti

Kar zadeva dostop do podatkov s strani javnih organov v EU in tretjih državah, WP29 opozarja na svojo analizo zadevnih temeljnih pravic, vključeno v delovni dokument o

upravičenosti poseganja v temeljne pravice do zasebnosti in varstva podatkov z nadzornimi ukrepi pri prenosu osebnih podatkov (bistvena evropska jamstva) (WP237).

Velik korak naprej od odločbe o varnem pristanu je, da je v osnutku sklepa o ustreznosti zdaj izčrpno obravnavan morebitni dostop do podatkov, ki se v okviru zasebnostnega ščita obdelujejo zaradi nacionalne varnosti in kazenskega pregona. WP29 priznava ta velik korak, pa tudi večjo preglednost, ki jo vlada ZDA zagotavlja glede zakonodaje, ki se uporablja za zbiranje obveščevalnih podatkov (Priloga VI).

Vendar ugotavlja, da zagotovila ameriškega urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) ne izključujejo množičnega in neselektivnega zbiranja osebnih podatkov, ki izvirajo iz EU. WP29 opozarja na svoje dolgoletno stališče, da se množični in neselektivni nadzor posameznikov v demokratični družbi nikoli ne more šteti za sorazmernega in nujno potrebnega, kot se zahteva v okviru varstva, ki ga zagotavljajo veljavne temeljne pravice. Poleg tega je ključen celovit nadzor vseh programov nadzora. WP29 ugotavlja, da obstaja težnja po zbiranju še večje količine podatkov na množični in neselektivni ravni zaradi boja proti terorizmu. Glede na pomisleke, ki jih to prinaša za varstvo temeljnih pravic do zasebnosti in varstva podatkov, WP29 pričakuje prihodnje sodbe Sodišča v zadevah, povezanih z množičnim in neselektivnim zbiranjem podatkov.

Kar zadeva pravno varstvo, WP29 pozdravlja vzpostavitev instituta varuha človekovih pravic kot novega mehanizma pravnega varstva. To lahko pomeni znatno izboljšanje pravic posameznikov iz EU v zvezi z obveščevalnimi dejavnostmi ZDA. Vendar WP29 izraža zaskrbljenost, da ta nova institucija ni dovolj neodvisna, da nima ustreznih pristojnosti za učinkovito izvajanje svojih obveznosti ter da ne zagotavlja zadovoljivega pravnega varstva v primeru nestrinjanja.

Skupni pregled

Mehanizem skupnega letnega pregleda, naveden v osnutku sklepa o ustreznosti, je ključni dejavnik za splošno verodostojnost zasebnostnega ščita, WP29 pa z veseljem pozdravlja priložnost, ki bi jo to predstavljalo za pregled sklepa o ustreznosti. Ob upoštevanju tega WP29 razume, da bodo lahko nacionalni predstavniki WP29 polno sodelovali v postopku pregleda, vendar prosi za pojasnilo glede natančnih dogovorov. O načinih (vključno s poročilom, njegovo objavo in morebitnimi posledicami, pa tudi financiranjem) se je treba dogovoriti precej pred prvim pregledom.

Sklepna ugotovitev

WP29 opaža velike izboljšave, ki jih zasebnostni ščit zagotavlja v primerjavi z razveljavljeno odločbo o varnem pristanu. Ob upoštevanju izraženih pomislekov in zahtevanih pojasnil poziva Komisijo k razrešitvi teh pomislekov, opredelitvi ustreznih rešitev in zagotovitvi zahtevanih pojasnil za izboljšanje osnutka sklepa o ustreznosti in zagotovitev, da je varstvo, ki ga zagotavlja zasebnostni ščit, v bistvu enakovredno varstvu, ki ga zagotavlja EU.

KAZALO

1. UVOD

Delovna skupina iz člena 29 (v nadaljnjem besedilu: WP29, delovna skupina) je na podlagi sodbe, ki jo je Sodišče izdalo 6. oktobra 2015 v zadevi Schrems[1], države članice Evropske unije (v nadaljnjem besedilu: EU) in druge evropske institucije pozvala, naj začnejo razprave z organi Združenih držav Amerike (v nadaljnjem besedilu: ZDA), da bi našle politične, pravne in tehnične rešitve, ki bi omogočale prenose podatkov na ozemlje ZDA ob spoštovanju temeljnih pravic.

Evropska komisija in ministrstvo za trgovino ZDA sta 2. februarja 2016 po več kot dveletnih pogajanjih dosegla politični dogovor o *novem okviru za čezatlantske izmenjave osebnih podatkov za poslovne namene: zasebnostni ščit EU–ZDA* (v nadaljnjem besedilu: zasebnostni ščit), ki naj bi nadomestil prejšnjo odločbo o varnem pristanu ZDA.

Komisija je 29. februarja 2016 objavila sporočilo[2], tj. osnutek sklepa o ustreznosti in priložena besedila, ki bodo tvorili zasebnostni ščit. WP29 je v skladu s členom 30(1)(c) Direktive 95/46/ES (v nadaljnjem besedilu: Direktiva) ocenila te dokumente, da bi izrazila svoje trenutno mnenje glede osnutka sklepa o ustreznosti, ki ga je pripravila Komisija, vključno z osnovnimi dokumenti zasebnostnega ščita. Med ocenjevanjem je razdelila delo na ocenjevanje poslovnega dela zasebnostnega ščita in analizo zaščitnih ukrepov, vzpostavljenih v zvezi z odstopanji od načel zasebnostnega ščita zaradi nacionalne varnosti, kazenskega pregona in javnih interesov.

WP29 je na podlagi sodbe v zadevi Schrems organizirala več srečanj z delegacijami vlade ZDA, predstavniki organizacij civilne družbe iz EU in ZDA ter strokovnjaki, da bi pripravila oceno posledic sodbe v zadevi Schrems. Med ocenjevanjem zasebnostnega ščita so bila organizirana dodatna srečanja z Evropsko komisijo in predstavniki vlade ZDA. Na teh srečanjih so bila podana nekatera pojasnila, ki so prav tako upoštevana v tem mnenju. WP29 poudarja, da so ta pojasnila v tej fazi zgolj neformalna in da jih ni mogoče šteti za sestavni del osnutka sklepa o ustreznosti, saj še niso zapisana.

Kljub temu pa WP29 zlasti pozdravlja zavezo, ki jo je ministrstvo za trgovino dalo na teh srečanjih, in sicer da bo sodelovalo z organi držav članic EU za varstvo podatkov glede uporabe zasebnostnega ščita ter da bo zagotovilo navodila in pravno razlago glede uporabe zasebnostnega ščita, ki bodo objavljeni na njenih spletnih mestih.

1.1 Splošne pripombe

1.1.1 Obseg ocene WP29

WP29 je najprej upoštevala veljavni okvir za varstvo podatkov v državah članicah Evropske unije, vključno s členom 8 Evropske konvencije o človekovih pravicah (v nadaljnjem besedilu: EKČP) o varstvu pravice do zasebnega in družinskega življenja, pa tudi členi 7, 8 in

[1] Zadeva C-362/14, Maximilian Schrems proti Data Protection Commissioner, z dne 6. oktobra 2015 (v nadaljnjem besedilu: zadeva Schrems).
[2] COM(2016) 117 final z dne 29. februarja 2016.

47 Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina) o varstvu pravice do zasebnega in družinskega življenja, pravice do varstva osebnih podatkov oziroma pravice do učinkovitega pravnega varstva in nepristranskega sodišča. Upoštevala je še ustrezno sodno prakso, pa tudi zahteve Direktive.

Sodišče je v zadevi Schrems dodatno opredelilo zahtevo, da tretja država zagotovi ustrezno raven varstva podatkov. Pojasnilo je, da je treba določbe Direktive razlagati „ob upoštevanju temeljnih pravic, ki jih zagotavlja Listina“[3], ter zlasti členov 7 in 8. Navedlo je tudi, da je treba izraz „ustrezna raven varstva“ razumeti tako, da „se z njim zahteva, da ta tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih svoboščin in pravic, ki je v bistvenem enaka ravni, zagotovljeni v Uniji na podlagi Direktive 95/46, razlagani ob upoštevanju Listine“[4]. Za prejšnjo odločbo o varnem pristanu tako ocenjevanje ni bilo nikoli opravljeno dovolj podrobno. Zato je WP29 ocenila osnutek sklepa o ustreznosti ob upoštevanju zahteve, da se zagotovi analiza ravni varstva temeljnih pravic in svoboščin, *ki so v bistvu enakovredne* tistim, zagotovljenim v EU. Poudarja, da to mnenje vsebuje njene glavne pomisleke, vendar se lahko zaradi omejenega časa, ki je minil od objave osnutka sklepa o ustreznosti, pozneje pojavijo dodatna vprašanja.

WP29 priznava, da je Sodišče z opredelitvijo besede „ustrezna“ v členu 25(6) Direktive kot „v bistvu enakovredna“ dodatno opredelilo ustreznost v zadevi Schrems. Sodišče je poudarilo, da je treba izraz „ustrezna raven varstva“, čeprav ne zahteva, da tretja država zagotovi raven varstva, enako tisti, ki jo zagotavlja pravni red EU, razumeti tako, da se z njim zahteva, da ta tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih pravic in svoboščin, ki je *v bistvenem enaka* ravni, zagotovljeni v Evropski uniji na podlagi Direktive, razlagani ob upoštevanju Listine.

1.1.2 Ocena poslovnega dela osnutka sklepa o ustreznosti

WP29 je že v delovnem dokumentu št. 12 z naslovom „Prenosi osebnih podatkov v tretje države: uporaba členov 25 in 26 direktive Evropske unije o varstvu podatkov“[5] pojasnila, kako uporablja temeljna načela EU glede varstva podatkov za prenose osebnih podatkov v tretje države. Poskušala je najti enakovredne zaščitne ukrepe, ki zagotavljajo raven varstva, enakovredno načelom, zagotovljenim v Direktivi, zlasti v zvezi omejitvijo namena, kakovostjo in sorazmernostjo podatkov, preglednostjo, varnostjo, pravicami do dostopa, popravka in ugovora, hrambo podatkov ter omejitvami glede prenosov tretjemu. Podobna metoda je bila uporabljena v mnenjih, ki jih je WP29 objavila med ocenjevanjem prvotne odločbe o varnem pristanu[6], pa tudi v priporočilih delovne skupine v njenem dopisu nekdanji podpredsednici in komisarki EU za pravosodje Viviane Reding, objavljenem 10. aprila 2014[7].

[3] Zadeva Schrems, točka 38.
[4] Zadeva Schrems, točka 73.
[5] Sprejela WP29 dne 24. julija 1998, glej zlasti stran 6.
[6] Glej WP62, WP32, WP27, WP23, WP21, WP19, WP15 in WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.

1.1.3 Ocena odstopanj za dostop javnih organov in njihovi zaščitni ukrepi

Ocena odstopanj za dostop javnih organov do osebnih podatkov, zajetih v zasebnostnem ščitu, je zapletena, zlasti ob upoštevanju večje ozaveščenosti organov za varstvo podatkov in splošne javnosti o programih nadzora ZDA po Snowdnovih razkritjih. Delovna skupina priznava in pozdravlja prizadevanja vlade ZDA za povečanje preglednosti programov nadzora in njihovo pripravljenost za vključitev dodatnih zaščitnih ukrepov v zasebnostni ščit. Hkrati poudarja, da mora biti vsako poseganje v temeljne pravice do zasebnega življenja in varstva podatkov mogoče upravičiti v demokratični družbi. Sodišče je kritiziralo dejstvo, da odločba o varnem pristanu ni vsebovala nobene ugotovitve v zvezi z obstojem pravil v ZDA, ki bi jih država sprejela in bi bila namenjena omejitvi kakršnega koli poseganja. Prav tako ne navaja obstoja učinkovitega pravnega varstva pred takim poseganjem[8].

WP29 je zato analizirala veljavni pravni okvir ZDA in prakse obveščevalnih agencij ZDA, kot so opisani v prilogah k osnutku sklepa, pa tudi pogoje, pod katerimi dovoljujejo kakršno koli poseganje v temeljne pravice do spoštovanja zasebnega življenja in varstva podatkov, kot so zaščitene na podlagi evropskega pravnega okvira.

Za ugotovitev, ali bi bilo kakršno koli poseganje mogoče upravičiti v demokratični družbi, je bila izvedena ocena ob upoštevanju evropske sodne prakse glede temeljnih pravic, ki določa štiri osnovna jamstva[9] za obveščevalne dejavnosti:

A. obdelava bi morala biti skladna s pravom ter temeljiti na jasnih, natančnih in dostopnih pravilih: to pomeni, da bi moral biti vsakdo, ki je primerno obveščen, sposoben predvideti, kaj se lahko zgodi z njegovimi podatki, ko se prenašajo;
B. dokazati je treba nujnost in sorazmernost v zvezi z zastavljenimi legitimnimi cilji: najti je treba ravnovesje med ciljem, zaradi katerega se zbirajo podatki in se dostopa do podatkov, ter pravicami posameznika;
C. obstajati bi moral neodvisen mehanizem nadzora, ki bi bil učinkovit in nepristranski: to je lahko sodnik ali drug neodvisni organ, če je zadostno usposobljen za izvajanje potrebnih pregledov;
D. posamezniku morajo biti na voljo učinkovita pravna sredstva: vsakdo bi moral imeti pravico, da brani svoje pravice pred neodvisnim organom.

1.2. Osnutek sklepa o ustreznosti

WP29 najprej pozdravlja dejstvo, da se lahko nov postopek za ugotavljanje ustreznosti vzpostavi v manj kot šestih mesecih po tem, ko je Sodišče razveljavilo odločbo o varnem pristanu. Glede na število prenosov podatkov, ki vsakodnevno potekajo med EU in ZDA in ki jih WP29 priznava kot ključni del gospodarstva na obeh straneh Atlantika, je čim prej potrebna pravna jasnost.

[8] Zadeva Schrems, točki 87 in 88.
[9] osnovna evropska jamstva temeljijo na sodni praksi Sodišča in ESČP in so podrobneje opisana v delovnem dokumentu WP29 št. WP237, objavljenem 13. aprila 2016.

Vendar WP29 obžaluje, da osnutek sklepa o ustreznosti, ki ga je objavila Komisija, ne vključuje celovite ocene nacionalne zakonodaje in mednarodnih obveznosti ZDA v obliki poročila o ustreznosti, kot je bila stalna praksa v preteklosti v podobnih postopkih in v skladu s členom 25 Direktive. To WP29 preprečuje, da bi izvedla popolno analizo pravnega okvira, v katerem bo deloval zasebnosti ščit. Ugotavlja na primer, da sedanji osnutek sklepa o ustreznosti ne vključuje ugotovitev o zakonodaji na področju varstva zasebnosti in podatkov, ki obstaja v ZDA na zvezni in državni ravni, vključno s sektorsko zakonodajo, niti o zakonodaji, ki dovoljuje oblike javnega dostopa, ki niso povezane z nadzorom. Prav tako ni opredeljena povezava med prenosi podatkov na podlagi zasebnostnega ščita in na podlagi drugih obstoječih ugotovitev glede ustreznosti, kot sta sporazum o evidenci podatkov o potnikih (PNR) med EU in ZDA ter sporazum o programu za sledenje financiranja terorističnih dejavnosti (TFTP).

1.2.1 Področje uporabe okvira EU za varstvo podatkov in zlasti načel Direktive 95/46/ES

WP29 opozarja, da se zakonodaja držav članic v skladu s pravnim okvirom EU za varstvo podatkov in zlasti z Direktivo (člen 4(1)) ne uporablja le za postopke obdelave, ki jih izvajajo upravljavci podatkov s sedežem na njihovem ozemlju, temveč tudi za primere, kadar upravljavci podatkov (čeprav nimajo sedeža v EU) uporabljajo opremo, ki je na ozemlju EU, zlasti za zbiranje osebnih podatkov. Zato se zakonodaja držav članic EU uporablja za kakršno koli obdelavo, ki poteka pred prenosom v ZDA, bodisi v okviru dejavnosti organizacije s sedežem v EU bodisi z uporabo opreme, ki je v EU in jo uporablja organizacija s sedežem zunaj EU. WP29 zahteva, da se to izrecno navede v osnutku sklepa o ustreznosti.

Pojasniti bi bilo treba, da bodo načela zasebnostnega ščita veljala od trenutka, ko se začnejo prenašati podatki. Poleg tega WP29 opozarja, da se za upravljavce podatkov s sedežem v EU, ki prenašajo podatke obdelovalcu podatkov v ZDA, še vedno uporablja zakonodaja EU o varstvu podatkov.

1.2.2 Pomanjkanje jasnosti dokumentov zasebnostnega ščita

Ker so načela in jamstva, ki jih zagotavlja zasebnostni ščit, določena v sklepu o ustreznosti in njegovih prilogah, je informacije težko najti, včasih pa so tudi neusklajene. To prispeva k splošnemu pomanjkanju jasnosti v zvezi z novim okvirom ter posameznikom, na katere se nanašajo osebni podatki, organizacijam in organom za varstvo podatkov otežuje dostopnost. Podobno tudi uporabljeni jezik ni dovolj jasen. Zato WP29 Komisijo poziva, naj poskrbi, da bo to jasno in razumljivo za obe strani Atlantika.

Predlaga vključitev ločene priloge, v kateri bi bili opredeljeni osnovni izrazi, ki se uporabljajo v dokumentih zasebnostnega ščita. Skupno in nedvoumno razumevanje obveznosti, uvedenih s sklepom o ustreznosti zasebnostnega ščita, je ključno za njegovo učinkovito delovanje na obeh straneh Atlantika, zaradi česar je WP29 zaskrbljena, da se bodo zaradi številnih sklicevanj in neusklajenih formulacij ter zapletenosti okvirnih dokumentov pojavile težave v zvezi z doslednostjo, razumljivostjo in jasnostjo izvajanja zasebnostnega ščita.

Še pomembneje je to, da se v dokumentih zasebnostnega ščita uporablja terminologija, ki ni skladna z besediščem, ki se običajno uporablja v EU pri obravnavanju varstva podatkov. To ni nujno težava, če je jasno, kakšna bi bila ustrezna terminologija v okviru prava EU (in prava ZDA). Vendar WP29 na žalost ugotavlja, da to ne velja, med drugim tudi za osnutek sklepa o ustreznosti. Na primer, beseda „dostop“ se v poglavju 3 osnutka sklepa o ustreznosti uporablja tako, da pomeni zbiranje osebnih podatkov namesto omogočanje nekomu, da si ogleda podatke, ki so že zbrani. Dostop do podatkov s strani podjetij in pravica posameznikov do dostopa sta dva ločena pojma, ki se ne bi smela zamenjavati.

WP29 poudarja, da bi se morala terminologija dosledno uporabljati tudi v vseh dokumentih, vključno z osnutkom sklepa o ustreznosti. Trenutno to ne velja na primer za pojma „obdelava“ in „osebni podatki“. Oba pojma sta načeloma dobro opredeljena v Prilogi II, vendar se ne uporabljata dosledno v vseh dokumentih, zaradi česar prihaja do vrzeli v varstvu[10,11].

WP29 pozdravlja dejstvo, da so opredelitve nekaterih uporabljenih izrazov vključene v dokumente, ki tvorijo zasebnostni ščit. Vendar to ne velja za številne druge ključne izraze, vključno z izrazi „posrednik“ ali „obdelovalec“, „podatki, kodirani s šifrirnim ključem“, „anonimizirani podatki“ in „posamezniki iz EU“, za katere je po mnenju WP29 zagotovljena jasna opredelitev, s katero se strinjajo ZDA in EU, da se prepreči poznejša zmeda pri upravljavcih in obdelovalcih podatkov, ki uporabljajo zasebnostni ščit, nadzornih organih ter splošni javnosti. Preprosta rešitev bi bila, da bi se pogosto zastavljenim vprašanjem o zasebnostnem ščitu dodal glosar izrazov.

WP29 opozarja tudi na zakonite razloge za obdelavo občutljivih podatkov iz dopolnilnega načela 1 (točka III.1 Priloge II) v primerih, kadar organizaciji ni treba pridobiti izrecnega soglasja (privolitve). To dopolnilno načelo 1 se lahko razume kot podrobna opredelitev zakonitih razlogov za zbiranje podatkov v EU, saj je ta seznam podoben členu 8 Direktive. WP29 bi rada spomnila, da morajo za kakršno koli obdelavo (vključno z zbiranjem in prenosom) občutljivih podatkov, za katere se uporablja pravo EU, v skladu s členom 8 Direktive obstajati zakoniti razlogi. Zasebnostnega ščita ni mogoče razlagati kot zagotavljanje drugih razlogov za tako obdelavo. Na primer, po mnenju WP29 organizacija iz ZDA na

[10] V nekaterih določbah so zgolj naštete nekatere vrste postopkov obdelave podatkov, namesto da bi se uporabljal izraz „obdelava“. Zato prihaja do vrzeli v varstvu. Na primer, v skladu z besedilom točke III.6.f Priloge II bi se načela zasebnostnega ščita uporabljala samo, če organizacija „hrani, uporablja ali razkriva“ prejete podatke (tj. ne za druge postopke, zajete z izrazom „obdelava“, kot so zbiranje, beleženje, predelava, pridobivanje, posvetovanje, brisanje). Varstvo podatkov bi se uvedlo samo za „pripravo, vzdrževanje, uporabo ali razširjanje“ osebnih podatkov (točka II.4 Priloge II). Opredelitev osebnih podatkov je omejena tudi na „prejete“ in „zapisane“ podatke. Kot nadaljnji primer načelo obvestila (točka II.1.a.iv Priloge II) navaja, da mora certificirana organizacija obvestiti posameznike o namenih, za katere „zbira in uporablja“ podatke o njih. V točki III.9.a.11 Priloge II je naveden samo „prenos“ podatkov ali „dostop“ do njih. Čeprav se zdi, da v večini takih primerov ni namen omejiti področja uporabe načel ali ustvariti vrzeli v varstvu, ta neskladna terminologija pomeni tveganje nastanka takih vrzeli. Ker je izraz „obdelava“ opredeljen v načelih, je ključno, da se uporablja dosledno za izogibanje obstoječim vrzelim. Sicer bi bilo preveč prostora za domnevno nenamerno razlago, ki bi sicer povzročila napačno razlago besedila sklepa.

