

Mnenje odbora (člen 70(1)(s))



Mnenje št. 5/2023 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA

Sprejeto 28. februarja 2023

Evropska komisija je 13. decembra 2022 objavila osnutek sklepa o ustreznosti (v nadaljevanju: osnutek sklepa), ki vključuje priloge, ki so del novega okvira za čezatlantske izmenjave osebnih podatkov, tj. okvira za varstvo zasebnosti podatkov med EU in ZDA (*Data Privacy Framework*, v nadaljevanju: DPF), ki naj bi nadomestil prejšnji zasebnostni ščit ZDA, ki ga je Sodišče Evropske unije (v nadaljevanju: Sodišče) razveljavilo 16. julija 2020 v zadevi *Schrems II*. Ključni sestavni del DPF so načela okvira za varstvo zasebnosti podatkov med EU in ZDA, vključno z dopolnilnimi načeli (v nadaljevanju skupaj: načela DPF).

Komisija je v skladu s členom 70(1)(s) Uredbe (EU) 2016/679¹ Evropskega parlamenta in Sveta (v nadaljevanju: Splošna uredba o varstvu podatkov) zaprosila Evropski odbor za varstvo podatkov (v nadaljevanju: EOVP) za mnenje o osnutku sklepa.

EOVP je na podlagi preučitve osnutka sklepa ocenil ustreznost ravni varstva, ki jo zagotavljajo ZDA. Ocenil je komercialne vidike in dostop javnih organov v ZDA do osebnih podatkov, prenesenih iz EU v ZDA, ter njihovo uporabo.

Upošteval je veljavni pravni okvir EU za varstvo podatkov, kot je določen v Splošni uredbi o varstvu podatkov, ter temeljne pravice do zasebnega življenja in varstva podatkov iz členov 7 in 8 Listine Evropske unije o temeljnih pravicah ter člena 8 Evropske konvencije o človekovih pravicah. Upošteval je tudi pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, določeno v členu 47 Listine, ter sodno prakso, povezano z različnimi temeljnimi pravicami.

Poleg tega je EOVP upošteval zahteve iz referenčnega dokumenta o ustreznosti, ki ga je sprejel².

Ključni cilj EOVP je podati mnenje Evropski komisiji glede ustreznosti ravni varstva, ki se zagotavlja posameznikom, katerih osebni podatki se prenesejo v ZDA. Treba je priznati, da EOVP od ZDA ne pričakuje, da bodo v svojem okviru varstva podatkov posnemale evropsko zakonodajo o varstvu podatkov.

EOVP pa kljub temu opozarja, da člen 45 Splošne uredbe o varstvu podatkov in sodna praksa Sodišča zahtevata, da se z zakonodajo tretje države posameznikom, na katere se nanašajo osebni podatki, zagotovi raven varstva, ki je v bistvenem enaka ravni, zagotovljeni v EU.

1.1 Splošni vidiki varstva podatkov

DPF določa, da je lahko zavezanost organizacij DPF načelom DPF v nekaterih primerih omejena (na primer kolikor je to potrebno za izpolnjevanje sodne odločbe ali uresničevanje javnega interesa). EOVP za boljšo opredelitev vpliva teh izjem na raven varstva posameznikov, na katere se nanašajo osebni podatki, priporoča, naj Komisija v osnutek sklepa vključi pojasnilo o področju uporabe izjem, vključno z veljavnimi zaščitnimi ukrepi v skladu z zakonodajo ZDA.

EOVP ugotavlja, da je zaradi sestave prilog in njihovega številčenja razmeroma težko najti informacije in se nanje sklicevati. To pripomore k zapleteni splošni predstavitvi novega okvira, katerega priloge

¹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

² Delovna skupina iz člena 29, [Referenčni dokument o ustreznosti, WP254 rev. 01, 28. november 2017, kakor je bil nazadnje spremenjen in sprejet 6. februarja 2018, ki ga je EOVP potrdil 25. maja 2018 \(v nadaljevanju: referenčni dokument o ustreznosti\)](#).

združujejo dokumente z različno pravno veljavnostjo in ki morda ne daje prednosti dobremu razumevanju načel DPF s strani posameznikov, na katere se nanašajo osebni podatki, organizacij DPF in organov EU za varstvo podatkov. EOVP tudi poudarja, da je treba izrazje v celotnem DPF uporabljati dosledno. Manjka tudi opredelitev nekaterih bistvenih izrazov³.

EOVP pozdravlja posodobitve načel DPF⁴, ki bodo zavezujoč pravni okvir za organizacije DPF, vendar ugotavlja, da so načela DPF, ki jih morajo organizacije DPF upoštevati, kljub številnim spremembam in dodatnim pojasnilom v uvodnih izjavah osnutka sklepa, v bistvu nespremenjena glede na načela, uporabljena v okviru zasebnostnega ščita (na katerih so temeljili letni skupni pregledi Delovne skupine iz člena 29 in EOVP). Načela DPF so večinoma enaka tudi načelom iz osnutka zasebnostnega ščita, ki so bila podlaga za mnenje Delovne skupine iz člena 29 iz leta 2016⁵. EOVP meni, da v zvezi z načeli DPF, ki se niso bistveno spremenila, ni treba ponoviti vseh predhodnih pripomb WP29. Odločil se je, da se bo osredinil na posebne vidike, za katere meni, da so danes še pomembnejši glede na razvoj pravnega in tehnološkega okolja.

EOVP na primer ugotavlja, da nekatera skrb vzbujajoča vprašanja, ki sta jih prej poudarila Delovna skupina iz člena 29 in EOVP v zvezi z načeli zasebnostnega ščita, še vedno niso rešena. Povezana so zlasti s pravicami posameznikov, na katere se nanašajo osebni podatki (na primer nekatere izjeme od pravice do dostopa ter rok in načini uveljavljanja pravice do ugovora), neobstoječem ključnih opredelitev, nejasnostjo v zvezi z uporabo načel DPF za obdelovalce in široko izjemo za javno dostopne informacije⁶.

EOVP želi tudi vnovič poudariti, da nadaljnji prenos od prvotnega uporabnika prenesenih podatkov ne sme ogroziti ravni varstva posameznikov, katerih osebni podatki se prenašajo⁷. EOVP vnovič poziva Komisijo, naj pojasni, da morajo biti zaščitni ukrepi, ki jih prvotni uporabnik naloži uvozniku v tretji državi, pred nadaljnjim prenosom podatkov v okviru DPF učinkoviti glede na zakonodajo tretje države.

Hiter razvoj na področju avtomatiziranega sprejemanja odločitev in oblikovanja profilov – vse bolj s pomočjo tehnologij umetne inteligence – zahteva posebno pozornost. EOVP pozdravlja sklicevanja Komisije na posebne zaščitne ukrepe, ki jih zagotavlja ustrezna zakonodaja ZDA na različnih področjih⁸. Vendar se zdi, da se raven varstva posameznikov razlikuje glede na to, katera pravila za posamezni sektor se v danih okoliščinah uporabljajo – če sploh katera. EOVP trdi, da so potrebna posebna pravila v zvezi z avtomatiziranim sprejemanjem odločitev, da se zagotovijo zadostni zaščitni ukrepi, vključno s pravico posameznika do seznanjenosti z razlogi zanje, pravico do izpodbijanja odločitve ter pravico do osebne posredovanja, če odločitev znatno vpliva na posameznika.

EOVP opozarja na pomen učinkovitega nadzora in izvrševanja DPF ter meni, da so preverjanja skladnosti v zvezi z bistvenejšimi zahtevami ključna. Te vidike bo pozorno spremljal, tudi v okviru rednih pregledov. Seznanjen je z obnovljenimi zavezami iz dopisov Zvezne komisije za trgovino (*Federal Trade Commission*, v nadaljevanju: FTC)⁹ in ministrstva za promet¹⁰ v zvezi z izvrševanjem, na primer, da se bodo preiskave domnevnih kršitev DPF obravnavale prednostno.

³ To velja za izraza „posrednik“ in „obdelovalec“. Poleg tega se je treba o pojmu „podatki o človeških virih“ še dogovoriti z organi ZDA.

⁴ Na primer pojasnilo, da so podatki, kodirani s šifrirnim ključem, osebni podatki.

⁵ [Mnenje št. 01/2016 Delovne skupine iz člena 29 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA, sprejeto 13. aprila 2016 \(v nadaljevanju: Mnenje št. 01/2016 Delovne skupine iz člena 29\)](#).

⁶ Zasebnostni ščit EU-ZDA – tretji skupni letni pregled, poročilo EOVP, sprejeto 12. novembra 2019, odstavek 11.

⁷ Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, 3.A.9.

⁸ Osnutek sklepa, uvodna izjava 35.

⁹ Osnutek sklepa, Priloga IV.

¹⁰ Osnutek sklepa, Priloga V.

EOVP ugotavlja, da je posameznikom iz EU, na katere se nanašajo osebni podatki, na voljo sedem možnosti pravnega varstva, če se njihovi osebni podatki obdelujejo v nasprotju z DPF. Ti mehanizmi pravnega varstva so enaki mehanizmom, vključenim v prejšnji zasebnostni ščit, na katerega je Delovna skupina iz člena 29 podala pripombe¹¹. EOVP bo natančno spremljal učinkovitost teh mehanizmov pravnega varstva, tudi v okviru rednih pregledov.

1.2 Dostop do osebnih podatkov, ki jih iz Evropske unije prenesejo javni organi v ZDA, in njihova uporaba

Evropska komisija je v osnutku sklepa sklenila, da bodo „vsi posegi javnih organov ZDA v temeljne pravice posameznikov, katerih osebni podatki se prenesejo iz Unije v Združene države, v javnem interesu, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter namene nacionalne varnosti v skladu z okvirom za varstvo zasebnosti podatkov med EU in ZDA, omejeni na tisto, kar je nujno potrebno za doseg zadevnega legitimnega cilja, ter da obstaja učinkovito pravno varstvo pred takimi posegi“¹².

Evropska komisija je sprejela svoj sklep po obsežni oceni Odredbe št. 14086 o krepitvi zaščitnih ukrepov za obveščevalne dejavnosti SIGINT v ZDA. Odredbo št. 14086 je izdal predsednik ZDA 7. oktobra 2022 po pogajanjih Evropske komisije z vlado ZDA, ko je Sodišče razveljavilo prejšnji sklep o ustreznosti, imenovan zasebnostni ščit.

Po mnenju EOVP bi bilo dobrodošlo, da so ne samo začetek veljavnosti, ampak tudi sprejetje sklepa pogojeni med drugim s sprejetjem posodobljenih politik in postopkov za izvajanje Odredbe št. 14086 s strani vseh obveščevalnih agencij ZDA. EOVP priporoča Komisiji, naj oceni te posodobljene politike in postopke ter mu posreduje svojo oceno.

EOVP je svojo analizo v zvezi z vladnim dostopom do osebnih podatkov, prenesenih v ZDA, osredinil na oceno nove Odredbe št. 14086, saj naj bi dejansko obravnavala in odpravila pomanjkljivosti, ki jih je Sodišče opredelilo v svoji sodbi v zadevi *Schrems II*, v kateri je prejšnji sklep o ustreznosti razglasilo za neveljaven.

EOVP priznava, da je bil pravni okvir ZDA za obveščevalne dejavnosti SIGINT spremenjen s sprejetjem Odredbe št. 14086, in vanjo vključene dodatne zaščitne ukrepe šteje za znatno izboljšavo. Odredba št. 14086 v pravni okvir ZDA o obveščevalni dejavnosti SIGINT uvaja pojma nujnosti in sorazmernosti ter zagotavlja nov mehanizem pravnega varstva za posameznike iz EU, če bi bila EU imenovana za organizacijo za regionalno gospodarsko povezovanje. EOVP meni, da je novi mehanizem pravnega varstva precej izboljšan v primerjavi s prejšnjim, tako imenovanim mehanizmom varuha človekovih pravic v okviru zasebnostnega ščita. V nasprotju s prejšnjim pravnim okvirom, ki ni ustvaril pravic za posameznike iz EU, na kar je Sodišče izrecno opozorilo, nova Odredba št. 14086 ustvarja take pravice ter zagotavlja več zaščitnih ukrepov za neodvisnost sodišča za presojo varstva podatkov (*Data Protection Review Court*) in učinkovitejša pooblastila za odpravo kršitev.

Ko je EOVP primerjal dodatne zaščitne ukrepe, vključene v Odredbo št. 14086, z evropskimi temeljnimi jamstvi, ki jih je kot standard oblikoval na podlagi sodne prakse Sodišča in Evropskega sodišča za človekove pravice (ESČP), je v svoji oceni še vedno opredelil številne točke, ki zahtevajo dodatna pojasnila, pozornost ali vzbujaajo zaskrbljenost. Iz teh točk je razvidno, da mnenje EOVP sicer temelji na sodbi v zadevi *Schrems II*, vendar mora obseg ocene EOVP nujno vključevati pomisleke, ki presegajo konkretne ugotovitve iz sodbe v zadevi *Schrems II*.

¹¹ Glej zlasti Mnenje št. 01/2016 Delovne skupine iz člena 29, oddelek 2.2.6 (a).

¹² Osnutek sklepa, uvodna izjava 195.

EOVP meni, da so v pravnem okviru ZDA potrebna nadaljnja pojasnila glede vprašanj, zlasti v zvezi z „začasnim množičnim zbiranjem“ ter nadaljnjo hrambo in razširjanjem (množično) zbranih podatkov.

Ker preizkus osnovne enakovrednosti ni preizkus identitete in ker so bili zaščitni ukrepi, vključeni v novi pravni okvir o obveščevalni dejavnosti SIGINT, okrepljeni, EOVP pozornost in skrb namenja predvsem oceni zaščitnih ukrepov v celoti z uporabo celovitega pristopa, ki zajema zaščitne ukrepe za celoten cikel obdelave – od zbiranja do razširjanja podatkov – ter vključuje elemente nadzora in pravnega varstva.

V zvezi s tem EOVP poudarja naslednje ugotovitve:

Čeprav priznava, da Odredba št. 14086 v pravni okvir o obveščevalni dejavnosti SIGINT uvaja pojma nujnosti in sorazmernosti, poudarja potrebo po natančnem spremljanju učinkov teh sprememb v praksi, vključno s pregledom notranjih politik in postopkov za izvajanje zaščitnih ukrepov iz Odredbe na ravni agencije.

Pozdravlja tudi dejstvo, da Odredba št. 14086 vsebuje seznam posebnih namenov, za katere se lahko zbirajo podatki ali se jih ne sme zbirati, pri čemer ugotavlja, da se cilji lahko posodobijo z dodatnimi – ne nujno javnimi – cilji glede na nove nacionalne varnostne zahteve.

Ugotovil je, da je pomanjkljivost sedanjega pravnega okvira ZDA zlasti ta, da dovoljuje zbiranje množičnih podatkov v skladu z Odredbo št. 12333, ne zahteva pa predhodne odobritve s strani neodvisnega organa, kot to zahteva najnovejša sodna praksa ESČP, niti ne določa sistematičnega neodvisnega naknadnega pregleda, ki bi ga izvedlo sodišče ali enakovreden neodvisni organ. Glede predhodne neodvisne odobritve nadzora v skladu s členom 702 FISA EOVP obžaluje, da sodišče FISA (*FISA Court*, v nadaljevanju: FISC), ko potrdi program, ki dovoljuje, da so predmet nadzora nedržavljeni ZDA, ne preveri, ali je zahtevek za program skladen z Odredbo št. 14086, čeprav so obveščevalni organi, ki program izvajajo, temu zavezani. EOVP meni, da bi bilo treba kljub temu upoštevati dodatne zaščitne ukrepe iz navedene odredbe, kar velja tudi za FISC. Opozarja, da bi bila poročila Odbora za nadzor zasebnosti in državljanskih svoboščin (*Privacy and Civil Liberties Oversight Board*, v nadaljevanju: PCLOB) še posebej koristna za oceno, kako se bodo izvajali zaščitni ukrepi iz Odredbe št. 14086 in kako se ti zaščitni ukrepi uporabljajo pri zbiranju podatkov v skladu s členom 702 FISA in Odredbo št. 12333.

Glede mehanizma pravnega varstva EOVP priznava znatne izboljšave v zvezi s pristojnostmi sodišča za presojo varstva podatkov in njegovo večjo neodvisnostjo v primerjavi z varuhom človekovih pravic. EOVP prav tako priznava dodatne zaščitne ukrepe, predvidene v novem mehanizmu pravnega varstva, kot sta vloga posebnih odvetnikov, ki vključuje zagovarjanje interesov pritožnika, ter pregled mehanizma pravnega varstva s strani PCLOB. EOVP je ob upoštevanju narave nacionalne varnosti in zaščitnih ukrepov iz Odredbe št. 14086 kljub temu zaskrbljen zaradi splošne uporabe standardnega odgovora, v katerem sodišče za presojo varstva podatkov pritožnika obvesti, da bodisi niso bile ugotovljene nobene zajete kršitve bodisi da je bila izdana odločitev, da je potrebna ustrezna odprava kršitve in da proti njej ni mogoče vložiti pritožbe. EOVP glede na pomembnost mehanizma pravnega varstva poziva Komisijo, naj pozorno spremlja delovanje tega mehanizma v praksi.

Pričakuje, da bo Komisija izpolnila svojo zavezo o začasnem zadržanju izvajanja, razveljavitvi ali spremembi sklepa o ustreznosti v nujnih primerih, zlasti če bi se izvršilna veja oblasti ZDA odločila omejiti zaščitne ukrepe, vključene v odredbo¹³.

¹³ Osnutek sklepa, uvodna izjava 212.

EOVP na splošno z zadovoljstvom ugotavlja, da Odredba zagotavlja znatne izboljšave v primerjavi s prejšnjim pravnim okvirom, zlasti glede uvedbe načel nujnosti in sorazmernosti ter posameznih mehanizmov pravnih sredstev za posameznike iz EU, na katere se nanašajo osebni podatki. Glede na izražene pomisleke in zahtevana pojasnila meni, da bi bilo treba te pomisleke obravnavati, in predlaga, naj Komisija zagotovi zahtevana pojasnila, da se okrepijo razlogi za osnutek sklepa in v prihodnjih skupnih pregledih zagotovi pozorno spremljanje konkretnega izvajanja tega novega pravnega okvira, zlasti zaščitnih ukrepov, ki jih zagotavlja.

Kazalo

1	UVOD.....	9
1.1	Okvir ZDA za varstvo podatkov.....	9
1.2	Obseg ocene EOVP.....	11
1.3	Splošne pripombe in pomisleki	13
1.3.1	Ocena nacionalnega prava.....	13
1.3.2	Mednarodne zaveze, ki so jih sprejele ZDA.....	13
1.3.3	Napredek na področju zakonodaje ZDA o varstvu podatkov.....	14
1.3.4	Področje uporabe osnutka sklepa	14
1.3.5	Omejitve dolžnosti spoštovanja načel DPF	14
1.3.6	Spremembe v zvezi z „zasebnostnim ščitom“.....	15
1.3.7	Nejasnost dokumentov DPF.....	15
2	SPLOŠNI VIDIKI VARSTVA PODATKOV	16
2.1	Vsebinska načela	16
2.1.1	Pojmi.....	16
2.1.2	Načelo omejitve namena.....	16
2.1.3	Pravica do dostopa, popravka, izbrisa in ugovora	17
2.1.4	Omejitve nadaljnjih prenosov podatkov.....	18
2.1.5	Avtomatizirano sprejemanje odločitev in oblikovanje profilov.....	19
2.2	Postopkovni mehanizmi in mehanizmi izvrševanja	20
2.3	Mehanizmi pravnega varstva.....	21
3	DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V ZDA, IN NJIHOVA UPORABA.....	22
3.1	Dostop in uporaba za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ..	22
3.1.1	Dostop organov kazenskega pregona do osebnih podatkov bi moral temeljiti na jasnih, natančnih in dostopnih pravilih	22
3.1.2	Dokazati je treba nujnost in sorazmernost v zvezi z zastavljenimi legitimnimi cilji	23
3.1.3	Obstajati bi moral neodvisen mehanizem nadzora	24
3.1.4	Posamezniku morajo biti na voljo učinkovita pravna sredstva	24
3.1.5	Nadaljnja uporaba zbranih informacij.....	25
3.2	Dostop in uporaba za namene nacionalne varnosti	26
3.2.1	Jamstvo A – obdelava bi morala biti skladna s pravom ter temeljiti na jasnih, natančnih in dostopnih pravilih	27
3.2.2	Jamstvo B – dokazati je treba nujnost in sorazmernost v zvezi z zastavljenimi legitimnimi cilji	30
3.2.3	Jamstvo C – Nadzor	39

3.2.4	Jamstvo D – posamezniku morajo biti na voljo učinkovita pravna sredstva.....	43
4	IZVAJANJE IN SPREMLJANJE OSNUTKA SKLEPA	51

Evropski odbor za varstvo podatkov je –

Evropski odbor za varstvo podatkov je sprejel naslednjo izjavo:

ob upoštevanju člena 70(1)(s) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov)¹,

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018²,

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE MNENJE:

1 UVOD

1.1 Okvir ZDA za varstvo podatkov

1. Združene države Amerike (v nadaljevanju: ZDA) in Evropska unija (v nadaljevanju: EU) imajo različne pristope k zasebnosti in varstvu podatkov. V EU sta zasebnost in varstvo podatkov temeljni pravici, ki ju zagotavljata člena 7 in 8 Listine o temeljnih pravicah, v ZDA pa se varstvo podatkov na splošno obravnava z vidika varstva potrošnikov. Posledično se regulativna pristopa v ZDA in EU razlikujeta³.
2. V nasprotju s celovitim pristopom EU, ki se uporablja v Splošni uredbi o varstvu podatkov, v ZDA ni celovitega splošnega zakona o varstvu podatkov na zvezni ravni. Varovanje zasebnosti se v ZDA uresničuje s sektorskim in državnim pristopom. Nekateri specifični sektorji so na primer zajeti v posebnih zakonih, kot so:
 - *Health Insurance Portability and Accountability Act* (Zakon o prenosu zdravstvenih podatkov in s tem povezani odgovornosti, v nadaljevanju: HIPAA)⁴;

¹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP) (UL L 119, 4. 5. 2016, str. 1).

² Sklicevanja na „države članice“ v tem mnenju je treba razumeti kot sklicevanja na „države članice EGP“.

³ Glej tudi oddelek I Priloge I k osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustrezni ravni varstva osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA, objavljenem 13. decembra 2022 (v nadaljevanju: osnutek sklepa).

⁴ *Health Insurance Portability and Accountability Act* (Zakon o prenosu zdravstvenih podatkov in s tem povezani odgovornosti) iz leta 1996 (v nadaljevanju: HIPAA) je zvezni zakon ZDA. Oblikuje nacionalne standarde za zaščito občutljivih zdravstvenih podatkov pacientov. Cilj HIPAA je ustrezno zaščititi zdravstvene podatke posameznikov, hkrati pa omogočiti pretok takih podatkov za zagotavljanje in spodbujanje visokokakovostne zdravstvene oskrbe. HIPAA ureja uporabo in razkritje zdravstvenih podatkov s strani subjektov, za katere velja pravilo o zasebnosti. Vključuje tudi standarde glede pravic posameznikov, da razumejo in nadzorujejo, kako se uporabljajo njihovi zdravstveni podatki.

<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>; <https://www.justice.gov/opcl/privacy-act-1974>.

- *Children's Online Privacy Protection Act* (Zakon o varstvu zasebnosti otrok na spletu, v nadaljevanju: COPPA)⁵;
- *Gramm-Leach-Bliley Act* (Gramm-Leach-Blileyjev zakon, v nadaljevanju: GLBA)⁶.

3. Na področju vladnega dostopa do osebnih podatkov, prenesenih iz EU v ZDA, se uporablja več različnih pravnih podlag, omejitev in zaščitnih ukrepov. Pravni postopki za dostop do podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj izvirajo neposredno iz ustave ZDA (četrti amandma), iz zakonskega in postopkovnega prava ali iz smernic in politik ministrstva za pravosodje na zvezni ali državni ravni. Dostop do podatkov za namene nacionalne varnosti ureja več pravnih instrumentov, zlasti *Foreign Intelligence Surveillance Act* (Zakon o nadzoru tujih obveščevalnih podatkov, v nadaljevanju: FISA), Odredba št. 12333, nedavno sprejeta Odredba št. 14086 in uredba pravosodnega ministra⁷ o ustanovitvi sodišča za presojo varstva podatkov.
4. Komisija je 13. decembra 2022 izdala osnutek izvedbenega sklepa v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustrezni ravni varstva osebnih podatkov na podlagi okvira za varstvo zasebnosti podatkov med EU in ZDA (v nadaljevanju: osnutek sklepa), katerega priloga vsebuje okvir za varstvo zasebnosti podatkov med EU in ZDA (*Data Privacy Framework*, v nadaljevanju: DPF). Osnutek sklepa zaradi zgoraj pojasnenih razlogov ne temelji na posebnem in celovitem zveznem pravnem okviru, temveč na DPF.
5. DPF deluje tako: „Ministrstvo za trgovino v okviru svojih zakonskih pooblastil za spodbujanje, pospeševanje in razvijanje mednarodne trgovine izdaja načela okvira za varstvo zasebnosti podatkov med EU in ZDA, vključno z dopolnilnimi načeli (v nadaljevanju skupaj: načela) in Prilogo I k načelom (v nadaljevanju: Priloga I) (člen 1512 naslova 15 zakonodajne zbirke ZDA)“⁸.
6. „Načela“ (v nadaljevanju: načela DPF) so se oblikovala po posvetovanju z Evropsko komisijo (v nadaljevanju: Komisija), industrijo in drugimi deležniki, da bi se dosegel cilj lajšanja trgovinskih in gospodarskih stikov med EU in ZDA⁹, hkrati pa da bi se posameznikom, na katere se nanašajo osebni podatki, zagotovila raven varstva, ki je v bistvenem enaka ravni, zagotovljeni v EU.
7. Načela DPF so opisana kot „ključni sestavni del“ DPF. Po eni strani zagotavljajo „mehanizem, pripravljen za uporabo“, za prenose podatkov iz EU v ZDA. Po drugi strani pa so osebni podatki, preneseni iz EU v ZDA, varovani in zaščiteni v skladu z zakonodajo EU.