[11] Opredelitev pojma „osebni podatki“, vključena v točko I.8.a Priloge II, se nanaša „podatke o znanem ali prepoznavnem posamezniku“. Vendar dopolnilno načelo navaja, da se v zvezi s podatki o človeških virih načela uporabljajo samo za „prenos podatkov, ki omogočajo identifikacijo, ali dostop do njih“. WP29 meni, da to odpira možnost za obdelavo osebnih podatkov na način, ki ni skladen niti z načeli varstva podatkov po pravu EU niti s splošno opredelitvijo osebnih podatkov v okviru zasebnostnega ščita.

podlagi delovnega prava ZDA ne more zbirati podatkov, za katere se uporablja pravo EU (glej točko III.1.a.v Priloge II). WP29 zato poudarja, da lahko kakršna koli razlaga dopolnilnega načela 1 vodi le do njegove uporabe za občutljive podatke, ki so že bili preneseni, potem ko so bili v EU zbrani na podlagi zakonitih razlogov iz člena 8 Direktive.

Nazadnje opozarja na pomanjkanje jasnosti v zvezi z vprašanjem, kdo se lahko šteje za posameznika iz EU, ki je tako upravičen do varstva na podlagi zasebnostnega ščita: vsi državljani EU ali vse osebe, ki prebivajo v EU. To je zlasti pomembno z vidika pravice do pravnega varstva, vključno z dostopom do mehanizma varuha človekovih pravic. Poleg tega bi moral sklep o ustreznosti obravnavati vprašanje, v kakšnem obsegu se bo zasebnostni ščit uporabljal tudi za državljane/prebivalce držav EGP in Švice, ki so bili v preteklosti zajeti v shemo varnega pristana.

1.2.3 Skupni pregled in zadržanje izvajanja

WP29 pozdravlja dejstvo, da sta se Evropska komisija in vlada ZDA dogovorili, da bosta redno pregledovali praktično uporabo zasebnostnega ščita. Ta skupni pregled je že več let znana praksa v skupnosti EU za varstvo podatkov, zlasti v zvezi s sporazumi o izmenjavi podatkov PNR s tretjimi državami in sporazumom o programu za sledenje financiranja terorističnih dejavnosti. WP29 pozdravlja tudi dejstvo, da lahko pri skupnih pregledih sodeluje poljubno število predstavnikov organov za varstvo podatkov.

Glede na njene izkušnje s skupnimi pregledi v zadnjih letih želi WP29 pojasniti, da pričakuje, da bo skupni pregled zasebnostnega ščita obsežnejši od skupnih pregledov sporazumov PNR in sporazuma o programu za sledenje financiranja terorističnih dejavnosti. Zlasti je zaželeno, da skupni pregled ne bi vključeval le sestankov s predstavniki agencij, organizacij in podjetij iz ZDA, temveč tudi preverjanja nekaterih elementov zasebnostnega ščita na kraju samem. Predstavniki organov za varstvo podatkov pri skupnem pregledu bi morali biti sposobni predlagati taka preverjanja na kraju samem.

WP29 meni, da skupni pregled zahteva skupno oceno ugotovitev. Doslej so bili rezultati skupnih pregledov predstavljeni v dokumentu služb Komisije, za katerega ni bila potrebna odobritev članov skupine za skupni pregled, ki se ne izvaja v okviru Komisije. Glede skupnega pregleda zasebnostnega ščita bi bila WP29 vesela, če bi bilo poročilo o ugotovitvah dejansko skupni produkt. Lahko pa bi se proučila tudi možnost izdaje ločenega poročila o skupnem pregledu organov za varstvo podatkov.

Nazadnje, kar zadeva skupni pregled, WP29 opozarja na obljubo Komisije, da bo povrnila stroške predstavnikov WP29, nastale med skupnimi pregledi. Delovna skupina predvideva, da bo to veljalo tudi za skupni pregled zasebnostnega ščita, vsekakor za razumno število predstavnikov organov za varstvo podatkov.

WP29 priporoča, da se Komisija, vlada ZDA in delovna skupina najpozneje tri mesece pred prvim skupnim pregledom zasebnostnega ščita dogovorijo o podrobnostih skupnega pregleda in jih zapišejo.

1.2.4 Pravni okvir EU v postopku revizije

Sklep o ustreznosti zasebnostnega ščita je prvi sklep o ustreznosti, ki je bil pripravljen na podlagi načelnega dogovora o besedilu splošne uredbe o varstvu podatkov. Vendar je WP29 potrdila, da zasebnostni ščit še ne izraža prihodnjega stanja. Na primer, pomembni novi pojmi, kot je pravica do prenosljivosti podatkov, in dodatne obveznosti za upravljavce podatkov, vključno s potrebo po ocenah učinka varstva podatkov ter upoštevanju načel vgrajene zasebnosti in privzete zasebnosti, niso bili vključeni v zasebnostni ščit. WP29 želi zato predlagati, da se zasebnostni ščit, tako kot kateri koli obstoječi sklepi o ustreznosti, pregleda kmalu po začetku uporabe splošne uredbe o varstvu podatkov. V končnem sklepu o ustreznosti bi bil dobrodošel izrecni sklic na ta postopek pregleda.

2. OCENA POSLOVNEGA DELA OSNUTKA SKLEPA O USTREZNOSTI

2.1 Splošne pripombe

2.1.1 Izboljšave

WP29 pozdravlja izboljšave, ki jih je prinesel zasebnostni ščit, in pripravljenost njegovih pogajalcev, da poskusijo obravnavati pomanjkljivosti varnega pristana, ki so v njem poudarjene. V primerjavi z varnim pristanom so opazne zlasti izboljšave naslednjih elementov: vključitev nekaterih ključnih opredelitev, kot so „osebni podatki“, „obdelava“ in „upravljavec“, mehanizmi, vzpostavljeni za zagotavljanje pregleda nad seznamom zasebnostnega ščita, ter zunanji in notranji pregledi skladnosti, ki so zdaj obvezni. Dosežene so tudi izboljšave načela dostopa, WP29 pa ugotavlja, da sta pravici do popravka in izbrisa zdaj zagotovljeni, kadar se podatki uporabljajo na način, ki ni skladen z načeli zasebnostnega ščita. Poleg tega je zdaj jasno, da mora posameznik prejeti potrditev, da se obdelujejo podatki v zvezi z njim, in obvestilo o obdelanih podatkih.

WP29 pozdravlja tudi okrepitev pravnih jamstev, kadar potekajo prenosi tretjemu, ter zaveze ministrstva za trgovino in zvezne komisije za trgovino (Federal Trade Commission, v nadaljnjem besedilu: FTC), da bosta uveljavljala obveznosti iz zasebnostnega ščita.

2.1.2 Uporaba zasebnostnega ščita za organizacije v vlogi obdelovalca (posrednika)

Na žalost še vedno ni jasno, v kakšnem obsegu se načela zasebnostnega ščita uporabljajo za certificirane organizacije, ki prejemajo osebne podatke iz EU zgolj zaradi obdelave (imenovane „posredniki“ ali „obdelovalci“). Čeprav določbe iz točke III.10.a Priloge II navajajo prenose podatkov certificiranim organizacijam za take namene, tj. navajajo zahtevo po sklenitvi pogodbe, v njih ni navedeno, kako se načela zasebnostnega ščita uporabljajo za obdelovalce (posrednike). To certificiranim organizacijam iz ZDA, ki prejemajo podatke zaradi obdelave, in podjetjem iz EU, ki izvajajo prenose certificiranim organizacijam, ki nastopajo v vlogi obdelovalcev podatkov, pa tudi posameznikom, katerih podatki se obdelujejo, prinaša negotovost. Zaradi tega bo težko ugotoviti, katere naloge se dejansko nanašajo na organizacije v ščitu, ki v vlogi obdelovalcev obdelujejo osebne podatke, prejete iz EU. Zato je vsekakor potrebno pojasnilo.

Upoštevati je treba, da več obveznosti, vključenih v načela, ni primernih za obdelovalce podatkov, saj je vedno upravljavec podatkov tisti, ki določi namene in načine obdelave podatkov (glej opredelitev izraza „upravljavec“ v točki I.8.c Priloge II). Zato so lahko nekatere obveznosti, vključene v načela, če se uporabljajo za organizacijo v vlogi posrednika, v nasprotju s pogodbo o obdelavi podatkov, ki se zahteva v skladu s pravom EU (pogodba, navedena v točki III.10.a Priloge II). Na primer, pogodba o obdelavi podatkov običajno obdelovalca (posrednika) ne pooblašča za prenos podatkov tretjemu upravljavcu, niti v okoliščinah, navedenih v točki II.3.a Priloge II. Prenosi tretjim posrednikom bi morali biti dovoljeni samo po predhodni odobritvi upravljavca podatkov. Poleg tega obdelovalec (posrednik) v skladu z zahtevami prava EU posameznikom ne more zagotoviti celotnega obvestila, kot predvideva načelo obvestila (točka II.1 Priloge II), ker ta organizacija na primer ne določa namenov obdelave.

Zato je treba v načelnih nujno pojasniti, da v primeru takega protislovja prevladajo določbe pogodbe o obdelavi podatkov in zlasti navodila organizacije, ki prenaša podatke iz EU. Brez takega pojasnila bi se lahko načela razlagala in uporablja na način, ki posredniku v ščitu ponuja preveč možnosti nadzora, s čimer bi bil izvoznik podatkov iz EU izpostavljen tveganju kršitve svojih obveznosti kot upravljavec podatkov v skladu s pravom EU na področju varstva podatkov, ki se zanj uporablja pri prenosu podatkov organizaciji v ščitu, ki nastopa v vlogi posrednika. Poleg tega to pomanjkanje jasnosti daje vtis, da lahko obdelovalec po svoji presoji ponovno uporabi podatke.

Določiti bi bilo treba tudi posebna pravila za primere, kadar organizacija nastopa v vlogi obdelovalca podatkov (posrednika), za zagotavljanje, da ta organizacija upošteva navodila upravljavca podatkov. Pojasniti bi bilo treba, da se organizacije v ZDA, ki prejemajo podatke zgolj zaradi obdelave, ne morejo odločiti, da bodo obdelovale podatke v svojem imenu. Ker ni posebnih pravil, ki bi se uporabljala za organizacije v vlogi obdelovalca, je težko ugotoviti, na podlagi katerih pravil bi se lahko obdelovalec (posrednik) samocertificiral.

2.1.3 Omejitve dolžnosti spoštovanja načel

Točka I.5 Priloge II med drugim določa izjeme od načel, kadar se podatki, zajeti z zasebnostnim ščitom, uporabljajo zaradi nacionalne varnosti[12], javnega interesa, kazenskega pregona ali na podlagi zakona, vladnega podzakonskega akta ali sodne prakse, kar ustvarja nasprotujoče si obveznosti ali izrecna pooblastila. WP29 brez celovitega poznavanja prava ZDA na zvezni in državni ravni težko oceni obseg te izjeme in prouči, ali so te omejitve upravičene v demokratični družbi. Evropska komisija bi morala v svoj osnutek sklepa o ustreznosti vključiti tudi analizo ravni varstva, kadar bi se uporabljale te izjeme. WP29 Komisijo poziva, naj zagotovi, da bo EU obveščena o kakršnem koli zakonu ali vladnem podzakonskem aktu, ki bi vplival na spoštovanje načel, veljavnih bodisi zdaj bodisi ob začetku veljavnosti novega zakona ali podzakonskega akta v ZDA.

[12] Glej poglavje 3 za več pripomb o uporabi osebnih podatkov, zajetih v zasebnostnem ščitu, za namene nacionalne varnosti in poglavje 4 za namene kazenskega pregona.

2.1.4 Neobstoj načela omejitve hrambe podatkov

Načelo omejitve hrambe podatkov (člen 6(1)(e) Direktive) je temeljno načelo prava EU na področju varstva podatkov, ki določa, da je treba osebne podatke hraniti le toliko časa, kot je potrebno, da se doseže namen, za katerega so bili podatki zbrani ali za katerega so bili nadalje obdelani.

Vendar WP29 v dokumentih, ki tvorijo zasebnostni ščit, ne najde nobenega sklicevanja na potrebo, da upravljavci podatki zagotovijo, da se podatki po tem, ko je dosežen namen, za katerega so bili zbrani ali nadalje obdelani, izbrišejo. Zato načela, kot se zdi, certificiranim organizacijam ne nalagajo omejitve glede obdobja hrambe podatkov, ki bi bilo primerljivo z obdobjem, določenim z načelom omejitve hrambe podatkov v skladu s pravom EU.

Za besedilo načela neokrnjenosti podatkov in omejitve namena (točka II.5 Priloge II) se nikakor ne more šteti, da organizaciji v vlogi upravljavca nalaga obveznost, da izbriše podatke, potem ko niso več potrebni za namene, za katere so bili zbrani ali nadalje obdelani, ali da organizaciji v vlogi obdelovalca nalaga obveznost, da izbriše podatke po prenehanju sporazuma o opravljanju storitev.

Delovna skupina poudarja, da neobstoj določb o uvedbi omejitve hrambe podatkov na podlagi zasebnostnega ščita organizacijam omogoča, da hranijo podatke, dokler želijo, tudi po tem, ko zapustijo zasebnostni ščit, kar ni v skladu z osnovnim načelom omejitve hrambe podatkov.

2.1.5 Pomanjkanje jamstev za samodejne odločitve, kar ima za posameznike pravne učinke ali znatno vpliva nanje

Zasebnostni ščit ne zagotavlja pravnih jamstev, če se za posameznike sprejme odločitev, ki ima zanje pravne učinke ali znatno vpliva nanje in ki temelji zgolj na samodejni obdelavi podatkov, namenjeni ovrednotenju nekaterih osebnih vidikov v zvezi s temi posamezniki, kot so njihova uspešnost pri delu, kreditna sposobnost, zanesljivost, ravnanje itd.

WP29 je potrebo po zagotovitvi pravnih jamstev za samodejne odločitve (ki imajo za posameznika pravne učinke ali znatno vplivajo nanj**),** da bi zagotovila ustrezno raven varstva, poudarila že v delovnem dokumentu št. 12.

Ta potreba je še toliko bolj pomembna, ker nenehno razvijajoče se nove tehnologije večjemu številu podjetij omogočajo, da razmislijo o možnosti izvajanja sistemov samodejnega odločanja, kar lahko oslabi položaj posameznikov, ki se ne morejo pritožiti zoper take računalniško sprejete odločitve. Če odločitve, sprejete izključno z uporabo navedenih avtomatiziranih sistemov, vplivajo na pravni položaj posameznikov ali znatno vplivajo nanje (na primer z njihovo uvrstitvijo na črne sezname in s tem odvzemom njihovih pravic), je treba nujno zagotoviti zadostne zaščitne ukrepe, vključno s pravico do seznanitve z načinom delovanja in do zahteve za ponovno proučitev na neavtomatizirani podlagi.

2.1.6 Vmesno obdobje za obstoječa trgovinska razmerja

Zasebnostni ščit predvideva, da načela začnejo veljati takoj po certificiranju. Vendar bodo morale organizacije, ki se bodo certificirale v prvih dveh mesecih po datumu začetka veljavnosti okvira zasebnostnega ščita, kakršna koli obstoječa trgovinska razmerje s tretjimi strankami čim prej uskladiti z načelom odgovornosti za prenos tretjemu. Vsekakor bi morale to storiti najpozneje v devetih mesecev od datuma, ko se certificirajo v okviru zasebnostnega ščita.

To pomeni, da je treba veljavne pogodbe v potrebnem obsegu uskladiti z načeli v dveh do devetih mesecih po certificiranju. V tem vmesnem obdobju zadostujeta obvestilo in možnost izbire. WP29 vztraja pri dejstvu, da se lahko prenosi na podlagi zasebnostnega ščita začnejo šele, ko organizacija v celoti izpolnjuje vse zahteve ščita. Za možnost pošiljanja podatkov v vmesnem obdobju, ne da bi prejemnik v celoti spoštoval načela ščita, se ne more šteti, da izpolnjuje pogoje za zakoniti prenos, in zato ni sprejemljiva.

2.2 Posebne pripombe

2.2.1 Preglednost

a) Splošne opombe glede obvestila

WP29 pozdravlja celovitejše in podrobnejše zahteve, določene v okviru načela obvestila, zlasti zahtevo, da mora obvestilo vsebovati povezavo do spletnega naslova ali spletni naslov seznama zasebnostnega ščita ter se sklicevati na pravico posameznikov do dostopa, pa tudi mehanizme za alternativno reševanje sporov[13]. Vendar predlaga večjo jasnost zahtev glede drugih zajetih pravic (do popravka, izbrisa, če so podatki netočni ali obdelani v nasprotju z zakonom).

Dokumenti, ki tvorijo zasebnostni ščit, vzbujajo pomisleke glede roka, kdaj mora organizacija v zasebnostnem ščitu posamezniku poslati obvestilo. V točki II.1.b Priloge II je navedeno, da „[mora biti] [t]o obvestilo [...] jasno in nedvoumno, ko posameznika prvič prosi za zagotovitev osebnih podatkov ali kakor hitro je izvedljivo za tem, v vsakem primeru pa pred uporabo teh podatkov za namene, ki niso tisti, za katere jih je prvotno zbrala in obdelala pošiljajoča organizacija, ali pred prvim razkrijem tretji stranki“. WP29 meni, da v številnih primerih organizacija v ščitu iz ZDA ne bo neposredno zbirala podatkov od posameznika, na katerega se nanašajo osebni podatki, zato bi moralo biti sporočilo poslano v trenutku, ko organizacija v ščitu zabeleži podatke.

WP29 ugotavlja, da bi bilo treba pri prvem letnem pregledu zasebnostnega ščita oceniti dejansko izvajanje zahtev glede načela obvestila in politike varovanja zasebnosti.

b) Javna dostopnost politike varovanja zasebnosti

[13] V točki II.1 Priloge II se WP29 sklicuje tudi na drugo priporočilo Komisije iz Sporočila COM(2103) 847, pa tudi na dopis WP29 podpredsednici Redingovi z dne 10. aprila 2014, zlasti na točko 4 pod naslovom „Preglednost“.

WP29 pozdravlja dejstvo, da je zdaj jasno, da bo zvezno ministrstvo za trgovino preverjalo, ali so podjetja, ki imajo javno spletno mesto, na tem spletnem mestu objavila svojo politiko varovanja zasebnosti, ali, če nimajo javnega spletnega mesta, kje je politika varovanja zasebnosti javno dostopna[14].

c) Objava pogojev glede varstva zasebnosti iz pogodb z obdelovalci

Zasebnostni ščit poleg pogojev, pod katerimi lahko organizacije v zasebnostnem ščitu prenašajo podatke obdelovalcu (posredniku), določa tudi obveznost samocertificiranih organizacij, da „na zahtevo Ministrstvu zagotovi[jo] povzetek ali reprezentativni izvod ustreznih določb o zasebnosti iz svoje pogodbe s tem posrednikom“ (glej točko II.3.b.v Priloge II). Delovna skupina pozdravlja to zahtevo po preglednosti za ministrstvo za trgovino.

2.2.2 Možnost izbire

Zasebnostni ščit določa pravico do zavrnitve razkritja osebnih podatkov tretji stranki ali do uporabe osebnih podatkov za bistveno drugačen namen[15] (točka III.2 Priloge II). Poleg tega posamezniki uživajo pravico, da lahko kadar koli „zavrnejo“ uporabo osebnih podatkov za neposredno trženje (točka III.12.1 Priloge II)[16].

Razen v zvezi z nameni neposrednega trženja ni navedenih podrobnosti o načinu in času, ko je ta zavrnitev mogoča. WP29 meni, da zgolj sklicevanje na obstoj te pravice v politiki varovanja zasebnosti ne more zadostovati, temveč bi morala biti *pred* razkritjem ali ponovno uporabo osebnih podatkov na voljo *posameznikom prilagojena* možnost uveljavljanja te pravice.

Poleg tega WP29 poudarja, da bi morala biti v okviru zasebnostnega ščita zagotovljena splošna pravica do ugovora (na podlagi nujnih razlogov, povezanih s posebnim položajem posameznika, na katerega se nanašajo osebni podatki), ki se razume kot pravica do zahteve po prekinitvi obdelave podatkov posameznika, kadar ima ta zakonite in nujne razloge, povezane z njegovim posebnim položajem[17]. WP29 zelo priporoča, da se v osnutku sklepa o ustreznosti pojasni, da bi morala pravica do ugovora obstajati v katerem koli danem trenutku in da ta ugovor ni omejen na uporabo podatkov za neposredno trženje[18].

WP29 se boji, da bo neopredelitev „bistveno drugačnega“ namena povzročila zmedo in pravno negotovost. Pojasniti bi bilo treba, da se načelo možnosti izbire nikakor ne more uporabljati za izogibanje načelu omejitve namena[19]. Možnost izbire bi se morala uporabljati samo v primerih, kadar je namen bistveno drugačen, vendar še vedno združljiv, saj je

[14] Glej prvo priporočilo Evropske komisije v njenem Sporočilu COM(2013) 847 in dopis WP29 podpredsednici Redingovi z dne 10. aprila 2014, zlasti točko 3 pod naslovom „Preglednost“.
[15] Dopolnilno načelo 14.c.I določa pravico do umika iz kliničnega poskusa, ki se lahko razlaga kot pravica do nasprotovanja ali umika soglasja.
[16] To je podobno pravici, zagotovljeni s shemo varnega pristana (F.A.Q. 12), v zvezi s tem pa ni bila izvedena nobena sprememba.

[18] Glej dopis WP29 podpredsednici Redingovi, besedilo pod naslovom „Možnost izbire“.
[19] Konkreten primer nadaljnje nezdružljive obdelave, dovoljene v skladu z načelom možnosti izbire, je naveden pri dodatnem načelu 9.b.i (glej pripombo WP29 glede tega pod točko, ki se nanaša na „podatke o človeških virih“).

obdelava za nezdružljiv namen prepovedana (točka II.5.a Priloge II). Pojasniti je treba, da pravica do zavrnitve organizaciji ne sme omogočati, da uporablja podatke za nezdružljiv namen. Zato predlaga uskladitev povezanega besedila z uporabo enotnega in opredeljenega besedila (npr. „bistveno drugačen, vendar kljub temu združljiv namen“).

Koristno bi bilo pojasnilo, kdaj sprejeta odločitev za obdelavo podatkov za drug namen ali za razkritje podatkov spada na področje prava EU. V tem primeru se neposredno uporabljajo običajni pravni pogoji EU v zvezi s to obdelavo (kot so prepoved obdelave za nezdružljive namene, zagotovitev zakonitega razloga za obdelavo in potreba po obveščanju posameznika), tudi za organizacije v ZDA, ki spadajo na področje uporabe prava EU. V praksi to pomeni, da bo moral izvoznik iz EU, ki bo sprejel tako odločitev, zagotoviti preglednost in zakonitost obdelave v skladu s pravom EU. Zato se bo načelo možnosti izbire uporabljalo samo, če bo odločitev sprejela izključno organizacija iz ZDA, ki je vključena v ščit in za katero se ne uporablja pravo EU.