⁵ Glavni cilj COPPA je zagotoviti staršem nadzor nad tem, katere osebne podatke o njihovih otrocih, mlajših od 13 let, zbirajo operaterji spletnih mest in spletnih storitev, namenjenih otrokom (vključno z mobilnimi aplikacijami in napravami interneta stvari, kot so pametne igrače), ali spletnih mest za splošno občinstvo. COPPA od teh operaterjev zahteva, da obvestijo starše in pridobijo njihovo preverljivo soglasje. To velja tudi za podatke tujih otrok, če se spletna mesta ali storitve upravljajo v ZDA in za nje velja COPPA. Hkrati se predpisi uporabljajo tudi za tuje spletne strani in storitve, če so namenjene otrokom v ZDA. Glej: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions> in osnutek sklepa, Priloga IV, str. 3.

⁶ Eden od ciljev GLBA je zaščititi zasebnost potrošnikov v finančnem sektorju. GLBA od finančnih institucij zahteva, da svojim strankam pojasnijo svoje prakse izmenjave podatkov in oblikujejo zaščitne ukrepe za zaščito podatkov o strankah (na primer podjetjih, za katere se uporablja pravilo FTC o zaščitnih ukrepih). <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

⁷ Uredba pravosodnega ministra št. 5517-2022, ki spreminja predpise ministrstva za pravosodje ZDA v skladu s pooblastili in napotki iz Odredbe št. 14086.

⁸ Osnutek sklepa, Priloga I, oddelek I.

⁹ Prav tam.

8. DPF se uporablja samo za organizacije v ZDA, ki so samocertificirane v skladu z zahtevami okvira (v nadaljevanju: organizacije DPF). Za zdaj je to mogoče le, če spadajo v pristojnost Zvezne komisije za trgovino (*Federal Trade Commission*, v nadaljevanju: FTC) ali ministrstva za promet. V prihodnjo prilogo bi se lahko v prihodnosti dodali še drugi z zakonom določeni organi – pristojni za nadzor nad izvajanjem načel DPF.
9. Načela DPF pojasnjujejo, da lahko pogoje okvira izvršuje (i) FTC v skladu s členom 5 *Trade Commission Act* (Zakon o zvezni komisiji za trgovino, v nadaljevanju: zakon o FTC), ki prepoveduje nepoštena in goljufiva dejanja v trgovini ali z vplivom nanjo¹⁰, (ii) ministrstvo za promet v skladu s členom 41712 naslova 49 zakonodajne zbirke ZDA, ki prevozniku ali agenciji za prodajo letalskih vozovnic prepoveduje nepošteno ali zavajajočo prakso v zračnem prevozu za prodajo ali zračni prevoz, ali (iii) da se lahko izvršujejo v skladu z drugimi zakoni ali predpisi, s katerimi so taka dejanja prepovedana.
10. V načelih DPF je poudarjeno, da ne omejujejo uporabe Splošne uredbe o varstvu podatkov niti obstoječih obveznosti glede zasebnosti, ki se sicer uporabljajo v skladu z zakonodajo ZDA.

1.2 Obseg ocene EOVP

11. Osnutek sklepa odraža oceno Komisije o DPF, ki je rezultat razprav z vlado ZDA. V skladu s členom 70(1)(s) Splošne uredbe o varstvu podatkov se od EOVP pričakuje, da predloži mnenje o ugotovitvah Komisije v zvezi z ustreznostjo ravni varstva v tretji državi in si po potrebi prizadeva pripraviti predloge za obravnavo morebitnih težav.
12. EOVP pozdravlja posodobitve načel DPF¹¹, ki bodo zavezujoč pravni okvir za organizacije DPF. Vendar ugotavlja, da so načela DPF pravzaprav enaka načelom zasebnostnega ščita¹² (na katerih so temeljili skupni letni pregledi Delovne skupine iz člena 29 (v nadaljevanju: WP29) in EOVP). Načela DPF so pretežno enaka tudi načelom iz osnutka zasebnostnega ščita, ki so bila podlaga za mnenje WP29 iz leta 2016¹³ (v nadaljevanju: Mnenje št. 01/2016 Delovne skupine iz člena 29). EOVP meni, da v zveziz načeli DPF, ki se niso bistveno spremenila, ni treba ponoviti vseh predhodnih pripomb WP29. Odločil se je, da se bo osredinil na posebne vidike, za katere meni, da so danes še pomembnejši glede na razvoj pravnega in tehnološkega okolja.
13. Poleg tega v skladu s sodno prakso Sodišča¹⁴ zelo pomemben del analize zajema pravno ureditev vladnega dostopa do osebnih podatkov, prenesenih v ZDA.
14. EOVP je v svoji oceni upošteval veljavni evropski okvir varstva podatkov, vključno s členi 7, 8 in 47 Listine EU o temeljnih pravicah, ki ščitijo pravico do zasebnega in družinskega življenja, pravico do varstva osebnih podatkov ter pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, ter členom 8 Evropske konvencije o človekovih pravicah (v nadaljevanju: EKČP), ki ščiti pravico do zasebnega in družinskega življenja. Poleg zgoraj navedenega je EOVP upošteval zahteve Splošne uredbe o varstvu podatkov, ustrezno sodno prakso in referenčni dokument o ustreznosti, ki ga je EOVP

¹⁰ Člen 45(a) naslova 15 zakonodajne zbirke ZDA.

¹¹ Na primer pojasnilo, da so podatki, kodirani s šifrirnim ključem, osebni podatki.

¹² Izvedbeni sklep Komisije (EU) 2016/1250 z dne 12. julija 2016 na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, ULL 207, 1. 8. 2016, str. 1.

¹³ Mnenje št. 01/2016 Delovne skupine iz člena 29 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA, sprejeto 13. aprila 2016 (v nadaljevanju: Mnenje št. 01/2016 Delovne skupine iz člena 29).

¹⁴ Zlasti: Sodba sodišča z dne 6. oktobra 2015, *Maximillian Schrems/Data Protection Commissioner*, C-392/14, ECLI:EU:C:2015:650, in Sodba Sodišča z dne 16. julija 2020, *Data Protection Commissioner/Facebook Ireland Limited in Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

sprejel (v nadaljevanju: referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov)¹⁵.

15. Cilj tega postopka je Komisiji podati mnenje o oceni ustreznosti ravni varstva, ki jo zagotavlja DPF. Pojem „ustrezna raven varstva“, ki je že obstajal v okviru Direktive 95/46/ES, je sodišče nadalje razvilo. Zato je treba opozoriti na standard, ki ga je Sodišče določilo v sodbah v zadevah *Schrems I*¹⁶ (v kateri je razveljavilo „varni pristan“) in *Schrems II*¹⁷ (v kateri je razveljavilo „zasebnostni ščit“).
16. Sodišče je v zadevi *Schrems I* razsodilo, da – čeprav mora biti „raven varstva“ v tretji državi „v bistvenem enaka“ ravni, zagotovljeni v EU – „so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Unije“¹⁸. Cilj torej ni v celoti prenesti vseh točk evropske zakonodaje, ampak določiti bistvene in temeljne zahteve zakonodaje, ki se pregleduje. Ustreznost se lahko doseže s kombinacijo pravic za posameznike, na katere se nanašajo osebni podatki, in obveznosti za tiste, ki obdelujejo osebne podatke ali izvajajo nadzor nad tako obdelavo, ter nadzora, ki ga izvajajo neodvisni organi. Vendar so predpisi o varstvu podatkov učinkoviti samo, če so izvršljivi in se izvajajo v praksi. Torej ni dovolj obravnavati samo vsebine predpisov, ki se uporabljajo za osebne podatke, prenesene v tretjo državo ali mednarodno organizacijo, ampak je treba preučiti tudi sistem, vzpostavljen za zagotavljanje učinkovitosti takih predpisov. Učinkoviti mehanizmi izvrševanja so zelo pomembni za učinkovitost predpisov o varstvu podatkov¹⁹.
17. Sodišče je v zadevi *Schrems II* ugotovilo, da zakoni, na podlagi katerih lahko obveščevalni organi ZDA dostopajo do osebnih podatkov, prenesenih v ZDA (člen 702 FISA/Odredba št. 12333), nesorazmerno omejujejo pravice iz členov 7 in 8 Listine EU o temeljnih pravicah, zato niso urejeni tako, da bi izpolnjevali zahteve, ki so v bistvu enakovredne zahtevam, ki jih v pravu Unije določa drugi stavek člena 52(1) Listine²⁰.
18. Poleg tega je Sodišče navedlo, da prej veljavni pravni okvir ni zagotavljal jamstev, ki so v bistvu enakovredna tistim, ki jih zahteva člen 47 Listine EU o temeljnih pravicah, saj mehanizem varuha človekovih pravic ni mogel nadomestiti dejstva, da niti Predsedniška politična direktiva št. 28 niti Odredba št. 12333 osebam, ki niso državljani ZDA, ne priznavata učinkovitega pravnega sredstva²¹. Varuh človekovih pravic ni bil neodvisen od izvršilne veje oblasti in ni imel pooblastil za sprejemanje zavezujočih odločitev v zvezi z ameriškimi obveščevalnimi službami²².
19. Z Odredbo št. 14086, ki na splošno nadomešča Predsedniško politično direktivo št. 28, sta bili uvedeni dve novi zahtevi v skladu z zakonodajo ZDA, ki odražata sodbo Sodišča v zadevi *Schrems II*: obveščevalne dejavnosti SIGINT se izvajajo le toliko, kolikor je potrebno za izboljšanje zbiranja podatkov v okviru potrjenih prednostnih nalog obveščevalnih služb, ter samo v obsegu in na način, ki

¹⁵ Delovna skupina iz člena 29, [Referenčni dokument o ustreznosti, WP 254 rev. 01, 28. november 2017, kakor je bil nazadnje spremenjen in sprejet 6. februarja 2018, ki ga je EOVP potrdil 25. maja 2018 \(v nadaljevanju: referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov\)](#).

¹⁶ Sodba Sodišča z dne 6. oktobra 2015, *Maximillian Schrems/Data Protection Commissioner*, C-392/14, ECLI:EU:C:2015:650 (v nadaljevanju: sodba Sodišča v zadevi *Schrems I*).

¹⁷ Sodba Sodišča z dne 16. julija 2020, *Data Protection Commissioner/Facebook Ireland Limited in Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559 (v nadaljevanju: sodba Sodišča v zadevi *Schrems II*).

¹⁸ Sodba Sodišča v zadevi *Schrems I*, točki 73 in 74.

¹⁹ [Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov](#), str. 2.

²⁰ Sodba Sodišča v zadevi *Schrems II*, točki 184 in 185.

²¹ Sodba Sodišča v zadevi *Schrems II*, točka 192.

²² Sodba Sodišča v zadevi *Schrems II*, točka 195.

sta sorazmerna s potrjeno prednostno nalogo obveščevalne službe, na eni strani in mehanizem pravnega varstva na drugi strani.

20. EOVP v tem mnenju zlasti ocenjuje, koliko DPF in nedavno sprejeta Odredba št. 14086 učinkovito obravnavata ugotovitve iz sodbe Sodišča.

1.3 Splošne pripombe in pomisleki

1.3.1 Ocena nacionalnega prava

21. EOVP razume, da se ocena iz osnutka sklepa nanaša na načela DPF. Kljub temu bi si želel nekaj informacij o pravnem okviru ZDA, v katerem delujejo organizacije DPF. To bi omogočilo boljše razumevanje medsebojnega vpliva med DPF in zakonodajo ZDA. Na primer, v oddelku 1 Priloge I²³ je določeno, da načela DPF ne „[...] omejujejo obveznosti v zvezi z varstvom zasebnosti, ki sicer veljajo v skladu z zakonodajo ZDA“, vendar te obveznosti niso opisane.

1.3.2 Mednarodne zaveze, ki so jih sprejele ZDA

22. Komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi v skladu s členom 45(2)(c) Splošne uredbe o varstvu podatkov in referenčnim dokumentom o ustreznosti v skladu s Splošno uredbo o varstvu podatkov med drugim upošteva mednarodne zaveze, ki jih je sprejela tretja država, ali druge obveznosti, ki izhajajo iz sodelovanja tretje države v večstranskih ali regionalnih sistemih, zlasti v zvezi z varstvom osebnih podatkov, pa tudi izvajanje takih obveznosti.
23. ZDA so podpisnica več mednarodnih sporazumov, ki zagotavljajo pravico do zasebnosti, na primer Mednarodnega pakta o državljanskih in političnih pravicah (člen 17), Konvencije o pravicah invalidov (člen 22) in Konvencije o otrokovih pravicah (člen 16). Poleg tega ZDA kot članica Organizacije za gospodarsko sodelovanje in razvoj spoštujejo okvir te organizacije za zagotavljanje zasebnosti, zlasti smernice, ki urejajo varstvo zasebnosti in čezmejni pretok osebnih podatkov. Ministri in visoki predstavniki članic Organizacije za gospodarsko sodelovanje in razvoj ter Evropske unije so 14. decembra 2022 sprejeli „Deklaracijo o vladnem dostopu do osebnih podatkov, ki jih hranijo subjekti zasebnega sektorja“. ZDA so tudi pogodbenica Konvencije o kibernetiski kriminaliteti iz Budimpešte.
24. Poleg tega so ZDA članica sistema čezmejnih pravil za varstvo zasebnosti Skupine za azijsko-pacifiško gospodarsko sodelovanje (*Asia-Pacific Economic Cooperation*, v nadaljevanju: APEC), tj. sistema certificiranja varstva podatkov, ki ga podpira vlada in se mu podjetja lahko pridružijo, da dokažejo skladnost z mednarodno priznanimi pravili za varstvo zasebnosti. Ta pravila za varstvo zasebnosti so potrdili voditelji APEC.
25. EOVP je seznanjen tudi s sodelovanjem ZDA kot države opazovalke pri delu posvetovalnega odbora po Konvenciji Sveta Evrope št. 108.
26. Poleg tega je seznanjen s stalnim sodelovanjem organov ZDA na „okrogli mizi organov G7 za varstvo podatkov in zasebnost“ v novovzpostavljeni obliki iz leta 2021, na kateri zasedajo neodvisni nadzorni organi G7 za varstvo podatkov in zasebnost iz držav G7, in pozdravlja to sodelovanje. V tem okviru so podprli na primer najnovejše sporočilo okrogle mize organov G7 za varstvo podatkov in zasebnost²⁴,

²³ Osnutek sklepa, Priloga I, oddelek I, zadnji stavek.

²⁴ Okrogla miza organov G7 za varstvo podatkov in zasebnost, spodbujanje prostega pretoka podatkov na podlagi zaupanja in izmenjave znanja o možnostih mednarodnih podatkovnih prostorov, 8. september 2022,

sprejeto 8. septembra 2022 v Bonnu v Nemčiji, ki se je osredinjalo na pojem „prostega pretoka podatkov na podlagi zaupanja“.

1.3.3 Napredek na področju zakonodaje ZDA o varstvu podatkov

27. EOVP še zlasti upošteva razvoj zakonodaje o zasebnosti podatkov na državni ravni v ZDA. Pozdravlja sprejetje zakonov o varstvu podatkov, ki so ali bodo začeli veljati do leta 2023 v petih zveznih državah (Kaliforniji, Koloradu, Connecticutu, Virginiji in Utah)²⁵.
28. EOVP ugotavlja tudi, da so bile ustrezne pobude za nadaljnje državne zakone že sprožene v številnih drugih zveznih državah ZDA.
29. Poleg tega izrecno pozdravlja prizadevanja v zvezi z dvostrankarsko pobudo za zvezni zakon o varstvu podatkov, *American Data Privacy and Protection Act* (Ameriški zakon o zasebnosti in varstvu podatkov, v nadaljevanju: ADPPA).

1.3.4 Področje uporabe osnutka sklepa

30. Komisija v skladu s členom 1 osnutka sklepa ugotavlja, da ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, prenesenih iz EU organizacijam v Združenih državah, ki so vključene na „seznam okvira o varstvu podatkov“, ki ga vodi in objavlja ameriško ministrstvo za trgovino v skladu z oddelkom I.3 Priloge I²⁶.
31. DPF je na voljo podjetjem v pristojnosti FTC ali ministrstva za promet. Poudariti je treba, da bi se lahko v prihodnosti dodali drugi z zakonom določeni organi ZDA s podobnimi pristojnostmi²⁷.

1.3.5 Omejitve dolžnosti spoštovanja načel DPF

32. V oddelku I.5 Priloge I je določeno, da se lahko spoštovanje načel DPF s strani organizacij DPF omeji, med drugim, (i) v obsegu, ki je potreben za izpolnitev sodne odločbe²⁸ ali za izpolnitev zahtev javnega interesa, kazenskega pregona ali nacionalnih zahtev glede varnosti²⁹ (tudi kadar zakon ali vladni podzakonski akt ustvari nezdružljivost obveznosti), in (ii) z zakonom, sodno odločbo ali vladnim podzakonskim aktom, ki ustvari izrecna pooblastila, pod pogojem, da lahko organizacija DPF dokaže, da je njeno nespoštovanje načel omejeno toliko, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takih pooblastil.

https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

²⁵ *California Consumer Privacy Act* (Zakon države Kalifornija o varstvu zasebnosti potrošnikov) (2018; datum začetka veljavnosti: 1. januar 2020); *California Privacy Rights Act* (Zakon države Kalifornija o varstvu pravic do zasebnosti) (2020; v celoti uveljavljen 1. januarja 2023); *Colorado Privacy Act* (Zakon države Kolorado o varstvu zasebnosti) (2021; datum začetka veljavnosti: 1. julij 2023); *Connecticut Data Privacy Act* (Zakon države Connecticut o varstvu zasebnosti) (2022; datum začetka veljavnosti: 1. julij 2023); *Virginia Consumer Data Protection Act* (Zakon države Virginija o varstvu podatkov potrošnikov) (2021; datum začetka veljavnosti: 1. januar 2023); *Utah Consumer Privacy Act* (Zakon države Utah o varstvu zasebnosti potrošnikov) (2022; datum začetka veljavnosti: 31. december 2023).

²⁶ Osnutek sklepa, Končni premisleki, člen 1, str. 57. EOVP razume, da osnutek sklepa ne bo zajemal prenosov s subjektov zunaj EU, za katere velja Splošna uredba o varstvu podatkov na podlagi njenega člena 3(2), na certificirane subjekte v ZDA.

²⁷ Osnutek sklepa, Priloga I, oddelek I.2.

²⁸ Za več pripombo uporabi osebnih podatkov, zajeti h v okviru za varstvo zasebnosti podatkov med EU in ZDA, za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj glej oddelek 3.1 tega mnenja.

²⁹ Za več pripombo uporabi osebnih podatkov, zajeti h v okviru za varstvo zasebnosti podatkov med EU in ZDA, za namene nacionalne varnosti glej oddelek 3.2 tega mnenja.

33. EOVP bo brez popolnega poznavanja zakonodaje ZDA na zvezni in državni ravni težko podrobno ocenil področje uporabe izjem, navedenih v tem odstavku. Zato predlaga, naj Komisija v osnutek sklepa vključi pojasnilo o področju uporabe izjem, vključno z veljavnimi zaščitnimi ukrepi v skladu z zakonodajo ZDA, da se bolje opredeli vpliv teh izjem na raven varstva posameznikov, na katere se nanašajo osebni podatki. EOVP tudi poudarja, da bi morala biti Komisija seznanjena z uporabo in sprejetjem kakršnega koli zakona ali vladnega podzakonskega akta, ki bi vplival na spoštovanje načel DPF, ter to uporabo in sprejetje spremljati.

1.3.6 Spremembe v zvezi z „zasebnostnim ščitom“

34. EOVP pozdravlja prizadevanja za obravnavo zahtev iz sodbe v zadevi *Schrems II*. Vendar bi želel, da bi bilo med pogajanji o DPF obravnavanih tudi več vprašanj, opredeljenih (i) v Mnenju št. 01/2016 WP29 in (ii) v preteklih skupnih pregledih³⁰.
35. EOVP tudi ugotavlja, da so načela DPF, ki jih morajo upoštevati organizacije DPF, kljub številnim spremembam in dodatnim pojasnilom v uvodnih izjavah osnutka sklepa pravzaprav nespremenjena glede na načela, ki so se uporabljala v okviru zasebnostnega ščita.

1.3.7 Nejasnost dokumentov DPF

36. EOVP ugotavlja, da je zaradi sestave prilog in njihovega številčenja razmeroma težko najti informacije in se nanje sklicevati. To pripomore k zapleteni splošni predstavitvi novega okvira, katerega priloge združujejo dokumente z različno pravno veljavnostjo in ki morda ne daje prednosti dobremu razumevanju načel DPF s strani posameznikov, na katere se nanašajo osebni podatki, organizacij DPF in organov EU za varstvo podatkov.
37. EOVP tudi poudarja, da je treba izrazje v celotnem DPF uporabljati dosledno. Trenutno ni tako, kar velja na primer za pojem „obdelava“. V nekaterih delih DPF so dejansko zgolj našteje nekatere vrste postopkov obdelave podatkov, namesto da bi se uporabljal izraz „obdelava“. To lahko povzroči pravno negotovost in morebitne vrzeli v varstvu³¹.
38. EOVP pozdravlja dejstvo, da so opredelitve nekaterih uporabljenih izrazov vključene v DPF³². Vendar to ne velja za nekatere druge bistvene izraze, vsaj ne za izraza „posrednik“ ali „obdelovalec“, ki jih je po mnenju EOVP treba jasno in natančno opredeliti v oddelku I.8 Priloge I in glede katerih se ZDA in EU strinjajo, da bi preprečili poznejšo zmedo organizacij DPF, ki se zanašajo na DPF, nadzornih organov in splošne javnosti.

³⁰ Letni pregledi: Zasebnostni ščit EU-ZDA – prvi skupni letni pregled, WP 255, poročilo WP29, sprejeto 28. novembra 2017 (v nadaljevanju: poročilo o prvem skupnem pregledu); Zasebnostni ščit EU-ZDA – drugi skupni letni pregled, poročilo EOVP, sprejeto 22. januarja 2019 (v nadaljevanju: poročilo o drugem skupnem pregledu); Zasebnostni ščit EU-ZDA – tretji skupni letni pregled, poročilo EOVP, sprejeto 12. novembra 2019 (v nadaljevanju: poročilo o tretjem skupnem pregledu).

³¹ Na primer (i) v skladu z besedilom oddelka III.6.(f) Priloge I k osnutku sklepa bi se načela DPF uporabljala le, če organizacija „shranjuje, uporablja ali razkriva“ prejete podatke (tj. ne za druga dejanja, ki jih zajema izraz „obdelava“, kot so zbiranje, beleženje, spreminjanje, priklic, vpogled, izbris), (ii) v skladu z oddelkom II.4.(a) Priloge I k osnutku sklepa pa bi varnost podatkov veljala samo za „ustvarjanje, ohranjanje, uporabo ali razširjanje“ osebnih podatkov.

³² Osnutek sklepa, Priloga I, str. 8.

39. EOVP se glede različnih razlag pojma „podatki o človeških virih“ v EU in ZDA strinja s tretjim poročilom Komisije o pregledu o cilju nadaljevanja razprave z organi ZDA³³.

2 SPLOŠNI VIDIKI VARSTVA PODATKOV

2.1 Vsebinska načela

2.1.1 Pojmi

40. Na podlagi referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov bi moral pravni okvir tretje države vključevati temeljne pojme in/ali načela v zvezi z varstvom podatkov. Čeprav ni treba, da so enaki izrazju Splošne uredbe o varstvu podatkov, bi morali izražati pojme iz zakonodaje EU o varstvu podatkov in biti skladni z njimi. Splošna uredba o varstvu podatkov na primer zajema naslednje pomembne pojme: „osebni podatki“, „obdelava osebnih podatkov“, „upravljavac podatkov“, „obdelovalec podatkov“, „uporabnik“ in „občutljivi podatki“. EOVP pozdravlja dejstvo, da so opredelitve izrazov „osebni podatki“, „obdelava“ in „upravljavac“ vključene v DPF, kot v primeru zasebnostnega ščita.
41. EOVP ugotavlja, da še vedno ni jasno, v kakšnem obsegu se načela DPF uporabljajo za organizacije DPF, ki prejemajo osebne podatke iz EU „zgolj zaradi obdelave“ (imenovane „posredniki“ ali „obdelovalci“). DPF ne razlikuje med načeli DPF, ki veljajo za posrednike, in načeli DPF, ki veljajo za upravljavce, več obveznosti, vključenih v načela DPF, pa ni primernih za posrednike oziroma obdelovalce. Na primer, posrednik oziroma obdelovalec ne bi smel imeti možnosti, da posameznikom sporoči vse elemente celotnega obvestila, kot zahteva načelo obvestila (na primer namenov, za katere se zbirajo in uporabljajo njihovi osebni podatki)³⁴, saj posrednik oziroma obdelovalec ne more sam določiti sredstev in namenov obdelave³⁵.

2.1.2 Načelo omejitve namena

42. Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov določa, da se osebni podatki obdelujejo za določen namen in se pozneje uporabljajo le, če to ni nezdržljivo z namenom obdelave.
43. Načeli celovitosti podatkov in omejitve namena določata, da organizacija ne sme obdelovati osebnih podatkov na način, ki je nezdržljiv z nameni, za katere so bili podatki zbrani ali ki jih je posameznik pozneje odobril³⁶. EOVP ugotavlja, da se v okviru načel obvestila, možnosti izbire ter celovitosti podatkov in omejitve namena uporablja različno izrazje. WP29 ugotavlja, da se v DPF izrazi, kot so „različni nameni“, „bistveno drugačni“ nameni ali „uporaba, ki ni v skladu z“, uporabljajo, ne da bi bili jasno opredeljeni v DPF, kar lahko kljub koristnim pojasnilom v uvodnih izjavah osnutka sklepa povzroči pravno negotovost.

³³ Tretje poročilo o skupnem pregledu, str. 5, 15, 16 in 30. Glej tudi delovni dokument služb Komisije, priložen poročilu Komisije Evropskemu parlamentu in Svetu o tretjem letnem pregledu delovanja zasebnostnega ščita EU-ZDA, str. 17 in 18.

³⁴ Osnutek sklepa, Priloga I, oddelek II.1.(a).

³⁵ Glej tudi Mnenje št. 01/2016 Delovne skupine iz člena 29, str. 16.

³⁶ Osnutek sklepa, Priloga I, oddelek II.5.

2.1.3 Pravica do dostopa, popravka, izbrisa in ugovora

44. V DPF so pravice posameznikov do dostopa, popravka in izbrisa obravnavane v okviru načela dostopa³⁷.
45. Načelo dostopa ostaja enako kot v zasebnostnem ščit. Zato še vedno veljajo nekateri pomisleki, izraženi v Mnenju št. 01/2016 WP29, kot je podrobno opisano v nadaljevanju.
46. EOVP meni, da je treba v zvezi s pravico posameznikov do dostopa ponoviti, da bi bilo podrobnosti o obveznosti odgovora na zahteve posameznikov bolje vključiti v glavno besedilo načela (še vedno so opisane le v opombi³⁸). Prav tako bi moralo biti jasno, da bi bilo treba dostop omogočiti v obsegu, v katerem organizacija DPF obdeluje osebne podatke, ne samo, ko jih „hrani“³⁹. EOVP meni, da bi sedanje besedilo lahko povzročilo ozko razlago pravice do dostopa.
47. V zvezi s seznamom izjem od pravice do dostopa⁴⁰ se nekatere še vedno nagibajo k temu, da bi imeli prednost interesi organizacij DPF. EOVP je še vedno zaskrbljen, ker ni videti, da bi se v teh primerih zahtevalo upoštevanje pravic in interesov posameznika⁴¹.
48. Še ena izjema, ki je zbujala zaskrbljenost WP29⁴² in ki se EOVP zdi preširoka, je izjema od pravice do dostopa do javno dostopnih informacij in informacij iz javnih evidenc⁴³. EOVP je večkrat navedel, da imajo posamezniki, na katere se nanašajo osebni podatki, v skladu s pravom Unije vedno pravico dostopa do svojih podatkov, ne glede na to, ali so bili osebni podatki objavljeni ali ne. Če bi se zahteve za dostop zavrnilo z obrazložitvijo, da so bili podatki pridobljeni iz javno dostopnih virov ali javnih evidenc, bi posamezniki izgubili možnost nadzora nad točnostjo podatkov in nad tem, ali so bili podatki sploh zakonito objavljeni.
49. EOVP opozarja, da je pravica do dostopa zapisana v členu 8(2) Listine EU o temeljnih pravicah. 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 so pravice do popravka, izbrisa in ugovora⁴⁴.
50. Poleg pravic do dostopa in izbrisa bi morali imeti posamezniki, na katere se nanašajo osebni podatki, tudi pravico, da na podlagi nujnih legitimnih razlogov, povezanih z njihovim posebnim položajem, kadar koli ugovarjajo obdelavi svojih podatkov pod posebnimi pogoji, določenimi v pravnem okviru tretje države⁴⁵.
51. DPF z načelom možnosti izbire določa pravico do ugovora (opt-out) razkritju osebnih podatkov tretji osebi ali uporabi osebnih podatkov za bistveno drugačen namen⁴⁶. Poleg tega imajo posamezniki pravico, da kadar koli zavrnejo uporabo svojih osebnih podatkov za namen neposrednega trženja⁴⁷. Načini in še posebej roki za uveljavljanje pravice do ugovora niso podrobno opredeljeni, razen glede namena neposrednega trženja. Zato EOVP poziva Komisijo, naj pojasni, kako lahko posamezniki uveljavljajo svojo pravico do ugovora.

³⁷ Osnutek sklepa, Priloga I, oddelka II.6 in III.8.a.(i).

³⁸ Osnutek sklepa, Priloga I, III.8.a.(i)1. – opomba 14.

³⁹ Osnutek sklepa, Priloga I, III.8.d(ii).

⁴⁰ Osnutek sklepa, Priloga I, III.8.e.

⁴¹ Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.5.

⁴² Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.9.

⁴³ Osnutek sklepa, Priloga I, III.15.d–e.

⁴⁴ Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.5.

⁴⁵ Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, oddelek 3.A.8.

⁴⁶ Osnutek sklepa, Priloga I, II.2.(a).

⁴⁷ Osnutek sklepa, Priloga I, III.12.(a).

52. Kot je navedeno v Mnenju št. 01/2016 WP29, EOVP meni, da preprosto sklicevanje na obstoj te pravice v politiki zasebnosti ni dovolj. Individualno prilagojena možnost uveljavljanja te pravice ne bi smela biti na voljo le v primeru razkritja ali ponovne uporabe osebnih podatkov. EOVP poudarja, da bi morala biti v okviru DPF na voljo splošna pravica do ugovora na podlagi nujnih legitimnih razlogov, povezanih s posebnim položajem posameznika, na katerega se nanašajo osebni podatki. EOVP predlaga, naj se taka pravica do ugovora zagotovi v vsakem trenutku in naj ne bo omejena na uporabo podatkov za neposredno trženje⁴⁸.
53. EOVP v zvezi s podatki o človeških virih ceni pojasnila Komisije glede uporabe načel obvestila in možnosti izbire, kadar namerava certificirana organizacija iz ZDA uporabiti podatke o človeških virih za namen, ki ni povezan z zaposlitvijo, kot je na primer neposredno trženje⁴⁹. Vendar EOVP trdi, da se bo nadaljnja obdelava podatkov o človeških virih za namene, ki niso povezani z zaposlitvijo, v večini primerov štela za nezdržljivo s prvotnim namenom in da bo privolitev le redko povsem prostovoljna, če bo dana v okviru zaposlitve.
54. EOVP tudi vnovič izraža pomisleke WP29 v zvezi z izjemami od načel obvestila in izbire glede podatkov o človeških virih „v obsegu in obdobju, potrebnem, da se prepreči poseganje v zmožnosti organizacije, da odloča o napredovanju, imenovanjih in drugih podobnih zaposlitvenih vidikih“⁵⁰, saj meni, da je ta opredelitev široka in nejasna⁵¹.

2.1.4 Omejitve nadaljnjih prenosov podatkov

55. Prvemu uporabniku prvotnega prenosa osebnih podatkov bi moralo biti dovoljeno nadalje prenesti osebne podatke samo, če tudi za nadaljnjega uporabnika (tj. uporabnika nadaljnjega prenosa podatkov) veljajo predpisi (vključno s pogodbenimi določbami), ki zagotavljajo ustrezno raven varstva in upoštevajo zadevna navodila za obdelavo podatkov v imenu upravljavca podatkov. Nadaljnji prenos ne sme ogroziti ravni varstva posameznikov, na katere se nanašajo podatki, ki se prenašajo. Prvotni uporabnik podatkov, prenesenih iz EU, mora zagotoviti ustrezne zaščitne ukrepe za nadaljnje prenose podatkov, če ne obstaja sklep o ustreznosti. Taki nadaljnji prenosi podatkov bi se lahko izvajali samo, če obstajajo omejeni in določeni nameni ter pravna podlaga za to obdelavo⁵².
56. V skladu z načelom odgovornosti za nadaljnji prenos DPF se nadaljnji prenosi lahko izvajajo samo za omejene in določene namene na podlagi pogodbe med organizacijo DPF in tretjo osebo (ali primerljivega dogovora znotraj skupine podjetij) in samo, če ta pogodba od tretje osebe zahteva, da zagotovi enako raven varstva, kot jo zagotavljajo načela DPF⁵³.
57. EOVP želi vnovič poudariti pomisleke, izražene v Mnenju št. 01/2016 WP29 glede izjeme od potrebe po sklenitvi pogodbe med upravljavci za prenose znotraj skupine⁵⁴. V zvezi s podatki o človeških virih še vedno ne razume utemeljitve za izjemo od obveznosti sklenitve pogodbe s tretjim upravljavcem v primeru nadaljnjih prenosov za „občasne potrebe, povezane z zaposlovanjem“⁵⁵.

⁴⁸ Mnenju št. 01/2016 WP29, točka 2.2.2.

⁴⁹ Osnutek sklepa, Priloga I, III.9.b.(i) ter uvodna izjava 15 in opomba 27.

⁵⁰ Osnutek sklepa, Priloga I, III.9.b.iv.

⁵¹ Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.7.

⁵² Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, oddelek 3.A.9.

⁵³ Osnutek sklepa, Priloga I, II.3.

⁵⁴ Osnutek sklepa, Priloga I, III.10.b(i), ki se nanaša na besedilo „ali drugi instrumenti znotraj skupine (na primer programi skladnosti in nadzora)“, za katere očitno ni nujno, da so zavezujoči.

⁵⁵ Osnutek sklepa, Priloga I, III.9.e(i), ki se nanaša na primere, kot je zavarovalno kritje.

58. Poleg tega želi EOVP ponoviti zahtevo WP29⁵⁶, da morajo organizacije, ki jih okvir zavezuje, pred nadaljnjim prenosom oceniti, da obvezne zahteve nacionalne zakonodaje tretje države, ki se uporabljajo za uporabnika, ne bodo ogrozile neprekinjenega varstva posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo⁵⁷.
59. EOVP trdi, da bi lahko nadaljnji prenosi osebnih podatkov v tretje države posegali v temeljne pravice posameznikov, in poziva Komisijo, naj pojasni, da morajo biti zaščitni ukrepi, ki jih prvotni uporabnik naloži uvozniku v tretji državi, pred nadaljnjim prenosom podatkov v okviru DPF učinkoviti glede na zakonodajo tretje države⁵⁸.

2.1.5 Avtomatizirano sprejemanje odločitev in oblikovanje profilov

60. Odločitve, ki temeljijo samo na avtomatizirani obdelavi (avtomatizirano sprejemanje posameznih odločitev), vključno z oblikovanjem profilov, in imajo pravne učinke na posameznika, na katerega se nanašajo osebni podatki, ali nanj znatno vplivajo, se lahko sprejemajo samo pod nekaterimi pogoji, določenimi v pravnem okviru tretje države. V evropskem okviru taki pogoji na primer vključujejo potrebo po pridobitvi izrecne privolitve, na katerega se nanašajo osebni podatki, ali potrebo po taki odločitvi za sklenitev pogodbe. Če odločitev ni v skladu s pogoji, ki so določeni v pravnem okviru tretje države, bi moral imeti posameznik, na katerega se nanašajo osebni podatki, pravico, da ta odločitev zanj ne velja. V vsakem primeru bi morali biti z zakonodajo tretje države zagotovljeni potrebni zaščitni ukrepi, vključno s pravico do obveščenosti o posebnih razlogih za odločitev in s tem povezani logiki, do popravka netočnih ali nepopolnih podatkov in do izpodbijanja odločitve, če je bila sprejeta na podlagi napačnih dejstev⁵⁹.
61. DPF ne zagotavlja posebnih pravnih jamstev, če se za posameznike sprejmejo odločitve, ki imajo zanje pravne učinke ali znatno vplivajo nanje in ki temeljijo zgolj na avtomatizirani obdelavi podatkov, namenjeni ovrednotenju nekaterih osebnih vidikov v zvezi s temi posamezniki, kot so njihova uspešnost pri delu, kreditna sposobnost, zanesljivost ali ravnanje.
62. Kot je bilo že navedeno v Mnenju št. 01/2016 Delovne skupine iz člena 29 in v prejšnjih mnenjih EOVP o odločitvah o ustreznosti v zvezi z Japonsko in Južno Korejo⁶⁰, EOVP ugotavlja, da hiter razvoj na področju avtomatiziranega sprejemanja odločitev in oblikovanja profilov – vse bolj s pomočjo tehnologij umetne inteligence – zahteva posebno pozornost v zvezi s tem⁶¹.
63. EOVP je seznanjen s trditvami Komisije, da dejstvo, da DPF ne vsebuje posebnih pravil o avtomatiziranem sprejemanju odločitev, najverjetneje ne bo vplivalo na raven varstva osebnih

⁵⁶ Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.3, str. 21.

⁵⁷ [Glede na sodbo v zadevi Schrems II je EOVP v številnih smernicah in priporočilih dodatno pojasnil obveznosti izvoznikov in uvoznikov podatkov v zvezi z nadaljnjimi prenosi: glej Priporočila EOVP 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravno varstva osebnih podatkov na ravni EU \(različica 2.0, sprejeta 18. junija 2021\); Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe \(sprejeta 10. novembra 2020\); Smernice 04/2021 o kodeksih ravnanja kot orodjih za prenose \(različica 2.0, sprejeta 22. februarja 2022\); Priporočila 1/2022 glede vloge za odobritev ter o elementih in načelih iz zavezujočih poslovnih pravilnih za upravljavce \(sprejeta 14. novembra 2022\); Smernice 07/2022 o certificiranju kot orodju za prenose \(sprejete 14. februarja 2023 po javnem posvetovanju\).](#)

⁵⁸ Mnenje št. 01/2016 Delovne skupine iz člena 29, točka 2.2.3, str. 21.

⁵⁹ Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, oddelek 3.B.3.

⁶⁰ [Mnenje EOVP 28/2018 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na Japonskem, sprejeto 5. decembra 2018; Mnenje EOVP 32/2021 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov v Republiki Koreji, sprejeto 24. septembra 2021.](#)

⁶¹ Glej med drugim zadevo C-634/21, *OQ/Land Hesse (SCHUFA Holding in drugi)*, predlog za sprejetje predhodne odločbe (postopek še poteka).

podatkov, ki so bili zbrani v Uniji (saj bi vsako odločitev na podlagi avtomatizirane obdelave običajno sprejel upravljavec v Uniji, ki ima neposreden odnos z zadevnim posameznikom, na katerega se nanašajo osebni podatki)⁶². Vendar pa meni, da ni mogoče izključiti, da bi upravljavec s sedežem v ZDA lahko uporabil avtomatizirano sprejemanje odločitev o podatkih, prenesenih v skladu z osnutkom sklepa (na primer v okviru zaposlitve, za ocenjevanje uspešnosti pri delu, zavarovanje ali nastanitev).

64. EOVP pozdravlja sklicevanja Komisije na posebne zaščitne ukrepe, ki jih na različnih področjih zagotavlja ustrezna zakonodaja ZDA⁶³. Vendar se mu zdi, da se raven zaščite posameznikov razlikuje glede na to, katera pravila za posamezni sektor se v danih okoliščinah uporabljajo – če sploh katera. Obstaja tveganje, da nekatere okoliščine ne bodo zajete, ker ne spadajo na področje uporabe navedenih aktov. Poleg tega je vsebina pravic posameznika v zvezi z avtomatiziranim sprejemanjem odločitev v različnih aktih različno opisana.
65. Glede na navedeno EOVP meni, da so potrebna posebna pravila v DPF v zvezi z avtomatiziranim sprejemanjem odločitev, da se zagotovijo zadostni zaščitni ukrepi, vključno s pravico posameznika do seznanjenosti z razlogi zanje, do izpodbijanja odločitve ter do osebnega posredovanja, če odločitev znatno vpliva na posameznika⁶⁴.

2.2 Postopkovni mehanizmi in mehanizmi izvrševanja

66. EOVP ugotavlja, da se DPF še vedno opira na sistem samocertificiranja, čeprav ga Komisija imenuje sistem „certificiranja“.
67. EOVP opozarja na izboljšave, dosežene pri preteklih skupnih pregledih. Na primer, kar zadeva vlogo ministrstva za trgovino pri postopku (ponovnega) samocertificiranja (...), spremljanje skladnosti podjetij z načeli DPF (na primer s pregledi na kraju samem, uporabo vprašalnikov o skladnosti) ter prepoznavanje in obravnavo lažnih trditev o udeležbi (na primer z iskanjem po internetu).
68. Hkrati sta WP29 in EOVP izrazila zaskrbljenost glede pomanjkanja nadzora nad skladnostjo z zahtevami zasebnostnega ščita⁶⁵. EOVP se zlasti strinja z ugotovitvami Komisije po tretjem letnem pregledu zasebnostnega ščita, da so bili v okviru zasebnostnega ščita pregledi na kraju samem, ki jih je izvajalo ministrstvo za trgovino, običajno omejeni na formalne zahteve (na primer neodzivnost določenih kontaktnih točk ali nedostopnost politike zasebnosti podjetja na spletu)⁶⁶. EOVP meni, da so pregledi skladnosti v zvezi z bistvenejšimi zahtevami ključni.
69. EOVP opozarja tudi na pomen učinkovitega nadzora (vključno s skladnostjo z bistvenimi zahtevami) in izvrševanja DPF. EOVP bo ta vidik pozorno spremljal, tudi v okviru rednih pregledov.
70. Kar zadeva izvrševanje, je EOVP seznanjen z obnovljenimi zavezami v dopisih FTC⁶⁷ in ministrstva za promet⁶⁸, da bosta prednostno obravnavala preiskave domnevnih kršitev DPF, sprejela ustrezne izvršilne ukrepe proti subjektom, ki lažno ali goljufivo navajajo udeležbo, spremljala izvršilne odloke v zvezi s kršitvami DPF in sodelovala z organi EU za varstvo podatkov. V zvezi s tem EOVP tudi priznava,

⁶² Osnutek sklepa, uvodni izjavi 33 in 34.

⁶³ Osnutek sklepa, uvodna izjava 35.

⁶⁴ Glej tudi poročilo o tretjem skupnem pregledu, točka 76.

⁶⁵ Poročilo o tretjem skupnem pregledu, točka 7.

⁶⁶ [Poročilo Komisije Evropskemu parlamentu in Svetu o tretjem letnem pregledu delovanja zasebnostnega ščita EU-ZDA \(23. 10. 2019, COM\(2019\) 495 final\)](#), str. 4.

⁶⁷ Osnutek sklepa, Priloga IV.

⁶⁸ Osnutek sklepa, Priloga V.

da je FTC navedla, da namerava svoja prizadevanja za izvrševanje še naprej osredinjati na bistvene kršitve DPF in preiskovati take kršitve (tudi) na lastno pobudo. EOVP bo te vidike pozorno spremljal, tudi v okviru rednih pregledov.

2.3 Mehanizmi pravnega varstva

71. EOVP pozdravlja jasno predstavitev sedmih možnosti pravnega varstva v osnutku sklepa, ki so na voljo posameznikom iz EU, na katere se nanašajo osebni podatki, če se njihovi osebni podatki obdelujejo v nasprotju z DPF⁶⁹.
72. Ti različni pritožbeni mehanizmi so vzpostavljeni v skladu z zahtevami načel pritožbenega mehanizma, izvrševanja in odgovornosti ter dopolnilnega načela 11 o „reševanju sporov in izvrševanju“, ki jih je izdalo ministrstvo za trgovino in so navedena v Prilogi I k osnutku sklepa⁷⁰.
73. Kot je v svojem osnutku sklepa poudarila Komisija, „mora imeti posameznik, na katerega se nanašajo osebni podatki, na voljo učinkovito upravno in sodno varstvo“⁷¹. To odraža zahtevo iz člena 45(2)(a) Splošne uredbe o varstvu podatkov, po kateri mora Komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi upoštevati zlasti „učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo“⁷². Na to zahtevo je opozorjeno tudi v referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov⁷³.
74. EOVP ugotavlja, da so ti mehanizmi pravnega varstva enaki mehanizmu, vključenim v prejšnji zasebnostni ščit, na katerega je WP29 podala pripombe⁷⁴.
75. EOVP v zvezi z arbitražnim mehanizmom ugotavlja, da ta možnost ni na voljo za izjeme od načel DPF⁷⁵, zato se sklicuje na svojo pripombo iz odstavka 33.
76. EOVP bi v zvezi z dodatnimi možnostmi pravnega varstva, ki so na voljo v skladu z zakonodajo ZDA, pozdravil tudi dodatne podrobnosti o navedeni zakonodaji⁷⁶ in se skliceval na svojo pripombo iz odstavka 21.
77. Poleg tega EOVP pozdravlja dopis FTC, v katerem opisuje, da namerava tesno sodelovati z organi EU za varstvo podatkov⁷⁷. EOVP prav tako pozdravlja prednostno obravnavo pritožb s strani FTC, čeprav to posamezniku, na katerega se nanašajo osebni podatki, morda ne zagotavlja, da bodo njegove pritožbe obravnavane v vseh primerih.
78. EOVP bi v zvezi z možnostjo, da posamezniki v nekaterih primerih svoje pritožbe vložijo pri organu EU za varstvo podatkov, pozdravil dodatne informacije (i) o tem, ali lahko možnost organa EU za varstvo podatkov, da svetuje o ukrepih glede reševanja pritožb in izplačila odškodnin, vključuje priporočilo za kazni ali uporabo preiskovalnih pooblastil, in (ii) v kolikšni meri bi FTC ali ministrstvo za promet upoštevalo ukrep organa EU za varstvo podatkov kot dokaz izvršilnega ukrepa⁷⁸.

⁶⁹ Osutek sklepa, uvodna izjava 67.

⁷⁰ Osutek sklepa, Priloga I, oddelka II.7 in III.11 ter Priloga I k Prilogi I.

⁷¹ Osutek sklepa, uvodna izjava 64.

⁷² Glej tudi uvodno izjavo 141 Splošne uredbe o varstvu podatkov, ki se sklicuje na člen 47 Listine EU o temeljnih pravicah glede pravice do učinkovitega pravnega sredstva v EU.

⁷³ Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, str. 8.

⁷⁴ Glej zlasti Mnenje št. 01/2016 Delovne skupine iz člena 29, oddelek 2.2.6 (a).

⁷⁵ Osutek sklepa, Priloga I k Prilogi I, A.

⁷⁶ Osutek sklepa, uvodna izjava 85.

⁷⁷ Osutek sklepa, Priloga IV.

⁷⁸ Osutek sklepa, Priloga I, III.5.b.(iii).

79. EOVP bo natančno spremljal učinkovitost teh mehanizmov pravnega varstva, tudi v okviru rednih pregledov.

3 DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V ZDA, IN NJIHOVA UPORABA

3.1 Dostop in uporaba za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

3.1.1 Dostop organov kazenskega pregona do osebnih podatkov bi moral temeljiti na jasnih, natančnih in dostopnih pravilih

80. EOVP pozdravlja podrobnejše informacije in pojasnila v primerjavi s prejšnjim sklepom o ustreznosti, zagotovljene v osnutku sklepa v zvezi z dostopom organov kazenskega pregona ZDA do osebnih podatkov in njihovo uporabo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Priloga IV k osnutku sklepa vsebuje tudi dopis kazenskega oddelka ministrstva za pravosodje ZDA, ki „vsebuje kratek pregled glavnih preiskovalnih orodij za pridobivanje poslovnih in drugih podatkov iz evidenc korporacij v Združenih državah za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali javnega (civilnega in regulativnega) interesa, vključno z omejitvami dostopa, ki so jih določili ti organi“. V skladu z dopisom se vsi v njem opisani pravni postopki uporabljajo za pridobivanje informacij od korporacij v ZDA ne glede na državljanstvo ali kraj prebivališča posameznika, na katerega se nanašajo osebni podatki, in izhajajo neposredno iz ustave ZDA (četrty amandma), iz zakonskega in postopkovnega prava ali iz smernic in politik ministrstva za pravosodje. Ta pregled ne zajema preiskovalnih orodij za nacionalno varnost, ki jih uporabljajo organi kazenskega pregona pri terorističnih in drugih preiskavah v zvezi z nacionalno varnostjo⁷⁹.
81. EOVP ugotavlja, da osnutek sklepa in Priloga VI k osnutku sklepa obravnavata predvsem zvezne organe kazenskega pregona in regulativne organe⁸⁰ ter se ne sklicujeta izrecno na državne zakone, ki določajo te postopke za pridobivanje informacij. V Prilogi VI je tudi navedeno, da „obstajajo 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“, in vsebuje več neizčrpnih primerov, kot so *Bank Secrecy Act* (Zakon o bančni tajnosti) in njegovi izvedbeni predpisi⁸¹, *Fair Credit Reporting Act* (Zakon o poštenem kreditnem poročanju)⁸² in *Right to Financial Privacy Act* (Zakon o pravici do finančne zasebnosti)⁸³. EOVP ugotavlja, da je veljavna pravna podlaga podane zahteve za dostop odvisna od narave zahtevanih podatkov, narave podjetja, narave pravnih postopkov (kazenski, upravni, povezani z drugim javnim interesom) in narave subjekta, ki zahteva dostop. Ker vsa veljavna pravila za omejevanje dostopa organov kazenskega pregona do podatkov, prenesenih v ZDA, temeljijo na ustavi, zakonodaji in preglednih politikah ministrstva za pravosodje, EOVP priznava dostopnost teh pravil in poziva Komisijo, naj ta element upošteva v osnutku sklepa. Iz Priloge VI izhaja, da se ti zakoni uporabljajo ne glede na državljanstvo ali kraj prebivališča posameznika, na katerega se nanašajo osebni podatki, in na splošno vključujejo zahteve četrtega amandmaja (čeprav jih pogosto presegajo in vključujejo dodatno varstvo).