2.2.3 Prenosi tretjemu

a) Področje uporabe

WP29 je zaskrbljena glede primerov, ko prenosi osebnih podatkov tretjemu potekajo od certificirane organizacije v zasebnostnem ščitu iz ZDA do prejemnika v tretji državi.

Ščit se ne bi smel obravnavati le kot orodje za prenos podatkov EU iz EU v ZDA, saj se bo uporabljal tudi kot orodje za prenos podatkov iz ZDA v tretje države. Določbe o prenosih tretjemu so zato pomemben element ščita, ki bi moral zagotavljati zadostna jamstva in ustrezno raven varstva, kadar se podatki prenašajo tretjemu zunaj ZDA. Posebno vprašanje je povezano z nacionalno varnostjo in kazenskim pregonom.

Načelo zasebnostnega ščita glede odgovornosti za prenos tretjemu ni omejeno na upravljavce podatkov, obdelovalce ali posrednike v ZDA, ki so prejemniki. Zato bi lahko prenosi v tretjo državo potekali na podlagi zasebnostnega ščita tudi, če ima tretja država vzpostavljene zakone, ki zagotavljajo javni dostop do osebnih podatkov, na primer zaradi nadzora. Zato pri podatkih EU obstaja tveganje neupravičenih posegov v varstvo temeljnih pravic.

Vsaka organizacija v zasebnostnem ščitu bi morala biti pri vsakem prenosu v tretjo državo obvezana, da pred prenosom oceni obvezne zahteve nacionalne zakonodaje tretje države, ki se uporablja za uvoznika podatkov. Če je ugotovljen znaten negativni učinek na jamstva, obveznosti in raven varstva, ki jo zagotavlja zasebnostni ščit, organizacija v zasebnostnem ščitu iz ZDA, ki nastopa v vlogi obdelovalca (posrednika), pred kakršnim koli prenosom tretjemu o tem nemudoma obvesti upravljavca podatkov iz EU. V teh primerih je izvoznik podatkov upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe. Kadar obstaja tako tveganje znatnega negativnega učinka, organizaciji v zasebnostnem ščitu v vlogi upravljavca ne bi smel biti dovoljen prenos podatkov tretjemu, saj bi to ogrozilo njeno obveznost zagotavljanja enake ravni varstva, kot jo zagotavljajo načela v primeru prenosov tretjemu (glej točko II.3.a Priloge II).

Podobno bi moral zasebnostni ščit organizacijo iz ZDA, ki je vključena v zasebnostni ščit in nastopa v vlogi obdelovalca (posrednika), zavezovati, da v primeru spremembe zakonodaje tretje države, ki bo verjetno znatno negativno vplivala na jamstva, obveznosti in raven varstva, ki jo zagotavlja zasebnostni ščit, to spremembo izvozniku podatkov sporoči takoj, ko zanjo izve, izvoznik podatkov pa je v tem primeru upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe. Tako organizaciji v ščitu, ki nastopa v vlogi upravljavca, v takem primeru ne bi smel biti dovoljen prenos podatkov tretjemu, saj mora zagotavljati enako raven varstva, kot jo zagotavljajo načela (glej točko II.3.a Priloge II).

WP29 opozarja na svoje stališče, da bi se moral prenos, če je upravljavec podatkov iz EU seznanjen s prenosom tretji stranki zunaj ZDA že pred prenosom v ZDA ali če je upravljavec podatkov iz EU soodgovoren za odločitev, da se dovoli prenos tretjemu, šteti za neposreden prenos iz EU v tretjo državo zunaj ZDA. To pomeni, da se za prenos namesto načela zasebnostnega ščita glede prenosa tretjemu uporabljata člena 25 in 26 Direktive.

b) Prenosi z organizacije v zasebnostnem ščitu na tretjega upravljavca

WP29 pozdravlja obveznost sklenitve pogodb (točka II.3.a Priloge II) za zagotovitev, da tretji upravljavec zagotovi najmanj enako raven varstva zasebnosti, kot jo zahtevajo načela zasebnostnega ščita. Namen je še naprej zagotavljati ustrezno varstvo osebnih podatkov, tudi po njihovem prenosu tretjemu. Vendar ima WP29 nekaj pripomb glede predlaganih pogojev.

Nesklicevanje na načelo omejitve namena

WP29 priporoča tudi vključitev jasnega sklicevanja na načelo omejitve namena (točka II.5 Priloge II) v pogoje za prenose tretjemu upravljavcu (točka II.3.a Priloge II). S tem bi se pojasnilo, da prenosi tretjemu niso dovoljeni, če tretji upravljavec obdeluje podatke za nezdružljiv namen.

Izjema od potrebe po pogodbi za prenose med upravljavci znotraj skupine

Izjema od potrebe po pogodbi je predvidena za prenose med upravljavci znotraj skupine. V takem scenariju načela navajajo, da bi lahko neprekinjeno varstvo zagotavljala zavezujoča poslovna pravila ali „drugi instrumenti znotraj skupine (npr. programi skladnosti in nadzora)“ (točka III.10.b Priloge II). WP29 meni, da sklicevanje na „druge instrumente znotraj skupine“ ne zagotavlja pravno zavezujočih obveznosti drugih članov skupine. Ker WP29 in zakonodaja EU[20] na splošno podpirata zavezujoče obveznosti za zagotovitev okvira prenosov znotraj skupine, je pomembno, da se prepreči uporaba zasebnostnega ščita, pri kateri gre za izogibanje taki zahtevi. WP29 opozarja, da je treba prenose tretjemu iz ZDA v tretje države, ki so načrtovani še pred prenosom v ZDA ali so predmet skupnega upravljanja z upravljavcem podatkov iz EU[21], šteti za neposredne prenose iz EU v tretjo državo zunaj ZDA. Za prenos se zato uporabljata člena 25 in 26 Direktive.

[20] Potreba po zavezujočih in izvršljivih obveznostih je poudarjena tudi v splošni uredbi o varstvu podatkov, ne glede na uporabljeno orodje (zavezujoča poslovna pravila, pogodbene klavzule, kodeksi ravnanja ali certifikacija).
[21] Na primer za podatke o človeških virih.

c) Prenosi z organizacije v zasebnostnem ščitu na tretjega obdelovalca (posrednika)

WP29 pozdravlja dejstvo, da je pogodba za prenose tretjemu zdaj obvezna za subjekte prejemnike v vlogi obdelovalcev (posrednikov), ne glede na to, ali sodelujejo v zasebnostnem ščitu ali imajo koristi od druge rešitve iz sklepa o ustreznosti. Pozdravlja tudi dodatne zaščitne ukrepe, ki zagotavljajo okvir za te prenose tretjemu (točke II.3.a.i, II.3.a.iii, II.3.a.iv, II.3.a.v in II.7.d Priloge II). Zadnja točka (točka II.7.d Priloge II) se nanaša na obveznost ohranitve odgovornosti, ko se podatki razkrijejo posredniku. Vendar se zdi, da to jamstvo ne bi veljalo, če se organizacija odloči, da bo sodelovala z organom za varstvo podatkov (glej na koncu točko II.5.a Priloge II). WP29 ne razume razloga za tako izjemo in meni, da bi morala odgovornost veljati tudi v tem primeru.

Nesklicevanje na načelo omejitve namena

WP29 opozarja, da načelo odgovornosti za prenos tretjemu (točka II.3 Priloge II) pojasnjuje, da se lahko osebni podatki prenašajo tretji stranki v vlogi posrednika samo za omejene in določene namene, vendar ne navaja izrecno, da morajo biti ti omejeni in določeni nameni skladni s prvotnimi nameni, za katere so bili podatki zbrani, in navodili upravljavca. V zvezi s tem je potrebna večja jasnost. WP29 zato predlaga, da se zagotovi, da sklep o ustreznosti zagotavlja več podrobnosti, na primer z dodajanjem jasnega sklicevanja na načelo omejitve namena (točka II.5 Priloge II), v skladu s katerim podatkov ni dovoljeno obdelovati (niti razkriti) za nezdružljive namene v okviru načela prenosa tretjemu (poleg načela zavrnitve).

Potreba po več dodatnih obveznostih za organizacije v zasebnostnem ščitu, ki nastopajo v vlogi obdelovalca (posrednika), za prenos podatkov drugemu obdelovalcu (posredniku).

Neobstoj jasnih pravil, kadar organizacija v zasebnostnem ščitu deluje kot posrednik (tj. v imenu upravljavca iz EU), pomeni vrzel in lahko upravljavcu iz EU preprečuje ohranjanje nadzora. Organizacija v ščitu, ki prejema podatke kot posrednik upravljavca iz EU, mora upoštevati njegova navodila. To bi moralo biti izrecno navedeno v načelih, s čimer bi se zagotovilo, da nespoštovanje navedenih navodil ne bo privedlo do kršitve pogodbe (točka III.10.a.ii Priloge II), pa tudi načel zasebnostnega ščita.

Možnost, da organizacija v ščitu, ki nastopa v vlogi posrednika, pozneje prenese podatke tretjemu posredniku, mora biti za upravljavca pregledna, pri čemer je zanjo potrebna predhodna odobritev. Zato bi moralo biti jasno navedeno, da je v pogodbi, ki jo posrednik podpiše z upravljavcem iz EU (navedena v F.A.Q 10 kot „pogodba iz člena 17“), določeno, ali je dovoljen prenos tretjemu[22].

Veljavni pogoji, ki se uporabljajo za prenos posredniku, temeljijo na predpostavki, da organizacija v zasebnostnem ščitu nastopa v vlogi upravljavca in lahko zato sama odloča o morebitnem posredovanju tretjega posrednika. Vendar to ne bi smelo biti mogoče, kadar organizacija v ščitu nastopa v vlogi posrednika, saj bi bile sicer upravljavcu iz EU odvzete njegove možnosti nadzora.

[22] Glej dopis WP29 podpredsednici Redingovi z dne 10. aprila 2014, točka 4 pod naslovom Prenos tretjemu.

Zadevne določbe o zasebnosti v pogodbi, sklenjeni s tretjim posrednikom, morajo biti na voljo upravljavcu in zagotavljati vsaj enako raven varstva, kot jo zagotavlja pogodba, podpisana z upravljavcem.

2.2.4 Neokrnjenost podatkov in omejitev namena

a) Sorazmernost

Glede manj pomembne točke se WP29 sklicuje na svoj dopis podpredsednici Redingovi, v katerem je zapisala, da „obdelava osebnih podatkov, čeprav ob strogem upoštevanju obvestila in možnosti izbire, ne more biti sorazmerna, kar zadeva interese, pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ali družbe“. Načelo sorazmernosti ali razumnosti je treba spoštovati v vseh fazah obdelave ter bi se moralo uporabljati poleg načel obvestila in možnosti izbire“[23].

V zasebnostnem ščitu (točka II.5.a Priloge II) je navedeno, da morajo biti podatki omejeni na tisto, kar je pomembno za obdelavo. WP29 bi raje videla, da bi se to besedilo v končnem sklepu o ustreznosti spremenilo, saj zgolj dejstvo, da so podatki pomembni za obdelavo, ne zadostuje za sorazmernost obdelave. Za spoštovanje načela sorazmernosti bi morala biti obdelava omejena na podatke, ki so nujni za zadevno obdelavo.

b) Točnost

Načelo neokrnjenosti podatkov in omejitve namena (točka II.5 Priloge II) navaja tudi: „V obsegu, potrebnem za ta namen, mora organizacija z ustreznimi ukrepi zagotoviti, da so podatki zanesljivi za nameravano uporabo, točni, popolni in trenutni“. WP29 ugotavlja, da je to besedilo povsem enako besedilu, ki se uporablja v ureditvi varnega pristana. Poleg tega ni prepričana, da bi moralo biti vključeno besedilo „v obsegu, potrebnem za te namene“, saj točnost podatkov po njenem mnenju ne bi smela biti odvisna od namena obdelave. Zato bi raje videla, da končni sklep o ustreznosti ne bi vseboval te povezave.

c) Omejitev namena

Kadar upravljavec podatkov s sedežem v EU prenaša osebne podatke organizaciji v ZDA, bi moral izvoznik podatkov organizacijo v ZDA izrecno obvestiti o namenih, za katere so bili podatki prvotno zbrani. To je bistveno za ugotovitev, ali se po prenosu pride spremeni namen, kar bi sprožilo načeli obvestila in možnosti izbire ter prispevalo k delitvi tveganja in odgovornosti.

Načelo neokrnjenosti podatkov in omejitve namena (točka II.5 Priloge II) navaja, da organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdružljiv z nameni, za katere so bili podatki zbrani ali jih je posameznik pozneje odobril. Vendar načelo možnosti izbire (točka II.2 Priloge II) predvideva zavrnitev „uporabe“ občutljivih podatkov (tj. osebnih podatkov, ki določajo zdravniško in zdravstveno stanje, rasno in etnično pripadnost, politična,

[23] Glej dopis WP29 podpredsednici Redingovi z dne 10. aprila 2014, str. 8.

verska ali filozofska prepričanja, sindikalno članstvo, ali podatkov o spolnem življenju posameznika, pa tudi podatkov v zvezi s kazenskimi evidencami) za namene, ki se bistveno razlikujejo od namenov, za katere so bili prvotno zbrani ali jih je posameznik pozneje odobril. Ta privolitev se ne zahteva v primerih, navedenih v dopolnilnem načelu 1.a (točka III.1.a Priloge II). Kar zadeva neobčutljive osebne podatke, je predviden sistem zavrnitve.

WP29 ugotavlja, da je področje uporabe načela omejitve namena pri načelih obvestila, možnosti izbire ter neokrnjenosti podatkov in omejitve namena različno. Dejansko se izraza „nezdružljiv namen“ in „bistveno drugačen namen“ uporabljata v enakem besedilu brez jasne opredelitve obeh pojmov[24].

WP29 ima resne pomisleke glede dejstva, da bi lahko taka neskladnost povzročila velike težave pri usklajevanju načela neokrnjenosti podatkov in omejitve namena (točka II.5 Priloge II) z načelom možnosti izbire (točka II.2 Priloge II), saj eno načelo navaja, da se podatki ne smejo obdelovati na način, ki je nezdružljiv z nameni, za katere so bili prvotno zbrani, medtem ko drugo načelo predvideva mehanizem zavrnitve, če se podatki obdelujejo za namen, ki je bistveno drugačen od prvotnega namena.

Tako se lahko načelo možnosti izbire razlaga kot dovoljenje za nadaljnjo nezdružljivo obdelavo[25]. Po mnenju WP29 je treba pojasniti, da organizaciji ni dovoljeno obdelovati podatkov za bistveno drugačen namen, ki je po načelu omejitve namena nezdružljiv. Povedano drugače, moralo bi biti jasno, da načelo možnosti izbire ni izjema od načela omejitve namena.

Vsekakor bi se morali tudi v primeru, če se nadaljnja obdelava lahko šteje za združljivo, prav tako uporabljati načeli obvestila in možnosti izbire.

2.2.5 Izjeme za novinarsko področje

Izjeme za novinarsko področje glede obdelave osebnih podatkov so zajete v dopolnilnem načelu 2 (točka III.2 Priloge II). Razume se, da te določbe izražajo ustavno varstvo ZDA glede svobode govora. Zato je v dokumentih zasebnostnega ščita navedeno, da „za osebne podatke, najdene v predhodno objavljenem gradivu, razširjenem iz medijskih arhivov, ne veljajo zahteve načel zasebnostnega ščita“ (točka III.2.b Priloge II). Zdi se, da ta izjema vključuje morebitno nadaljnjo obdelavo s strani upravljavca ali obdelovalca podatkov, kar pomeni, da ni omejena na nadaljnjo obdelavo za novinarske namene. Kot je bilo že navedeno v dopisu podpredsednici Redingovi z dne 10. aprila 2014, bi WP29 raje izbrala bolj omejen

[24] WP29 ugotavlja, da se uporabljajo tudi nekateri drugi izrazi: „uporaba, ki ni skladna z“ (točka III.14.b.ii Priloge II), „uporaba za drugačne namene“ (točka III.9.B.i Priloge II), „uporaba za namene, ki niso tisti, za katere jih je prvotno zbrala“ (točka II.1.b Priloge II). Ta nejasnost bi lahko privedla do pomanjkanja zadostnih jamstev, kar zadeva načelo omejitve namena.

[25] Glej tudi pripombo pod načelom možnosti izbire. WP29 meni, da dejstvo, da se pravila za prenos tretjemu (točka II.3 Priloge II) nanašajo samo na načelo možnosti izbire, ne pa tudi na načelo omejitve namena, povečuje tveganje takega razumevanja.

pristop k izjemam za novinarsko področje, ki bi bil bolj usklajen z načelom, ki se uporablja v EU, pa tudi s pravico do izbrisa s seznama na podlagi sodbe v zadevi Google Spain[26].

2.2.5 Pravica posameznikov, na katere se nanašajo osebni podatki, do dostopa, popravka in izbrisa

V skladu z zasebnostnim ščitom imajo posamezniki pravico, da pridobijo *potrditev*, ali organizacija obdeluje njihove podatke, in da se jim taki podatki *sporočijo* (točka III.8.a.i Priloge II). Vendar je obveznost organizacij, da odgovarjajo na zahteve posameznikov v zvezi z nameni obdelave, kategorijami zadevnih osebnih podatkov in prejemniki ali kategorijami prejemnikov, ki se jim osebni podatki razkrivajo, precej šibka. WP29 meni, da bi morale biti podatki, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, navedeni v glavnem besedilu in ne samo v opombi ter oblikovani kot jasna obveznost (povezava s točko III.8.a.i.1 Priloge II).

V skladu z dopolnilnim načelom 8 „je treba dostop zagotoviti samo do osebnih podatkov, ki jih hrani organizacija“ (točka III.8.d.ii Priloge II). To pravilo se ne bi smelo razlagati omejevalno v smislu, da je treba načeloma zagotoviti dostop do podatkov, ki jih organizacija kakor koli obdeluje in ne samo hrani. Zato je treba zaradi učinkovitosti pravice do dostopa pojasniti, da „hrani“ pomeni „obdeluje“ v smislu opredelitve iz točke I.8.b Priloge II. Uporabo tega pravila bi bilo treba pozorno proučiti med skupnim pregledom zasebnostnega ščita.

Še vedno obstajajo pomisleki glede seznama izjem iz točke III.8.e.(i) Priloge II, ki je podoben seznamu iz F.A.Q. 8 varnostnega pristana in ki lahko spremeni ravnovesje v korist interesov organizacije. V tem smislu posameznikom ne bo odobren dostop do njihovih osebnih podatkov zaradi naslednjih razlogov: „kršitve poklicnih privilegijev ali obveznosti“ (točka III.8.e.3 Priloge II), „vplivanja na preiskave o varnosti zaposlenih in pritožbene postopke ali v zvezi z načrtovanjem zamenjav zaposlenih in z reorganizacijo podjetja“ (točka III.8.e.4 Priloge II) ter „vplivanja na zaupnost, ki je potrebna v zvezi s spremljanjem, inšpekcijo ali nadzornimi funkcijami, povezanimi s smotrnim upravljanjem, ali v zvezi s prihodnjimi ali tekočimi pogajanji, ki vključujejo organizacijo“ (točka III.8.e.5 Priloge II). Te razloge je treba razlagati ob upoštevanju splošne izjeme glede zaupne tržne informacije iz točke III.8.c Priloge II. Zato posameznik v navedenih primerih nikoli ne bo imel dostopa do svojih podatkov, pri čemer ne bo vzpostavljeno ravnovesje med pravicami in interesi posameznika in organizacije, da bi se dosegla rešitev glede zahteve po dostopu.

WP29 poudarja, da je pravica do dostopa do lastnih podatkov posameznikom zagotovljena s členom 8(2) Listine. Čeprav to ni absolutna pravica, je bistvena za pravico do varstva osebnih podatkov, saj olajšuje uveljavljanje drugih pravic posameznika, na katerega se nanašajo osebni podatki, kot sta pravici do popravka in izbrisa.

[26] Sodba v zadevi C-131/12 – Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu, 13. maj 2014.

Kar zadeva pravici do popravka in izbrisa, WP29 pozdravlja velik napredek, ki so ga načela zasebnostnega ščita prinesla v primerjavi z načeli varnega pristana, saj zagotavljajo, da se zadevne pravice ne dodelijo le, kadar so podatki netočni, temveč tudi, kadar so obdelani ob kršitvi načel (točka II.6 Priloge II).

2.2.6 Pritožbeni mehanizem, izvrševanje in odgovornost (mehanizem pravnega varstva)

a) Učinkovito uveljavljanje pravic posameznikov iz EU do pravnega varstva

WP29 priznava obveznosti organov ZDA, kar zadeva različne ravni mehanizma pravnega varstva. Vendar jo ob upoštevanju zapletenosti in pomanjkanja jasnosti splošne strukture mehanizma skrbi, da bo učinkovito uveljavljanje pravice posameznika, na katerega se nanašajo osebni podatki, v praksi oteženo. Poleg tega poudarja, da bi morala imeti kakovost mehanizma pravnega varstva prednost pred številom mehanizmov, ki so na voljo posameznikom iz EU. Obstajajo tudi pomisleki, da večina pritožbenih mehanizmov, če že ne vsi, predvideva postopek v ZDA, kar organom za varstvo podatkov v EU otežuje spremljanje postopka.

Dejansko se pritožbeni mehanizem, predviden v zasebnostnem ščitu, osredotoča zlasti na možnost, da posameznik, na katerega se nanašajo osebni podatki, „zahteva svoje pravice in spremlja primer nezdružljivosti načel zasebnosti z neposrednimi stiki s samocertificiranim podjetjem v ZDA“[27]. Poleg tega morajo organizacije imenovati neodvisni organ za reševanje sporov, ki raziskuje in rešuje posamezne pritožbe. WP29 pozdravlja dejstvo, da bo to za posameznika brezplačno.

Druga možnost je, da se pritožbe vložijo neposredno pri FTC, čeprav jih ta ni obvezana obravnavati. Pritožbo bi lahko poslal tudi organ za varstvo podatkov, ministrstvo za trgovino pa se je zavezalo, da bo pregledalo pritožbe in si čim bolj prizadevalo za olajšanje reševanja pritožb (Priloga I), ki jih bo zvezna komisija za trgovino „prednostno obravnavala“ (točka III.7.e Priloge II). Vendar prednostna obravnava pritožb s strani FTC posamezniku, na katerega se nanašajo osebni podatki, ne zagotavlja, da bodo njegove pritožbe obravnavane.

Posamezniki bodo lahko kot zadnjo možnost uveljavljali zavezujočo arbitražo. Arbitražni senat bo imel sedež v ZDA in bo pod nadzorom sodišč v ZDA.