⁷⁹ Osnutek sklepa, opomba 1 k Prilogi VI.

⁸⁰ Glej osnutek sklepa, uvodne izjave 90–93.

⁸¹ Člen 5318 naslova 31 za zakonodajne zbirke ZDA; naslov 31 kodeksa zveznih predpisov, poglavje X.

⁸² Člen 1681b naslova 15 zakonodajne zbirke ZDA.

⁸³ Členi 3401–3423 naslova 12 zakonodajne zbirke ZDA.

82. EOVP na koncu ugotavlja, da je ocena v osnutku sklepa v zvezi z dostopom zveznih organov kazenskega pregona podrobnejša kot v prejšnjem sklepu o ustreznosti. Glede dostopa državnih organov kazenskega pregona EOVP prav tako ugotavlja, da mora biti v skladu s Prilogo VI varstvo državnih zakonov vsaj enakovredno varstvu po ameriški ustavi, vključno s četrtem amandmajem, vendar ne omejeno nanj. EOVP poziva Komisijo, naj v prihodnjih pregledih nadalje oceni element varstva po državnih zakonih.

3.1.2 Dokazati je treba nujnost in sorazmernost v zvezi s postavljenimi legitimnimi cilji

83. EOVP ustrezno ugotavlja, da se lahko zahteva za dostop do podatkov za namene kazenskega pregona splošno šteje za legitimen cilj. Hkrati pa so taki posegi sprejemljivi le, če so nujni in sorazmerni.⁸⁴
84. V skladu z ustaljeno sodno prakso Sodišča načelo sorazmernosti zahteva, da je z zakonodajnimi ukrepi, ki uvajajo posege v pravice do zasebnega življenja in varstva osebnih podatkov, „mogoče uresničiti legitime cilje, ki jim sledi zadevna ureditev, in da to ravnanje ne prestopi meje tega, kar je primerno in potrebno za uresničitev teh ciljev“⁸⁵. Zato se ocena nujnosti in sorazmernosti načeloma vedno izvede v povezavi s posebnim ukrepom, ki ga določa zakonodaja.
85. Organi ZDA v Prilogi VI navajajo, da lahko zvezni tožilci in zvezni preiskovalni agenti pridobijo dostop do dokumentov in drugih podatkov iz evidenc organizacij z „več vrstami obveznih pravnih 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“⁸⁶. Poleg tega lahko agencije s civilno in regulativno odgovornostjo organizacijam izdajo pozive za „poslovne evidence, elektronsko shranjene informacije ali druge oprijemljive predmete“⁸⁷. Postopki so pojasnjeni tudi v uvodnih izjavah 90–93 osnutka sklepa. EOVP glede tega opaža pozitiven razvoj sodne prakse ZDA v zvezi z elektronsko shranjenimi informacijami, naveden v osnutku sklepa⁸⁸.
86. Poleg tega je v Prilogi VI določeno, da so ti pravni postopki nediskriminatorni in se na splošno uporabljajo za pridobivanje informacij od „korporacij“ v ZDA, ne glede na to, ali so certificirane v okviru za varstvo zasebnosti podatkov med EU in ZDA ali ne in „ne glede na državljanstvo ali kraj prebivališča posameznika, na katerega se nanašajo osebni podatki“.
87. Poleg tega Priloga VI vsebuje ugotovitve v zvezi z zaščitnimi ukrepi v skladu s četrtem amandmajem ustave ZDA, v skladu s katerimi je za preiskave in zasege, ki jih izvajajo organi kazenskega pregona,

⁸⁴ Glej sodbo Sodišča z dne 6. oktobra 2020 v združenih zadevah C-511/18, C-512/18 in C-520/18, *La Quadrature du Net in drugi*, ECLI:EU:C:2020:791 (v nadaljevanju: sodba Sodišča v zadevi *La Quadrature du Net*), točka 140. Glej tudi ENVP [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit](#) (Ocena nujnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: nabor orodij), 11. april 2017 in ENVP, [Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data](#) (Smernice o oceni sorazmernosti ukrepov, ki omejujejo temeljni pravici do zasebnosti in do varstva osebnih podatkov), 19. december 2019.

⁸⁵ Glej sodbo Sodišča z dne 8. aprila 2014 v združenih zadevah C-293/12 in C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238 (v nadaljevanju: sodba Sodišča v zadevi *Digital Rights Ireland*), točka 46 in navedena sodna praksa.

⁸⁶ Osnutek sklepa, Priloga VI, str. 2.

⁸⁷ Osnutek sklepa, Priloga VI, str. 4.

⁸⁸ Glej osnutek sklepa, opomba 146. Vrhovno sodišče ZDA je v sodbi iz leta 2018 potrdilo, da morajo i meti organi kazenskega pregona nalog za preiskavo ali da mora obstajati izjema, zaradi katere nalog ni potreben, tudi za dostop do evidenc historičnih lokacijskih podatkov baznih postaj, ki zagotavljajo celovit pregled gibanja uporabnika, in da lahko uporabnik razumno pričakuje zasebnost v zvezi s takimi podatki (*Timothy Ivory Carpenter proti Združenim državam Amerike*, št. 16-402, 585 ZDA (2018)).

načeloma potreben sodni nalog ob dokazanem utemeljenem razlogu in zahtevah po določnosti, ter se sklicuje na dejstvo, da se v izjemnih primerih, ko zahteva po izdanem nalogu ne velja, za kazenski pregon izvede preizkus utemeljenosti v skladu s četrtem amandmajem⁸⁹. Oseba, ki se preišče ali katere lastnina se preišče, lahko poskuša doseči, da se dokazi, predloženi zoper njo med kazenskim postopkom, ki so bili pridobljeni ali izhajajo iz nezakonite preiskave, izločijo⁹⁰.

88. EOVP na koncu ugotavlja, da sistem preiskovalnih orodij, ki se uporablja za pridobivanje poslovnih in drugih podatkov iz evidenc korporacij v ZDA za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali javnega interesa – vključno z omejitvami dostopa in zaščitnimi ukrepi – zagotavlja celovit, toda tudi zapleten sistem ukrepov, ki med drugim odraža zvezno naravo ameriške vlade.
89. Zato se lahko šteje, da sistem preiskovalnih ukrepov organov kazenskega pregona v ZDA na splošno izpolnjuje zahteve po nujnosti in sorazmernosti v zvezi s temeljnimi pravicami do zasebnega življenja in varstva podatkov.

3.1.3 Obstajati bi moral neodvisen mehanizem nadzora

90. EOVP ustrezno ugotavlja, da večina postopkov, opisanih v osnutku sklepa in Prilogi VI, predpostavlja odločitev sodišča, preden organi pridobijo dostop do podatkov (na primer sodne odredbe za snemalnike klicev ter sledilne naprave⁹¹, sodne odredbe za nadzor v skladu s *Federal Wiretap Law* (Zveznim zakonom o prisluškovanju telefonskim pogovorom)⁹², naloge za preiskavo – zvezna pravila o izvajanju kazenskega postopka, pravilo 41⁹³). Vendar se zdi, da vsi ne zahtevajo vnaprejšnje vključenosti sodišča. Na primer, civilne oblasti in regulativni organi „lahko izdajo pozive“⁹⁴. Vendar v teh primerih obstaja možnost naknadnega sodnega nadzora nad primernostjo poziva, saj „lahko prejemnik upravnega poziva oporeka izvršitvi zadevnega poziva na sodišču“⁹⁵.
91. Poleg tega je v osnutku sklepa opisan nadzor nad zveznimi organi kazenskega pregona s strani različnih organov, od notranjega nadzora s strani uradnikov za varstvo zasebnosti in državljanske svoboščine do zunanjega nadzora, ki ga izvajajo generalni inšpektor in posebni odbori ameriškega Kongresa⁹⁶. Evropska komisija zagotavlja raznolike in podrobne informacije ter načeloma sprejema razumljive sklepe. Zato EOVP v tem mnenju ne povzema dejanske ugotovitve in ocen.
92. EOVP na podlagi informacij, ki so na voljo, ugotavlja, da je, kar zadeva dostop organov kazenskega pregona do podatkov, ki jih hranijo podjetja v ZDA, očitno vzpostavljen precej zanesljiv neodvisen mehanizem nadzora.

3.1.4 Posamezniku morajo biti na voljo učinkovita pravna sredstva

93. V skladu s sodno prakso Sodišča mora biti posamezniku na voljo učinkovito pravno sredstvo za uveljavljanje njegovih pravic, kadar meni, da se ne spoštujejo ali da niso bile spoštovane. Sodišče je v sodbi v zadevi *Schrems I* pojasnilo, da „ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravilo oziroma izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega

⁸⁹ Glej osnutek sklepa, Priloga VI, str. 2.

⁹⁰ Glej osnutek sklepa, uvodna izjava 90.

⁹¹ Glej osnutek sklepa, uvodna izjava 92.

⁹² Glej osnutek sklepa, Priloga VI, str. 3.

⁹³ Glej osnutek sklepa, uvodna izjava 90 in Priloga VI, str. 3.

⁹⁴ Glej osnutek sklepa, Priloga VI, str. 4, in uvodna izjava 91.

⁹⁵ Glej osnutek sklepa, Priloga VI, str. 4, in uvodna izjava 91.

⁹⁶ Glej osnutek sklepa, uvodne izjave 103–106.

varstva, določene v členu 47 Listine. Člen 47, prvi odstavek, Listine namreč določa, da ima vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Unije, pravico do učinkovitega pravnega sredstva pred sodiščem v skladu s pogoji, določenimi v tem členu.”⁹⁷

94. Osnutek sklepa⁹⁸ in njegova Priloga VI vsebujeta nadaljnje informacije o mogočih pravnih sredstvih, ki izhajajo iz zakonskih določb ter bi bile na voljo posameznikom, če bi javni organi nezakonito pridobili dostop do njihovih podatkov.
95. Po navedbah Komisije⁹⁹ člen 702 naslova 5 zakonodajne zbirke ZDA (*Administrative Procedure Act* (Zakon o upravnem postopku, v nadaljevanju: APA)) glede tega določa, da ima vsaka oseba, ki ji je bila storjena pravna krivica zaradi ukrepanja agencije ali na katero je to ukrepanje agencije negativno vplivalo ali jo oškodovalo, pravico, da zahteva sodno presojo.
96. Poleg tega *Stored Communications Act* (Zakon o shranjenih komunikacijah, v nadaljevanju: SCA) določa, da lahko vsaka oseba, ki je bila oškodovana zaradi kakršne koli kršitve tega poglavja, vloži proti osebi ali subjektu, ki niso Združene države in ki je sodeloval/-a pri tej kršitvi, civilno tožbo za izplačilo ustrezne odškodnine, če je bilo ravnanje, ki pomeni kršitev, storjeno zavestno ali namerno¹⁰⁰. Vsaka oseba, ki je bila oškodovana zaradi kakršne koli namerne kršitve tega poglavja ali poglavja 119, lahko na *United States District Court* (okrožno sodišče Združenih držav Amerike) vloži tudi tožbo proti Združenim državam za izplačilo denarne odškodnine¹⁰¹.
97. Poleg tega osnutek sklepa vsebuje tudi informacije o pravici do dostopa do evidenc zvezne agencije v skladu s *Freedom of Information Act* (Zakon o dostopu do informacij javnega značaja, v nadaljevanju: FOIA)¹⁰² in številnimi drugimi zakoni, ki posameznikom dodeljujejo pravico, da vložijo tožbo zoper javni organ ali uslužbenca ZDA zaradi obdelave njegovih osebnih podatkov; taki zakoni so *Wiretap Act* (Zakon o prisluškovanju telefonskim pogovorom), *Computer Fraud and Abuse Act* (Zakon o računalniških goljufijah in zlorabah), *Federal Torts Claim Act* (Zvezni zakon o odškodninskih zahtevkih), *Right to Financial Privacy Act* (Zakon o pravici do finančne zasebnosti) in *Fair Credit Reporting Act* (Zakon o poštenem kreditnem poročanju)¹⁰³.
98. EOVP zato pozdravlja pojasnila Komisije o številu možnosti pravnega varstva, ki so na voljo posameznikom. EOVP tudi poziva Komisijo, naj dodatno pojasni, ali ta pravna sredstva posamezniku, na katerega se nanašajo osebni podatki, omogočajo, da bi „imel dostop do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravek ali izbris takih podatkov“, kot zahteva Sodišče.

3.1.5 Nadaljnja uporaba zbranih informacij

3.1.5.1 Nadaljnja uporaba prenesenih podatkov, do katerih dostopajo organi kazenskega pregona v ZDA

99. EOVP z zadovoljstvom ugotavlja, da je v osnutku sklepa ocenjena nadaljnja uporaba podatkov, do katerih dostopajo organi kazenskega pregona v ZDA. Vendar obžaluje, da je naveden samo en primer razlogov za nadaljnje razširjanje informacij¹⁰⁴. EOVP glede tega priporoča Komisiji, naj v osnutek sklepa

⁹⁷ Sodba Sodišča v zadevi *Schrems I*, točka 95.

⁹⁸ Glej osnutek sklepa, uvodne izjave 107–112.

⁹⁹ Glej osnutek sklepa, uvodna izjava 109.

¹⁰⁰ Člen 2707 naslova 18 zakonodajne zbirke ZDA.

¹⁰¹ Člen 2712 naslova 18 zakonodajne zbirke ZDA.

¹⁰² Glej osnutek sklepa, uvodna izjava 111.

¹⁰³ Glej osnutek sklepa, uvodna izjava 112.

¹⁰⁴ Glej osnutek sklepa, uvodna izjava 102.

vključi dodatna pojasnila o načelih in zaščitnih ukrepih, ki se uporabljajo za nadaljnjo uporabo podatkov, kot so tisti, vključeni v *Privacy Act* (Zakon o varstvu zasebnosti) (člen 552a naslova 5 zakonodajne zbirke ZDA)¹⁰⁵.

3.1.5.2 Nadaljnji prenosi zunaj ZDA

100. EOVP nadalje ugotavlja, da se je Evropska komisija sklicevala tudi na nadaljnje prenose od organov kazenskega pregona v ZDA organom v tretjih državah, vendar vnovič le v zvezi s smernicami pravosodnega ministra o notranjem delovanju FBI¹⁰⁶. EOVP meni, da so take informacije in ocene ključne, da se omogoči celovita ocena ravni varstva, ki jo zagotavljajo zakonodajni okvir in prakse ZDA v zvezi z razkritjem in nadaljnjo uporabo v tujini. Ker je Komisija navedla samo en, omejen primer v zvezi z nadaljnjimi prenosi zunaj ZDA kot celote, jo EOVP poziva, naj dodatno pojasni veljavna pravila in zaščitne ukrepe za nadaljnje prenose, nadaljnjo uporabo in razkritje osebnih podatkov, zbranih za namene kazenskega pregona v ZDA in nadalje prenesenih v tretje države, tudi prek mednarodnih sporazumov.

3.2 Dostop in uporaba za namene nacionalne varnosti

101. EOVP na splošno priznava, da imajo države na voljo široko polje proste presoje pri vprašanih nacionalne varnosti, kar priznava tudi ESČP. EOVP tudi opozarja, da, kot je poudarjeno v njegovih posodobljenih priporočilih o osnovnih evropskih jamstvih za nadzorne ukrepe¹⁰⁷, člen 6(3) Pogodbe o Evropski uniji določa, da so temeljne pravice iz EKČP splošna načela prava Unije. Vendar, kot EOVP opozarja v svoji praksi, EKČP, dokler EU ne bo pristopila k njej, ni pravni instrument, ki je formalno vključen v pravo Unije¹⁰⁸. Zato je treba raven varstva temeljnih pravic, ki jo zahteva člen 45 Splošne uredbe o varstvu podatkov, določiti na podlagi določb navedene uredbe, ki se razlagajo ob upoštevanju temeljnih pravic iz Listine EU o temeljnih pravicah. Glede na navedeno morajo imeti v skladu s členom 52(3) Listine EU o temeljnih pravicah pravice, vsebovane v njej, ki ustrezajo pravicam, ki jih zagotavlja EKČP, enak pomen in področje uporabe kot tiste, ki so določene v EKČP. Zato je treba, kot je opozorilo Sodišče, upoštevati sodno prakso ESČP v zvezi s pravicami, ki so predvidene tudi v Listini EU o temeljnih pravicah, kot minimalni prag varstva za razlago ustreznih pravic iz Listine EU¹⁰⁹. Vendar v skladu z zadnjim stavkom člena 52(3) Listine EU o temeljnih pravicah „[t]a določba ne preprečuje širšega varstva po pravu Unije“.
102. Zato je EOVP pri naslednji oceni upošteval sodno prakso ESČP, kolikor Listina EU o temeljnih pravicah, kot jo razlaga Sodišče, ne določa višje ravni varstva, ki predpisuje druge zahteve kot sodna praksa ESČP.
103. Več pravnih instrumentov v pravnem okviru ZDA omogoča obveščevalnim agencijam ZDA zbiranje podatkov, nadaljnji dostop do njih in njihovo obdelavo.
104. Kot je v svojem osnutku sklepa opozorila Komisija, lahko „obveščevalne agencije ZDA zahtevajo dostop do osebnih podatkov, ki so bili preneseni v organizacije v Združenih državah, za namene nacionalne varnosti le, kot je dovoljeno z zakonom, natančneje v skladu z zakonom o nadzoru tujih obveščevalnih podatkov (FISA), ali zakonskimi določbami, ki dovoljujejo dostop prek sodnih pozivov v zvezi z nacionalno varnostjo“¹¹⁰. „Obveščevalne agencije ZDA imajo tudi možnost zbiranja osebnih podatkov

¹⁰⁵ Glej smernice pravosodnega ministra o notranjem delovanju FBI (AGG-DOM), stran 36, B(1)(g).

¹⁰⁶ Glej osnutek sklepa, uvodna izjava 102.

¹⁰⁷ Glej Priporočila EOVP 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe.

¹⁰⁸ Glej sodbo Sodišča v za deva *Schrems II*, točka 98.

¹⁰⁹ Glej sodbo Sodišča v za deva *La Quadrature du Net*, točka 124.

¹¹⁰ Glej osnutek sklepa, uvodna izjava 115.

zunaj Združenih držav, med drugim osebnih podatkov v tranzitu med Unijo in Združenimi državami“ v skladu z Odredbo št. 12333¹¹¹.

105. Odredba št. 14086 v zvezi s posebnimi ureditvami zbiranja podatkov, zlasti členom 702 FISA in Odredbo št. 12333, zdaj določa nova pravila za izboljšanje zaščitnih ukrepov za dejavnosti SIGINT v ZDA. Ta splošna pravila se uporabljajo horizontalno in „jih je treba nadalje izvajati s politikami in postopki agencije, s katerimi se prenašajo v konkretne smernice za vsakodnevno delovanje“¹¹². Odredba št. 14086 je večinoma nadomestila prejšnjo Predsedniško politično direktivo 28 (*Presidential Policy Directive 28*, v nadaljevanju: PPD-28)¹¹³.
106. Da bi ocenili pravni okvir, ki se uporablja za zbiranje in nadaljnjo obdelavo podatkov ter dostop do njih za namene nacionalne varnosti, je pomembno preučiti poseben pravni okvir, ki ureja zbiranje podatkov znotraj in zunaj ZDA, tj. člen 702 FISA in Odredbo št. 12333, ki se od prejšnjega pregleda zasebnostnega štita nista spremenila, ob upoštevanju dejstva, da nova Odredba št. 14086 zagotavlja zaščitne ukrepe, ki jih je treba izvajati tudi pri zbiranju podatkov na podlagi posebnih besedil, kot sta na primer člen 702 FISA in Odredba št. 12333.

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

107. EOVP želi pri oceni splošne ureditve zbiranja podatkov za namene nacionalne varnosti opozoriti na prvo od štirih tako imenovanih „osnovnih evropskih jamstev“, v skladu s katerimi „bi morala biti obdelava skladna s pravom ter temeljiti na jasnih, natančnih in dostopnih pravilih“¹¹⁴.
108. V skladu z ustaljeno sodno prakso Sodišča mora biti vsaka omejitev pravice do varstva osebnih podatkov določena z zakonom, pravna podlaga, ki dovoljuje poseganje v tako pravico, pa mora že sama opredeljevati obseg omejitve izvrševanja zadevne pravice¹¹⁵. Poleg tega je Sodišče opozorilo, da „mora biti ureditev zakonsko zavezujoča v nacionalnem pravu“¹¹⁶. V zvezi s tem sodna praksa ESČP pojasnjuje, da je treba izraz „pravo“ razumeti v stvarnem in ne formalnem pomenu. Zajema lahko besedila nižjega ranga od zakonskih aktov in tudi predpise, ki jih sprejme strokovno združenje na podlagi pooblastila zakonodajalca v okviru svojega avtonomnega pooblastila za normativno urejanje, ter celo nezapisano pravo. Norma se lahko šteje za „zakon“, če je ustrezno dostopna in je oblikovana z zadostno določenostjo¹¹⁷.
109. Stopnjo potrebne določenosti je treba meriti glede na obseg omejitve pravice¹¹⁸. Poleg tega je ESČP v zvezi s „predvidljivostjo“ prava v zadevi *Zakharov* opozorilo, da v okviru tajnih nadzornih ukrepov, kot je prestrezanje komunikacije, „zahteva po predvidljivosti ne more pomeniti, da je treba posamezniku

¹¹¹ Glej osnutek sklepa, uvodna izjava 117.

¹¹² Glej osnutek sklepa, uvodna izjava 120.

¹¹³ Navedena odredba razveljavlja PPD-28, razen njenih členov 3 in 6 ter tajne priloge k navedeni direktivi, ki ostajajo v veljavi. Glej predsedniški memorandum o nacionalni varnosti z dne 7. oktobra 2022.

¹¹⁴ Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, sprejeta 10. novembra 2020. Glej točki 175 in 180 sodbe v zadevi *Schrems II* in Mnenje št. 1/15 (sporazum med EU in Kanado o evidenci PNR) z dne 26. julija 2017, točka 139 in navedena sodna praksa.

¹¹⁵ Glej sodbo v zadevi *Schrems II*, točki 174 in 175 ter navedena sodna praksa. Glede dostopa javnih organov držav članic glej tudi sodbo v zadevi C-623/17, *Privacy International*, ECLI:EU:C:2020:790 (v nadaljevanju: sodba Sodišča v zadevi *Privacy International*), točka 65, in sodbo Sodišča v zadevi *La Quadrature du Net*, točka 175.

¹¹⁶ Sodba Sodišča v zadevi *Privacy International*, točka 68.

¹¹⁷ ESČP, *Sunday Times proti Združenemu kraljestvu* (št. 1), 26. april 1979, CE:ECHR:1979:0426JUD000653874 (v nadaljevanju: sodba ESČP v zadevi *Sunday Times proti Združenemu kraljestvu* št. 1), točka 49.

¹¹⁸ Sodba ESČP v zadevi *Sunday Times proti Združenemu kraljestvu* št. 1, točka 49.

omogočiti, da predvidi, ali in kdaj lahko organi prestrezajo njegove komunikacije, da bi lahko skladno s tem prilagodil svoje ravnanje“. Vendar pa so jasna in podrobna pravila o ukrepih tajnega nadzora bistvena, da se prepreči tveganje samovoljnosti, kadar se pooblastila, dodeljena izvršilni veji oblasti, izvajajo tajno. „Domače pravo mora biti dovolj jasno, da lahko državljani v zadostni meri razberejo, v katerih okoliščinah in pod katerimi pogoji so javni organi pooblašteni za uporabo kakršnih koli takih ukrepov“¹¹⁹.

110. Poleg tega je Sodišče pojasnilo, da bi se bilo treba pri oceni veljavne zakonodaje tretje države osrediniti na to, ali se lahko posamezniki pred sodiščem nanjo sklicujejo in zanesejo. Pravice, dodeljene posameznikom, na katere se nanašajo osebni podatki, bi zlasti morale biti mogoče uveljavljati pred sodišči, posameznikom pa je treba zagotoviti izvršljive pravice v razmerju do javnih organov¹²⁰, kar v okviru prejšnje PPD-28 ni bilo zagotovljeno. Odredba št. 14086, za katero se po mnenju EOVP šteje, da ima enak pravni učinek v pravnem redu ZDA kot PPD-28 (tj. je zavezujoča za izvršilno vejo oblasti), zdaj določa pravice, ki jih je v razmerju do javnih organov mogoče uveljavljati pred sodišči. Podrobna ocena novih izvršljivih pravic posameznikov, na katere se nanašajo osebni podatki, je na voljo v oddelku o pravnem varstvu.
111. Uvodne izjave 114–152 osnutka sklepa in Priloga VII zagotavljajo povzetek nekaterih vidikov veljavnega pravnega okvira, omejitev zbiranja, omejitev hrambe in razširjanja, skladnosti in nadzora, preglednosti in pravnega varstva. Pravni sistem ZDA za obveščevalne dejavnosti je sestavljen iz številnih različnih dokumentov, vključno s poročili, politikami in postopki posameznih agencij. V zvezi s tem se je EOVP v svoji oceni osredinil na omejeno število vprašanj, za katera meni, da so ključna.
112. V skladu z uvodnimi izjavami 115 do 119 osnutka sklepa imajo lahko organi ZDA za nacionalno varnost dostop do prenesenih osebnih podatkov le v skladu s FISA, v skladu z drugimi zakonskimi določbami člena 3414 naslova 15 zakonodajne zbirke ZDA, členov 1681u–1681v naslova 15 zakonodajne zbirke ZDA in člena 2709 naslova 18 zakonodajne zbirke ZDA ali, v zvezi z osebnimi podatki v tranzitu, na podlagi Odredbe št. 12333. Iz uvodnih izjav 116 in 118 osnutka sklepa izhaja, da se je Komisija glede dostopa do osebnih podatkov s strani nacionalnih varnostnih organov ZDA v svoji oceni osredinila na člene 105, 302, 402, 501 in 702 FISA (tuje obveščevalne dejavnosti, usmerjene v nedržavljanke ZDA zunaj ZDA) in Odredbo št. 12333 (tuje obveščevalne dejavnosti v zvezi z osebnimi podatki v tranzitu), ki so najpomembnejši. Mnenje EOVP je zato omejeno na oceno teh določb, ki jo je pripravila Komisija, ob upoštevanju omejitev in zaščitnih ukrepov iz Odredbe št. 14086¹²¹.
113. Glede tega je treba opozoriti, da so vsi pravni instrumenti, navedeni v osnutku sklepa, dostopni širši javnosti (v ZDA in zunaj njih) ter na voljo na spletu. Poleg tega so zahteve, določene v odredbi, zavezujoče za celotno obveščevalno skupnost¹²² in se medsektorsko uporabljajo za vse namene tujih obveščevalnih dejavnosti.
114. Pojem „obveščevalna dejavnost SIGINT“ v Odredbi št. 14086 ni opredeljen. Slednja se sklicuje na opredelitve iz Odredbe št. 12333 za določitev obsega tujih obveščevalnih in protiobveščevalnih dejavnosti, ki so opredeljene široko. Čeprav se je trdilo, da se lahko Odredba št. 12333 od uvedbe FISA uporablja le za zbiranje podatkov zunaj ozemlja ZDA, EOVP glede tega opozarja, da v Odredbi št. 12333, ki ostaja nespremenjena, niso dovolj podrobno opredeljeni njeno geografsko področje uporabe, obseg, v katerem se podatki lahko zbirajo, hranijo ali nadalje razširjajo, niti narava kaznivih dejanj, zaradi

¹¹⁹ ESČP, *Zakharov proti Rusiji*, 4. december 2015 (v nadaljevanju: sodba ESČP v zadevi *Zakharov*), točka 229.

¹²⁰ Sodba Sodišča v zadevi *Schrems II*, točka 181.

¹²¹ Navedena odredba razveljavlja PPD-28, razen njenih členov 3 in 6 ter tajne priloge k navedeni direktivi, ki ostajajo v veljavi. Glej [predsedniški memorandum o nacionalni varnosti z dne 7. oktobra 2022](#).

¹²² Glej osnutek sklepa, uvodna izjava 120.

katerih se lahko uvede nadzor, ali vrsta podatkov, ki se lahko zbirajo ali uporabljajo. Načeloma se lahko vsi tuji obveščevalni podatki v okviru Odredbe št. 12333 zbirajo po presoji predsednika ZDA¹²³. Toda, kot razume EOVP, je glavni namen Odredbe št. 14086 predpisati omejitve za zbiranje in obdelavo osebnih podatkov v okviru tujih obveščevalnih služb, ne glede na to, kateri program nadzora se uporablja in od kod se podatki pridobivajo. EOVP zato meni, da se dodatni zaščitni ukrepi, predvideni v Odredbi št. 14086, uporabljajo tudi v okviru programov nadzora, ki se uporabljajo za osebne podatke v tranzitu v skladu z Odredbo št. 12333¹²⁴.

115. V zvezi s tem Odredba št. 14086 navaja 12 legitimnih ciljev, ki jih je treba uresničevati pri zbiranju obveščevalnih podatkov v okviru SIGINT, pet ciljev, za katere se zbiranje obveščevalnih podatkov v okviru SIGINT ne sme izvajati¹²⁵, in šest legitimnih ciljev za uporabo množično zbranih podatkov¹²⁶. Nekateri so precej podrobni (na primer „reševanje talcev“), drugi pa so splošnejši (na primer „globalna varnost“). V Odredbi št. 14086 je opredeljen tudi seznam prepovedanih ciljev, ki vključuje zlasti zaviranje ali omejevanje „zakonitih zasebnih interesov“¹²⁷. V Odredbi št. 14086 je določena tudi možnost, da predsednik Združenih držav na seznam doda cilje, za katere je zbiranje dovoljeno in za katere se lahko odloči, da se ne objavijo, če meni, da bi to ogrožalo nacionalno varnost Združenih držav¹²⁸. Take posodobitve se lahko odobrijo samo „glede na nove nacionalne varnostne zahteve“.
116. Obveščevalne agencije zbiranja obveščevalnih podatkov v okviru SIGINT ne morejo upravičiti samo s cilji, temveč ga je treba za operativne namene dodatno utemeljiti s konkretnimi prednostnimi nalogami, za katere se lahko zbirajo obveščevalni podatki v okviru SIGINT. V Odredbi št. 14086 je podrobno opisan postopek potrjevanja prednostnih nalog, za katere se lahko zbirajo obveščevalni podatki v okviru SIGINT¹²⁹. EOVP razume, da je postopek za opredelitev potrjenih prednostnih nalog obveščevalnih služb načeloma odvisen od direktorja obveščevalne skupnosti, in priznava, da bi moral praviloma vključevati oceno uradnika za varstvo državljskih svoboščin urada direktorja nacionalne obveščevalne službe (*Civil Liberties Protection Officer of the Office of the Director of National Intelligence*, v nadaljevanju: CLPO ODNI), s katero se direktor ne strinja nujno, ter v tem primeru „vključuje oceno CLPO in mnenje direktorja, ko se predsedniku predloži nacionalni okvir prednostnih nalog obveščevalnih služb (*National Intelligence Priorities Framework*, v nadaljevanju: NIPF)“¹³⁰.
117. Vendar EOVP tudi ugotavlja, da v skladu z opredelitvijo „potrjene prednostne naloge obveščevalne službe“ take prednostne naloge za „večino dejavnosti zbiranja obveščevalnih podatkov v okviru SIGINT v ZDA“¹³¹ pomenijo prednostno nalogo, potrjeno v skladu s členom 2(b)(iii) navedene odredbe (opisano v prejšnjem odstavku). V nekaterih primerih se lahko postopek potrjevanja razlikuje od tega postopka v „omejenih okoliščinah“ in v tem primeru lahko predsednik ali vodja organa obveščevalne skupnosti določi prednostno nalogo, „kolikor je to izvedljivo“ v skladu z merili, opredeljenimi v istem členu 2(b)(iii)(A)(1)–(3), ki zahteva, da se ustrezno upoštevajo zasebnost in državljske svoboščine vseh oseb, vendar brez vpletenosti CLPO.

¹²³ V skladu s členom II ustave ZDA je za zagotavljanje nacionalne varnosti, vključno zlasti z zbiranjem tujih obveščevalnih podatkov, pristojen predsednik kot vrhovni poveljnik oboroženih sil.

¹²⁴ Glej osnutek sklepa, uvodna izjava 134.

¹²⁵ Glej Odredbo št. 14086, člen 2, (b), (ii), A, 1 do 5.

¹²⁶ Glej osnutek sklepa, uvodna izjava 134, in Odredbo št. 14086, člen 2(c)(ii).

¹²⁷ Glej Odredbo št. 14086, člen 2(b)(ii)(A)(2).

¹²⁸ Glej Odredbo št. 14086, člen 2(b)(i)(B).

¹²⁹ Glej osnutek sklepa, uvodna izjava 129.

¹³⁰ Glej Odredbo št. 14086, člen 2(b)(iii)(B).

¹³¹ Glej Odredbo št. 14086, člen 4, (n).

118. Odredba št. 14086 poleg tega poudarja, da se „dejavnosti zbiranja obveščevalnih podatkov v okviru SIGINT, kolikor je to izvedljivo, prilagodijo“ za izboljšanje potrjene prednostne naloge obveščevalne službe in da „obveščevalna skupnost upošteva razpoložljivost, izvedljivost in ustreznost drugih manj vsiljivih virov“ ter zagotavlja splošne zahteve glede nujnosti in sorazmernosti¹³².
119. Poleg tega Odredba št. 14086 v skladu s členom 5(h) ustvarja pravico do vložitve upravičenih pritožb pri CLPO in do revizije odločitev CLPO s strani sodišča za presojo varstva podatkov v skladu z mehanizmom pravnega varstva, vzpostavljenim s členom 3 navedene odredbe.
120. Zdi se, da je besedilo FISA jasnejše in natančnejše od Odredbe št. 12333 glede vrste obveščevalnih operacij, ki se lahko odredijo. FISA in Odredbo št. 12333 je treba zdaj uporabljati glede na Odredbo št. 14086 in med drugim zlasti ob upoštevanju načel nujnosti in sorazmernosti.
121. Zahteve, določene v Odredbi št. 14086, je treba nadalje izvajati s politikami in postopki agencije, s katerimi se prenašajo v konkretne smernice za vsakodnevno delovanje. V zvezi s tem imajo ameriške obveščevalne agencije na podlagi Odredbe št. 14086 največ eno leto časa, da posodobijo svoje obstoječe politike in postopke (tj. do 7. oktobra 2023) in jih uskladijo z zahtevami navedene odredbe. Take posodobljene politike in postopke je treba pripraviti v posvetovanju s pravosodnim ministrom, CLPO ter Odborom za nadzor zasebnosti in državljskih svoboščin (PCLOB) ter jih v največji možni meri dati na voljo javnosti¹³³.
122. Po mnenju EOVP bi bilo dobrodošlo, da ne bi bil samo začetek veljavnosti, ampak tudi sprejem sklepa med drugim pogojen s sprejetjem posodobljenih politik in postopkov za izvajanje Odredbe št. 14086 s strani vseh obveščevalnih agencij ZDA. EOVP priporoča Komisiji, naj te posodobljene politike in postopke oceni ter mu posreduje svojo oceno.
123. Nazadnje, EOVP v zvezi s hrambo prenesenih podatkov, zbranih za namene nacionalne varnosti, ugotavlja, da Odredba št. 14086 zagotavlja, da se pravila, ki se uporabljajo za osebne podatke državljanov ZDA, uporabljajo tudi za osebne podatke nedržavljanov ZDA¹³⁴. Iz osnutka sklepa je razvidno, da so ta pravila določena v členu 309 *Intelligence Authorization Act For Fiscal Year 2015* (Zakon o pooblastilih za obveščevalno dejavnost za davčno leto 2015)¹³⁵, ki za vso nejavno telefonsko ali elektronsko komunikacijo, pridobljeno brez privolitve osebe, načeloma določa najdaljše obdobje hrambe pet let. EOVP glede tega priporoča, naj Komisija v sklepu zagotovi več jasnosti glede svoje ocene pravil o hrambi, ki se uporabljajo za osebne podatke državljanov ZDA.

3.2.2 Jamstvo B – dokazati je treba nujnost in sorazmernost v zvezi postavljenimi legitimnimi cilji

3.2.2.1 Horizontalni zaščitni ukrepi, ki jih zagotavlja nova Odredba št. 14086 – nujnost in sorazmernost

124. Namen nove Odredbe št. 14086, ki na splošno nadomešča PPD-28, je zagotoviti pravila za izboljšanje zaščitnih ukrepov za dejavnosti SIGINT v ZDA, ki jih bodo organi obveščevalne skupnosti nadalje izvajali v svojih notranjih politikah in postopkih.

¹³² Glej Odredbo št. 14086, člen 2(c)(i) (A) in (B).

¹³³ Glej Odredbo št. 14086, člen 2(c)(iv)(B) in (C).

¹³⁴ Osnutek sklepa, uvodna izjava 150.

¹³⁵ Osnutek sklepa, opomba 272.

125. Odredba št. 14086 uvaja dve novi zahtevi v skladu z zakonodajo ZDA, ki odražata zahteve, na katere je Sodišče opozorilo v svoji sodbi v zadevi *Schrems II*, in sicer, da se dejavnosti SIGINT izvajajo le toliko, kolikor je potrebno za izboljšanje zbiranja podatkov v okviru potrjenih prednostnih nalog obveščevalnih služb, ter samo v obsegu in na način, ki sta sorazmerna s potrjeno prednostno nalogo obveščevalne službe¹³⁶.
126. EOVP meni, da so bili ti elementi vključeni, da bi odražali načeli nujnosti in sorazmernosti, predvideni v pravu Unije ter v sodni praksi Sodišča in ESČP, katerih cilj je zagotoviti, da bi bila zbiranje in obdelava podatkov omejena na tisto, kar je nujno potrebno in sorazmerno.
127. EOVP glede tega opozarja na postopek, predviden za potrjevanje prednostnih nalog obveščevalnih služb, ter morebitno odstopanje (glej odstavek 116 in 117).
128. Poleg tega EOVP ugotavlja, da bo treba ti načeli nujnosti in sorazmernosti, določeni v Odredbi, uveljaviti in v enem letu izvesti v politikah in postopkih vsakega organa obveščevalne skupnosti¹³⁷.

3.2.2.2 Posebni zaščitni ukrepi za zbiranje obveščevalnih podatkov SIGINT

129. EOVP tudi opozarja, da Odredba št. 14086 določa omejitve glede ciljev, za katere se osebni podatki v okviru zbiranja obveščevalnih podatkov SIGINT lahko zbirajo in za katere se ne smejo¹³⁸.
130. EOVP pozdravlja dejstvo, da navedena odredba določa, da mora imeti ciljno zbiranje prednost pred množičnim zbiranjem¹³⁹. V Odredbi sta določena seznam 12 ciljev, za katere se lahko zbirajo obveščevalni podatki v okviru SIGINT, ki jih je treba dodatno utemeljiti v prednostnih nalogah obveščevalnih služb (glej odstavek 117), in seznam petih ciljev, za katere se dejavnosti zbiranja obveščevalnih podatkov v okviru SIGINT ne smejo izvajati¹⁴⁰. Te določbe so načeloma jamstvo za zagotovitev nujnosti zbiranja podatkov.
131. Vendar EOVP opozarja, da Odredba št. 14086 določa tudi možnost, da predsednik Združenih držav na seznam doda druge cilje (glej odstavek 114 in 115)¹⁴¹.

3.2.2.3 Posebni zaščitni ukrepi za množično zbiranje

132. Sodišče je v svoji sodbi v zadevi *Schrems I* poudarilo, da „varstvo temeljne pravice do spoštovanja zasebnega življenja na ravni Unije zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno“¹⁴², in odločilo, da „ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, pomeni poseg v bistvo temeljne pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine“.
133. Sodišče je v zadevi *Schrems II*¹⁴³ glede svoje analize množičnega zbiranja v povezavi z razlago Odredbe št. 12333 in PPD-28 ter zlasti točk od 183 do 185 poudarilo, kot je navedeno zgoraj, da ta možnost množičnega zbiranja, „ki v okviru programov nadzora, ki temeljijo na Odredbi št. 12333, omogoča dostopanje do podatkov v tranzitu proti Združenim državam, ne da bi bilo to dostopanje predmet

¹³⁶ Glej Odredbo št. 14086, člen 2(a)(ii), A in B.

¹³⁷ Glej Odredbo št. 14086, člen 2, (c), (iv), B.

¹³⁸ Glej Odredbo št. 14086, člen 2, (b), (i), (A), 1 do 12.

¹³⁹ Glej Odredbo št. 14086, člen 2, (c), (ii), A.

¹⁴⁰ Glej Odredbo št. 14086, člen 2, (b), (ii), (A), 1 do 5.

¹⁴¹ Glej Odredbo št. 14086, člen 2, (b), (i), (B).

¹⁴² Sodba Sodišča v zadevi *Schrems I*, točka 92.

¹⁴³ Glej sodbo Sodišča v zadevi *Schrems II*.

kakršnega koli sodnega nadzora, nikakor pa ne vsebuje dovolj jasne in natančne omejitve obsega takega množičnega zbiranja osebnih podatkov.“

134. EOVP zato ugotavlja, da Sodišče načeloma ni izključilo množičnega zbiranja, temveč je v zadevi *Schrems II* odločilo, da so potrebne dovolj jasne in natančne omejitve obsega množičnega zbiranja, da bi bilo to zakonito.
135. EOVP tudi priznava, da Odredba št. 14086 nadomešča PPD-28 ter hkrati določa nove zaščitne ukrepe in omejitve za zbiranje in uporabo podatkov, zbranih zunaj ZDA, saj omejitve FISA ali drugih bolj specifičnih zakonov ZDA ne veljajo.
136. EOVP v zvezi z množičnim zbiranjem podatkov ugotavlja, da Odredba št. 14086 določa, da je množično zbiranje še vedno dovoljeno. EOVP dejansko poudarja, da opredelitev množičnega zbiranja ostaja enaka kot v prejšnji PPD-28: „množično‘ zbrani obveščevalni podatki v okviru SIGINT pomenijo pooblaščen zbiranje velikih količin obveščevalnih podatkov v okviru SIGINT, ki se zaradi tehničnih ali operativnih razlogov pridobivajo brez uporabe diskriminant (na primer brez uporabe posebnih identifikatorjev ali izbirnih izrazov)“¹⁴⁴.
137. Sodišče od sodbe v zadevi *Schrems II* ni natančno opredelilo zaščitnih ukrepov, potrebnih za množično zbiranje. Vendar EOVP opozarja, da je ESČP izdalo pomembne sklepe v zvezi z množičnim zbiranjem in ustreznimi zaščitnimi ukrepi v tem okviru.
138. EOVP opozarja tudi, da množično zbiranje, ki omogoča zbiranje velikih količin podatkov brez diskriminant, pomeni večje tveganje za posameznike¹⁴⁵ kot ciljno zbiranje, zato so zanj potrebni dodatni zaščitni ukrepi.
139. EOVP tudi ugotavlja, da je Sodišče razvilo nadaljnjo sodno prakso v zvezi s hrambo prometnih in lokacijskih podatkov ter poznejšim dostopom do teh podatkov, ki jih hranijo telekomunikacijski operaterji, tudi za namene nacionalne varnosti, ki bi lahko bili deloma pomembni za sedanjo oceno množičnega zbiranja podatkov v okviru Odredbe št. 12333, čeprav jih ni mogoče šteti za neposredno upoštevne v tem okviru.

1) Omejitev namena

140. Odredba določa, da bi bilo treba za množično zbiranje najprej ugotoviti, da „informacij, potrebnih za izboljšanje zbiranja podatkov v okviru potrjenih prednostnih nalog obveščevalnih služb, ni mogoče pod razumnimi pogoji pridobiti s ciljnim zbiranjem“¹⁴⁶ in da „organ obveščevalne skupnosti uporablja razumne metode in tehnične ukrepe za omejitev zbranih podatke le na tisto, kar je potrebno za pospeševanje potrjene prednostne naloge obveščevalne službe“¹⁴⁷. Poleg teh zaščitnih ukrepov EOVP tudi priznava, da se množično zbrani podatki uporabljajo za doseganje enega ali več od šestih navedenih ciljev¹⁴⁸. EOVP nadalje poudarja, da so ti cilji sicer podrobnejši od tistih, ki so bili določeni v

¹⁴⁴ Glej Odredbo št. 14086, člen 4(b).

¹⁴⁵ Glej na primer sodbo ESČP (veliki senat) v zadevi *Big Brother Watch in drugi proti Združenemu kraljestvu*, 25. maj 2021 (v nadaljevanju: sodba ESČP v zadevi *Big Brother Watch*), uvodna izjava 363, kjer Sodišče navaja, da „ni prepričano, da je pridobivanje zadevnih komunikacijskih podatkov z množičnim prestrezanjem nujno manj vsiljivo kot pridobivanje vsebine“.

¹⁴⁶ Odredba št. 14086, člen 2(c)(ii)(A).

¹⁴⁷ Odredba št. 14086, člen 2(c)(ii)(A).

¹⁴⁸ Odredba št. 14086, člen 2(c)(ii)(B).

prejšnji PPD-28, ki jo je na splošno nadomestila Odredba št. 14086, toda obseg teh možnosti zbiranja je lahko še vedno širok, tj. zajema velike količine podatkov.

141. EOVP glede tega tudi opozarja, da Odredba št. 14086 omogoča, da predsednik Združenih držav na seznam doda druge cilje (glej odstavek 115)¹⁴⁹.

2) Predhodna neodvisna odobritev

142. EOVP poudarja, da ESČP daje velik pomen predhodni neodvisni odobritvi v okviru množičnega zbiranja podatkov za namene nacionalne varnosti. Sodišče je namreč zlasti razsodilo, „da Sodišče meni, da je treba za postopek uporabiti celovite zaščitne ukrepe, da bi se zmanjšalo tveganje zlorabe pooblastil za množično prestrežanje, kar pomeni, da je treba na nacionalni ravni na vsaki stopnji oceniti nujnost in sorazmernost sprejetih ukrepov; da bi morala biti za množično prestrežanje potrebna neodvisna odobritev na samem začetku, ko se opredelita cilj in obseg operacije, in da bi morala biti operacija predmet nadzora in neodvisnega naknadnega pregleda. Po mnenju Sodišča so to osnovni zaščitni ukrepi, ki bodo temelj vsake ureditve množičnega prestrežanja, skladne s členom 8.“¹⁵⁰
143. EOVP opozarja tudi na naslednjo točko te sodbe velikega senata, kjer je ESČP nadalje poudarilo, da se „strinja s senatom, da čeprav je sodna odobritev ‚pomemben zaščitni ukrep proti samovoljnemu ravnanju‘, ni ‚nujna zahteva‘ (glej točke 318–320 sodbe senata). Kljub temu bi moral množično prestrežanje odobriti neodvisen organ; torej organ, ki je neodvisen od izvršilne veje oblasti“¹⁵¹.
144. EOVP glede tega ugotavlja, da Odredba ne določa take neodvisne predhodne odobritve za množično zbiranje in da tudi ni predvideno v Odredbi št. 12333 (glej oddelek v nadaljevanju o Odredbi št. 12333).

3) Pravila hrambe

145. EOVP opozarja, da so pravila o trajanju zbiranja in hrambe podatkov še en pomemben sklop zaščitnih ukrepov. Glede tega je ESČP poudarilo, da „bi morala nacionalna zakonodaja določati omejitve trajanja prestrežanja, postopek, ki ga je treba upoštevati pri pregledu, uporabi in hrambi pridobljenih podatkov, varnostne ukrepe, ki jih je treba sprejeti pri sporočanju podatkov drugim osebam, ter okoliščine, v katerih se prestreženi podatki lahko izbrišejo ali uničijo ali jih je treba izbrisati in uničiti“¹⁵², saj so ti zaščitni ukrepi „enako pomembni za množično prestrežanje“¹⁵³.
146. EOVP glede tega meni, da Odredba določa pravila o hrambi podatkov, ki se nanašajo na osebne podatke, zbrane v okviru SIGINT, tudi množično¹⁵⁴. EOVP ugotavlja, da v skladu s členom 2(c)(iii)(A) Odredbe št. 14086 vsak organ obveščevalne skupnosti, ki obdeluje osebne podatke, zbrane v okviru SIGINT, vzpostavi in uporablja politike ter postopke za zmanjšanje razširjanja in hrambe osebnih podatkov, zbranih v okviru SIGINT. Vendar ta pravila ne določajo specifičnega obdobja hrambe, temveč se na splošno nanašajo na enaka veljavna pravila za hrambo podatkov v zvezi z državljani ZDA in na primere, ko ni bila sprejeta dokončna odločitev o hrambi. EOVP je zato zaskrbljen, da v navedeni odredbi ta obdobja hrambe niso jasno opredeljena v zvezi z množično zbranimi podatki, kot so v zvezi s ciljnim zbiranjem (glej odstavek 122). Komisijo poziva, naj sporoči oceno o nujnosti in sorazmernosti obdobja hrambe, ki se uporabljajo za državljane ZDA, ter informacije, ki so na voljo o obdobjih hrambe

¹⁴⁹ Glej Odredbo št. 14086, člen 2(c)(ii)(C).

¹⁵⁰ Glej sodbo ESČP v za deva *Big Brother Watch*, točka 350.

¹⁵¹ Glej sodbo ESČP v za deva *Big Brother Watch*, točka 351.

¹⁵² Glej sodbo ESČP v za deva *Big Brother Watch*, točka 348.

¹⁵³ Glej sodbo ESČP v za deva *Big Brother Watch*, točka 348.

¹⁵⁴ Glej Odredbo št. 14086, člen 2, (c), (iii), A, (2)(a)–(c).

v praksi, ko v skladu z zakonodajo ZDA ni bila sprejeta dokončna odločitev o hrambi, saj sedanji osnutek sklepa na to splošno pravilo opozarja le v enem samem kratkem odstavku¹⁵⁵ in opombi¹⁵⁶, na podlagi katerih ni mogoče določiti, ali so ta obdobja hrambe nujno potrebna in sorazmerna. Ker je to, kot je poudarilo ESČP, ključni zaščitni ukrep, ki posameznikom, na katere se nanašajo osebni podatki, omogoča, da uveljavljajo svoje pravice, ko se njihovi podatki zbirajo s posebej vsiljivim ukrepom, EOVP poziva Evropsko komisijo, naj zagotovi dodatna pojasnila v zvezi z različnimi obdobji hrambe v praksi.