Zasebnostni ščit organizacijam ponuja tudi možnost, da se odločijo za sodelovanje z organi za nadzor podatkov v EU (točka III.5.a Priloge II). To je celo obvezno za podatke o človeških virih, zbrane v okviru zaposlitvenega razmerja (točka III.9.d.ii Priloge II). V takem scenariju se ne bo uporabljalo alternativno reševanje sporov (točka III.5.a Priloge II). Zasebnostni ščit ne določa jasno, kako bo sodelovanje z organi za varstvo podatkov v EU organizirano v praksi. Zlasti ni jasno, ali bo arbitražni senat obravnaval vse zadeve ali pa bo vsako posamezno zadevo obravnaval drug senat.

[27] Evropska komisija, osnutek sklepa o ustreznosti, točka 30.

WP29 meni, da je v sklepu o ustreznosti potrebnih več podrobnosti, kar zadeva pristojnost organov za varstvo podatkov za obravnavanje pritožb. To je očitno odvisno od usposobljenosti organizacije, vendar ni jasno, kako.

Če organizacija deluje kot posrednik v imenu upravljavca iz EU, se bodo lahko posamezniki vsekakor pritožili pristojnemu organu za varstvo podatkov v EU. Podobno bo veljalo za obdelavo podatkov o človeških virih in drugih poslovnih podatkov.

Če je organizacija v zasebnostnem ščitu v vlogi upravljavca podatkov, bo pristojnost organa za varstvo podatkov za obravnavanje pritožbe omejena na obdelavo, za katero se uporablja pravo EU (obdelava, ki se izvaja pod odgovornostjo upravljavca – vključno s skupnim upravljanjem z organizacijo v ZDA –, ali če bi se za organizacijo v zasebnostnem ščitu neposredno uporabljalo pravo EU, na primer z uporabo opreme v EU). Vendar se bodo za obdelavo podatkov, ki se izvaja samo v skladu s pravom ZDA, uporabljali izključno mehanizmi zasebnostnega ščita. Za odpravo jezikovnih ovir in pomanjkanja znanja o pravnem sistemu ZDA bi bilo koristno, če bi imeli organi za varstvo podatkov v EU pravico, da delujejo kot posredniki za pritožbe posameznikov ali da jim pomagajo pri postopkih alternativnega reševanja sporov z organizacijami iz ZDA ali med njihovimi stiki z organi ZDA, če organ za varstvo podatkov meni, da je to ustrezno.

WP29 poudarja, da mehanizem, pojasnjen v zasebnostnem ščitu, ne temelji na prejšnjem priporočilu, v skladu s katerim bi moralo biti posameznikom iz EU „omogočeno, da vložijo odškodninski zahtevek v Evropski uniji“, in „odobrena pravica do vložitve zahtevka na pristojnem nacionalnem sodišču EU“[28]. Dobrodošlo bi bilo, če bi organizacije v zasebnostnem ščitu tako možnost vključile v svoje politike varovanja zasebnosti.

WP29 za zagotovitev učinkovitosti predlaga, da bi moral sistem organom za varstvo podatkov iz EU po možnosti omogočati, da zastopajo posameznika, na katerega se nanašajo osebni podatki, in delujejo v njegovem imenu ali kot posredniki. Vseboval pa bi lahko tudi posebne klavzule o sodni pristojnosti, na podlagi katerih bi lahko posamezniki, na katere se nanašajo osebni podatki, uveljavljali svoje pravice v Evropi.

b) Arbitraža

Končni arbitražni postopki se še niso končali, kar WP29 otežuje ocenjevanje. Ker kaže, da se bo arbitražni sistem izvajal v skladu s pravom ZDA in da bo edini jezik postopka angleščina, bodo organi za varstvo podatkov iz EU morda želeli imeti pravico, da pomagajo posameznikov v postopku.

Poleg tega je bil arbitražni postopek vzpostavljen, ker ni bilo zagotovila, da bo pritožba obravnavana, saj FTC ni obvezana obravnavati vsake pritožbe. WP29 opozarja, da bo moral posameznik iz EU, ki se mu bo zdelo, da potrebuje pomoč odvetnika, sam kriti stroške odvetnika, kar lahko posameznike odvrne od vložitve pritožbe za arbitražni postopek.

[28] Glej dopis WP29 podpredsednici Redingovi z dne 10. aprila 2014.

c) Nadzor, uveljavljanje in učinkovitosti mehanizma pravnega varstva

Pogoji za vstop v ščit

Po mnenju Sodišča „zanesljivost sistema samocertificiranja […] temelji predvsem na uvedbi učinkovitih mehanizmov za prepoznavanje in nadzor, ki v praksi omogočajo odkrivanje in sankcioniranje morebitnih kršitev pravil, s katerimi se zagotavlja varstvo temeljnih pravic […]“[29].

WP29 ugotavlja, da naj bi bila vloga zasebnostnega ščita, ki jo ima ministrstvo za trgovino v postopku certificiranja, omejena le na preverjanje popolnosti dokumentov. Čeprav WP29 priznava, da samocertificiranje ne pomeni sistematičnega predhodnega preverjanja izvajanja politik varovanja zasebnosti, bi se moralo ministrstvo za trgovino vsaj zavezati, da bo sistematično preverjalo, ali politike varovanja zasebnosti vključujejo vsa načela zasebnostnega ščita. Taka zaveza je navedena v osnutku sklepa o ustreznosti, vendar je ni mogoče jasno opredeliti v spremnem dopisu ministrstva za trgovino[30].

Kršitev načel zasebnostnega ščita lahko dolgo časa ostane neopažena in se lahko odkrije šele po resni kršitvi temeljnih pravic posameznika, na katerega se nanašajo osebni podatki, katere škode morda ni mogoče odpraviti. Zato bi lahko bil ta pristop v nasprotju z evropskim načelom previdnosti.

Preglednost s seznamom zasebnostnega ščita in umikom evidence organizacij s seznama

Znatne izboljšave so bile dosežene v zvezi s preglednostjo za posameznika, na katerega se nanašajo osebni podatki. Nov seznam zasebnostnega ščita bo poleg vseh organizacij v ZDA, ki so se samocertificirale pri ministrstvu za trgovino, vključeval tudi evidenco vseh organizacij, ki so bile umaknjene s seznama, vključno z razlogom za umik[31]. Spletno mesto zasebnostnega ščita ministrstva za trgovino se bo v prihodnje bolj osredotočalo na ciljne skupine, tako da bo olajšalo preverjanje vrste podatkov, vključenih v samocertifikacijo organizacije, pa tudi politike varovanja zasebnosti, ki se uporablja za zajete podatke, in metode, ki jo organizacija uporablja za preverjanje svoje zavezanosti k načelom[32]. WP29 pozdravlja dejstvo, da je zdaj jasno, da bo ministrstvo za trgovino preverjalo, ali so podjetja, ki imajo javno spletno mesto, na tem spletnem mestu objavila svojo politiko varovanja zasebnosti, ali, če nimajo javnega spletnega mesta, kje je politika varovanja zasebnosti javno dostopna[33]. Dokumenti vsebujejo več informacij tudi glede vsebine politike varovanja zasebnosti[34].

[29] Sodišče, zadeva Schrems, točka 81.
[30] Evropska komisija, osnutek sklepa o ustreznosti, točka 34.
[31] Stran 5 Priloge I in točka II.1 Priloge II; WP29 se sklicuje tudi na četrto priporočilo Komisije iz Sporočila COM(2103) 847, pa tudi na svoj dopis podpredsednici Redingovi z dne 10. aprila 2014, zlasti točko 5 pod naslovom „Preglednost“.
[32] Stran 8 Priloge I; WP29 se sklicuje tudi na svoj dopis podpredsednici Redingovi z dne 10. aprila 2014, zlasti točko 2 pod naslovom „Preglednost“.
[33] Strani 3 in 4 Priloge I; WP29 se sklicuje tudi na prvo priporočilo Komisije iz Sporočila COM(2103) 847, pa tudi na svoj dopis podpredsednici Redingovi z dne 10. aprila 2014, zlasti točko 3 pod naslovom „Preglednost“.
[34] Strani 5 in 6 Priloge I in točka III.6 Priloge II.

WP29 meni, da bi se lahko pojavile težave, če bi organizacija, ki je že vključena na seznam zasebnostnega ščita, pozneje razširila certifikacijo na druge kategorije podatkov. V takih primerih seznam ne bo izražal različnih obdobij uporabe načel za različne kategorije podatkov. To predstavlja tveganje, da posamezniki in podjetja iz EU ne bodo mogli v celoti oceniti, ali se za določen sklop podatkov dejansko uporabljajo načela zasebnostnega ščita, in če se, od kdaj. Da bi se izognili tej pomanjkljivosti, delovna skupina predlaga, da so v evidenci organizacij na seznamu zasebnostnega ščita za vsako kategorijo osebnih podatkov ločeno navedeni podatki o začetku uporabe samocertificiranja.

WP29 pozdravlja dejstvo, da bo ministrstvo za trgovino vodilo evidenco organizacij, ki so bile umaknjene s seznama zasebnostnega ščita, in da bo ta evidenca vključevala razlago s pojasnilom, da zadevnim organizacijam niso več zagotovljene koristi zasebnostnega ščita, vendar da morajo, dokler hranijo take podatke, še naprej uporabljati načela za osebne podatke, ki so jih prejele, ko so imele status certificiranih organizacij v zasebnostnem ščitu (str. 3 Priloge I). Vendar ker se lahko nekatere organizacije, ki so bile umaknjene s seznama zasebnostnega ščita, odločijo, da vrnejo ali izbrišejo podatke, prejete v okviru zasebnostnega ščita, medtem ko druge organizacije hranijo podatke, ki so jih prejele v okviru zasebnostnega ščita, je treba zagotoviti večjo preglednost glede tega vprašanja za posameznike. Zato bi moralo biti v evidenci podjetij, ki jo vodi ministrstvo za trgovino, navedeno, ali organizacija še vedno hrani osebne podatke, ki jih je prejela v okviru zasebnostnega ščita, ali pa je take podatke vrnila ali izbrisala. Če organizacija še vedno hrani take podatke, bi moralo biti v evidenci izrecno navedeno, da mora organizacija za take podatke še naprej uporabljati načela.

Poleg tega bi moralo biti v evidenci, ki jo vodi ministrstvo za trgovino, navedeno, da tem organizacijam za nove prenose niso več zagotovljene koristi zasebnostnega ščita, kar pomeni, da organizacija ne sme več prejemati osebnih podatkov iz EU v skladu z načeli.

Postopki preverjanja

Da bi organizacija preverila, ali je samocertificiranje učinkovito v praksi, lahko izvede samooceno ali zunanje preglede skladnosti. WP29 obžaluje, da se usposabljanje zaposlenih zahteva le, kadar se organizacija odloči za preverjanje s samooceno (točka III.7.c Priloge II). Zdi se tudi, da se preverjanje, ali so politike točne, celovite, vidno prikazane, dostopne in ali se izvajajo, zahteva samo, če se organizacija odloči za notranji pregled (samooceno), in da je ta pregled, ki se opravi z zunanjim mehanizmom, omejen le na skladnost s politiko varovanja zasebnosti organizacije.

Naknadne ugotovitve

WP29 pozdravlja dejstvo, da imata FTC in ministrstvo za trgovino preiskovalna pooblastila v primeru pritožb. Poleg tega WP29 ugotavlja, da bo lahko ministrstvo za trgovino preverjanja izvajalo po uradni dolžnosti, zlasti s pošiljanjem vprašalnikov. Vendar se želi prepričati, da tak pristop zadostuje za izpolnitev zahteve Sodišča po učinkovitih mehanizmih za odkrivanje in nadzor kršitev. Dejansko ima WP29 še vedno vprašanja glede tega, kakšna so natančna pooblastila organov kazenskega pregona ZDA za izvajanje inšpekcijskih pregledov na kraju samem v prostorih samocertificiranih organizacij za preiskovanje kršitev zasebnostnega ščita, kako je mogoče na ozemlju ZDA pridobiti *uradno dovoljenje za izvršitev* odločbe organa EU in ali imajo sankcije na podlagi zasebnostnega ščita v praksi odvračilni učinek.

2.2.7 Obdelava podatkov o človeških virih

Področje uporabe

Dopolnilno načelo 9 (točka III.9 Priloge II) se uporablja za osebne podatke o zaposlenem (nekdanjem ali sedanjem), zbrane v okviru zaposlitvenega razmerja. Glede na besedilo dopolnilnega načela 9.a.ii se načela zasebnostnega ščita uporabljajo samo za „prenos ali dostop do podatkov, ki omogočajo identifikacijo“. Besedilo „ki omogočajo identifikacijo“ ni skladno z opredelitvijo „osebnih podatkov“ iz točke I.8.a Priloge II, ki vsebuje besedilo „podatki o znanem ali prepoznavnem posamezniku“, in zato ni skladno z opredelitvijo, uporabljeno v Direktivi[35].

Dopolnilno načelo 9.a.ii navaja, da „[se] pri statističnem poročanju, ki temelji na zbirnih podatkih o zaposlenosti […] in ne vsebuje osebnih podatkov ali vključuje uporabo anonimnih podatkov, […] vprašanje varstva zasebnosti ne pojavlja“. Ta izjava je v nasprotju s številnimi mnenji WP29. WP29 želi poudariti, da je mogoče združene podatke še vedno ponovno identificirati, zaradi česar bi se morali šteti za osebne podatke[36].

[35] Kot je bilo že poudarjeno, omejitev na evidence, „ki so bile prenesene ali do katerih se je dostopalo“, prav tako ni skladna z izrazom „obdelava“ (točka I.8.b Priloge II).
[36] Glej Mnenje št. 4/2007 o pojmu osebnih podatkov in Mnenje št. 5/2014 o tehnikah anonimizacije.

Obvestilo, možnost izbire in omejitev namena

Dopolnilno načelo 9.b.i navaja primer uporabe načel obvestila in možnosti izbire, kadar se podatki o človeških virih uporabljajo za drugačen namen. Primer se nanaša na organizacijo v ZDA, ki „namerava uporabiti podatke, zbrane v zaposlitvenem razmerju, za namene, ki niso povezani z zaposlitvenim razmerjem, kot so tržne komunikacije“. V tem scenariju je sprememba namena dovoljena, če se upoštevata načeli obvestila in možnosti izbire. Po mnenju WP29 bi bilo treba nadaljnjo obdelavo podatkov o človeških virih za namene neposrednega trženja v večini primerov obravnavati kot nezdružljiv namen, ki je v nasprotju z načelom omejitve namena (točka II.5.a Priloge II). Poleg tega WP29 meni, da možnost izbire ne more biti ustrezna podlaga za zaposlenega, da „soglaša“ s (zavrne) spremembo namena v okviru zaposlitvenega razmerja, če tako soglasje morda ni povsem prostovoljno.

WP29 močno dvomi, da so s tem, ko je glavni poudarek zasebnostnega ščita na načelu možnosti izbire kot pogoju za nadaljnjo uporabo podatkov za drug namen, upoštevane Smernice OECD o zasebnosti, saj ni zadostnih jamstev, ki bi preprečevala uporabo tega mehanizma zavrnitve tudi za nadaljnjo obdelavo za nezdružljive namene. Dopolnilno načelo 9.b.iv določa splošno in izrecno izjemo uporabe načel obvestila in možnosti izbire „v obsegu in obdobju, potrebnem za preprečitev poseganja v sposobnost organizacije za sprejemanje odločitev o napredovanju delavcev, imenovanjih in drugih podobnih zaposlitvenih odločitev“. Prvič, uporaba podatkov o človeških virih za take namene bi morala biti izrecno navedena že pri zbiranju podatkov. Poleg tega je besedilo „drugih podobnih zaposlitvenih odločitvah“ preveč nedoločno in preširoko. Posledično bodo podatki o človeških virih v celoti izvzeti iz načel obvestila in možnosti izbire, če se obdelujejo v okviru zaposlitvenega razmerja. Pojem je tako širok, da ne omogoča ocene, ali je nadaljnja uporaba združljiva s prvotnim namenom. WP29 predlaga izbris te izjeme.

Pravica do dostopa

Dopolnilno načelo 9.e.i določa oprostitev uporabe načela dostopa ali sklenitve pogodbe s tretjim upravljavcem za podatke o človeških virih, če se ti nanašajo na občasne, z zaposlitvijo povezane operativne (npr. rezervacija leta, hotelske sobe ali zavarovalno kritje) prenose osebnih podatkov majhnega števila zaposlenih ter če se upoštevata načeli obvestila in možnosti izbire. WP29 ne najde razumne utemeljitve za tako oprostitev in predlaga, da se ta odstavek izbriše.

2.2.8 Farmacevtski in medicinski izdelki

Področje uporabe

Glede na zasebnostni ščit prenosi podatkov, kodiranih s šifrirnim ključem, iz Evropske unije v ZDA v zvezi s farmacevtskimi in medicinskimi izdelki ne pomenijo prenosov, ki bi bili predmet zasebnostnega ščita (točka III.14.g.i Priloge II). Vendar je prenos podatkov, kodiranih s šifrirnim ključem, upravičen do zaščite na podlagi evropske zakonodaje o varstvu podatkov. To pomeni, da zasebnostni ščit v praksi vključuje take prenose. WP29 Komisijo

EU poziva, naj izrecno določi, da osnutek sklepa o ustreznosti ne bo zajemal prenosa podatkov, kodiranih s šifrirnim ključem, za farmacevtske ali medicinske namene in da morajo biti taki prenosi zato zajeti v drugih zaščitnih ukrepih, kot so standardne pogodbene klavzule (v nadaljnjem besedilu: SPK) ali zavezujoča poslovna pravila. Predlaga, naj se to pojasni v končnem sklepu o ustreznosti.

Prenosi za regulativne in nadzorne namene (točka III.14.d Priloge II).

WP29 ima pomisleke, da se lahko v skladu s temi določbami osebni podatki, ki so zaradi medicinskega ozadja večinoma občutljivi, prenašajo regulativnim organom v ZDA. Ker je zasebnostni ščit zasnovan za prenose podatkov med zasebnimi subjekti, se zdi, da javni organ, kot je regulativni organ ZDA, ni upravičen do samocertificiranja v okviru zasebnostnega ščita, zaradi česar se postavlja vprašanje ustreznega varstva podatkov za take prenose. Če je treba take prenose izvajati za regulativne namene, je treba sprejeti ustrezne ukrepe za zagotovitev stalnega varstva temeljnih pravic posameznikov iz EU, na katere se nanašajo osebni podatki. WP29 poudarja dejstvo, da osnutek sklepa o ustreznosti ne vključuje nobene ugotovitve glede tega. Zato WP29 nima nobenega jamstva, da bodo občutljivi podatki posameznikov iz EU, na katere se nanašajo osebni podatki, v takih primerih ustrezno zaščiteni.

Poleg tega WP29 navaja, da ne razume, zakaj je „trženje“ kot namen navedeno kot primer obdelave za prihodnje znanstvene raziskave. Tudi izvajanje prenosov sedežem podjetij in drugim raziskovalcem, ki je kot razlog navedeno pod naslovom Prenosi za regulativne in nadzorne namene (točka III.14.d Priloge II), ni jasno. Ta vprašanja zahtevajo pojasnilo v končnem sklepu o ustreznosti.

Varnost izdelkov, spremljanje učinkovitosti (vključno s poročanjem vladnim agencijam) in sledenje pacientov, ki uporabljajo nekatera zdravila ali medicinske pripomočke

Zasebnostni ščit določa oprostitev uporabe načel obvestila, možnosti izbire, prenosa tretjemu in dostopa, če spoštovanje načela posega v skladnost z regulativnimi zahtevami. Osnutek sklepa o ustreznosti ne vključuje ugotovitev v zvezi s primeri, kadar načela zasebnosti posegajo v skladnost z regulativnimi zahtevami. WP29 lahko razume, da lahko vladne preiskave upravičujejo omejitve glede obvestila in pravice do dostopa za zaščito preiskav, vendar ne vidi razlogov, ki bi upravičili take splošne oprostitve, kadar obdelavo izvaja organizacija ali tretja stranka v zasebnem sektorju. Na primer, ker je zdravljenje pacientov vse bolj individualizirano, je taka splošna oprostitev od uporabe načel zasebnosti v primeru sledenja pacientov, ki uporabljajo nekatera zdravila ali medicinske pripomočke, nesprejemljiva, saj bo taka vrsta oskrbe postala splošna praksa. To velja tudi za primere, kadar farmacevtske družbe uporabljajo podatke za varnost izdelkov in spremljanje učinkovitosti (preskušanje ali prodaja novih zdravil).

2.2.9 Javno dostopne informacije

Izjema glede pravice dostopa v primeru javno dostopnih informacij in podatkov iz javnih evidenc (točki III.15.d. in e Priloge II) vzbuja pomisleke, saj želi posameznik pri uveljavljanju svojih pravic do dostopa vedeti, ali določen upravljavec obdeluje podatke o njem in kateri podatki se obdelujejo, da lahko nadzoruje obdelavo svojih podatkov. WP29 je večkrat navedla, da imajo posamezniki, na katere se nanašajo osebni podatki, v skladu s pravom EU vedno pravico dostopati do svojih podatkov in po potrebi zahtevati popravek ali izbris podatkov, če podatki niso bili obdelani zakonito ali če so nepopolni ali netočni, ne glede na to, ali so bili osebni podatki objavljeni[37]. Če je posameznikova zahteva za dostop zavrnjena, ker so bili podatki pridobljeni iz javno dostopnih virov ali javnih evidenc, posameznik izgubi zmožnost preverjanja točnosti podatkov in zlasti ne more preveriti, ali so bili podatki zakonito objavljeni.

Vendar zasebnostni ščit javne evidence in javno dostopne informacije izključuje iz načel obvestila, možnosti izbire, dostopa in odgovornosti za prenose tretjemu (točka II.15.d Priloge II). Te izjeme se zdijo preveč splošne v primerjavi z Direktivo in vzbujajo pomisleke, saj med drugim slabijo zmožnosti posameznikov za preverjanje točnosti svojih podatkov in omejitev njihovega razširjanja.

2.3 Sklepne ugotovitve

WP29 priznava, da so organi ZDA in Evropska komisija dosegli pomembne izboljšave glede komercialnih vidikov za prenos podatkov med dvema celinama. Vendar na podlagi zgornje analize ugotavlja, da komercialni del zasebnostnega ščita zahteva dodatna pojasnila glede številnih točk. Skrb vzbuja na primer pomanjkanje izrecnega načela hrambe podatkov. Zato ima WP29 resne pomisleke, da bi lahko zasebnostni ščit zagotovil raven varstva, ki je v bistvu enakovredna ravni varstvi v EU.

V sklepu o ustreznosti je treba dodatno pojasniti načeli omejitve namena in možnosti izbire. Še vedno obstaja tveganje vrzeli v zvezi z več načeli, zlasti v zvezi s prenosi tretjemu, mehanizmom za obravnavanje pritožb in obdelavo podatkov o človeških virih ali farmacevtskih podatkov. Poleg tega je treba podrobneje opredeliti, kako se načela zasebnostnega ščita uporabljajo za obdelovalce podatkov (posrednike), ter posebno pozornost nameniti zagotavljanju jasne in nedvoumne uporabe terminologije.

3. OCENA JAMSTEV NA PODROČJU NACIONALNE VARNOSTI IZ OSNUTKA SKLEPA O USTREZNOSTI

3.1 Zaščitni ukrepi in omejitve, ki veljajo za nacionalne varnostne organe ZDA

Posegi v temeljne pravice do zasebnega življenja in varstva podatkov so lahko dovoljeni, če jih je mogoče upravičiti v demokratični družbi. To pomeni, da načela zasebnosti niso absolutna in da so možna odstopanja, vendar le, če so zagotovljena veljavna (bistvena)

[37] Glej WP20, str. 4.

jamstva. V skladu s ciljem krepitve varstva zasebnosti si morajo organizacije tudi prizadevati, da načela uveljavijo v celoti in pregledno, med drugim tudi tako, da v svoji politiki varovanja zasebnosti navedejo, kdaj se bodo izjeme od načel, dovoljene s pravnim okvirom ZDA, redno uporabljale. Iz istega razloga se od organizacij pričakuje, da se, kadar načela in/ali pravo ZDA dopuščajo izbiro, po možnosti odločijo za višjo raven varstva.

V točki I.5 Priloge II je navedeno, da „je lahko zavezanost k načelom zasebnosti omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa ali kazenskega pregona; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel omejeno na obseg, ki je potreben za izpolnitev prevladujočih zakonitih interesov na podlagi takšnih pooblastil, ali (c) če direktiva ali pravo države članice dovoljuje izjeme ali odstopanja, če se te izjeme ali odstopanja uporabljajo v primerljivih okoliščinah.

Vprašanje je, ali so odstopanja iz Priloge II upravičena v demokratični družbi. Komisija je na podlagi osnutka sklepa o ustreznosti zasebnostnega ščita ugotovila, da „so v ZDA vzpostavljena pravila, ki so namenjena omejitvi morebitnih posegov za namene nacionalne varnosti v temeljne pravice oseb, katerih osebni podatki se prenašajo iz Unije v ZDA v okviru zasebnostnega ščita EU−ZDA, na tisto, kar je nujno potrebno za doseganje zadevnega legitimnega cilja“[38].

WP29 je z uporabo okvira, kot je opisan v oddelku 1.2 tega mnenja, ter ob upoštevanju zagotovil organov ZDA in ugotovitev Komisije ocenila veljavni pravni okvir ZDA in prakse obveščevalnih agencij ZDA ter pogoje, pod katerimi te omogočajo poseganje v temeljne pravice do spoštovanja zasebnega življenja in varstva podatkov, kot so zaščitene z evropskim pravnim okvirom. Ta ocena temelji na analizi Predsedniške politične direktive št. 28 (v nadaljnjem besedilu: PPD-28), Odredbe št. 12333 (v nadaljnjem besedilu: EO12333) in različnih pravnih podlag, vzpostavljenih z zakonom o nadzoru tujih obveščevalnih podatkov (Foreign Intelligence Act, v nadaljnjem besedilu: FISA − členi 104, 402, 215, 501 in 702). WP29 se sklicuje na Prilogo VI zasebnostnega ščita, ki vključuje dopis urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za nacionalne varnostne organe ZDA, in povzema informacije, ki jih je Evropska komisija zagotovila v zvezi z zbiranjem obveščevalnih podatkov v okviru obveščevalnih dejavnosti pri zaznavanju signalov (SIGINT) v ZDA.

3.2 Jamstvo A − obdelava bi morala biti skladna s pravom ter temeljiti na jasnih, natančnih in dostopnih pravilih

V skladu z evropskim pravom mora biti kakršno koli poseganje v skladu z zakoni, uveljavljenimi politikami in postopki ter dovolj jasno in dostopno (v skladu z diskrecijsko

[38] Osnutek sklepa Komisije v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU−ZDA, točka 75.

pravico, dodeljeno posameznih državam), da se državljanom zagotovijo ustrezne informacije o okoliščinah in pogojih, v katerih lahko javni organi uporabijo nadzorne ukrepe[39].

WP29 ugotavlja, da se obveščevalne dejavnosti SIGINT izvajajo na podlagi dostopnega pravnega okvira. Vsi zakoni, navedeni v Prilogi VI (PPD-28, FISA, USA FREEDOM ACT, FOIA), so javnosti na voljo na spletu (v ZDA in zunaj njih). V Prilogi VI je povzetek ureditvenega pravnega okvira, omejitev glede zbiranja, omejitev glede hrambe in razširjanja, skladnosti in nadzora ter preglednosti in pravnega varstva. Pravni sistem ZDA za obveščevalne dejavnosti obsega veliko različnih dokumentov, med drugim tudi poročila posameznih agencij, politike in postopke, ki jih je treba analizirati za boljše razumevanje načina izvajanja dejavnosti v teoriji in praksi. V zvezi s tem se WP29 osredotoča na omejeno število točk, ki so po njenem mnenju ključne.

3.2.1 Odredba št. 12333 in Predsedniška politična direktiva št. 28

Področje uporabe EO12333 je široko, kar pomeni, da se lahko na podlagi Odredbe vsako zbiranje tujih obveščevalnih podatkov načeloma izvaja po presoji predsednika ZDA. Vendar nekateri trdijo, da se lahko EO12333 od uvedbe zakona FISA uporablja le za zbiranje podatkov zunaj ozemlja ZDA. WP29 ugotavlja, da EO12333 ne zagotavlja veliko podrobnosti niti v zvezi s svojim geografskim področjem uporabe in obsegom zbiranja, hrambe ali nadaljnjega razširjanja podatkov niti v zvezi z vrsto kršitev, zaradi katerih se lahko začne izvajati nadzor, ali vrsto podatkov, ki se lahko zbirajo ali uporabljajo.

Po mnenju WP29 je glavni namen Predsedniške politične direktive št. 28 (PPD-28) predpisati omejitve za zbiranje in obdelavo osebnih podatkov, ne glede na to, kateri program nadzora se uporablja in kje so bili podatki pridobljeni.

PPD-28 je direktiva predsednika ZDA, ki določa načela skladnosti, na podlagi katerih se odobri in izvaja zbiranje obveščevalnih podatkov v okviru SIGINT, vendar PPD-28 ni pravna podlaga za zbiranje. Učinkovita je pri uveljavljanju navedenih načel za organe obveščevalne skupnosti, da bi jih vključila v njihove politike in postopke. Direktiva se uporablja za obveščevalne dejavnosti SIGINT, ne glede na lokacijo podatkov v času, ko se zbirajo, v ZDA ali zunaj njih. Zato se uporablja tudi za podatke, zbrane za obveščevalne namene v okviru SIGINT, kadar se prenašajo iz EU v ZDA.

PPD-28 zlasti navaja, da so obveščevalne dejavnosti SIGINT prilagojene in izvedljive[40]. V zvezi z uporabo podatkov določa postopke za zmanjšanje količine podatkov (vključno s

[39] Sodba ESČP v zadevi Zakharov, točka 247: „Sodišče je v zadevi predhodno ugotovilo, da zahteva po ‚predvidljivosti' prava ne sega tako daleč, da bi države prisilila, da vzpostavijo pravne določbe s podrobno navedbo vseh ravnanj, ki lahko spodbudijo odločitev, da se nad posameznikom izvaja nadzor zaradi ‚nacionalne varnosti'. Običajno so lahko grožnje nacionalni varnosti različne in nepričakovane ali pa jih je težko opredeliti vnaprej (glej Kennedy, navedeno zgoraj, točka 159). Hkrati je sodišče tudi poudarilo, da bi bilo v zadevah, ki vplivajo na temeljne pravice, v nasprotju s pravno državo, enim od osnovnih načel demokratične družbe iz Konvencije, če bi se diskrecijska pravica, dodeljena izvršnemu organu na področju nacionalne varnosti, izražala kot neomejeno pooblastilo. Zato morata biti z zakonom dovolj jasno določena obseg vsake take diskrecijske pravice, dodeljene pristojnim organom, in način njenega izvajanja, ob upoštevanju legitimnega cilja zadevnega ukrepa, da se posamezniku zagotovi ustrezno varstvo pred samovoljnim poseganjem".

pogoji za hrambo in razširjanje podatkov), varstvo podatkov in dostop s strani ustreznega osebja (tj. pravila, ki vključujejo zaščitne ukrepe za omejitev tveganj zlorabe in nepravilne uporabe), kakovost podatkov in nadzor. Ta jamstva veljajo ne glede na državljanstvo posameznikov, na katere se nanašajo osebni podatki, tj. za državljane in nedržavljane ZDA.

Med prenašanjem podatkov v ZDA se uporabljajo tudi zaščitni ukrepi, vzpostavljeni s PPD-28. Priloga VI vsebuje zavezo ODNI, da če bi obveščevalna skupnost ZDA zbirala podatke po čezatlantskih kabelskih vezah med prenosom v Združene države, "bi to naredila v skladu z omejitvami in zaščitnimi ukrepi, določenimi v tem dokumentu, vključno z zahtevami PPD-28"[41]. WP29 ugotavlja, da še primanjkuje uveljavljene sodne prakse, ki bi določala zakonitost prestrezanja prek kabelskih vez, če bi ga katera država izvajala. Vsekakor ZDA niti ne potrjujejo niti ne zanikajo, da kot sredstvo zbiranja obveščevalnih podatkov uporabljajo prestrezanje prek kabelskih vez.

Pojem „obveščevalna dejavnost SIGINT" ni opredeljen niti v PPD-28 niti v katerem koli drugem ustreznem veljavnem besedilu.

3.2.2 Zakon o nadzoru tujih obveščevalnih podatkov (Foreign Intelligence Surveillance Act, v nadaljnjem besedilu: FISA)

Na splošno se zdi, da je besedilo FISA jasnejše in natančnejše. Vendar sta razlaga številnih določb z vidika PPD-28 in s tem njihova praktična uporaba večinoma odvisni od tega, kako jih izvajajo različne agencije. Čeprav celotno poročilo o izvajanju novih zaščitnih ukrepov še ni na voljo, so delegati ZDA predstavnike WP29 obvestili, da se je izvajanje zaščitnih ukrepov iz PPD-28 dejansko končalo in da se izvaja podobno v celotni obveščevalni skupnosti ZDA.

Natančneje, člen 501 je razmeroma jasen glede vrste obveščevalnih dejavnosti, ki se lahko izvajajo: „zbiranje kakršnih koli oprijemljivih predmetov (vključno s knjigami, evidencami, spisi, dokumenti in drugimi listinami)". Vendar je treba opozoriti, da je obseg pooblastila zaradi dejstva, da opredelitev „oprijemljivih predmetov" vključuje „druge listine", precej širok.

Člen 702, ki dovoljuje pridobivanje podatkov od nedržavljanov ZDA, za katere se razumno predvideva, da so zunaj Združenih držav, da lahko pridobijo tuje obveščevalne podatke[42], ne zagotavlja enake stopnje podrobnosti kot člen 501. Kar zadeva področje uporabe člena 702, se ta člen osredotoča na ponudnike elektronskih komunikacijskih storitev v ZDA za zbiranje tujih obveščevalnih podatkov posameznikov zunaj ZDA. Opredelitev „tujih obveščevalnih podatkov" je široka. Med drugim vključuje „podatke v zvezi s tujo silo ali tujim ozemljem, ki

[40] „Obveščevalne dejavnosti SIGINT so prilagojene in izvedljive. ZDA pri odločanju, ali naj zbirajo obveščevalne podatke v okviru SIGINT, upoštevajo razpoložljivost drugih informacij, vključno z informacijami iz diplomatskih in javnih virov. Takim ustreznim in izvedljivim alternativam obveščevalni dejavnosti SIGINT bi bilo treba dati prednost." (člen 1(d)).
[41] Priloga VI zasebnostnega ščita, dopis urada direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence, v nadaljnjem besedilu: ODNI) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za nacionalne varnostne organe ZDA, str. 2.
[42] Zakonik ZDA, naslov 50, odstavek 1881a (D)(1).

so povezani s pristojnostjo za zunanje zadeve Združenih držav“[43], kar vzbuja negotovost glede vrste „podatkov, ki se lahko zbirajo v praksi.

Kljub odpravi zaupnosti dokumentov, poročil Kongresu ter poročil Nadzornega odbora za zasebnost in državljanske svoboščine (Privacy and Civil Liberties Oversight Board, v nadaljnjem besedilu: PCLOB) o nadzoru sta obseg in uporaba opredeljenih izbirnih izrazov še vedno nejasna in zavajajoča. Uporaba opredeljenih izbirnih izrazov („določenih izbirnikov“) je navedena v poročilu PCLOB[44], vendar po mnenju WP29 to ni v skladu s ciljno usmerjenimi pravili, ki izhajajo iz člena 702[45]. Ti izrazi niso navedeni v splošno dostopnih pravilih, kot je lahko potrdila WP29.

3.2.3 Sklepna ugotovitev

WP29 na splošno ugotavlja, da so veljavna besedila v zvezi z obveščevalnimi dejavnostmi na voljo na spletu in da so organi ZDA naredili več pomembnih korakov za večjo preglednost.

Ugotavlja tudi, da je bilo od leta 2013 objavljenih veliko dokumentov, kot so politike, postopki, odločbe sodišča FISA in drugi dokumenti, ki niso več zaupni. Poleg tega je PCLOB izdal pomembna poročila o dejavnostih, ki se izvajajo na podlagi člena 702 in zakona ZDA o svobodi. Podobno poročilo se pričakuje o dejavnostih na podlagi EO12333.

Več zakonodajnih prilog, ki bi lahko pojasnile posledice odredbe o posameznikih zunaj Združenih držav, in morebitni veljavni zaščitni ukrepi so zaupni in kot taki niso dostopni javnosti ali posameznikom, na katere bi lahko vplivala njihova uporaba. Če je bila za besedila odpravljena zaupnost, imajo le omejeno vrednost in zagotavljajo le omejene informacije v zvezi z obveščevalnimi dejavnostmi.

Kljub prizadevanjem za pojasnitev delovanja EO12333 po Snowdnovih razkritjih, zlasti s sprejetjem PPD-28, je sedanja praktična uporaba EO12333 še vedno nejasna. WP29 ugotavlja, da Priloga VI zasebnostnega ščita ne zagotavlja podrobnih informacij o delovanju EO12333.

Čeprav WP29 pozdravlja omejitve, zajete v PPD-28, je težko ugotoviti, ali je pravni okvir ZDA za nadzor dovolj predvidljiv, tj. ali vsebuje „ustrezne podatke o okoliščinah in pogojih, v katerih lahko javni organi uporabijo katerega koli od takih ukrepov“, saj se pričakuje dodatno pojasnilo, vključno z objavo poročila PCLOB o EO12333.

[43] Zakonik ZDA, naslov 50, odstavek 1801 (e)(2).
[44] Poročilo PCLOB o programu nadzora, ki se izvaja v skladu s členom 702 FISA, str. 32.
[45] Zakonik ZDA, naslov 50, odstavek 1881a(D).

3.3 Jamstvo B − dokazati je treba nujnost in sorazmernost v zvezi z zastavljenimi legitimnimi cilji

3.3.1 Predsedniška politična direktiva št. 28

PPD-28 je uvedla omejitve v zvezi z nameni, za katere se lahko osebni podatki uporabljajo, in glede pogojev, pod katerimi se lahko razširjajo, ter vpliva na zbiranje obveščevalnih podatkov v okviru SIGINT ne glede na uporabljeno pravno podlago.

Zlasti člen 1 PPD-28 določa, da morajo biti obveščevalne dejavnosti SIGINT vedno „prilagojene in izvedljive“. Ob upoštevanju te omejitve je težko ugotoviti, ali „prilagojene in izvedljive“ pomeni, da so vsi zbrani podatki nujno potrebni in sorazmerni.

V PPD-28 se priznava, da bo množično zbiranje podatkov še naprej dovoljeno, „da bi se odkrile nove ali nastajajoče grožnje in pridobile druge bistvene informacije v zvezi z nacionalno varnostjo, ki so pogosto skrite v velikem in zapletenem sistemu sodobnih globalnih komunikacij“[46]. Po ugotovitvah WP29 je v PPD-28 navedeno, da „‚množično‘ zbrani obveščevalni podatki v okviru SIGINT pomenijo pooblaščeno zbiranje velikih količin obveščevalnih podatkov v okviru SIGINT, ki se zaradi tehničnih ali operativnih razlogov pridobivajo brez uporabe diskriminant (npr. posebni identifikatorji, izbirni izrazi itd.)“.

PPD-28 uvaja omejitve za uporabo množično zbranih obveščevalnih podatkov v okviru SIGINT, kar zadeva namen uporabe. Navedenih je šest namenov, za katere se lahko podatki „množično“ zbirajo, vključno z bojem proti terorizmu in drugim oblikam hudih (nadnacionalnih) kaznivih dejanj. Analiza WP29 kaže, da je omejitev namena precej široka (in morda preširoka), da bi se lahko štela za ciljno usmerjeno.

PPD-28 ne izključuje možnosti neselektivnega množičnega zbiranja osebnih podatkov in tega, da bo obseg takih možnosti zbiranja še naprej nejasen in morda širok. WP29 v zvezi s tem ugotavlja, da ODNI v Prilogi VI potrjuje, da „se vsaka dejavnost množičnega zbiranja podatkov v zvezi s komunikacijo po internetu, ki jo izvaja ameriška obveščevalna skupnost z dejavnostjo SIGINT, izvaja na majhnem deležu interneta“[47], zato si želi dodatnih dokazov, zagotovljenih z ukrepi v zvezi s preglednostjo.

3.3.2 Zakon o nadzoru tujih obveščevalnih podatkov

Uvedeni so bili postopki za zmanjšanje količine podatkov v skladu s členoma 215 in 702 FISA za zaščito državljanov ZDA pred daljnosežnim vladnim dostopom do njihovih podatkov. Te omejitve se uradno ne uporabljajo za tujce, čeprav so vladni uradniki ZDA na javnih in zasebnih srečanjih s predstavniki WP29 večkrat izjavili, da se je področje uporabe

[46] Člen 2 PPD-28 in Priloga VI zasebnostnega ščita, dopis urada direktorja nacionalne obveščevalne službe (ODNI) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za nacionalne varnostne organe ZDA, str. 3.
[47] Priloga VI zasebnostnega ščita, dopis urada direktorja nacionalne obveščevalne službe (ODNI) v zvezi z zaščitnimi ukrepi in omejitvami, ki veljajo za nacionalne varnostne organe ZDA, str. 4; WP29 v zvezi s tem opozarja na poročilo o ugotovitvah predstavnikov EU, ki so sopredsedovali *ad hoc* delovni skupini EU−ZDA za varstvo podatkov, v katerem je navedeno, da „komunikacijski podatki predstavljajo zelo majhen del svetovnega internetnega prometa“ glede na to, da „veliko večino svetovnega internetnega prometa sestavljajo pretakanje velikih količin podatkov in prenesene vsebine, kot so televizijske serije, filmi in športni dogodki“ (točka 3.1.2 poročila) 44.

postopkov za zmanjšanje količine podatkov od začetka njihove uporabe razširilo in zdaj vključuje vse osebe, ne glede na njihovo državljanstvo ali običajno prebivališče.

Člen 702 določa, da se pooblaščeno pridobivanje podatkov „izvaja na način, ki je skladen s četrtim amandmajem Ustave ZDA, ki omejuje zbiranje podatkov na to, kar se šteje za skladno z načelom razumne preiskave. Glede tega ni razlik med ameriškimi in neameriškim podjetji“. Povedano drugače, če bi se četrti amandma uporabljal za vse podatke, zbrane v ZDA, bi bilo „množično“ zbiranje podatkov v ZDA „nerazumno“ in zato neustavno.

WP29 pozdravlja ugotovitve iz poročila PCLOB, da „imajo nedržavljani ZDA ‚v praksi' koristi tudi od omejitev dostopa in hrambe, ki se v postopkih različnih agencij za zmanjšanje količine podatkov in/ali ciljno usmerjenih postopkih zahtevajo zaradi stroškov, pri čemer težave pri identifikaciji in izbrisu podatkov državljana ZDA za veliko količino podatkov pomenijo, da se celoten sklop podatkov običajno obravnava v skladu z višjimi podatkovnimi standardi ZDA“.

WP29 nadalje ugotavlja, da v skladu z ugotovitvami PCLOB „program ne deluje na podlagi množičnega zbiranja sporočil“. Statistično poročilo o preglednosti za leto 2014, ki ga je izdal ODNI, potrjuje te ugotovitve. Poleg tega se, kot navaja poročilo PCLOB, za usmerjanje nadzora uporabljajo „določeni izbirniki“, kot je e-naslov ali telefonska številka[48].

Vendar ustrezna in dostopna javna pravila v zvezi s ciljnim usmerjanjem ne določajo takih ciljno usmerjenih pravil in so namenjena le preprečevanju ciljnega usmerjanja na državljane ZDA ali osebe, ki živijo v ZDA. Poleg tega ugodnosti, ki po navedbah PCLOB veljajo za nedržavljane ZDA, v praksi niso pravno zavezujoče, saj razpoložljiva zakonodaja v zvezi s ciljnim usmerjanjem ne določa takih ciljno usmerjenih pravil in je namenjena le preprečevanju ciljnega usmerjanja na državljane ZDA ali osebe, ki živijo v ZDA.

WP29 nadalje opozarja, da osebe za namene člena 702 niso le posamezniki, temveč tudi skupine, subjekti, združenja, družbe ali tuje sile. Poleg tega dejstvo, da je zbiranje podatkov upravičeno s tem, da je „pomemben namen pridobivanja zbrati tuje obveščevalne podatke“, prinaša nekaj negotovosti glede njegovega namena in nujnosti. Vendar WP29 pozdravlja podatek iz Priloge VI, da je bilo leta 2014 skupaj približno 90 000 posameznikov, o katerih so se zbirali podatki na podlagi člena 702[49]. Prvi pregled zasebnostnega ščita bo zagotovil možnost predložitve dodatnih dokazov o ciljno usmerjenih pravilih.