4) Zaščitni ukrepi glede „razširjanja“

147. EOVP tudi opozarja, da je ESČP za zagotovitev dejanskosti nujnosti in sorazmernosti ter načela omejitve namena priznalo tudi pomen pravil, ki jih določa zakon o nadaljnjem razširjanju zbranih podatkov, tudi v okviru množičnega zbiranja¹⁵⁷.
148. Člen 2(c)(iii)(A)(1)(c) Odredbe št. 14086 določa, da se lahko informacije o nedržavljanih ZDA, zbrane v okviru dejavnosti SIGINT, razširjajo samo, če pooblaščen in ustrezno usposobljeni posameznik razumno domneva, da bodo osebni podatki ustrezno varovani in da mora biti uporabnik z njimi seznanjen.
149. EOVP ob upoštevanju navedenega razume, da določbe o razširjanju iz Odredbe št. 14086 ne predvidevajo niti izrecne prepovedi razširjanja za druge namene, ki niso nameni nacionalne varnosti, kadar gre za razširjanje podatkov pristojnim organom ZDA¹⁵⁸. EOVP poziva Komisijo, naj dodatno pojasni veljavna pravila in zaščitne ukrepe v tem primeru.
150. EOVP je zato zaskrbljen, da bi se lahko podatki, ki so jih pridobili pristojni organi obveščevalne skupnosti, nato razširjali pristojnim organom ZDA za namene boja proti kriminalu, vključno s hudimi kaznivimi dejanji, v okviru kazenskih preiskav, s čimer bi se organom kazenskega pregona brez kakršnih koli posebnih dodatnih omejitev omogočilo pridobivanje podatkov, ki bi jih bilo prepovedano zbirati neposredno, in poziva Komisijo, naj to točko nadalje oceni.
151. EOVP opozarja na svoje mnenje, da je treba varstvo podatkov ohraniti tudi v posebnem okviru nadaljnjih prenosov (razširjanje podatkov uporabnikom zunaj vlade Združenih držav, vključno s tujimi vladami ali mednarodnimi organizacijami¹⁵⁹), vključno s področjem nacionalne varnosti¹⁶⁰.
152. Odredba glede tega določa nekatere zaščitne ukrepe, in sicer zahtevo, da se pred razširjanjem podatkov ustrezno upošteva namen razširjanja – čeprav brez izrecne zahteve, da mora biti namen razširjanja tudi zaščita nacionalne varnosti – ter narava in obseg osebnih podatkov, ki se razširjajo, in morebiten škodljiv vpliv na zadevno osebo ali osebe.
153. Čeprav EOVP priznava, da nekateri od teh zaščitnih ukrepov, zlasti da je treba upoštevati „morebiten škodljiv vpliv“¹⁶¹ na zadevne posameznike, na katere se nanašajo osebni podatki, odražajo nekatere zahteve ESČP, poudarja tudi, da sodišče v Strasbourgu poleg tega določa pravno zavezujočo obveznost, „da se analizira in ugotovi, ali tuji uporabniki obveščevalnih podatkov zagotavljajo sprejemljivo

¹⁵⁵ Glej osnutek sklepa, odstavek 150.

¹⁵⁶ Glej osnutek sklepa, opomba 271.

¹⁵⁷ Glej sodbo ESČP v za deva *Big Brother Watch*, točka 348.

¹⁵⁸ Glej Odredbo št. 14086, člen 2(c)(iii)(A)(1).

¹⁵⁹ Glej Odredbo št. 14086, člen 2(c)(iii)(A)(1), zlasti točko (d).

¹⁶⁰ Glej na primer Mnenje št. 14/2021 EOVP o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu posameznikov pri obdelavi osebnih podatkov v Združenem kraljestvu. Sprejeto 13. aprila 2021, oddelka 4.3.2.1 in 4.3.2.2.

¹⁶¹ Glej Odredbo št. 14086, člen 2(c)(iii)(A)(1), (d).

minimalno raven zaščitnih ukrepov“¹⁶², česar EOVP ne najde izrecno navedenega v določbah Odredbe v zvezi z razširjanjem podatkov tujim uporabnikom. EOVP zato poziva Komisijo, naj ta element dodatno oceni.

154. EOVP tudi ugotavlja, da Evropska komisija v okviru svoje ocene ustreznosti ni preučila obstoja mednarodnih sporazumov, sklenjenih s tretjimi državami ali mednarodnimi organizacijami, ki morda vsebujejo posebne določbe za mednarodni prenos osebnih podatkov s strani obveščevalnih služb v tretje države. EOVP meni, da bo sklenitev dvostranskih ali večstranskih sporazumov s tretjimi državami za namene sodelovanja obveščevalnih služb verjetno vplivala na ocenjeni pravni okvir varstva podatkov.
155. EOVP zato poziva Evropsko komisijo, naj pojasni, ali taki sporazumi obstajajo in pod katerimi pogoji se lahko sklenejo, ter oceni, ali lahko njihove določbe vplivajo na raven varstva, ki se zagotavlja za osebne podatke, prenesene iz EGP, z zakonodajnim okvirom in praksami v zvezi z nadaljnjimi prenosi za namene nacionalne varnosti.

5) Začasno množično zbiranje za podporo začetni tehnični fazi ciljnega zbiranja

156. EOVP opozarja, da so se razprave v okviru zadnjega skupnega pregleda zasebnostnega ščita osredinjale predvsem na razlago in uporabo dodatne podlage (situacija/scenarij) za množično zbiranje, predvideno v prvem stavku opombe 5 člena 2 PPD 28, v katerem je določeno, da „se omejitve iz tega člena ne uporabljajo za obveščevalne podatke v okviru SIGINT, pridobljene začasno za olajšanje ciljnega zbiranja“. Organi ZDA so takrat pojasnile pomen „obveščevalnih podatkov v okviru SIGINT, pridobljenih začasno za olajšanje ciljnega zbiranja“. EOVP je na podlagi teh razprav razumel, da navedena opomba pomeni, da se podatki lahko zbirajo množično – in ne glede na predvidenih šest namenov –, če se zbirajo začasno z namenom določitve identifikatorja za opredeljen cilj. To bi bila torej dodatna podlaga za množično zbiranje podatkov in v tem primeru bi še vedno veljala le splošna načela iz člena 1 PPD-28. Kot je navedeno zgoraj, je Sodišče v sodbi v zadevi *Schrems II* menilo, da Odredba št. 12333 in PPD-28 v zvezi z množičnim zbiranjem skupaj „ne vsebuje[ta] dovolj jasne in natančne omejitve obsega takega množičnega zbiranja osebnih podatkov“¹⁶³.
157. EOVP ugotavlja, da je v Odredbi št. 14086 še vedno določeno odstopanje, ki dovoljuje tako množično zbiranje¹⁶⁴, vendar pozdravlja dejstvo, da se je to odstopanje omejilo v primerjavi s PPD-28 in da so zagotovljeni dodatni zaščitni ukrepi v skladu z Odredbo št. 14086.
158. EOVP razume, da nova Odredba št. 14086 zagotavlja zaščitne ukrepe, ki se še naprej uporabljajo v okviru te vrste začasnega tehničnega množičnega zbiranja, zlasti splošna načela nujnosti in sorazmernosti v zvezi s potrjeno prednostno nalogo obveščevalne službe, kadar se podatki pridobijo brez diskriminant pred ciljnimi zbiranjem (člen 2(a) in (b), člen 2(c)(i) Odredbe št. 14086). EOVP prav tako razume, da se za tako množično zbiranje, ki podpira naknadno ciljno zbiranje obveščevalnih podatkov v okviru SIGINT, uporabljajo tudi dodatni zaščitni ukrepi, določeni v podčlenu (2)(c)(iii) in naslednjih¹⁶⁵.

¹⁶² Glej sodbo ESČP (veliki senat) v zadevi *Centrum För Rättvisa proti Švedski*, 25. maj 2021, točka 326.

¹⁶³ Sodba Sodišča v zadevi *Schrems II*, točka 183.

¹⁶⁴ Glej Odredbo št. 14086, člen 2(c), (ii), (D), in osnutek sklepa, opomba 226.

¹⁶⁵ Glej prejšnje oddelke za dodatne elemente o teh določbah.

159. Vendar EOVP tudi opozarja – glej odstavek 117 zgoraj –, da opredelitev „potrjene prednostne naloge obveščevalne službe“ določa postopek odstopanja, v katerega CLPO urada direktorja nacionalne obveščevalne službe ne bi bil vključen.
160. Vendar EOVP kljub temu ugotavlja, da zaščitni ukrepi iz podčlena v zvezi z množičnim zbiranjem ne veljajo za začasno množično zbiranje, ki se uporablja za podporo začetni tehnični fazi dejavnosti ciljnega zbiranja obveščevalnih podatkov v okviru SIGINT, kot je opisano v členu 2(c)(ii)(D) Odredbe št. 14086, kar predvsem pomeni, da se lahko množično zbrani podatki v tem okviru uporabijo za namene, ki niso navedeni v podčlenu 2(c)(ii). EOVP želi pozdraviti pojasnila v osnutku sklepa o namenu, za katerega se lahko uporabljajo množično zbrani podatki v tem okviru, ter o uporabi omejitev iz podčlena 2(c)(i) za zbiranje obveščevalnih podatkov v okviru SIGINT na splošno (namreč samo za tam navedene legitimne cilje) v okviru začasnega množičnega zbiranja.
161. Na koncu EOVP tudi poudarja, da navedeno odstopanje za začasno množično zbiranje glede na ciljno zbiranje in preostale zaščitne ukrepe, ki jih je treba uporabiti, še vedno ni jasno, zlasti ne, kateri zaščitni ukrepi iz Odredbe št. 14086 bi se uporabljali v posameznih fazah (množično zbiranje, nadaljnje ciljno zbiranje), in poziva Komisijo, naj nadalje oceni te elemente ter te vidike presodi tudi v praksi v prihodnjih skupnih pregledih.
162. Poleg tega tudi obžaluje, da čeprav je pojem „začasno“ v Odredbi nekoliko podrobneje opredeljen kot v PPD-28, po njegovem mnenju še vedno pomeni, da se lahko množično zbiranje nadaljuje, če ciljni subjekt ni identificiran. Glede tega opozarja, da so potrebna jasna in natančna pravila, ter tukaj tudi poudarja, da so ta pravila ključni zaščitni ukrep za posameznike, na katere se nanašajo osebni podatki.
163. Skratka, EOVP je v zvezi z zaščitnimi ukrepi, ki se uporabljajo za množično zbiranje, še vedno zaskrbljen, da je kljub dodatnim zaščitnim ukrepom iz Odredbe št. 14086 še vedno mogoče množično zbiranje podatkov, tj. brez diskriminant, brez ključnih zaščitnih ukrepov, kot je predhodnaodobritev za zbiranje teh podatkov – vključno v primeru odstopanja začasnega tehničnega množičnega zbiranja –, tudi ob upoštevanju potrebe po nadaljnjih pojasnilih in izraženih pomislekih glede stroge omejitve namena za naknadni dostop do podatkov, jasnih in strogih pravil o hrambi podatkov ter strožjih zaščitnih ukrepov v zvezi z razširjanjem množično zbranih podatkov, tudi v okviru nadaljnjih prenosov.
164. EOVP na splošno poudarja, da navedena odločitev ESČP vnovič kaže na pomen celovitega nadzora neodvisnih nadzornih organov. Poudarja, da je neodvisni nadzor v vseh fazah postopka vladnega dostopa za namene nacionalne varnosti pomemben zaščitni ukrep pred samovoljnimi nadzornimi ukrepi in torej pomemben za oceno ustrezne ravni varstva podatkov. Jamstvo neodvisnosti nadzornih organov v smislu člena 8(3) Listine EU o temeljnih pravicah je namenjeno zagotavljanju učinkovitega in zanesljivega spremljanja skladnosti s pravili o varstvu posameznikov pri obdelavi osebnih podatkov. To velja zlasti v okoliščinah, ko posameznik zaradi narave tajnega nadzora ne more zahtevati pregleda ali neposredno sodelovati v morebitnem postopku pregleda pred izvršitvijo nadzornega ukrepa ali med njegovim izvrševanjem.
165. EOVP opozarja, da je po njegovem mnenju ocena ustreznosti odvisna od vseh okoliščin primera, zlasti od učinkovitosti naknadnega nadzora in pravnih sredstev, določenih v pravnem okviru.

3.2.2.4 Pravni okvir, ki ureja posebno zbiranje s strani organov obveščevalne skupnosti za namene nacionalne varnosti na ozemlju ZDA in zunaj njih

166. Sodišče je v sodbi v zadevi *Schrems II* v zvezi s členom 702 FISA poudarilo, da to besedilo „nikakor ne vsebuje omejitev v njem vsebovanega pooblastila za izvajanje programov nadzora za pridobivanje tujih obveščevalnih podatkov in tudi ne zaščitnih ukrepov za neameriške osebe, na katere se lahko ti

programi nanašajo¹⁶⁶. Sodišče je zato menilo, da „[v] teh okoliščinah [...] ta člen ne more zagotoviti ravni varstva, ki je v bistvu enakovredna ravni varstva, zagotovljeni z Listino [...], v skladu s katero morajo biti v aktu, ki je pravna podlaga za poseg v temeljne pravice, zaradi spoštovanja načela sorazmernosti določene omejitve izvrševanja zadevne pravice ter jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter minimalne zahteve“¹⁶⁷.

167. V zvezi z Odredbo št. 12333 je Sodišče navedlo, da „ne dodeljuje pravic, na katere bi se bilo mogoče pred sodišči sklicevati zoper ameriške organe“¹⁶⁸ in na podlagi analize pogojev, pod katerimi se lahko izvaja množično zbiranje po navedeni odredbi v povezavi s PPD-28, ugotovilo, da „[Ta možnost, ki] v okviru programov nadzora, ki temeljijo na Odredbi št. 12333, omogoča dostopanje do podatkov v tranzitu proti Združenim državam, ne da bi bilo to dostopanje predmet kakršnega koli sodnega nadzora, pa nikakor ne vsebuje dovolj jasne in natančne omejitve obsega takega množičnega zbiranja osebnih podatkov“¹⁶⁹.
168. Odredba št. 14086 v zvezi s posebnimi ureditvami zbiranja podatkov zdaj določa nova pravila.

3.2.2.4.1 Zbiranje podatkov za namene nacionalne varnosti v skladu s členom 702

169. EOVP opozarja, da je bilo v zadnjem poročilu PCLOB izraženo, da so dobrodošle ugotovitve o členu 702 FISA¹⁷⁰, da „imajo ‚v praksi‘ tudi nedržavljeni ZDA koristi od omejitev dostopa in hrambe, ki se v postopkih različnih agencij za zmanjšanje količine podatkov in/ali postopkih izbire cilja zahtevajo zaradi stroškov, pri čemer težave pri identifikaciji in izbrisu podatkov državljanov ZDA za veliko količino podatkov pomenijo, da se celoten sklop podatkov običajno obravnava v skladu z višjimi podatkovnimi standardi ZDA“.
170. Glede na te ugotovitve „program ne deluje v smislu množičnega zbiranja obveščevalnih podatkov“. Statistični poročili o preglednosti za leti 2014 in 2021, ki ju je izdal urad direktorja nacionalne obveščevalne službe, potrjujeta to ugotovitev. Poleg tega se, kot je navedeno v poročilu PCLOB, za usmerjanje nadzora uporabljajo „določeni izbirniki“, kot je e-naslov ali telefonska številka.
171. Vendar EOVP tudi opozarja, da je bilo sočasno v okviru člena 702 med zadnjim pregledom zasebnostnega ščita pojasnjeno, da se lahko „oseba“, ki se opredeli kot ciljna oseba, nanaša na več posameznikov, ki uporabljajo isti identifikator, če nobena od teh oseb ni državljan ZDA in vse izpolnjujejo veljavna merila za ciljne osebe. Poleg tega opozarja, da se je med tretjim letnim skupnim pregledom zasebnostnega ščita leta 2019 zahtevalo dodatno pojasnilo v okviru programa UPSTREAM, da se izključi množičen in neselektiven dostop do osebnih podatkov nedržavljanov ZDA¹⁷¹.
172. Nadalje opozarja, da dejstvo, da se zbiranje v skladu s členom 702 FISA upravičuje s tem, da „je pomemben namen pridobivanja pridobiti tuje obveščevalne podatke“, še vedno dopušča določeno negotovost glede omejitve namena in nujnosti. Vendar ugotavlja, da se v skladu s členom 2(a)(A) in (B) Odredbe št. 14086 dejavnosti SIGINT izvajajo samo, če se ugotovi, da so potrebne za izboljšanje potrjene prednostne naloge, in samo v obsegu in na način, ki sta sorazmerna s tako prednostno nalogo, ter da morajo biti čim bolj prilagojene za izboljšanje potrjene prednostne naloge, pri čemer se ustrezno upoštevajo ustrezni dejavniki, kot sta vsiljivost zbiranja in občutljivost podatkov, ter da ne smejo

¹⁶⁶ Glej sodbo Sodišča v za deva *Schrems II*, točka 180.

¹⁶⁷ Glej sodbo Sodišča v za deva *Schrems II*, točka 180.

¹⁶⁸ Glej sodbo Sodišča v za deva *Schrems II*, točka 182.

¹⁶⁹ Glej sodbo Sodišča v za deva *Schrems II*, točka 183.

¹⁷⁰ Glej Poročilo PCLOB o programu nadzora, ki se izvaja v skladu s členom 702 FISA, str. 100.

¹⁷¹ Glej tretji letni skupni pregled, stran 17, odstavek 83.

nesorazmerno vplivati na zasebnost in državljanske svoboščine. Pričakuje še nadaljnja pojasnila o tem, kako se bo to konkretno izvajalo in uveljavilo, tudi v okviru uporabe člena 702 FISA.

173. Ker ni imel neposrednega dostopa do teh informacij, je v zvezi s tem pozval k neodvisni oceni nujnosti in sorazmernosti opredelitve „ciljnih oseb“ in pojma „tuji obveščevalni podatki“ v skladu s členom 702 FISA po njegovi prenovitvi (tudi v okviru programa UPSTREAM). EOVP meni, da je njegov prejšnji poziv k nadaljnji neodvisni oceni postopka uporabe izbirnikov v posebnih primerih („določanje izbirnikov“) in k dodatnim pojasnilom v okviru programa UPSTREAM relevanten. Zato ob upoštevanju nove Odredbe št. 14086 poziva k dodatnim informacijam, da bi ocenil in spremljal tudi, kako in koliko se bosta novo uvedeni načeli nujnosti in sorazmernosti v tem okviru uporabljali v praksi, ter pričakuje, da se bo to ocenilo tudi v okviru prihodnjih skupnih pregledov.
174. EOVP pozdravlja dejstvo, da se je popolnoma delujoč Odbor za nadzor zasebnosti in državljskih svoboščin (PCLOB) kot neodvisna agencija za nadzor odločil izvesti „projekt nadzora za preučitev programa nadzora, ki ga izvaja izvršilna veja oblasti v skladu s členom 702 FISA, v pričakovanju datuma poteka veljavnosti člena 702 decembra 2023 ter bližajoče se javne in kongresne obravnave njegove ponovne odobritve¹⁷². Prav tako pozdravlja dejstvo, da „pregled zajema izbrana prednostna področja preiskave, vključno z, vendar ne nujno omejena na poizvedbe državljanov ZDA o informacijah, zbranih v skladu s členom 702, in zbiranje podatkov v okviru programa UPSTREAM v skladu s členom 702“¹⁷³, ter „vključuje tudi pregled pretekle in predvidene vrednosti in učinkovitosti programa ter ustreznost obstoječih ukrepov za zaščito zasebnosti in državljskih svoboščin“¹⁷⁴. Zato poudarja, da bi bil za ustrezno in celovito oceno ukrepov za zaščito zasebnosti, zagotovljenih in uporabljenih v okviru tega programa nadzora, potreben dostop do ugotovitev PCLOB o členu 702 v navedenem poročilu.
175. EOVP ob upoštevanju nove Odredbe št. 14086 poziva tudi k dodatnim informacijam, da bi ocenil in spremljal tudi, kako in koliko se bodo v tem okviru v praksi uporabljali novo uvedeni načeli nujnosti in sorazmernosti ter drugi zaščitni ukrepi, določeni v tem besedilu.

3.2.2.4.2 Zbiranje podatkov za namene nacionalne varnosti v skladu z Odredbo št. 12333

176. Kot priznava Sodišče v svoji sodbi v zadevi *Schrems II*, analiza zakonov tretje države, katerih ustreznost se obravnava, ne bi smela biti omejena na zakone in prakse, ki omogočajo nadzor znotraj fizičnih meja te države, temveč bi morala vključevati tudi analizo pravne podlage v pravu te tretje države, ki ji dovoljuje izvajanje nadzora zunaj njenega ozemlja, kar zadeva podatke EU. Potrebne omejitve vladnega dostopa do podatkov bi bilo treba razširiti na osebne podatke „v tranzitu“ v državo, ki ji je priznana ustreznost.
177. EOVP pozdravlja splošno javno poročilo, ki ga je PCLOB izdal o Odredbi št. 12333 in je bilo objavljeno aprila 2021, vendar ugotavlja, da je to poročilo še vedno splošno, saj je večina ugotovitev tajnih.
178. Zaradi negotovosti in nejasnosti v zvezi s tem, kako se je uporabljala Odredba št. 12333, in glede na pomen pojasnitve, kako se bo uporabljala v luči nove Odredbe št. 14086, v tem okviru poudarja pomen pričakovanih poročil PCLOB o navedenem besedilu¹⁷⁵. Vendar razume, da bo njihova vsebina verjetno

¹⁷² Glej [NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT \(FISA\) \(OBVESTILO O PROJEKTU NADZORA PCLOB ZA PREUČITEV ČLENA 702 ZAKONA O NADZORU TUJIH OBVEŠČEVALNIH PODATKOV \(FISA\)\)](#).

¹⁷³ Glej zgoraj.

¹⁷⁴ Glej zgoraj.

¹⁷⁵ Splošno poročilo o Odredbi št. 12333 je večinoma še vedno tajno – objavljena je bila le kratka javna različica, prav tako je le delno preklicana tajnost poročila in priporočil o protiterorističnih dejavnostih CIE, ki se izvajajo v skladu z Odredbo št. 12333.

večinoma ostala tajna, tako da niti javnosti niti EOVP ne bodo na voljo nobene dodatne informacije o konkretnem izvajanju Odredbe št. 12333 ter o njeni nujnosti in sorazmernosti.

179. Zato želi EOVP posebej pozdraviti dejstvo, da poročilo PCLOB o uporabi Odredbe št. 14086 ni tajno, temveč bo v celoti dostopno, ko bo dokončano, vključno z deli z oceno, kako se bodo zaščitni ukrepi iz Odredbe št. 14086 uporabljali za zbiranje podatkov v okviru Odredbe št. 12333. EOVP tudi poziva Komisijo, naj tej točki v okviru prihodnjih skupnih pregledov nameni posebno pozornost.
180. Na splošno želi EOVP v zvezi z različnimi pravnimi instrumenti, ki zagotavljajo možnost zbiranja in nadaljnjega dostopa do podatkov ter njihove obdelave za obveščevalne agencije ZDA v pravnem okviru ZDA, pozdraviti pojasnila o njihovem medsebojnem vplivu z novo Odredbo št. 14086 in pričakuje zagotovila, da se bodo prejšnji pomisleki, ki jih je v zvezi s tem izrazil v svojih prejšnjih mnenjih, odpravili s sprejetjem navedenih novih zaščitnih ukrepov.
181. EOVP tudi poziva Komisijo, naj bo v okviru prihodnjih skupnih pregledov posebej pozorna na te vidike.

3.2.2.4.3 Poročilo PCLOB

182. EOVP pozdravlja dejstvo, da Odredba št. 14086 določa tudi zahtevo, da PCLOB pripravi poročilo o izvajanju Odredbe. Poleg tega poudarja, da bi moralo to poročilo vključevati oceno posebne možnosti, ki jo zagotavlja Odredba za zbiranje podatkov za namene, navedene za ciljno zbiranje, pa tudi množično zbiranje, tudi iz tehničnih razlogov, da bi bolje razumeli ključne izraze iz Odredbe št. 14086 ter njihovo razumevanje in uporabo v praksi v različnih programih nadzora. To poročilo bi bilo potrebno tudi za oceno, kako se bo Odredba izvajala v notranjih postopkih in politikah organov obveščevalnih skupnosti.

3.2.3 Jamstvo C – Nadzor

3.2.3.1 Uvod

183. Ameriške obveščevalne dejavnosti so predmet večplastnega postopka nadzora. Nadzorno strukturo v ZDA lahko razdelimo na notranji in zunanji nadzor. Vsi organi obveščevalne skupnosti imajo uradnike za nadzor in preverjanje skladnosti, ki redno nadzorujejo dejavnosti SIGINT, vključno z uradniki na področju varstva zasebnosti in državljskih svoboščin ter generalnimi inšpektorji. Poleg tega obstajajo zunanji nadzorni organi, kot sta Odbor za nadzor zasebnosti in državljskih svoboščin (PCLOB) ter obveščevalni nadzorni odbor.
184. EOVP opozarja, da do posega pride v času zbiranja podatkov, pa tudi v času, ko javni organ dostopa do podatkov za nadaljnjo obdelavo. Evropsko sodišče za človekove pravice je že večkrat navedlo, da je treba za vsak poseg v pravico do zasebnosti in varstva podatkov uporabljati učinkovit, neodvisen in nepristranski nadzorni sistem, ki ga mora zagotoviti bodisi sodnik bodisi drug neodvisni organ¹⁷⁶ (na primer upravni organ ali parlamentarno telo).
185. ESČP je izrazilo naklonjenost temu, da je za zagotavljanje nadzora odgovoren sodnik, vendar ni izključilo možnosti, da je lahko odgovoren tudi drug organ, „če je dovolj neodvisen od izvršilne veje oblasti“¹⁷⁷

¹⁷⁶ Sodba ESČP v zadevi *Klass in drugi proti Nemčiji*, 6. september 1978 (v nadaljevanju: sodba ESČP v zadevi *Klass*), točki 17 in 51.

¹⁷⁷ Sodba ESČP v zadevi *Zakharov*, točka 258; ESČP, *lordachi in drugi proti Moldaviji*, 10. februar 2009, točki 40 in 51; ESČP, *Dumitru Popescu proti Romuniji*, 26. april 2007, točke 70–73.

in „od organov, ki izvajajo nadzor ter ima zadostna pooblastila in pristojnosti za izvajanje učinkovitega in stalnega nadzora“¹⁷⁸.