Doslej ni bilo prepričljive sodne prakse o zakonitosti množičnega in neselektivnega zbiranja podatkov ter poznejši uporabi osebnih podatkov za boj proti kriminalu, vključno z vprašanjem, v kakšnih okoliščinah se lahko izvajata tako zbiranje in uporaba osebnih podatkov. Pričakuje se, da bo Sodišče v letu 2016 vsaj v določenem obsegu obravnavalo to vprašanje, in sicer v združenih zadevah Tele2 Sverige AB proti Post- och telestyrelsen in Secretary of State for the Home Department proti Davisu in drugim[50] ter v nasvetu o

[48] Poročilo PCLOB o programu nadzora, ki se izvaja v skladu s členom 702 FISA, str. 32.
[49] Priloga VI, str. 11.
[50] Sodišče, združeni zadevi C-203/15 in C-698/15.

veljavnosti sporazuma s Kanado o obdelavi podatkov iz PNR[51]. Medtem WP29 opozarja, da je dosledno upoštevala, da množičnega in neselektivnega zbiranja podatkov nikakor ni mogoče šteti za sorazmernega[52].

3.3.3 Sklepna ugotovitev

WP29 ima kljub omejitvam po uvedbi PPD-28 še vedno pomisleke, zlasti glede sorazmernosti zbiranja podatkov. Prvič, obstajajo dokazi, da ZDA še naprej zbirajo množične in neselektivne podatke, ali pa vsaj ni izključeno, da tega ne bodo počele v prihodnosti. WP29 vztraja, da tako zbiranje podatkov ni skladno s pravom EU in da zato ni sprejemljivo.

Drugič, WP29 opozarja, da se lahko tudi ciljno usmerjena obdelava podatkov ali obdelava, ki je „prilagojena in izvedljiva“, šteje za množično. V zvezi s tem, ali bi moralo biti tako množično zbiranje podatkov dovoljeno ali ne, trenutno poteka postopek pred Sodiščem. Zato WP29 ne bo dala končne ocene glede zakonitosti ciljno usmerjene, vendar množične obdelava podatkov. Poudarja pa, da če bi bila ciljno usmerjena, vendar množična obdelava podatkov dovoljena, bi se morala ciljno usmerjena načela uporabljati za zbiranje in poznejšo uporabo podatkov, pri čemer ne smejo biti omejena samo na uporabo. Vsekakor je potrebno pojasnilo osnutka sklepa o ustreznosti v zvezi s šestimi nameni iz PPD-28, za katere se lahko podatki „množično“ zbirajo. WP29 v tej fazi ni prepričana, ali so ti nameni dovolj omejeni za zagotavljanje, da je zbiranje podatkov dejansko omejeno na tisto, kar je nujno potrebno in sorazmerno.

3.4 Jamstvo C − obstajati bi moral neodvisen mehanizem nadzora

ZDA nimajo enotnega nadzornega organa na zvezni ravni, ki bi bil odgovoren za nadziranje posledic obveščevalnih in nadzornih programov za varstvo zasebnosti in podatkov. Obveščevalne dejavnosti ZDA so predmet večstopenjskega postopka nadzora: razlikovati je mogoče med notranjim in zunanjim nadzorom. WP29 ugotavlja, da je poročanje nadzornih organov ZDA zelo podrobno in večinoma javno.

3.4.1 Notranji nadzor

Vse obveščevalne in varnostne agencije imajo člane osebja, ki so pristojni za zagotavljanje skladnosti z zakonodajnim okvirom, vključno z generalnimi inšpektorji, katerih glavna naloga je oceniti splošno skladnost dela agencij z zakonodajo, ki med drugim vključuje tudi zakonodajo, povezano z varstvom zasebnosti in podatkov. Generalni inšpektorji so vzpostavljeni z zakonom in jih po potrditvi senata imenuje (ali jih bo kmalu imenoval) predsednik, s čimer se zagotovi, da so organizacijsko neodvisni in da poročajo kongresu. WP29 meni, da bodo generalni inšpektorji zato verjetno izpolnjevali merilo glede organizacijske neodvisnosti, kot sta ga opredelila Sodišče in Evropsko sodišče za človekove pravice (ESČP), vsaj od trenutka, ko začne za vse veljati nov postopek imenovanja. Za zdaj še

[51] Sodišče, zadeva A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_sl.pdf.

vedno obstaja nekaj pomislekov v zvezi z generalnimi inšpektorji, ki jih še vedno imenuje direktor agencije, ki jo ti inšpektorji nadzorujejo.

Generalni inšpektorji lahko dajo priporočila, ki se lahko nato predložijo ministrstvu za obrambo in PCLOB ali celo kongresnemu odboru, ki jih lahko uveljavi. Če generalni inšpektor ugotovi kršitev, se lahko kršitev obravnava z notranjimi ukrepi in ukrepi politike ter sporoči kongresu. Generalni inšpektor je lahko na primer pristojen za izvajanje revizij in inšpekcijskih pregledov.

WP29 opozarja, da se lahko javnosti onemogoči dostop do poročil generalnega inšpektorja in da se lahko generalnemu inšpektorju onemogoči poročanje, če so pregledani podatki zaupni. Vendar bo kongres stalno nadzoroval poročila, kar je ključni zaščitni ukrep, čeprav ne zagotavlja razlogov za uporabo individualnih pravnih sredstev.

Vse agencije imajo uradnike za varstvo zasebnosti in državljanske svoboščine, ki pomagajo pri sistemu obveznega samoporočanja v okviru kongresnega nadzora.

Na splošno se lahko vzpostavljeni mehanizmi za notranji nadzor štejejo za precej zanesljive, vendar mora biti nadzor popolnoma neodvisen, da se upraviči poseganje v temeljne pravice do zasebnosti in varstva podatkov. Čeprav WP29 spoštuje in ceni delo različnih uradnikov za varstvo zasebnosti in državljanske svoboščine, ne more sklepati, da dosegajo zahtevano stopnjo neodvisnosti, da bi delovali kot neodvisni nadzorniki.

3.4.2 Zunanji nadzor

Zunanji nadzor zajema več različnih mehanizmov: sodni nadzor na podlagi členov 501 in 702, ki ga zagotavlja sodišče FISA (v nadaljnjem besedilu: FISC), nadzor preiskovalnih obveščevalnih odborov kongresa in naloge, ki jih izvaja PCLOB.

WP29 opozarja, da bi bilo najprimerneje, če bi o nadzoru odločal sodnik, kot sta navedla tudi Sodišče in ESČP, da bi se tako zagotovili neodvisnost in nepristranskost postopka. Do nedavnega je bil postopek FISC enostranski postopek, v katerem zadevnim posameznikom ni bilo omogočeno, da so zaslišani ali celo seznanjeni s primerom. Ta postopek je sicer še vedno enostranski, vendar so bili po sprejetju zakona ZDA o svobodi uvedeni prijatelji sodišča (*amici curiae*) FISC. Prijatelji sodišča delujejo neodvisno, vendar niso vzpostavljeni za to, da branijo določene posameznike, ki so morda vpleteni v zadevo.

Z zakonom ZDA o svobodi je bila ustanovljena skupina prijateljev sodišča za poročanje FISC o pomembnih zadevah. Sodišče je izbralo pet pravnikov, ki so pridobili ustrezna varnostna potrdila in zagotavljajo tehnične nasvete, se udeležujejo zaslišanj FISC in pošiljajo poročila ter odločajo o utemeljenosti primera z vidika zasebnosti in državljanskih pravic. Vendar to počnejo samo pri pomembnih zadevah ali kadar se pojavijo nova pravna vprašanja[53].

[53] Zakon o svobodi, NASLOV IV − REFORME SODIŠČA ZA NADZOR TUJIH OBVEŠČEVALNIH PODATKOV, člen 401, Imenovanje prijateljev sodišča.

Člen 215 je skoraj v celoti predmet predhodnega (vendar ne naknadnega) sodnega nadzora, saj je za vse programe, ki člen 215 uporabljajo kot podlago za zbiranje podatkov, potrebna odobritev FISC. V poročilu PCLOB je navedeno, da „se člen 702 razlikuje od tega tradicionalnega okvira elektronskega nadzora FISA, in sicer glede uporabljenih standardov in pomanjkanja individualiziranih ugotovitev FISC. Generalni državni pravobranilec in direktor nacionalne obveščevalne službe v skladu s zakonom opravljata letna certificiranja, s katerimi dovoljujeta ciljno usmerjanje na nedržavljane ZDA, za katere se razumno predvideva, da so zunaj Združenih držav, za pridobivanje tujih obveščevalnih podatkov, ne da bi FISC sporočila imena posameznih nedržavljanov ZDA, na katere bo usmerjeno pridobivanje podatkov. […] Poleg tega se ne zahteva, da mora vlada dokazati verjetni vzrok za domnevo, da je cilj iz člena 702 tuja sila ali agent tuje sile, kot zahteva tradicionalni FISA“[54].

V okviru kongresa preiskovalni obveščevalni odbori nadzirajo tudi obveščevalne dejavnosti, povezane z odobritvijo nalog, zlasti z glasovanjem o proračunu. Senat in odbori predstavniškega doma prejemajo zaupna poročila o obveščevalnih dejavnostih. Generalni državni pravobranilec vsakih šest mesecev poroča tem odborom o elektronskem nadzoru na podlagi FISA. WP29 še vedno ni jasno, v kakšnem obsegu lahko razpravljajo o obdelavi osebnih podatkov posameznikov, zlasti nedržavljanov ZDA.

PCLOB je neodvisni del izvršilne oblasti v vladi ZDA, ki ima dve temeljni pooblastili, in sicer za (1) pregled in analizo ukrepov, ki jih izvršilna oblast sprejme za zaščito naroda [ZDA] pred terorizmom, s čimer se zagotavlja, da je potreba po takih ukrepih usklajena s potrebo po varstvu zasebnosti in državljanskih svoboščin, ter (2) zagotavljanje, da se pomisleki glede svobode ustrezno obravnavajo pri pripravi in izvajanju zakonov, predpisov in politik, ki so povezani s prizadevanji za zaščito naroda pred terorizmom. WP29 ugotavlja, da ima PCLOB pooblastilo za izdajo sodnega poziva in dostop do zaupnih podatkov. Med opravljanjem svoje naloge preverja tudi učinkovitost programov. Nadzora ne izvaja pred dejstvom, temveč po njem. PCLOB svoja neodvisna pooblastila uveljavlja tako, da izraža nestrinjanje s stališči predsednika Združenih držav glede pravnih vprašanj. Zlasti je ugotovil, da program za zbiranje telefonskih metapodatkov iz člena 215 ni bil zakonito odobren, in sklenil, da ni bil učinkovit, saj ni bilo dokazov o prekinitvi napadov. PCLOB je izvedel tudi enoletno študijo programa iz člena 702 in ugotovil, da je zakonit in jasno odobren z zakonom ter da se je člen 702 izkazal za zelo učinkovitega, tudi kar zadeva vprašanja, povezana s terorizmom. Obravnaval je tudi zahtevo po preglednosti in ugotovil, da več zaupnih podatkov ne bi bilo treba opredeliti kot zaupnih. PCLOB je seznanjen s tem, da mora v bližnji prihodnosti poročati o izvajanju PPD-28. V zvezi s tem po njegovem mnenju zgolj dejstvo, da je oseba tujec, ne zadostuje za hrambo podatkov o njem.

WP29 nazadnje ugotavlja, da EO12333 ne določa mehanizmov sodnega pregleda, nadzora ali pravnega varstva za programe nadzora, ki se izvajajo na njegovi podlagi.

[54] Poročilo PCLOB o programu nadzora, ki se izvaja v skladu s členom 702 FISA, str. 24 in 25.

3.4.3 Sklepna ugotovitev

Osnutek sklepa o ustreznosti kaže, da je v ZDA vzpostavljen večstopenjski pristop mehanizmov notranjega in zunanjega nadzora. Čeprav je lahko delovanje mehanizmov nadzora zavajajoče, je WP29 zadovoljna, da so na splošno vzpostavljeni zadostni mehanizmi notranjega nadzora. Vendar je zaskrbljena, da nadzor programov nadzora, ki se izvajajo na podlagi EO12333, ni zadosten.

Ugotavlja, da se je njena prejšnja kritika, da postopki pred FISC niso kontradiktorni, nekoliko zmanjšala z uvedbo prijateljev sodišča, katerih naloga je „krepitev varstva zasebnosti in državljanskih svoboščin posameznikov“. Vendar FISC ne zagotavlja učinkovitega sodnega nadzora nad ciljnim usmerjanjem na nedržavljane ZDA. Še vedno obstaja nekaj pomislekov v zvezi z zmožnostjo FISC, da učinkovito obravnava ciljno usmerjene postopke in postopke zmanjševanja količine podatkov, kot je navedel tudi PCLOB[55].

3.5 Jamstvo D − posamezniku morajo biti na voljo učinkovita pravna sredstva

3.5.1 Pravna sredstva

3.5.1.1 Zahteva po procesnem upravičenju

Sistem ZDA, povezan s pravnimi sredstvi, vključuje pomembno omejitev: Ustava ZDA zahteva, da posameznik dokaže procesno upravičenje: „zahteva, da je tožnik utrpel ali bo utrpel neposredno poškodbo ali škodo in da je zoper to škodo mogoče uveljavljati pravno varstvo. Na zvezni ravni ni mogoče začeti pravnih postopkov zgolj na podlagi dejstva, da sta posameznik ali skupina nezadovoljna z delovanjem vlade ali zakonom“[56]. Zdi se, da je taka zahteva izničena z neobveščanjem posameznikov, ki so predmet nadzora, tudi po koncu teh ukrepov. Sodišče in ESČP sta večkrat navedla, da mora biti posameznikom omogočen dostop do upravnega ali pravnega varstva. ESČP je v odločbi v zadevi Zakharov potrdilo, da lahko v skladu s sodno prakso vsak začne postopek na sodišču, če ima utemeljen razlog za sum, da se posega v njegove temeljne pravice[57].

Poleg tega tujcem zunaj ZDA v skladu s sodno prakso Vrhovnega sodišča Združenih držav ni zagotovljeno popolno ustavno varstvo[58]. To velja zlasti v zvezi s četrtim amandmajem, ki državljane ZDA, ne pa tudi nedržavljane ZDA, ščiti pred nerazumnimi preiskavami in zasegi ter iz katerega izhaja velik del pravice ZDA do zasebnosti. Evropski državljani in drugi Evropejci, ki živijo zunaj ZDA, so preprosto izključeni iz varstva, ki ga zagotavlja četrti amandma[59].

Omejena uporaba zakona o pravnem varstvu (Judicial Redress Act) (z vidika vsebine, saj izključuje nacionalno varnost, pa tudi v zvezi z osebami, ki se lahko sklicujejo na pravo),

[55] Poročilo PCLOB o programu nadzora, ki se izvaja v skladu s členom 702 FISA, str. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standing; Clapper proti Amnesty International USA.
[57] Odločba ESČP v zadevi Zakharov, točka 171.
[58] ZDA proti Verdugo - Urquidez, str. 264−266.
[59] Poročilo sodelujočih predstavnikov EU, oddelek 2.

številne izjeme in pravna negotovost v zvezi z agencijami, za katere se bo uporabljal zakon o pravnem varstvu, ne izpolnjujejo zahteve po zagotavljanju učinkovitega mehanizma pravnega varstva vsem zadevnim posameznikom v zadevah, povezanih z nadzorom s strani obveščevalnih služb v okviru nacionalne varnosti.

3.5.1.2 Predsedniška politična direktiva št. 28

WP29 ugotavlja, da je PPD-28 zgolj direktiva in da zato posameznikom ne more dajati nobenih pravic. To je mogoče doseči le z zakonodajo. Zato posamezniki ne morejo začeti postopka na sodišču na podlagi domnevne kršitve zaščitnih ukrepov iz PPD-28.

3.5.1.3 Zakon o nadzoru tujih obveščevalnih podatkov

V skladu s FISA obstajajo nekatera pravna sredstva za posameznike v primeru nezakonitega nadzora. V skladu s FISA lahko „oškodovana oseba, ki ni tuja sila ali agent tuje sile […], ali oseba, nad katero se izvaja elektronski nadzor ali katere podatki, pridobljeni z elektronskim nadzorom take osebe, so bili razkriti ali uporabljeni s kršitvijo člena 1809 tega naslova, vloži pritožbo zoper katero koli osebo, ki je povzročila tako kršitev“. Vendar to izrecno izključuje tujo silo ali agenta tuje sile, ki je bil predmet ukrepa. Kljub temu mora tožnik, kot je bilo že navedeno, dokazati procesno upravičenje, kar v praksi ni mogoče.

Z zakonom ZDA o svobodi je bil ustanovljen svetovalni odbor prijateljev sodišča FISA, ki (neobvezno) zagotavlja nasvete v primeru nove pomembne pravne razlage. Vendar je njihova naloga zagotavljati nepristranske nasvete, ne pa ščititi interesa določenega posameznika na njegovo zahtevo.

3.5.2 Upravna sredstva

3.5.2.1 Generalni inšpektorji

Pravna sredstva se lahko uveljavljajo tudi prek generalnega inšpektorja, pri katerem se lahko vloži pritožba. Vendar generalni inšpektorji niso zavezani proučiti vsake posamezne pritožbe: ne obstaja pravica biti zaslišan, temveč diskrecijska pravica. Generalni inšpektor lahko tudi izdaja poročila o ugotovljenih kršitvah, kadar je odpravljena zaupnost podatkov. Če lahko posameznik domneva, da bo poročilo vplivalo nanj, lahko začne postopek na sodišču na podlagi ugotovitve kršitve prava.

3.5.2.2 Zakon o dostopu do informacij javnega značaja

Pravno sredstvo, ki je na voljo vsem osebam, je vložitev zahtevka za dostop do informacij javnega značaja na podlagi zakona o dostopu do informacij javnega značaja (Freedom of Information Act, v nadaljnjem besedilu: FOIA). Po navedbah vlade ZDA lahko zahtevek na podlagi FOIA načeloma vloži katera koli oseba, ne glede na to, ali je državljan ZDA ali ne, tako da preprosto zaprosi za kakršno koli evidenco agencije. To vključuje evidence o posamezniku, čeprav se v takem primeru zahteva predložitev potrdila o istovetnosti. Vendar če so podatki zaupni za zaščito nacionalne varnosti, zahtevek na podlagi FOIA verjetno ne bo

odobren, saj se uporablja izjema: agencije niso zavezane zagotoviti dostopa do zaupnih podatkov, tudi če se ti podatki nanašajo na posameznike, ki so vložili zahtevek. Podatki v zvezi s preiskavami kazenskega pregona, ki še potekajo, so v celoti izključeni iz zahtevkov na podlagi FOIA. Ne nazadnje, razlaga zahtevka na podlagi FOIA s strani WP29 neodvisnemu organu ne daje pravice, da preveri zakonitost obdelave.

3.5.3 Varuh človekovih pravic na področju zasebnostnega ščita

3.5.3.1 Ustanovitev varuha človekovih pravic

Zasebnostni ščit vzpostavlja nov mehanizem „za posameznike iz EU“, ki lahko vložijo zahtevke v zvezi z „obveščevalnimi dejavnostmi SIGINT v ZDA“ pri novoustanovljenem varuhu človekovih pravic. Na mesto varuha človekovih pravic, kot je pojasnjeno v memorandumu, priloženem k dopisu zunanjega ministra Johna Kerryja z dne 22. februarja 2016, bo imenovana namestnica ministra C. Novelli. To funkcijo bo opravljala poleg svoje vloge „višje koordinatorke za mednarodno diplomacijo v informacijski tehnologiji“, tj. vloge, vzpostavljene s členom 4(d) PPD-28. V dopisu in memorandumu je poudarjeno, da „namestnica ministra poroča neposredno zunanjemu ministru in je neodvisna od obveščevalne skupnosti“.

V memorandumu je pojasnjeno, da varuh človekovih pravic na področju zasebnostnega ščita kljub svojemu nazivu ne bo obdeloval le zahtevkov, ki se nanašajo na dostop za potrebe nacionalne varnosti do podatkov, prenesenih iz EU v ZDA v skladu z zasebnostnim ščitom, temveč tudi zahtevke, pri katerih so bili podatki preneseni v skladu s standardnimi pogodbenimi klavzulami, zavezujočimi poslovnimi pravili, odstopanji (na podlagi člena 26 Direktive 95/46/ES) ali „morebitnimi prihodnjimi odstopanji“, kot je opredeljeno v opombi 2 memoranduma.

Način delovanja mehanizma je mogoče povzeti tako: posameznik iz EU vloži zahtevek pri pristojnem organu države članice za nadzor nad nacionalnimi varnostnimi službami ali centraliziranem „organu za obravnavo pritožb posameznikov iz EU“, če bo ta ustanovljen ali imenovan. Organ, ki zahtevek posreduje varuhu človekovih pravic, bo moral najprej preveriti, ali je zahtevek popoln, kot je opredeljeno v točki 3(b) dopisa[60]. Ko je zahtevek predložen varuhu človekovih pravic in je ugotovljeno, da je skladen s točko 3(b), varuh človekovih pravic na področju zasebnostnega ščita zagotovi odgovor, kar pomeni, da bo končno potrdil, da „(i) je bila pritožba primerno proučena in (ii) da so bili pravo, zakoni, odredbe,

[60] b. Organ za obravnavo pritožb posameznikov iz EU bo v skladu z naslednjimi ukrepi zagotovil, da je zahtevek popoln:
(i) preverjanje identitete posameznika ter preverjanje, da posameznik nastopa v svojem imenu in ne kot predstavnik vladne ali medvladne organizacije;
(ii) zagotovitev, da je zahtevek pripravljen pisno in da vsebuje naslednje osnovne informacije:
• vse informacije, ki tvorijo podlago za zahtevek;
• vrsto informacij ali zahtevanega nadomestila;
• morebitne vladne subjekte Združenih držav, ki naj bi bili vpleteni, in
• druge ukrepe, izvedene za pridobivanje informacij ali zahtevanega nadomestila, ter odgovore, prejete na podlagi teh drugih ukrepov;
(iii) preverjanje, ali se zahtevek nanaša na podatke, za katere obstaja utemeljen sum, da so bili preneseni iz EU v Združene države v skladu z zasebnostnim ščitom, standardnimi pogodbenimi klavzulami, zavezujočimi poslovnimi pravili, odstopanji ali morebitnimi prihodnjimi odstopanji;
(iv) sprejem začetne ugotovitve, da zahtevek ni neresen, nadležen ali predložen v slabi veri.

predsedniške direktive in politike agencij ZDA, ki določajo omejitve in zaščitne ukrepe, opisane v dopisu urada direktorja obveščevalne službe, upoštevani ali da je bilo v primeru neupoštevanja to neupoštevanje odpravljeno“[61]. V odgovoru „ne bo niti potrjeno niti zanikano, ali je posameznik tarča nadzora, prav tako pa varuh človekovih pravic na področju zasebnostnega ščita ne bo potrdil posebnega pravnega sredstva, ki je bilo uporabljeno“[62]. Kar zadeva vprašanje, kako se izvede preiskava varuha človekovih pravic, je pojasnjeno, da bo varuh človekovih pravic na področju zasebnostnega ščita „tesno sodeloval z drugimi ameriškimi vladnimi uradniki, tudi z ustreznimi neodvisnimi nadzornimi organi“[63], in natančneje, da bo „lahko tesno sodeloval z uradom direktorja nacionalne obveščevalne službe, ministrstvom za pravosodje ter po potrebi z drugimi ministrstvi in agencijami, vključenimi v nacionalno varnost Združenih držav, ter generalnimi inšpektorji, uradniki, pooblaščenimi po zakonu o dostopu do informacij javnega značaja, ter uradniki na področju državljanskih svoboščin in zasebnosti“[64]. To usklajevanje je takšno, da zagotavlja, da lahko varuh človekovih pravic na področju zasebnostnega ščita pošlje odgovor, vključno s potrditvami, kot je opisano zgoraj.

3.5.3.2 Ocena novega mehanizma varuha človekovih pravic

Delovna skupina priznava prizadevanja Evropske komisije in vlade ZDA za uvedbo novega mehanizma za izboljšanje možnosti uporabe pravnih sredstev v zvezi z nadzornimi dejavnostmi ZDA. Zaveda se, da je ocena tega mehanizma kot novosti v mednarodnih odnosih, kar zadeva obveščevalne dejavnosti SIGINT ali nacionalno varnost, še posebno pomembna.

V tem oddelku bo WP29 ocenila, kako je ustanovitev varuha človekovih pravic na področju zasebnostnega ščita povezana s potrebnimi zahtevami, da posamezniki uporabijo pravna sredstva, kot določajo Listina, EKČP in sodna praksa evropskih sodišč.

3.5.3.3 Ali je lahko ustanovitev varuha človekovih pravic sama po sebi zadostna?

Prvič, treba si je postaviti vprašanje, ali se lahko ustanovitev „varuha človekovih pravic“ sploh kdaj šteje za skladno s členom 47 Listine, ki navaja učinkovito pravno sredstvo pred nepristranskim sodiščem[65], vsaj če ni nobene druge možnosti za uporabo učinkovitega pravnega sredstva. To je pomembno, saj se Sodišče v zadevi Schrems, v pomembnem premisleku št. 95 sklicuje na člen 47 Listine, pri čemer ne navaja, da bi bilo treba člen 47 razlagati ob upoštevanju sprememb v okviru nadzornih ukrepov. V nasprotju s tem pa je

[61] Člen 4.e Priloge III zasebnostnega ščita.
[62] Člen 4.e Priloge III zasebnostnega ščita.
[63] Člen 2.a Priloge III zasebnostnega ščita.
[64] Člen 2.a Priloge III zasebnostnega ščita.
[65] V pojasnilih v zvezi z Listino o temeljnih pravicah je poleg tega navedeno, da bi bilo treba člen 47 razlagati kot zagotavljanje jamstva pravice do učinkovitega pravnega sredstva pred sodiščem (pojasnilo v zvezi z Listino o temeljnih pravicah, pojasnilo člena 47 (2007/C 303/02)).

Sodišče že uporabilo člen 47 Listine v zadevi Kadi II[66] za ukrepe nadzora za namene nacionalne oziroma mednarodna varnosti[67].

Vendar sodna praksa ESČP jasno kaže, da pravna sredstva pred rednimi sodišči niso pogoj, da se sistemi nadzora štejejo za skladne s členom 8 (in členom 13 EKČP)[68]. Sodišče je namesto tega v skladu s členom 8 kot potreben zaščitni ukrep za dejavnosti nadzora določilo, da je lahko upoštevno tudi pravno varstvo pred drugimi organi. Vendar ESČP veliko pričakuje od drugih organov, ki zagotavljajo učinkovita pravna sredstva, pri čemer navaja, da mora biti tak organ „neodvisen od organov, ki izvajajo nadzor, ter imeti zadostna pooblastila in pristojnosti za izvajanje učinkovitega in stalnega nadzora“[69].

V zadevi Kennedy in zadevi Klass je ESČP pojasnilo, kaj bi lahko ta pričakovanja pomenila v okviru tajnega nadzora, kadar posameznik, na katerega se nanašajo osebni podatki, ni obveščen o obdelavi svojih podatkov. ESČP je organe v obeh sodbah obravnaval kot neodvisne, zlasti neodvisne od organov, ki izvajajo nadzor, pa tudi neodvisne od navodil[70] katerega koli drugega organa. Natančneje, v zadevi Kennedy je Sodišče odobrilo neodvisni in nepristranski organ, ki je sprejel svoj poslovnik in ki so ga sestavljali člani na visokih sodniških položajih ali izkušeni pravniki[71].

Organi so pri proučevanju pritožb posameznikov v obeh sodbah imeli tudi dostop do vseh ustreznih informacij, vključno z zaupnim gradivom. Ne nazadnje, obe stranki sta imeli pooblastila za odpravo neskladnosti[72].

Poleg vprašanja, ali se lahko varuh človekovih pravic šteje za „sodišče“, uporaba člena 47(2) pomeni dodaten izziv, saj določa, da mora biti sodišče „ustanovljeno z zakonom“. Vendar je vprašljivo, ali se lahko memorandum, ki določa delovanje novega mehanizma, šteje za „zakon“.

Zato se je delovna skupina ob upoštevanju načela enakovrednosti odločila, da bo namesto, da bi ocenila, ali se lahko varuh človekovih pravic šteje za sodišče, ustanovljeno z zakonom, dodatno pojasnila podrobnosti sodne prakse v zvezi s posebnimi zahtevami, potrebnimi za obravnavanje „pravnih sredstev“ in „pravnega varstva“ kot skladnih s temeljnimi pravicami iz členov 7, 8 in 47 Listine ter člena 8 (in 13) EKČP. V dodatni analizi se bo delovna skupina po razpravi o področju uporabe novega mehanizma tako osredotočila na naslednja merila: zahtevo po predložitvi zahtevka varuhu človekovih pravic in prejetju odgovora („procesno upravičenje“), neodvisnost varuha človekovih pravic, njegova preiskovalna pooblastila, da

[66] Združene zadeve C-584/10 P, C-593/10 P in C-595/10 P, Evropska komisija in Združeno kraljestvo proti Kadi, z dne 18. julija 2013.
[67] Točki 97 in 100 v zadevi Kadi II: vsi akti Unije, vključno s tistimi, ki so namenjeni izvajanju resolucij, ki jih je Varnostni svet sprejel v skladu s poglavjem VII Listine Združenih narodov, so zdaj v postopku pregleda zakonitosti s strani sodišč Evropske unije (poglavje VII se nanaša na ukrepe v zvezi z ogrožanjem miru, kršitvami miru in agresijo).
[68] Člen 13 EKČP države članice zavezuje, da zagotovijo, da ima „vsakdo, čigar pravice in svoboščine […] so kršene, […] pravico do učinkovitih pravnih sredstev pred domačimi oblastmi […]“. Ni nujno, da je to pravosodni organ, kot je ESČP pojasnilo v zadevi Klass, točki 56 in 67.
69 Zadeva Klass, točki 56 in 67.
[70] ESČP, zadeva Klass, točki 21 in 53.
[71] Komisijo G-10 (med sodbo) sestavljajo trije člani, pri čemer mora biti predsednik usposobljen za opravljanje sodne funkcije (točki 21 in 53 v zadevi Klass).
[72] ESČP, zadeva Kennedy, točka 167; zadeva Klass, točki 21 in 53.

dostopa do potrebnega gradiva, vključno z zaupnimi dokumenti, in zahteva pomoč drugih agencij, ter ne nazadnje njegovo pooblastilo za odpravo neskladnosti.

3.5.3.4 Področje uporabe mehanizma varuha človekovih pravic

Kar zadeva dostop do mehanizma varuha človekovih pravic, WP29 meni, da bi morali za vse osebe, za katere se uporablja pravo EU, veljati zaščitni ukrepi v okviru zasebnostnega ščita. Razlikovanje na podlagi državljanstva ne bi bilo sprejemljivo, zlasti ob upoštevanju, da bi morale temeljne pravice v EU veljati za vsakogar in ne le za tiste, ki imajo potni list EU. Priloga III se nanaša na „posameznika iz EU“, pri čemer ni nadalje opredeljeno, kdo je to. Delovna skupina obžaluje to negotovost in predlaga pojasnilo v smislu, da imajo vse osebe, za katere se uporablja pravo EU, pravico, da se njihov zahtevek, predložen varuhu človekovih pravic, obravnava v skladu s pogoji iz memoranduma. Poleg tega bi morali Komisija in ZDA obravnavati vprašanje, v kakšnem obsegu se bo zasebnostni ščit uporabljal tudi za državljane/prebivalce držav EGP in Švice, ki so bili v preteklosti zajeti v shemo varnega pristana.

WP29 nadalje ugotavlja določeno negotovost glede področja uporabe mehanizma varuha človekovih pravic. Čeprav memorandum določa, da je varuh človekovih pravic odgovoren za obdelavo zahtevkov v zvezi z nacionalno varnostjo glede podatkov, prenesenih iz EU v ZDA v skladu z vsemi razpoložljivimi orodji za prenos na podlagi prava EU, je v njem tudi pojasnjeno, da določa mehanizem „v zvezi z obveščevalnimi dejavnostmi SIGINT“. Slednji izraz pomeni, da so zajeti samo taki prenosi podatkov, pri katerih so bili podatki zbrani z obveščevalnimi dejavnostmi SIGINT, zaradi česar se postavlja vprašanje, ali se podatki, zbrani na primer na podlagi FISA, štejejo za „obveščevalne podatke v okviru SIGINT“. Zdi se, da to velja, kar zadeva člen 702, kot je pojasnjeno v zagotovilu ODNI, str. 10[73]. Vendar WP29 obžaluje, da uporaba izraza „obveščevalni podatki v okviru SIGINT“ povzroča nepotrebno negotovost v zvezi s tem.

Druga posledica je razumevanje delovne skupine, da mehanizem varuha človekovih pravic ne zajema zahtevkov, povezanih z dostopom organov kazenskega pregona[74]. V tem primeru še vedno ne bi bilo jasno, ali bi mehanizem zajemal zahtevke nekaterih agencij, predvsem CIE.

3.5.3.5 „Procesno upravičenje“ in postopek zahtevka

Začetek sodnega postopka zoper nadzorne ukrepe s strani vlade ZDA pred rednimi sodišči v Združenih državah je zelo težaven. Delovna skupina se zaveda, da je Vrhovno sodišče v zadevah, povezanih z obveščevalnimi dejavnostmi, v katerih prosilec ni mogel dokazati individualne „konkretne, podrobno opredeljene in dejanske ali neposredne škode“, odreklo procesno upravičenje[75]. Iz tega vidika je ustanovitev varuha človekovih pravic pomemben korak, saj pomeni dodatno možnost za določeno obliko pravnega varstva, ki sicer ne bi obstajala. Zato delovna skupina pozdravlja pojasnilo v točki 3(c). V skladu s tem oddelkom za

[73] Priloga VI zasebnostnega ščita, str. 10.
[74] Memorandum o ustanovitvi varuha človekovih pravic, str. 1.
[75] Clapper proti Amnesty International USA, 568 U.S. ___ (2013) II. str. 10.

vložitev zahtevka v okviru novega mehanizma ni potrebno dokazilo, da se je z obveščevalnimi dejavnostmi SIGINT dejansko dostopalo do podatkov vlagatelja zahtevka.

Delovna skupina večinoma podpira postopek za identifikacijo pritožnika v okviru mehanizma varuha človekovih pravic. Popolnoma smiselno je, da identifikacija poteka na ozemlju EU, kar velja tudi za mehanizem dostopa v okviru sporazuma o TFTP2 med EU in ZDA. Vendar delovna skupina ne razume, zakaj bi morali preverjanje v EU izvajati „organi držav članic, pristojni za nadzor nacionalnih varnostnih služb“. Prvič, ne zdi se verjetno, da bi lahko Evropska komisija na podlagi člena 4(2) Pogodbe o Evropski uniji tem organom dodeljevala naloge, ki nedvoumno spadajo v pristojnost držav članic.

Poleg tega lahko vključenost ustreznih organov glede na raznolikost mehanizmov za nadzor nacionalnih varnostnih služb v državah članicah resno vpliva na učinkovitosti sistema za državljane v državah članicah. Na primer, kadar je več organov odgovornih za nadzor nacionalnih varnostnih služb in posamezniki morda težko ugotovijo, kateri se pomembni, kadar veljavni nacionalni pravni predpisi ne zagotavljajo možnosti, da posamezniki vzpostavijo stik z ustreznim nadzornim organom, ali kadar ti organi niso ustanovljeni tako, da bi bili primerni za opravljanje nalog, ki so jim naložene v osnutku sklepa o ustreznosti[76]. Ob upoštevanju vključenosti organov za varstvo podatkov pri uporabi in nadzoru zasebnostnega ščita, pa tudi njihove podobne vloge na podlagi sporazuma o TFTP2 je bolj smiselno dodeliti to nalogo nacionalnim organom za varstvo podatkov držav članic. Delovna skupina poudarja, da po njenem mnenju ni verjetno, da bi se zaupni podatki obdelovali v okviru postopka pred varuhom človekovih pravic na področju zasebnostnega ščita, saj bo vsak odgovor le „skladen ali neskladen, ne bodo pa odpravljene neskladnosti“.

3.5.3.6 Neodvisnost

V zagotovilih zunanjega ministra je jasno navedeno, da bo mnenje varuha človekovih pravic izdal namestnik ministra za zunanje zadeve. Imenuje ga predsednik, potrditi pa ga mora senat. Vloga varuha človekovih pravic ne zahteva dodatnih informacij; zadostuje dodelitev vloge varuha človekovih pravic. Namestnika ministra imenuje predsednik ZDA, usmerja ga zunanji minister kot varuh človekovih pravic, njegovo vlogo namestnika ministra pa potrdi senat ZDA. Kot je poudarjeno v dopisu in zagotovilih iz memoranduma, je varuh človekovih pravic „neodvisen od obveščevalne skupnosti ZDA“. Vendar se WP29 sprašuje, ali je varuh človekovih pravic ustanovljen v okviru najbolj primernega ministrstva. Zdi se, da je potrebna določena mera poznavanja in razumevanja delovanja obveščevalne skupnosti za učinkovito izpolnjevanje vloge varuha človekovih pravic, hkrati pa se je treba za njegovo neodvisno delovanje dejansko dovolj oddaljiti od obveščevalne skupnosti.

Zasebnostni ščit ne določa posebnih meril za razrešitev varuha človekovih pravic. Delovna skupina zato to razume tako, kot je mogoče varuha človekovih pravic razrešiti funkcije varuha človekovih pravic enako, kot ga je mogoče razrešiti funkcije namestnika ministra na

[76] Na primer, v nekaterih državah članicah EU lahko posamezniki pridobijo dostop do podatkov, ki jih hranijo nacionalne varnostne službe, samo na podlagi zahtevka, vloženega pri višjem sodišču.

ministrstvu za zunanje zadeve, kar bi lahko ogrozilo neodvisni položaj varuha človekovih pravic.

Očitno se imenovanje namestnika ministra na ministrstvu za zunanje zadeve, kot je varuh človekovih pravic, z vidika neodvisnosti razlikuje od določitve pristojnosti rednega sodišča za pravno varstvo posameznika. Zato se postavlja vprašanje, ali se lahko varuh človekovih pravic z vidika neodvisnosti šteje za enakovrednega drugim neodvisnim nadzornim organom, za katere je bilo ugotovljeno, da izpolnjujejo zahteve. V okviru nadzora sta to zlasti sodišče s preiskovalnimi pooblastili (Investigatory Powers Tribunal − IPT) v Združenem kraljestvu in Komisija G-10 v Nemčiji.

Če to drži, je potrebna dodatna ocena z analizo pooblastil, dodeljenih „neodvisnemu“.

3.5.3.7 Preiskovalna pooblastila

Sodišče je v zadevi Kadi II ob upoštevanju člena 47 Listine odločilo, da „mora biti zadevni osebi omogočeno, da se seznani z razlogi, na katerih temelji odločba v njeni zadevi, bodisi z upoštevanjem same odločbe bodisi z zahtevanjem in pridobitvijo razkritja zadevnih razlogov, brez poseganja v pristojnost sodišča, da od zadevnega organa zahteva, da razkrije zadevne informacije, zato da se ji omogoči obramba njenih pravic v čim boljših okoliščinah“[77]. Sodišča Evropske unije morajo zagotoviti, da se odločba sprejme na dovolj trdni dejanski podlagi[78]. Jasno navaja, da „se ni mogoče sklicevati na tajnost ali zaupnost […] informacij ali dokazov“, vsaj ne pred sodišči Evropske unije[79]. Zato je delovna skupina sklenila, da je treba varuhu človekovih pravic zagotoviti informacije in dokaze, ki podpirajo razloge za izvajanje ukrepa, da se izpolnijo zahteve Sodišča[80].

Ni še jasno, kakšen naj bi bil obseg preiskovalnih pooblastil varuha človekovih pravic. Osnutek sklepa Komisije in Priloga III ministrstva za zunanje zadeve sta popolnoma jasna v zvezi s tem vprašanjem. Glede na razumevanje delovne skupine bi moral varuh človekovih pravic dobiti dovolj informacij, da bi lahko ugotovil, ali postopek obdelave podatkov, ki ga izvajajo varnostne službe, poteka v skladu z zakonom, če to ne velja, pa poskrbeti, da se neskladnosti odpravijo. Vendar niti v dopisu ministrstva za zunanje zadeve niti v osnutku sklepa Komisije ni opredeljeno, ali bi imel varuh človekovih pravic neposredni dostop do podatkov o zadevnem posamezniku in bi tako lahko izvedel svojo preiskavo ali pa bi se lahko zanašal le na poročila drugih vladnih uradnikov ZDA.

3.5.3.8 Pooblastila za odpravo neskladnosti

Iz memoranduma je še vedno precej nejasno, kako lahko varuh človekovih pravic odredi odpravo neskladnosti. Poleg pomanjkanja jasnosti v zvezi s preiskovalnimi pooblastili je še vedno nejasno tudi to, v kakšnem obsegu bo varuh človekovih pravic kot tak dejansko

[77] Zadeva Kadi II, točka 100.
78 Zadeva Kadi II, točka 119.
79 Zadeva Kadi II, točka 125.
[80] Zadeva Kadi, točka 122; čeprav zadevnemu organu ni treba predložiti vseh informacij in dokazov, na katerih temeljijo razlogi.

sposoben odrediti odpravo neskladnosti in kakšen bi lahko bil rezultat tega. Ali bi lahko to pomenilo, da se podatki, ki so bili pridobljeni neskladno (tj. nezakonito), ne smejo več uporabiti v nobenem postopku in bi jih bilo treba izbrisati?

Poleg tega delovna skupina meni, da zasebnostni ščit ne omogoča kakršne koli pritožbe zoper „odločitev“ varuha človekovih pravic ali pregleda njegove „odločitve“.

Ne nazadnje, kar zadeva obvestilo varuha človekovih pravic pritožniku po proučitvi pritožbe, varuh človekovih pravic ne sme razkriti, ali je obveščevalna skupnost ravnala nezakonito. Odgovor bo vedno enak in splošen. Sodišče je v zadevi Kadi II odločilo, da mora pristojni organ (kot nadzorni organ) navesti razloge, ki vključujejo vse okoliščine, čeprav člen 296 PDEU ne zahteva podrobnega odgovora[81].

3.5.4 Zaključek

Obstoj učinkovitih pravnih sredstev za posameznike je za WP29 še vedno vzrok za zaskrbljenost. Prvič, osnutek sklepa o ustreznosti ne zagotavlja jasnega odgovora na vprašanje, v katerih primerih in pod kakšnimi pogoji lahko posamezniki vložijo pritožbo, da se določijo njihove pravice.

WP29 priznava in pozdravlja uvedbo alternativnega mehanizma pravnega varstva v obliki varuha človekovih pravic, kar je edinstvena sprememba v odnosih med EU in tretjimi državami. Poleg potrebe po pojasnitvi izraza „posamezniki iz EU“, kot je bilo že poudarjeno, mehanizem posameznikom zagotavlja dodatno možnost uveljavljanja pravnega varstva pri vladi ZDA za zagotovitev, da se kakršni koli osebni podatki prosilca obdelajo v skladu s pravom ZDA.

Hkrati WP29 pri ocenjevanju mehanizma varuha človekovih pravic glede na standarde za neodvisno sodišče v smislu člena 47 Listine ter zahteve, ki sta jih Sodišče in ESČP uveljavila v svoji sodni praksi v zadevah, povezanih z nadzorom, ugotavlja, da obstajajo večje pomanjkljivosti. Prvič, obstajajo pomisleki glede tega, ali se lahko varuh človekovih pravic šteje za (formalno in popolnoma) neodvisnega, zlasti zaradi razmeroma enostavne razrešitve politično imenovanih oseb. Drugič, še vedno obstajajo pomisleki glede pooblastil varuha človekovih pravic za izvajanje učinkovitega in stalnega nadzora. WP29 na podlagi razpoložljivih informacij iz Priloge III ne more sklepati, niti da bo imel varuh človekovih pravic stalno neposreden dostop do vseh informacij, spisov in sistemov IT, ki so potrebni za njegovo oceno, niti da lahko pristojne obveščevalne agencije dejansko prisili, da končajo kakršno koli neskladno obdelavo podatkov, in to prav gotovo v primeru nestrinjanja glede vprašanja, ali je obdelava podatkov skladna s pravom ali ne. Morda lahko dodatno pojasnilo funkcije in pooblastil varuha človekovih pravic odpravi te pomisleke WP29.

[81] Zadeva Kadi II, točka 116.

3.6 Sklepne opombe glede zaščitnih ukrepov in omejitev, ki se uporabljajo za nacionalne varnostne organe ZDA

WP29 želi zlasti Komisijo in organe ZDA pohvaliti za vsa njihova prizadevanja za povečanje preglednosti učinka, ki ga lahko imajo nadzorni programi ZDA na podatke, ki se prenašajo v okviru zasebnostnega ščita ali kakršnega koli drugega orodja za prenos. Od prvih Snowdnovih razkritij junija 2013 so bili sprejeti pomembni ukrepi. Vendar WP29 ugotavlja, de še vedno obstajajo pomisleki. Zahtevajo se vsaj dodatne razlage in pojasnila pravic in obveznosti v okviru zasebnostnega ščita.