186. ESČP je dodalo, da je treba pri ocenjevanju neodvisnosti upoštevati „način imenovanja in pravni status članov nadzornega organa“¹⁷⁹.
187. ESČP je tudi navedlo, da bo preučilo, ali so dejavnosti nadzornega organa odprte za javni nadzor. To bi lahko na primer dosegli tako, da bi se poročila o nadzoru vsako leto predložila vladi, javna poročila pa parlamentu, ki bi o njih razpravljala¹⁸⁰.
188. Sodišče je neodvisni nadzor nad izvajanjem nadzornih ukrepov upoštevalo tudi v sodbi v zadevi *Schrems II*, saj „[...] je namen nadzora, ki ga izvaja FISC, preveriti, ali ti programi nadzora ustrezajo cilju pridobivanja tujih obveščevalnih podatkov, ne nanaša pa se na ‚ustreznost ciljnega osredotočanja na posameznike za pridobivanje tujih obveščevalnih podatkov‘.“¹⁸¹

3.2.3.2 Notranji nadzor

3.2.3.2.1 Generalni inšpektorji

189. EOVP priznava, da imajo generalni inšpektorji številna pooblastila, potrebna za spremljanje obveščevalnih dejavnosti. Zlasti imajo dostop do vseh informacij, potrebnih za oceno splošne skladnosti dela agencij z zakonodajo, med drugim z zakoni, povezanimi z zasebnostjo in varstvom podatkov, ter lahko v zvezi s svojo preiskavo izdajo sodne pozive in zaprisežejo katero koli osebo.
190. EOVP na podlagi zgoraj navedenega meni, da imajo generalni inšpektorji na splošno obsežna preiskovalna pooblastila. Vendar nimajo nobenih zavezujočih pooblastil za odpravo kršitev in izdajajo le nezavezujoča priporočila¹⁸².
191. EOVP priznava, da generalnim inšpektorjem načeloma nič ne preprečuje ali prepoveduje, da bi začeli, izvedli ali zaključili kakršno koli revizijo ali preiskavo ali da bi med katero koli revizijo ali preiskavo izdali kakršen koli sodni poziv.¹⁸³ V zvezi s tem ugotavlja, da je za generalne inšpektorje pristojen ustrezni vodja oddelka, ki jih tudi usmerja in nadzoruje ter jim lahko prepove dostop do informacij, izvajanje preiskav in med drugim izdajo kakršnih koli sodnih pozivov, če presodi, da je taka prepoved nujna za varovanje nacionalnih interesov. Vendar mora vodja oddelka o izvajanju navedenega pooblastila obvestiti pristojne odbore ameriškega kongresa¹⁸⁴.
192. EOVP ugotavlja, da lahko generalne inšpektorje odstavi le predsednik ZDA, ki mora kongres obvestiti o razlogih za tako odstavitev.

¹⁷⁸ Sodba ESČP v zadevi *Klass*, točka 56.

¹⁷⁹ Sodba ESČP v zadevi *Zakharov*, točka 278.

¹⁸⁰ Sodba ESČP v zadevi *Zakharov*, točka 283; ESČP, *L. proti Norveški*, 9. junij 1990; ESČP, *Kennedy proti Združenemu kraljestvu*, 18. maj 2010, točka 166.

¹⁸¹ Sodba Sodišča v zadevi *Schrems II*, točka 179.

¹⁸² Osnutek sklepa, uvodna izjava 105.

¹⁸³ *Inspector General Act of 1978* (Zakon o generalnih inšpektorjih iz leta 1978), člen 3(a).

¹⁸⁴ Glej Zakon o generalnih inšpektorjih iz leta 1978, člen 8 (za ministrstvo za obrambo); člen 8E (za pravosodno ministrstvo), člen 8G(d)(2)(A), (B) (za Nacionalno varnostno agencijo); člen 403q(b) naslova 50 zakonodajne zbirke ZDA (za CIO); Zakon o pooblastilih za obveščevalno dejavnost za davčno leto 2010, člen 405(f) (za obveščevalno skupnost).

193. EOVP ugotavlja, da se mehanizem notranjega nadzora od izdaje mnenj WP29 in EOVP ni znatno spremenil. Zato v skladu z Mnenjem št. 01/2016 Delovne skupine iz člena 29¹⁸⁵ ugotavlja, da so na splošno vzpostavljeni zadostni mehanizmi notranjega nadzora.

3.2.3.3 Zunanji nadzor

194. EOVP ugotavlja, da poleg spodaj navedenih organov dejavnosti ameriških obveščevalnih agencij nadzirajo tudi različni drugi organi znotraj vlade ZDA, kot so obveščevalni nadzorni odbor (*Intelligence Oversight Board*, v nadaljevanju: IOB) ali kongresni odbori. Slednji lahko izvajajo lastne preiskave in izdajajo lastna poročila.

3.2.3.3.1 Odbor za nadzor zasebnosti in državljskih svoboščin (PCLOB)

195. EOVP priznava celovito nadzorno vlogo PCLOB v zvezi z novim mehanizmom pravnega varstva in izvajanjem Odredbe št. 14086.
196. Prvič, njegove nove funkcije vključujejo posvetovanje s pravosodnim ministrom glede imenovanja sodnikov sodišča za presojo varstva podatkov in posebnih odvetnikov. Drugič, PCLOB vsako leto pregleda postopek uveljavljanja pravnih sredstev, tj. obravnavo upravičenih pritožb z mehanizmom pravnega varstva. To vključuje pregled, ali sta CLPO in sodišče za presojo varstva podatkov pravočasno obravnavala upravičene pritožbe, pridobila popoln dostop do potrebnih informacij in delujeta skladno z Odredbo št. 14086 ter ali obveščevalna skupnost spoštuje ugotovitve CLPO in sodišča za presojo varstva podatkov.
197. Poleg tega se morajo obveščevalne agencije posvetovati s PCLOB, ko posodablja svoje notranje politike in postopke za izvajanje Odredbe št. 14086. PCLOB bo pregledal tudi posodobljene politike in postopke ter ocenil njihovo skladnost z Odredbo št. 14086¹⁸⁶. Ugotovitve PCLOB v strogem pomenu niso zavezujoče, vendar mora vodja vsakega organa obveščevalne skupnosti v skladu z veljavno zakonodajo skrbno pretehtati in izvajati ali kako drugače obravnavati vsa priporočila, ki jih vsebuje vsak tak pregled¹⁸⁷. EOVP poziva Komisijo, naj v prihodnjih pregledih posebno pozornost nameni temu, ali in kako se priporočila PCLOB izvajajo na ravni agencije, če bo osnutek sklepa sprejet.
198. EOVP opozarja, da se PCLOB „spodbuja“ k pregledu, ali se zaščitni ukrepi iz Odredbe št. 14086 pravilno upoštevajo in ali je obveščevalna skupnost v celoti izpolnila zahteve postopka uveljavljanja pravnih sredstev, vendar k temu ni zavezan, ker je neodvisen. Vendar EOVP razume, da je PCLOB v svojem dodatnem pojasnilu in tudi javno¹⁸⁸ navedel, da bo prevzel vlogo, predvideno v Odredbi št. 14086.
199. Poleg tega EOVP pozdravlja dejstvo, da so rezultati poročil PCLOB namenjeni javni objavi. Ob upoštevanju dejstva, da morajo različni organi v okviru mehanizma pravnega varstva in organi obveščevalne skupnosti načeloma izvajati priporočila iz poročil PCLOB ali jih drugače obravnavati, priznava, da imajo ta priporočila pri varovanju zasebnosti pomembno vlogo.

¹⁸⁵ Mnenje št. 01/2016 Delovne skupine iz člena 29.

¹⁸⁶ Odločba št. 14086, člen 2(c)(iv) in 2(c)(v).

¹⁸⁷ Odločba št. 14086, člen 2(c)(v)(B).

¹⁸⁸ [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

200. Poleg tega ugotavlja, da je dostop PCLOB do informacij omejen, če predsednik ZDA ministrstvom, agencijam ali subjektom vlade Združenih držav dovoli izvajanje „tajnih akcij“¹⁸⁹.¹⁹⁰
201. EOVP na podlagi svojih prejšnjih mnenj meni, da je PCLOB kot neodvisen organ, katerega priporočila pomembno pripomorejo k reformam v ZDA in katerega poročila so posebej koristen vir za razumevanje delovanja različnih programov nadzora, bistven element nadzorne strukture.
202. Vendar je EOVP v svojem tretjem letnem skupnem pregledu nekdanjega zasebnostnega ščita EU-ZDA obžaloval, da mu je PCLOB zagotovil le tiste informacije, ki jih je zagotovil tudi splošni javnosti. Poleg tega je bilo obžalovanja vredno, da PCLOB ni izdal nadaljnjih poročil o PPD-28, s katerimi bi nadgradil svoje prvo poročilo, da bi zagotovil dodatne elemente o uporabi zaščitnih ukrepov iz PPD-28, in splošnega posodobljenega poročila o členu 702 FISA.
203. Zato EOVP pozdravlja obljubo PCLOB, da lahko v bližnji prihodnosti pričakuje objavo nadaljnjega poročila o členu 702 FISA. Poleg tega je zadovoljen, da ga je PCLOB obvestil o svoji zavezi, da bo dovolil objavo svojih poročil v zvezi z Odredbo št. 14086. Vendar pa opozarja, da objavo nezaupnih poročil ureja zakonodaja ZDA in jo je treba uskladiti z agencijami obveščevalne skupnosti ter da PCLOB o njej ne more odločati sam.
204. EOVP tudi opozarja, da če bo osnutek sklepa sprejet, bi morali imeti varnostno preverjeni strokovnjaki EOVP, v prihodnjih pregledih okvira za varstvo zasebnosti podatkov med EU in ZDA možnost pregledati dodatne dokumente in razpravljati o dodatnih tajnih elementih, kot je potrebno za zagotovitev, da se lahko informacije v poročilih ustrezno ocenijo ob upoštevanju zadevnih interesov nacionalne varnosti in veljavnega varstva zasebnosti.
205. Poleg tega pozdravlja neodvisnost PCLOB in nadzor nad nacionalno obveščevalno skupnostjo, ki mora spoštovati priporočila PCLOB ali jih drugače obravnavati, kar bo navedeno v poročilu PCLOB ameriškemu kongresu.
206. Ob upoštevanju zahtev ESČP glede javnega nadzora¹⁹¹, da je treba poročila nadzornega organa predložiti parlamentu in da mora parlament o njih razpravljati, EOVP meni, da zadostuje, da PCLOB svoja poročila najmanj polletno predloži predsedniku ZDA ter zlasti kongresnim odborom senata in predstavnškega doma¹⁹², ki sta parlamentarni telesi ZDA.

3.2.3.3.2 Sodišče ZDA za nadzor nad obveščevalnimi podatki iz tujine (FISC)

207. Sodišče za nadzor nad obveščevalnimi podatki iz tujine je odgovorno za nadzor zbiranja osebnih podatkov v skladu s členom 702 FISA¹⁹³, na odločbe FISC pa se je mogoče pritožiti pri drugostopenjskem sodišču za nadzor obveščevalnih podatkov iz tujine (*Foreign Intelligence Court of Review*, v nadaljevanju: FISCR).
208. FISC nadzira postopek certificiranja za zbiranje obveščevalnih podatkov iz tujine v skladu s členom 702 FISA in dovoljuje elektronski nadzor, fizično preiskavo in druge preiskovalne ukrepe za namene

¹⁸⁹ V skladu s členom 3093(e)(1) naslova 50 zakonodajne zbirke ZDA) pojem „tajna akcija“ pomeni dejavnost ali dejavnosti vlade Združenih držav, namenjene vplivanju na politične, gospodarske ali vojaške razmere v tujini, pri čemer naj vloga vlade Združenih držav ne bi bila vidna ali javno priznana, vendar ne vključuje (1) dejavnosti, katerih glavni namen je pridobivanje obveščevalnih podatkov, tradicionalnih protiobveščevalnih dejavnosti [...].

¹⁹⁰ Člen 2000ee (g) (5) naslova 42 zakonodajne zbirke ZDA; člen 3093(a) naslova 50 zakonodajne zbirke ZDA.

¹⁹¹ Sodba ESČP v zadevi *Zakharov*, točka 283, ESČP, *L. proti Norveški*, 9. junij 1990; sodba ESČP v zadevi *Kennedy proti Združenemu kraljestvu*, 18. maj 2010, točka 166.

¹⁹² Člen 2000ee (e) naslova 42 zakonodajne zbirke ZDA.

¹⁹³ Člen 1881 (a) naslova 50 zakonodajne zbirke ZDA.

obveščevalnih podatkov iz tujine¹⁹⁴. FISC tudi odobri postopke izbire cilja, zmanjševanja količine podatkov in poizvedovanja po certifikatih, ki so za ameriške obveščevalne agencije pravno zavezujoči¹⁹⁵. Če FISC ugotovi, da zahteve niso izpolnjene, lahko certificiranje v celoti ali delno zavrne in zahteva spremembo postopkov.

209. Če so ugotovljene kršitve postopkov izbire cilja, lahko FISC ustrezni obveščevalni agenciji odredi sprejetje popravilnih ukrepov¹⁹⁶. Ti popravni ukrepi lahko zajemajo posamezne ali strukturne ukrepe, na primer od prenehanja pridobivanja podatkov in izbrisa nezakonito pridobljenih podatkov do spremembe prakse zbiranja podatkov, vključno s smernicami in usposabljanjem osebja.
210. EOVP priznava, da Odredba št. 14086 določa, da morata CLPO in sodišče za presojo varstva podatkov o kršitvah poročati pomočniku pravosodnega ministra za nacionalno varnost, ta pa o teh kršitvah poroča FISC¹⁹⁷.
211. Kot je Sodišče ugotovilo v zadevi *Schrems II*, FISC ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe¹⁹⁸. Zato je EOVP še vedno zaskrbljen, ker FISC ne zagotavlja učinkovitega sodnega nadzora nad ciljnim usmerjanjem na osebe, ki niso državljani ZDA, kar se, kot kaže, z novo Odredbo št. 14086 ni rešilo.
212. EOVP v zvezi s predhodno neodvisno odobritvijo¹⁹⁹ nadzora v skladu s členom 702 FISA obžaluje, da, kot razume iz osnutka sklepa²⁰⁰ in pojasnil vlade ZDA, FISC pri certificiranju programov, ki dovoljujejo ciljno usmerjanje na osebe, ki niso državljani ZDA, ne zavezujejo dodatni zaščitni ukrepi iz Odredbe št. 14086. EOVP meni, da bi bilo treba v tem okviru kljub temu upoštevati dodatne zaščitne ukrepe iz navedene odredbe. Opozarja, da bi bila poročila PCLOB še posebej koristna za oceno, kako se bodo izvajali zaščitni ukrepi iz Odredbe št. 14086 in kako se ti zaščitni ukrepi uporabljajo, ko se podatki zbirajo v skladu s členom 702 FISA.

3.2.4 Jamstvo D – posamezniku morajo biti na voljo učinkovita pravna sredstva

213. EOVP opozarja, da so učinkovite in izvršljive pravice posameznika temeljnega pomena za ugotovitev ustrezne ravni varstva podatkov v tretji državi. Posameznikom, na katere se nanašajo osebni podatki, mora biti na voljo učinkovito pravno sredstvo za uveljavljanje njihovih pravic, kadar menijo, da se jih ne spoštuje ali da niso bile spoštovane. Sodišče je v sodbah v zadevah *Schrems I* in *II* pojasnilo, da „ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravilo oziroma izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine“²⁰¹.
214. Ameriški sistem v zvezi s pravnimi sredstvi vsebuje pomembno omejitev, zaradi katere je zelo težko sprožiti pravni postopek zoper nadzorne ukrepe vlade ZDA pred rednimi sodišči. Ustava ZDA od posameznika zahteva, da dokaže aktivno legitimacijo, tj. „konkretno, podrobno opredeljeno in

¹⁹⁴ www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

¹⁹⁵ Člen 1881a (i) naslova 50 zakonodajne zbirke ZDA.

¹⁹⁶ Člen 1803 (h) naslova 50 zakonodajne zbirke ZDA.

¹⁹⁷ Odredba št. 14086, člen 3 (c) (i) (D); Odredba št. 14086, člen 3 (d) (i) (F).

¹⁹⁸ Sodba Sodišča v zadevi *Schrems II*, točka 179.

¹⁹⁹ EOVP je glede množičnega zbiranja podatkov v skladu z Odredbo št. 12333, ki ne spada v pristojnost FISC, zaskrbljen, ker ni vzpostavljen postopek predhodne odobritve za množično zbiranje podatkov (glej tudi jamstvo B).

²⁰⁰ Osnutek sklepa, uvodna izjava 165.

²⁰¹ Sodba Sodišča v zadevi *Schrems I*, točka 95; sodba Sodišča v zadevi *Schrems II*, točka 187.

dejansko ali neizogibno škodo“²⁰². Zdi se, da je v primerih nadzora taka zahteva izničena z neobveščanjem posameznikov, ki so predmet nadzora, tudi po koncu teh ukrepov.

215. EOVP glede tega pozdravlja dejstvo, da Odredba št. 14086 vzpostavlja poseben mehanizem pravnega varstva za obravnavo in reševanje pritožb posameznikov, ki niso državljani ZDA, v zvezi z dejavnostmi SIGINT v ZDA. V skladu s tem novim mehanizmom se zahteva po aktivni legitimaciji ne uporablja: tožeci stranki v skladu s členom 4(k)(ii) Odredbe št. 14086 ni treba dokazati, da so bili njeni podatki dejansko vključeni v obveščevalne dejavnosti SIGINT v ZDA. Posamezniki, na katere se nanašajo osebni podatki, se tako lahko sklicujejo na zaščitne ukrepe iz Odredbe št. 14086, vključno s tistimi, ki so predvideni z drugimi ustreznimi zakoni in določbami, kot je navedeno v členu 4(d)(iii) Odredbe št. 14086²⁰³. V zvezi s tem novi mehanizem prinaša možnost pravnega varstva, ki sicer ne bi obstajala.
216. Novi mehanizem je sestavljen iz dveh ravni: na prvi lahko posamezniki vložijo pritožbo pri uradniku za varstvo državljskih svoboščin urada direktorja nacionalne obveščevalne službe (CLPO). Na drugi ravni imajo možnost, da se pritožijo na odločitev CLPO pri novoustanovljenem organu, tako imenovanem sodišču za presojo varstva podatkov. V oddelkih v nadaljevanju je glavni poudarek na drugi ravni mehanizma pravnega varstva. EOVP meni, da CLPO kot vršilec dolžnosti uradnika vlade ni dovolj neodvisen od izvršilne veje oblasti in zato sam po sebi ne more ustrezno izpolniti zahtev iz člena 47 Listine EU o temeljnih pravicah. Komisija je to oceno večkrat potrdila.

3.2.4.1 Ali lahko ustanovitev sodišča za presojo varstva podatkov na podlagi Odredbe sama po sebi zadostuje

217. Sodišče za presojo varstva podatkov ni redno sodišče, ki ga ustanovi kongres v skladu s členom III ustave ZDA, temveč temelji na odredbi, ki jo je izdal predsednik ZDA. Čeprav se EOVP zaveda osnovnega premisleka in ga na splošno pozdravlja, tj. izogibanje zahtevi po dokazovanju aktivne legitimacije (glej tudi odstavek 215), se ob tem postavlja temeljno vprašanje: ali lahko tak mehanizem pravnega varstva (sploh) izpolni zahteve iz člena 47 Listine EU o temeljnih pravicah? V skladu s to določbo ima vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Unije, pravico do učinkovitega pravnega sredstva pred sodiščem, predhodno ustanovljenim z zakonom.
218. Angleško besedilo člena 47 Listine EU o temeljnih pravicah se nanaša na „tribunal“ (razsodišče), druge jezikovne različice pa dajejo prednost besedi „sodišče“²⁰⁴. Sodišče je v zadevi *Schrems II* ponovilo, da „morajo posamezniki, na katere se nanašajo osebni podatki, zlasti imeti možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da bi si tako zagotovili dostop do osebnih podatkov, ki se nanje nanašajo, ali dosegli popravilo oziroma izbris takih podatkov“²⁰⁵. Vendar pa v istem okviru ocenjevanja ustreznosti ravni varstva podatkov meni, da lahko učinkovito sodno varstvo pred takim posegom poleg sodišča zagotovi tudi organ, ki zagotavlja jamstva, ki so v bistvu enakovredna tistim, ki se zahtevajo s členom 47 Listine EU o temeljnih pravicah²⁰⁶. EKČP prav tako določa, da ima „vsakdo, čigar pravice in svoboščine so kršene, [...] pravico do učinkovitih pravnih sredstev pred domačimi oblastmi“²⁰⁷, ki v skladu s sodno prakso ESČP niso nujno sodni organi²⁰⁸. Namesto tega so pooblastila in procesna jamstva, ki jih ima organ, zlasti da je neodvisen od izvršilne veje oblasti in

²⁰² *Clapper proti Amnesty International USA*, zvezek 568 mnenj vrhovnega sodišča ZDA, 398 (2013) II., str. 10.

²⁰³ Člen 5(h) Odredbe št. 14086 daje posameznikom, na katere se nanašajo osebni podatki, izrecno pravico do vložitve pritožbe v skladu z mehanizmom pravnega varstva.

²⁰⁴ Na primer „*Gericht*“ v različici v nemškem jeziku.

²⁰⁵ Sodba Sodišča v zadevi *Schrems II*, točka 194.

²⁰⁶ Glej sodbo Sodišča v zadevi *Schrems II*, točka 197.

²⁰⁷ Člen 13 EKČP.

²⁰⁸ Sodba ESČP v zadevi *Klass*, točka 67. Sodba ESČP v zadevi *Big Brother Watch*, točka 359.

zagotavlja poštenost postopka, pomembna za presojo učinkovitosti pravnega sredstva pred tem organom²⁰⁹. Zdi se, da se nobeno od sodišč pri svoji presoji ni oprlo zgolj na formalistična merila, temveč se kot odločilni štejejo vsebinski zaščitni ukrepi.

219. Sodišče je v zadevi *Schrems II* posebno pozornost namenilo učinkovitim pravnim sredstvom na področju dostopa do osebnih podatkov zaradi nacionalne varnosti. EOVP ugotavlja, da Sodišče pri tem ni razpravljalo o elementu „z zakonom predhodno ustanovljeno“ iz člena 47 Listine EU o temeljnih pravicah, čeprav tudi mehanizem varuha človekovih pravic na področju zasebnostnega ščita ni temeljil na zakonskem pravu ZDA. Namesto da bi obravnavalo to vprašanje, je Sodišče za svoj preizkus ustreznosti ocenilo različne vidike, kot je pomanjkanje pooblastil za odpravo kršitev. Tako sodba v zadevi *Schrems II* ne zagotavlja nobenih smernic glede ocene „z zakonom predhodno ustanovljeno“ v skladu s členom 47 Listine EU o temeljnih pravicah. Obstajajo pa druge sodbe, v katerih je Sodišče podalo pripombe o tej zadevi. Sodišče je v sodbah v zadevah C-487/19 in C-132/20 ob sklicevanju na ustaljeno sodno prakso ESČP v zvezi s tem opozorilo, da je namen uvedbe izraza „z zakonom ustanovljeno“ preprečiti, da bi bila organizacija sodnega sistema prepuščena prosti presoji izvršne oblasti, in zagotoviti, da je to področje urejeno z zakonom, ki ga je sprejela zakonodajna oblast, v skladu s pravili, ki urejajo izvajanje njene pristojnosti²¹⁰. Kot je razvidno iz te izjave, je pravica do z zakonom predhodno ustanovljenega sodišča zelo tesno povezana z jamstvom neodvisnosti.
220. EOVP glede na navedeno ugotavlja, da v okviru ocenjevanja ustreznosti ravni varstva posebni mehanizem pravnega varstva, vzpostavljen v skladu z Odredbo št. 14086, v nasprotju s sodnim varstvom pred sodišči iz člena III, sam po sebi ni nezadosten. Analiza ravni varstva je v tem pogledu odvisna od tega, ali zaščitni ukrepi iz Odredbe št. 14086, dopolnjeni z uredbo pravosodnega ministra, dovolj zagotavljajo neodvisnost sodišča za presojo varstva podatkov v primerjavi z drugimi pristojnostmi.
221. Komisija bi morala stalno spremljati, ali se pravila iz Odredbe št. 14086 in njenih dopolnilnih določb, zlasti tista, ki so namenjena spodbujanju neodvisnosti sodišča za presojo varstva podatkov, izvajajo v celoti in učinkovito delujejo v praksi. Poleg tega je treba vse spremembe okvira natančno pregledati glede vpliva na oceno Komisije v skladu z osnutkom sklepa. EOVP glede tega ugotavlja, da lahko spremembe Odredbe št. 14086 in uredbe pravosodnega ministra sprožijo sprejetje izvedbenih aktov, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje sklepa o ustreznosti oziroma se sklep razveljavi ali spremeni²¹¹.

3.2.4.2 Zadostna neodvisnost od izvršilne veje oblasti

222. Sodišče je v sodbi v zadevi *Schrems II* poudarilo, da je treba zagotoviti neodvisnost sodišča ali organa, zlasti od izvršilne veje oblasti, z vsemi potrebnimi jamstvi, tudi v zvezi z njegovimi pogoji za odpoklic ali razveljavitev imenovanja. Natančneje, Sodišče je kritiziralo dejstvo, da je varuha človekovih pravic imenoval zunanji minister in da varuh poroča neposredno zunanjemu ministru. Varuh človekovih pravic se je štel za sestavni del zunanjega ministrstva ZDA. Sodišče je tudi ugotovilo, da ni posebnih zagotovitev za odpoklic ali razveljavitev imenovanja varuha človekovih pravic, kar vzbuja dvom o njegovi neodvisnosti od izvršilne veje oblasti.
223. EOVP priznava, da določbe Odredbe št. 14086 in dopolnilna uredba pravosodnega ministra sodišču za presojo varstva podatkov ne nalagajo obveznosti poročanja pravosodnemu ministru, kot bi to veljalo

²⁰⁹ Sodba ESČP v zadevi *Klass*, točka 67. Sodba ESČP v zadevi *Big Brother Watch*, točka 359.