Dva glavna pomisleka WP29 sta dejstvo, da organi ZDA ne izključujejo v celoti množičnega in neselektivnega zbiranja podatkov ter da pooblastila in funkcija varuha človekovih pravic niso podrobneje opredeljeni. Poleg tega bi morali biti nacionalni organi za varstvo podatkov pristojni, da začnejo postopek pred varuhom človekovih pravic v imenu posameznika namesto nadzornih organov za obveščevalne agencije. Čeprav WP29 vsekakor priznava poskuse za odpravo pomislekov organov za varstvo podatkov, bi bili dobrodošli dodatni zaščitni ukrepi za zagotovitev, da so kakršni koli posegi, ki so lahko posledica programov nadzora ZDA, potrebni v demokratični družbi.

4. OCENA JAMSTEV ZASEBNOSTNEGA ŠČITA, POVEZANIH S KAZENSKIM PREGONOM

4.1 Uvod

WP29 glede javnega dostopa do osebnih podatkov zaradi kazenskega pregona ugotavlja, da načela zasebnosti iz Priloge II zasebnostnega ščita vsebujejo izjemo, ki je enaka izjemi, določeni v načelih zasebnosti varnega pristana. Splošna narava izjeme je bila zato ohranjena, kar pomeni, da nova načela zasebnostnega ščita omogočajo poseganje v temeljne pravice posameznikov, katerih podatki se prenašajo iz EU v ZDA, „ki temeljijo na zahtevah nacionalne varnosti, javnega interesa ali odkrivanja in pregona“[82].

Vendar je bila ena od glavnih kritik Sodišča glede odločbe o varnem pristanu v zadevi Schrems to, da „ne vsebuje nobene ugotovitve glede tega, ali v Združenih državah obstajajo državni predpisi, katerih namen bi bil omejiti morebitne posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Unije v Združene države“.

WP29 zato pozdravlja prizadevanja vlade ZDA, da bi zagotovila več informacij o pravnem okviru v zvezi s poseganjem v osebne podatke, ki se prenašajo v okviru zasebnostnega ščita zaradi kazenskega pregona, vključno z veljavnimi omejitvami in zaščitnimi ukrepi. Hkrati poudarja, da proučuje vprašanje javnega dostopa, pri čemer upošteva dejstvo, da mora biti vsako poseganje v temeljne pravice do zasebnega življenja in varstva podatkov mogoče upravičiti v demokratični družbi. Zato je analizirala jamstva zasebnostnega ščita, povezana s kazenskim pregonom, pri čemer je uporabila okvir iz oddelka 1.2 tega mnenja.

[82] Zadeva Schrems, točka 87.

4.2 Uporaba bistvenih evropskih jamstev za dostop organov kazenskega pregona do podatkov, ki jih hranijo korporacije

4.2.1 Dostop organov kazenskega pregona do osebnih podatkov bi moral biti skladen s pravom ter temeljiti na jasnih, natančnih in dostopnih pravilih.

Priloga VII k zasebnostnemu ščitu vsebuje dopis ministrstva ZDA za pravosodje, ki „podaja kratek pregled glavnih preiskovalnih sredstev za pridobivanje poslovnih podatkov in drugih podatkov iz evidenc korporacij v Združenih državah za (civilne ali regulativne) potrebe kazenskega pregona ali javnega interesa, vključno z omejitvami dostopa, določenimi v teh pooblastilih“.

Vsi postopki iz Priloge VII izhajajo neposredno iz Ustave ZDA (četrtega amandmaja), zakonskega ali procesnega prava ali iz smernic in politik ministrstva za pravosodje. Vendar se Priloga VII ne nanaša izrecno na vse zakone, ki določajo te postopke, temveč se namesto tega osredotoča na kratek opis samih postopkov. V Prilogi VII je tudi navedeno, da „[…] so [tukaj] tudi druge pravne podlage za podjetja, s katerimi lahko izpodbijajo zahteve za podatke upravnih organov na podlagi njihove posebne panoge in vrst podatkov, ki jim imajo v lasti“, z več neizčrpnimi primeri, kot so zakon o bančni tajnosti (Bank Secrecy Act), zakon o poštenem kreditnem poročanju (Fair Credit Reporting Act) in zakon o pravici do finančne zasebnosti (Right to Financial Privacy Act).

WP29 ugotavlja, da je okvir zakonov, postopkov in politik razdrobljen ter da bo veljavna pravna podlaga za posamezno zahtevo za dostop odvisna od vrste zahtevanih podatkov, vrste podjetja, vrste pravnih postopkov (kazenski, upravni, povezani z drugim javnim interesom) in vrste subjekta, ki zahteva dostop.

Ker vsa veljavna pravila, s katerimi organi kazenskega pregona omejijo dostop na podatke, ki se prenašajo v okviru zasebnostnega ščita, temeljijo na ustavi, zakonskem pravu in preglednih politikah ministrstva za pravosodje, WP29 upošteva domnevo o dostopnosti teh pravil. Vendar se lahko jasnost in natančnost pravil ocenita le za vsako posamezno vrsto postopka in zahteve za dostop. WP29 zato z obžalovanjem ugotavlja, da taka ocena glede na razpoložljive informacije iz Priloge VII k zasebnostnemu ščitu in ugotovitve iz osnutka sklepa trenutno ni mogoča.

4.2.2 Dokazati je treba nujnost in sorazmernost v zvezi z zastavljenimi legitimnimi cilji

WP29 ustrezno ugotavlja, da se lahko zahteva za dostop do podatkov za namene kazenskega pregona šteje za legitimen cilj. Na primer, člen 8(2) EKČP dopušča posege javnega organa v pravico do varstva zasebnega življenja „v interesu […] javne varnosti, […] za preprečevanje kršitev reda ali kriminala“. Vendar so taki posegi sprejemljivi samo, če so nujni in sorazmerni[83].

[83] Glej delovni dokument o bistvenih evropskih jamstvih, str. 7−9. Za splošno oceno pojmov nujnost in sorazmernost glej „Mnenje št. 1/2014 WP29 o uporabi pojmov nujnost in sorazmernost ter o varstvu podatkov v sektorju kazenskega pregona“ z dne 27. februarja 2014.

V skladu z ustaljeno sodno prakso Sodišča načelo sorazmernosti zahteva, da je z zakonodajnimi ukrepi, ki predlagajo posege v pravice do zasebnega življenja in varstva osebnih podatkov, „mogoče uresničiti legitimne cilje, ki jim sledi *zadevna ureditev*, in da to ravnanje ne prestopi meje tega, kar je primerno in potrebno za uresničitev teh ciljev“[84] (naš poudarek). Zato se ocena nujnosti in sorazmernosti vedno izvede v povezavi s posebnim ukrepom, ki ga predvideva zakonodaja.

Organi ZDA v Prilogi VII navajajo, da lahko zvezni tožilci in zvezni preiskovalni agenti pridobijo dostop do dokumentov in drugih podatkov iz evidenc organizacij z „več vrstami obveznih sodnih postopkov, vključno s pozivi velike porote, sodnimi pozivi in nalogi za preiskavo“, ter lahko pridobijo druge komunikacije „v skladu z zveznimi kazenskimi pooblastili za prisluškovanje telefonskim pogovorom in uporabo snemalnikov klicev“[85]. Poleg tega lahko agencije s civilno in regulativno odgovornostjo organizacijam izdajo pozive za „poslovne evidence, elektronsko shranjene informacije ali druge oprijemljive predmete“[86]. V Prilogi VII je poleg tega navedeno, da se ti sodni postopki na splošno uporabljajo za pridobitev informacij od „korporacij“ v ZDA, ne glede na to, ali so certificirane v okviru zasebnostnega ščita ali ne in „ne glede na narodnost posameznika, na katerega se nanašajo [osebni] podatki“. Povedano drugače, zdi se, da so predmet te zaščite organizacije in ne sami posamezniki.

Osnutek sklepa, ki temelji na načelih zasebnostnega ščita, poleg ugotovitev iz Priloge VII vsebuje ugotovitve Komisije v zvezi z obstojem pravil v ZDA za omejitev posegov v temeljne pravice oseb, katerih osebni podatki se prenašajo iz EU v ZDA v okviru zasebnostnega ščita.

Ugotovitve iz osnutka sklepa se nanašajo zlasti na veljavne omejitve in zaščitne ukrepe na podlagi četrtega amandmaja Ustave ZDA, v skladu s katerimi se za preiskave in zasege s strani organov kazenskega pregona načeloma zahteva sodni nalog na podlagi dokazanega utemeljenega razloga[87]. Ugotovitve se nanašajo tudi na dejstvo, da je v izjemnih primerih, ko se zahteva za nalog ne uporablja, kazenski pregon predmet preskusa razumnosti[88].

Vendar v ugotovitvah ni pojasnjeno, kako se ti zaščitni ukrepi uporabljajo za nedržavljane ZDA. Dejansko osnutek sklepa v uvodni izjavi potrjuje, da „varstvo na podlagi četrtega amandmaja ne zajema nedržavljanov ZDA, ki ne živijo v Združenih državah“[89]. Nadalje je v istih odstavkih osnutka sklepa navedeno, da imajo nedržavljani ZDA „posredne koristi od varstva, ki je zagotovljeno podjetjem v ZDA, ki hranijo osebne podatke in so prejemniki zaprosil organov kazenskega pregona“. Vendar WP29 z obžalovanjem ugotavlja, da ta ugotovitev ne vsebuje nobenega sklica na pravni vir, niti iz zakonskega prava niti iz sodne prakse.

[84] Zadeva Digital Rights Ireland, točka 46 in navedena sodna praksa.
[85] Priloga VII, str. 2.
[86] Priloga VII, str. 4.
[87] Osnutek sklepa o ustreznosti, odstavek 107.
[88] Zasebnostni ščit, člen 107.
[89] Osnutek sklepa o ustreznosti, odstavek 108.

WP29 na splošno ugotavlja, da je sistem preiskovalnih sredstev, ki se uporabljajo za pridobivanje poslovnih podatkov in drugih podatkov iz evidenc korporacij v Združenih državah zaradi kazenskega pregona ali javnega interesa, vključno z omejitvami dostopa in zaščitnimi ukrepi, zapleteno področje ukrepov. Na podlagi razpoložljivih informacij tega sistema trenutno ni mogoče na splošno oceniti. Potrebna je posebna ocena v posameznih primerih, da bi se resnično ocenili nujnost in sorazmernost preiskovalnih ukrepov organov kazenskega pregona v zvezi s temeljnimi pravicami do zasebnega življenja in varstva podatkov.

4.2.3 Obstajati bi moral neodvisen mehanizem nadzora

WP29 ustrezno ugotavlja, da večina postopkov, opisanih v Prilogi VII, predpostavlja vključenost odločbe sodišča, preden organi pridobijo dostop do podatkov (npr. sodne odločbe za snemalnike klicev ter naprave za pasti in sledenje, sodne odločbe za nadzor v skladu z zveznim zakonom o prisluškovanju telefonskim pogovorom, nalogi za preiskavo – pravilo 41). Vendar se zdi, da vsi ne zahtevajo vnaprejšnje vključenosti sodišča. Na primer, civilne oblasti in regulativni organi „lahko izdajo pozive“[90]. V teh primerih obstaja možnost naknadnega sodnega nadzora nad primernostjo poziva, saj „lahko prejemnik upravnega poziva oporeka izvršitvi zadevnega poziva na sodišču“[91].

WP29 na podlagi razpoložljivih informacij ugotavlja, da je, kar zadeva dostop organov kazenskega pregona do podatkov, ki jih hranijo podjetja v ZDA, očitno vzpostavljen precej zanesljiv neodvisen mehanizem nadzora.

4.2.4 Posamezniku morajo biti na voljo učinkovita pravna sredstva

Kot je bilo že navedeno, „varstvo na podlagi četrtega amandmaja ne zajema nedržavljanov ZDA, ki ne živijo v Združenih državah“[92]. To pomeni, da nedržavljan ZDA ne bi mogel izpodbijati nalogov ali pozivov na sodišču s sklicevanjem na četrti amandma. V osnutku sklepa je določeno, da imajo nedržavljani ZDA posredne koristi od varstva, ki je zagotovljeno podjetjem v ZDA, ki hranijo osebne podatke in so prejemniki zaprosil organov kazenskega pregona. Vendar WP29 ugotavlja, da čeprav je to varstvo učinkovito, ne pomeni, da so posameznikom na voljo učinkovita pravna sredstva, saj se zdi, da je subjekt pravice do učinkovitega pravnega sredstva v tem scenariju podjetje, ki prejme zahtevo za dostop, in ne posameznik, katerega varstvo podatkov je ogroženo.

Priloga VII ne vsebuje nobenih dodatnih informacij v zvezi z morebitnimi pravnimi sredstvi, ki bi izhajala iz zakonskega prava in bi bila na voljo nedržavljanom ZDA, kadar organi ali podjetja nezakonito zagotovijo ali pridobijo dostop do vsebine njihovih podatkov.

WP29 pozdravlja dejstvo, da nedavno sprejeti zakon o pravnem varstvu[93] nedržavljanom ZDA zagotavlja pravice do pravnega varstva. Vendar so te pravice omejene na jasno

[90] Priloga VII, str. 4.
[91] Priloga VII, str. 4.
[92] Osnutek sklepa o ustreznosti, odstavek 108.
[93] Zakona o pravnem varstvu iz leta 2015, H.R. 1428.

opredeljene razloge za pravno varstvo: pravico do popravka ter dostopa do podatkov in odvetniških stroškov, kadar „imenovana zvezna agencija ali organ“ zavrne spremembo podatkov ali dostop do njih, in pravico do pridobitve pravnih sredstev v primerih „namernega ali zavestnega“ razkritja podatkov.

Poleg tega sodna praksa ZDA, navedena v opombah ustreznih uvodnih izjav osnutka sklepa, zlasti zadeve City of Ontario proti Quon[94], Maryland proti King[95] in Samson proti California[96], ni ustrezna za oceno, ali lahko nedržavljani ZDA vložijo tožbo na sodišču, da bi izpodbijali zakonitost poseganja v njihovo zasebnost[97]. Vse zadeve se nanašajo na pravico do zasebnega življenja in vsebujejo odločbe Vrhovnega sodišča ZDA, ki dejansko omejujejo uporabo četrtega amandmaja.

Na splošno WP29 priznava in pozdravlja sprejetje zakona o pravnem varstvu, vendar še vedno obstajajo dvomi, ali so posameznikom, na katere se nanašajo osebni podatki, dejansko na voljo učinkovita pravna sredstva.

4.3 Sklepne opombe

WP29 pozdravlja in priznava prizadevanja vlade ZDA, da zagotovi več informacij o pravnem okviru v zvezi s poseganjem v osebne podatke, ki se v okviru zasebnostnega ščita EU−ZDA prenašajo zaradi kazenskega pregona, vključno z veljavnimi omejitvami in zaščitnimi ukrepi.

Ugotavlja, da je sistem preiskovalnih sredstev organov kazenskega pregona, vključno z veljavnimi omejitvami in zaščitnimi ukrepi, obsežen in zapleten ter da so informacije, vključene v zasebnostni ščit, strnjene. WP29 zato obžaluje, da zaradi omejenih informacij (tj. iz Priloge VII k zasebnostnemu ščitu in o ugotovitvah iz osnutka sklepa) trenutno ne more zagotoviti celovite ocene glede dostopnosti, predvidljivosti ter nujnosti in sorazmernosti veljavnih pravil. Ne glede na druge ugotovitve WP29 v zvezi z zasebnostnim ščitom v tem mnenju bi lahko bila taka ocena del letnega pregleda zasebnostnega ščita.

Kar zadeva dostop organov kazenskega pregona, WP29 ugotavlja, da je očitno vzpostavljen precej zanesljiv neodvisen mehanizem nadzora. Poleg tega pozdravlja sprejetje zakona o pravnem varstvu, ki nedržavljanom ZDA zagotavlja pravice do pravnega varstva. Vendar ugotavlja, da so te pravice omejene. Poleg ugotovitve, da nedržavljan ZDA na sodišču s sklicevanjem na četrti amandma ne bi mogel izpodbijati nalogov ali pozivov, še vedno

[94] *City of Ontario, Cal. proti Quon*, Zbirka odločb Državnega sodišča št. 130, str. 2619, 2630 (2010).
[95] *Maryland proti King*, Zbirka odločb Državnega sodišča št. 133, str. 1958 in 1970 (2013).
[96] *Samson proti California*, Zbirka odločb Vrhovnega sodišča št. 547, str. 843 in 848 (2006).
[97] V zadevi *Ontario proti Quon* je sodišče odločilo, da mesto Ontario ni kršilo pravic svojih zaposlenih, ki izhajajo iz četrtega amandmaja, saj je bil dostop mestnih oblasti do vsebine zasebnih sporočil zadevnega zaposlenega razumen, ker je bil utemeljen z zakonitim namenom, povezanim z delom, in ni bil preobsežen. V zadevi *Samson proti California* je sodišče ugotovilo, da „četrti amandma policistu ne prepoveduje, da opravi preiskavo pogojno izpuščene osebe, ki ne temelji na sumu“. V zadevi *Maryland proti King* je sodišče odločilo, da če policisti izvedejo odvzem prostosti na podlagi verjetnega razloga za pridržanje osumljenca zaradi hudega kaznivega dejanja in ga privedejo na postajo na pridržanje, pri čemer odvzamejo vzorec DNK pridržane osebe na osnovi sline in ga analizirajo, je to tako kot odvzem prstnih odtisov in fotografiranje zakonit postopek registriranja osumljenca na policijski postaji ob odvzemu prostosti, ki je po četrtem amandmaju razumen.

obstajajo pomisleki, ali so posameznikom, na katere se nanašajo osebni podatki, dejansko na voljo učinkovita pravna sredstva na področju kazenskega pregona.

5. SKLEPNE UGOTOVITVE IN PRIPOROČILA

WP29 predvsem pozdravlja dejstvo, da je bil devet mesecev po razveljavitvi varnega pristana predstavljen nov osnutek sklepa o ustreznosti, ki vsebuje številne izboljšave v primerjavi s prejšnjim mehanizmom. Zlasti je zadovoljna z večjo preglednostjo, ki je na voljo z uvedbo dveh seznamov zasebnostnega ščita na spletnem mestu ministrstva za trgovino: enega, ki vsebuje evidence organizacij, ki so zavezane zasebnostnemu ščitu, in enega, ki vsebuje evidence organizacij, ki so bile ščitu zavezane v preteklosti, vendar zdaj niso več. Pozdravlja tudi večjo preglednost v zvezi z javnim dostopom do podatkov, ki se v okviru zasebnostnega ščita prenašajo zaradi nacionalne varnosti ali kazenskega pregona. Ne nazadnje, WP29 je zelo vesela spoznanja, da bo za vse prenose podatkov v ZDA odslej zagotovljeno enako varstvo: posebne pravne določbe, ki bi dajale prednost enemu orodju pred drugim, niso vzpostavljene.

5.1 Trije vzroki za zaskrbljenost

Vendar še vedno obstajajo trije glavni vzroki za zaskrbljenost, ki jih bo treba po mnenju WP29 obravnavati.

Prvi vzrok za zaskrbljenost je, da besedilo v osnutku sklepa o ustreznosti organizacije ne obvezuje, da izbriše podatke, če niso več potrebni. To je bistveni element prava EU na področju varstva podatkov za zagotovitev, da se podatki ne hranijo dlje, kot je potrebno, da se doseže namen, za katerega so bili zbrani. Drugič, WP29 na podlagi Priloge VI sklepa, da vlada ZDA ne izključuje v celoti nadaljnjega zbiranja množičnih in neselektivnih podatkov. Vztraja, da je tako zbiranje podatkov neupravičeno poseganje v temeljne pravice posameznikov. Tretji vzrok za zaskrbljenost pa se nanaša na uvedbo mehanizma varuha človekovih pravic. Čeprav WP29 pozdravlja ta ukrep brez primere, s katerim je bil ustvarjen dodatni mehanizem pravnega varstva in nadzora za posameznike, še vedno obstajajo pomisleki, ali ima varuh človekovih pravic dovolj pooblastil za učinkovito delovanje. Pojasniti je treba vsaj pooblastila in funkcijo varuha človekovih pravic, da se dokaže, da je njegova vloga resnično neodvisna in da lahko zagotovi učinkovito pravno varstvo za neskladno obdelavo podatkov.

5.2 Predlagana pojasnila

Poleg zgoraj navedenih vzrokov je WP29 v tem mnenju navedla različne točke, v katerih je primerno dodatno pojasnilo sklepa o ustreznosti. Najpomembnejše je, da se to nanaša na potrebo po zagotovitvi, da so ključni pojmi v zvezi z varstvom podatkov, ki so uporabljeni v zasebnostnem ščitu, opredeljeni in se uporabljajo skladno. Trenutno to ne velja. Dobro bi bilo pripraviti glosar izrazov v F.A.Q. zasebnostnega ščita, skupaj z opredelitvami, o katerih so se po možnosti dogovorile EU in ZDA. WP29 tudi ugotavlja, da prenosi osebnih podatkov iz EU tretjemu niso dovolj izdelani, zlasti kar zadeva njihov obseg, omejitev njihovega namena in jamstva, ki se uporabljajo za prenose posrednikom. Kar zadeva dostop do podatkov

zasebnostnega ščita s strani organov kazenskega pregona, obstajajo pomisleki zlasti v zvezi s predvidljivostjo zakonodaje zaradi obsežnega in zapletenega sistema kazenskega pregona ZDA na zvezni in državni ravni ter omejenih informacij, vključenih v sklep o ustreznosti.

Zasebnostni ščit je prvi sklep o ustreznosti, ki je bil pripravljen od načelnega dogovora o besedilih splošne uredbi o varstvu podatkov. Še vedno pa se številne izboljšave na ravni varstva podatkov, zagotovljene posameznikov, ne kažejo v zasebnostnem ščitu. WP29 zato predlaga, da bi bilo treba kmalu po začetku uporabe splošne uredbe o varstvu podatkov opraviti pregled zadevnega sklepa o ustreznosti, pa tudi sklepov o ustreznosti, ki so jih izdale druge tretje države.

Končno priporočilo WP29, ki ga je treba poudariti, se nanaša na skupni pregled. WP29 pozdravlja dejstvo, da se bo sklep o ustreznosti zasebnostnega ščita dejansko pregledal vsako leto, z obsežnim sodelovanjem organov za varstvo podatkov in drugih ustreznih strani. Želi si, da bi se vse strani precej pred prvim pregledom dogovorile o elementih skupnega pregleda, vključno s pripravo in predstavitvijo poročila o pregledu.