²¹⁰ Glej sodbe Sodišča v zadevah C-487/19 z dne 6. oktobra 2021, *W.Ż.*, ECLI:EU:C:2021:798, in C-132/20 z dne 29. marca 2022 ter *Getin Noble Bank S.A.*, ECLI:EU:C:2022:235, točki 129 in 121.

²¹¹ Osutek sklepa, uvodna izjava 212.

v razmerju nadrejeni-podrejeni. Nad sodiščem za presojo varstva podatkov se tudi ne izvaja „vsakodnevni nadzor“ s strani pravosodnega ministra²¹². Ti zaščitni ukrepi so pomembna izboljšava v primerjavi z zasebnostnim ščitom. Toda sodišče za presojo varstva podatkov je ustanovljeno znotraj izvršilne veje oblasti, in sicer ministrstva za pravosodje. Prav zato bosta izvajanje in učinkovito delovanje zaščitnih ukrepov v praksi bistvena za ugotavljanje, ali se lahko sodišče za presojo varstva podatkov, ki sicer ni sestavni del ministrstva za pravosodje, je pa subjekt znotraj izvršilne veje oblasti, v praksi šteje za dovolj neodvisno. EOVP poziva Komisijo, naj skrbno spremlja, ali se ti zaščitni ukrepi v celoti odražajo v praksi. Poleg tega predlaga, naj se izraz „vsakodnevni nadzor“ pojasni v smislu, da se nad „sodniki“ sodišča za presojo varstva podatkov ne izvaja nikakršen nadzor. Komisija je potrdila, da je treba „vsakodnevni nadzor“ razumeti v tem smislu.

224. Poleg zgoraj navedenih zaščitnih ukrepov okvir za varstvo zasebnosti podatkov med EU in ZDA predvideva nekatera jamstva v zvezi z imenovanjem in odpoklicem „sodnikov“ sodišča za presojo varstva podatkov. Čeprav jih imenuje pravosodni minister, njihovo imenovanje temelji na merilih, ki se uporabljajo za ocenjevanje kandidatov za funkcije zveznih sodnikov, in vključuje posvetovanje s PCLOB. „Sodnike“ je mogoče predčasno odpoklicati ali jih odstraniti iz postopka, ki teče, le v ozko opredeljenih okoliščinah, ki, kolikor razume EOVP, temeljijo na določbah, ki se uporabljajo za zvezne sodnike²¹³. Uporaba teh pravil je nadaljnji korak h krepitvi neodvisnega položaja sodišča za presojo varstva podatkov in tudi tu bo bistveno izvajanje v praksi. Vendar iz osnutka sklepa ni razvidno, ali in kako se bo skladnost s temi zahtevami upoštevala v Združenih državah. EOVP na podlagi dodatnih pojasnil, ki sta jih zagotovili Komisija in vlada ZDA, razume, da lahko PCLOB obravnava zgoraj navedene določbe v svojem letnem pregledu postopka uveljavljanja pravnih sredstev in da odgovornost za spremljanje ter zagotavljanje skladnosti z vsemi pravnimi zahtevami generalnega inšpektorja znotraj ministrstva za pravosodje vključuje zahteve iz Odredbe št. 14086 in predpisov o ustanovitvi sodišča za presojo varstva podatkov. EOVP poziva Komisijo, naj ta vidik pojasni v osnutku sklepa. Ob tem bi morala Komisija te zaščitne ukrepe upoštevati pri spremljanju dejanske prakse obdelave osebnih podatkov, kot je ocenjena v osnutku sklepa.
225. Osnutek sklepa ne obravnava vprašanja, ali ima predsednik ZDA pooblastilo za odpoklic ali odstranitev „sodnikov“ s sodišča za presojo varstva podatkov, in če ga ima, pod kakšnimi pogoji. Kot razume EOVP, naj tako pooblastilo ne bi obstajalo, kar je pojasnila Evropska komisija in so potrdili predstavniki vlade ZDA. EOVP predlaga, naj se ta vidik pojasni v sklepu o ustreznosti.
226. „Sodniki“ sodišča za presojo varstva podatkov se imenujejo za štiriletni mandat z možnostjo ponovnega imenovanja, pri čemer dve leti pred prvim imenovanjem ne smejo biti zaposleni v izvršilni veji oblasti²¹⁴. Med svojim mandatom „sodnika“ sodišča za presojo varstva podatkov ne smejo imeti nobenih drugih uradnih dolžnosti ali zaposlitve v vladi ZDA²¹⁵. Vendar pa v nasprotju z zveznimi sodniki ZDA lahko sodelujejo v zunajsodnih dejavnostih, vključno s poslovnimi dejavnostmi, finančnimi dejavnostmi, neprofitnimi dejavnostmi zbiranja sredstev, fiduciarnimi dejavnostmi in opravljanjem odvetniške prakse, če take dejavnosti ne vplivajo na nepristransko opravljanje njihovih dolžnosti ali na učinkovitost ali neodvisnost sodišča za presojo varstva podatkov²¹⁶. Neodvisnost sodnikov ne izhaja le iz dejstva, da jih ne zavezujejo navodila, temveč tudi iz osebne neodvisnosti. V tem okviru so pomembni dejavniki, kot so trajanje mandata, možnost ponovnega imenovanja in možnost navzkrižja interesov. Štiriletni mandat, predviden v Odredbi št. 14086 oziroma uredbi pravosodnega ministra, je sicer krajši

²¹² Uredba pravosodnega ministra, člen 201.7 (d).

²¹³ Odredba št. 14086, člen 3(d)(iv); uredba pravosodnega ministra, člen 201.7.

²¹⁴ Uredba pravosodnega ministra, člen 201.3 (a).

²¹⁵ Uredba pravosodnega ministra, člen 201.3 (c).

²¹⁶ Uredba pravosodnega ministra, člen 201.7 (c).

od na primer mandata sodnikov Sodišča (šest let z možnostjo ponovnega imenovanja) in ESČP (devet let brez možnosti ponovnega imenovanja), vendar kot tak ne povzroča resne zaskrbljenosti. EOVP ni seznanjen s sodno prakso, ki bi v zvezi s tem določala najkrajše trajanje mandata²¹⁷. Priznava tudi, da je možnost sodelovanja v zunajsodnih dejavnostih pogojena s tem, da, preprosto povedano, te dejavnosti ne povzročijo navzkrižja interesov, ki bi ogrozilo dolžnosti sodišča za presojo varstva podatkov. Iz dodatnih pojasnil vlade ZDA razume, da tudi te zahteve pregledujeta in spremljata PCLOB in generalni inšpektor ministrstva za pravosodje (glej zgornji odstavek 226). V okviru skupnih pregledov bi bilo treba obravnavati tudi, kako se bo ta zahteva uporabljala in dokazala v praksi.

227. V skladu s členom 3(d)(i)(B) Odredbe št. 14086 morajo imeti vsi „sodniki“ sodišča za presojo varstva podatkov varnostna potrdila, da lahko dostopajo do zaupnih podatkov, tj. za opravljanje svoje naloge razsojanja v zadevah nacionalne varnosti²¹⁸. Nasprotno pa so v skladu z nekaterimi evropskimi zakoni in predpisi o varnostnem preverjanju sodniki izvzeti iz zahteve po varnostnem preverjanju v obsegu, v katerem izvajajo funkcijo sodnika, saj se šteje, da bi lahko bil tako podroben nadzor v nasprotju z neodvisnostjo sodnikov²¹⁹. Po pojasnilih vlade ZDA kandidat za sodniško funkcijo na ameriškem sodišču prestane temeljito preverjanje, ko se ga imenuje za zveznega sodnika ameriškega sodišča, vendar mu kot zveznemu sodniku ni treba pridobiti varnostnega potrdila za dostop do tajnih dokumentov, pomembnih za zadevo.
228. Po mnenju EOVP zgoraj opisane okoliščine delno razkrivajo razlike med funkcijo in statusom zveznega sodnika ZDA in „sodnika“ sodišča za presojo varstva podatkov. Vendar zagotovljeni zaščitni ukrepi ne vzbujajo dvoma o neodvisnosti sodišča za presojo varstva podatkov. EOVP poziva Komisijo, naj se v primeru sprejetja osnutka sklepa zgoraj navedeni zaščitni ukrepi pri prvem skupnem pregledu okvira za varstvo zasebnosti podatkov med EU in ZDA obravnavajo prednostno. Poleg tega pričakuje, da bo Komisija izpolnila svojo zavezo o začasnem zadržanju izvajanja, razveljavitvi ali spremembi sklepa o ustreznosti, če bo sprejet, če bi se izvršilna veja oblasti ZDA odločila omejiti zaščitne ukrepe, vključene v Odredbo²²⁰.

3.2.4.3 Pristojnost sodišča za presojo varstva podatkov

3.2.4.3.1 Dostop do informacij

229. Učinkovito pravno varstvo zahteva, da ima sodišče zadostna preiskovalna pooblastila za pregled izpodbijanega ukrepa. Sodišče je v zadevi *Kadi II* v zvezi s členom 47 Listine EU o temeljnih pravicah razsodilo, da mora sodišče Unije zagotoviti, da odločba temelji na dovolj trdni dejanski osnovi²²¹. Sodišče navaja, da „mora sodišče Unije opraviti ta preizkus tako, da če je to potrebno, pristojni organ Unije pozove k predložitvi informacij ali dokazov, ki so upoštevní pri takem preizkusu, ne glede na to, ali so zaupni“²²², pri čemer „se ni mogoče sklicevati na tajnost ali zaupnost [...] informacij ali dokazov“²²³.

²¹⁷ Smiselno glej tudi sodbo ESČP (veliki senat) v zadevi *Centrum För Rättvisa proti Švedski*, 25. maj 2021, točka 346.

²¹⁸ Glej tudi uredbo pravosodnega ministra, člen 201.11 (b), in osnutek sklepa, uvodna izjava 177.

²¹⁹ Na primer, člen 2(3) nemškega Zakona o varnostnem preverjanju.

²²⁰ Osnutek sklepa, uvodna izjava 212.

²²¹ Sodišče, združene zadeve C-584/10 P, C-593/10 P in C-595/10 P, *Evropska komisija in drugi/Yassin Abdullah Kadi*, sodba z dne 18. julija 2013 (v nadaljevanju: sodba Sodišča v zadevi *Kadi II*), točka 119.

²²² Sodba Sodišča v zadevi *Kadi II*, točka 120.

²²³ Sodba Sodišča v zadevi *Kadi II*, točka 125.

230. Sodišče za presojo varstva podatkov v skladu z uvodno izjavo 181 osnutka sklepa pregleda ugotovitve CLPO, ki temeljijo vsaj na evidenci preiskave CLPO, pa tudi vse informacije in vloge, ki jih predloži pritožnik, posebni odvetnik ali obveščevalna agencija. V osnutku sklepa je tudi navedeno, da ima sodišče za presojo varstva podatkov dostop do vseh potrebnih informacij, ki jih lahko pridobi prek CLPO. To temelji na določbi člena 201.9(b) uredbe pravosodnega ministra, ki sodišče za presojo varstva podatkov pooblašča, da „zahteva, da ODNI CLPO dopolni evidenco s posebnimi pojasnili ali pojasnjevalnimi informacijami in da po potrebi oblikuje dodatne dejanske ugotovitve, da senatu sodišča za presojo varstva podatkov omogoči izvedbo pregleda“. EOVP razume, da ocena, ki jo je izvedlo sodišče za presojo varstva podatkov, nikakor ni omejena na ugotovitve CLPO na prvi ravni novega mehanizma pravnega varstva. Nasprotno, sodišče za presojo varstva podatkov lahko zahteva dodatne pravne informacije in, kar je pomembno, dodatne dejanske okoliščine za analizo, ali je prišlo do zajete kršitve. EOVP hkrati ugotavlja, da ta na splošno obsežna preiskovalna pooblastila ne zajemajo neposrednega dostopa do podatkov o posamezniku. Komisija je pojasnila, da bo CLPO vedno deloval kot posrednik, ko bo sodišče za presojo varstva podatkov zahtevalo dodatne informacije. Zato je dostop sodišča za presojo varstva podatkov do informacij, potrebnih za neodvisno odločanje o zahtevku za pregled, deloma odvisen od tega, ali CLPO zagotovi potrebne informacije. EOVP priznava, da je CLPO dolžan sodišču za presojo varstva podatkov „zagotoviti vso potrebno podporo“, obveščevalne agencije pa morajo CLPO zagotoviti dostop do informacij, ki jih sodišče za presojo varstva podatkov potrebuje za pregled²²⁴. Poleg tega EOVP ugotavlja, da sam CLPO ni neodvisen in izvede začetno preiskavo pritožbe na prvi ravni postopka pravnega varstva. Zato pozdravlja dejstvo, da bo PCLOB med letnimi pregledi mehanizma pravnega varstva preveril, ali je sodišče za presojo varstva podatkov pridobilo popoln dostop do vseh potrebnih informacij²²⁵. Poleg tega poziva Komisijo, naj ta vidik vključi v skupne preglede, če bo osnutek sklepa sprejet, da se preuči posledice tega sistema v praksi.

3.2.4.3.2 Pooblastila za odpravo kršitev

231. Ena od osrednjih pomanjkljivosti zasebnostnega štita, zaradi katere ga je Sodišče v zadevi *Schrems II* razglasilo za neveljavnega, je bilo pomanjkanje zavezujočih pooblastil varuha človekovih pravic za odpravo kršitev. Sodišče EU je ugotovilo, da „[...] ne vsebuje nobene navedbe, da bi bil ta varuh pristojen za sprejemanje zavezujočih odločitev v zvezi s temi službami“²²⁶. Zgolj (politična) zaveza ameriške vlade, da bo obveščevalna skupnost odpravila vsako kršitev veljavnih pravil, ki jih odkrije varuh človekovih pravic, ni zadoščala za zagotovitev ravni varstva, ki bi bila v bistvu enakovredna ravni varstva, zagotovljeni s členom 47 Listine EU o temeljnih pravicah.
232. Nasprotno so v skladu z novim mehanizmom pravnega varstva odločitve, ki jih sprejmeta CLPO in sodišče za presojo varstva podatkov, zavezujoče²²⁷. EOVP po eni strani priznava, da to pooblastilo ni omejeno na posebne ukrepe, temveč omogoča „ustrezno odpravo kršitve“ za „popolno odpravo posledic“ ugotovljene zajete kršitve. Zlasti v členu 4(a) Odredbe št. 14086 je izrecno navedeno brisanje nezakonito zbranih podatkov. Po drugi strani pa EOVP ugotavlja, da besedilo člena 4(a) Odredbe št. 14086 povzroča nekaj negotovosti glede postopka določanja take „ustrezne odprave kršitve“. Ukrepi bi moral biti zasnovani tako, da v celoti odpravi posledice kršitve, pri tem pa je treba upoštevati tudi

²²⁴ Odredba št. 14086, člen 3(c)(i)(H) in 3(d)(iii).

²²⁵ Odredba št. 14086, člen 3(e)(i).

²²⁶ Sodba Sodišča v zadevi *Schrems II*, točka 196.

²²⁷ Odredba št. 14086, člen 3(c)(ii) in člen 3(d)(ii).

„načine, na katere se običajno obravnava kršitev take vrste“²²⁸. Pomen in učinek take zahteve nista jasna. Zato EOVP poziva Komisijo, naj pozorno spremlja v praksi sprejete ukrepe za odpravo kršitve.

3.2.4.4 Vložitev pritožbe v skladu z novim mehanizmom pravnega varstva

233. Mehanizem pravnega varstva, vzpostavljen v skladu z Odredbo št. 14086, se uporablja samo za upravičene pritožbe glede kakršnih koli kršitev, ki jih posreduje ustrezen javni organ v državi, ki izpolnjuje pogoje, v zvezi z dejavnostmi SIGINT v ZDA²²⁹. Za uveljavljanje tega pravnega varstva mora biti torej izpolnjenih več pogojev.

3.2.4.4.1 Določitev države, ki izpolnjuje pogoje

234. Prvič, država ali organizacija za regionalno gospodarsko povezovanje, iz katere so bili podatki preneseni v Združene države, mora biti pred prenosom podatkov, na katerem temelji pritožba, določena kot država, ki izpolnjuje pogoje²³⁰. Seveda je bistveno, da je zagotovljeni mehanizem pravnega varstva na voljo, ko začne veljati sklep o ustreznosti. V skladu s tem uvodna izjava 196 osnutka sklepa določa, da je začetek veljavnosti sklepa med drugim pogojen z določitvijo Unije kot subjekta, ki izpolnjuje pogoje za namene mehanizma pravnega varstva. Dejansko se zdi, da Komisija domneva, da bo določitev izvedena pred sprejetjem sklepa, saj osnutek že vključuje označbo mesta za določitev EU²³¹ s strani pravosodnega ministra (namesto da bi bila določitev vključena v izrek osnutka sklepa kot odložni pogoj).

3.2.4.4.2 Negativen vpliv na interese v zvezi z varstvom zasebnosti in državljanskimi svoboščinami ter „aktivno legitimacijo“

235. „Upravičena pritožba“ mora temeljiti na domnevni „zajeti kršitvi“, pri čemer mora kršitev negativno vplivati na interese pritožnika v zvezi z varstvom zasebnosti in državljanskimi svoboščinami²³². EOVP na podlagi dodatnih pojasnil Komisije razume, da „negativen vpliv“ ne pomeni kakršne koli omejitve dopustnosti pritožbe. Nasprotno, kot je navedla Komisija, bi se tak negativen vpliv nanašal na vse pritožbe v zvezi z obdelavo osebnih podatkov za dejavnosti SIGINT, ki krši določbe iz člena 4(d)(iii), na primer zaščitne ukrepe iz Odredbe št. 14086. EOVP obžaluje, da to ni navedeno v besedilu osnutka sklepa, in poziva Komisijo, naj dodatno pojasni pojem „negativen vpliv“ za zagotovitev, da se vsaka kršitev pravic posameznikov, na katere se nanašajo osebni podatki, oceni in odpravi ter da za dostop do pravnih sredstev in ustrezno odpravo kršitve ni treba dokazovati stopnje „resnosti“.
236. Kot je bilo že navedeno, tožniku za pritožbo v skladu z Odredbo št. 14086 ni treba dokazati aktivne legitimacije (glej odstavek 215)²³³. EOVP pozdravlja pojasnilo v členu 4(k) Odredbe št. 14086, da bo uporabljen „preizkus razumne domneve“ in da ni treba dokazati, da se je do podatkov pritožnika dejansko dostopalo prek dejavnosti SIGINT. Vzpostavitev mehanizma pravnega varstva je pomemben korak, saj zahteva glede aktivne legitimacije zelo otežuje izpodbijanje nadzornih ukrepov pred rednimi sodišči v Združenih državah.

²²⁸ Odredba št. 14086, člen 4(a).

²²⁹ Odredba št. 14086, člen 3(a).

²³⁰ Odredba št. 14086, člen 4(d)(i) in 4(k)(i).

²³¹ Osnutek sklepa, opomba 320.

²³² Odredba št. 14086, člen 4(k)(i) in 4(d)(ii).

²³³ *Clapper proti Amnesty International USA*, zvezek 568 mnenj vrhovnega sodišča ZDA, 398 (2013) II., str. 10.

237. EOVP na podlagi zgoraj navedenega meni, da sprožitev postopka pred rednimi sodišči, na kar se osnutek sklepa tudi nanaša²³⁴, ne zagotavlja ustrezne ravni varstva²³⁵. Glede tega opozarja na pomisleke, ki jih je že večkrat izrazil glede zahteve po aktivni legitimaciji pred rednimi sodišči²³⁶. Poleg tega na podlagi dodatnih izjav ameriške vlade meni, da Odredba št. 14086 ne izključuje uporabe sodišč splošne pristojnosti, vendar ni gotovo, kako bi tako sodišče navedeno odredbo uporabilo. To vprašanje bi se lahko podrobneje raziskalo v prihodnjih pregledih, če bo osnutek sklepa sprejet.

3.2.4.4.3 Postopek pritožbe

238. EOVP načeloma podpira postopek za usmerjanje pritožbe prek nadzornih organov držav članic in še vedno meni, da bi bilo treba pritožnika identificirati na ozemlju EU. Vendar pa je v osnutku sklepa, tako kot v okviru mehanizma varuha človekovih pravic na področju zasebnostnega ščita, določeno, da mora posameznik, na katerega se nanašajo osebni podatki in ki želi vložiti takšno pritožbo, to predložiti nadzornemu organu v državi članici EU, pristojnemu za nadzor nacionalnih varnostnih služb in/ali obdelavo osebnih podatkov s strani javnih organov²³⁷. EOVP glede tega opozarja na svoje pomisleke, ki jih je izrazil že v mnenju WP29 o zasebnostnem ščitu, na primer o morebitnih težavah posameznikov pri ugotavljanju, kateri organ je pristojen, saj se mehanizmi nadzora nacionalnih varnostnih služb v državah članicah razlikujejo²³⁸. Ob upoštevanju vključenosti nacionalnih organov za varstvo podatkov v uporabo in nadzor DPF je ustreznejše, da se pritožbe usmerjajo prek njih.

3.2.4.5 Sklep sodišča za presojo varstva podatkov

239. Ko sodišče za presojo varstva podatkov konča pregled pritožbe pritožnika, ne sme razkriti, ali je bil pritožnik predmet dejavnosti SIGINT v ZDA ali ne. Namesto tega se pritožnika obvesti, da „pri pregledu bodisi niso bile ugotovljene nobene zajete kršitve bodisi da je sodišče za varstvo podatkov izdalo odločitev, ki zahteva ustrezno odpravo kršitve“²³⁹. S tem standardnim odgovorom se izpolni na splošno zakoniti namen varovanja občutljivih informacij o dejavnostih SIGINT v ZDA. Vendar je EOVP zaskrbljen, ker Odredba št. 14086 ne določa nobenih izjem od standardnega odgovora sodišča za presojo varstva podatkov.
240. Sodišče je moralo v zadevi *Kadi II* obravnavati nasprotujoče si interese državne tajnosti na eni strani ter poštene in, kolikor je mogoče, kontradiktorne postopke na drugi strani. Sodišče je razsodilo, da morajo sodišča v okoliščinah, v katerih nujni preudarki, ki se nanašajo na nacionalno varnost, nasprotujejo temu, da se zadevne osebe obvestijo o nekaterih informacijah ali dokazih, v okviru sodnega nadzora vendarle uporabiti načine, ki jim omogočajo uskladiti legitimne preudarke glede varnosti, ob upoštevanju vrst in virov informacij, ter tega, da morajo posamezniku v zadostni meri zagotoviti spoštovanje postopkovnih pravic, kot sta pravica do izjave in načelo kontradiktornosti²⁴⁰. Sodišče je nadalje pojasnilo, da morajo sodišča na podlagi preizkusa vseh pravnih in dejanskih elementov, ki jih je predložil pristojni organ Unije, preveriti utemeljenost razlogov, ki jih je ta organ navedel, da bi zavrnil njihovo razkritje²⁴¹. Če se izkaže, da razlogi, ki jih je navedel pristojni organ Unije, dejansko nasprotujejo temu, da se zadevna oseba obvesti o informacijah in dokazih, je treba na primeren način uravnotežiti zahteve, ki izhajajo iz pravice do učinkovitega sodnega varstva, z

²³⁴ Osnutek sklepa, uvodna izjava 187 in naslednje.

²³⁵ Glej tudi sodbo Sodišča v zadevi *Schrems II*, točki 191 in 192.

²³⁶ Glej Mnenje št. 01/2016 Delovne skupine iz člena 29, str. 43.

²³⁷ Osnutek sklepa, uvodna izjava 169.

²³⁸ Mnenje št. 01/2016 Delovne skupine iz člena 29, str. 48 in 49.

²³⁹ Odredba št. 14086, člen 3(d)(i)(H). Člen Odredbe št. 14086 določa ta odgovor tudi za CLPO.

²⁴⁰ Sodba Sodišča v zadevi *Kadi II*, točka 125.

²⁴¹ Sodba Sodišča v zadevi *Kadi II*, točka 126.

zahtevami, ki izhajajo iz nacionalne varnosti²⁴². Za tako uravnoteženje se lahko uporabijo možnosti, kot je predložitev povzetka vsebine zadevnih informacij ali dokazov²⁴³. Čeprav ugotovitve sodišča ne nalagajo zahtev glede odločbe, ki jo izda sodišče, temveč se nanašajo na odločitev pristojnega organa in vodenje sodnega postopka, pa kažejo na uravnoteženje zgoraj navedenih interesov v okviru pravice do učinkovitega pravnega varstva. Za nadaljnje smernice se je mogoče sklicevati tudi na zadevo *Big Brother Watch*, v kateri je ESČP, sklicujoč se na poštenost postopka in zlasti na načelo kontradiktornosti, razsodilo, da je treba odločbe sodnega ali drugega neodvisnega organa utemeljiti²⁴⁴.

241. EOVP priznava, da so odločbe sodišča za presojo varstva podatkov dejansko utemeljene. Od sodišča za presojo varstva podatkov se izrecno zahteva pisna odločba, v kateri navede svoje odločitve in opredeli morebitno ustrezno odpravo kršitve²⁴⁵. EOVP tudi ugotavlja, da bo posameznik obveščen, če bo preklicana stopnja tajnosti informacij, ki se nanašajo na pregled sodišča za presojo varstva podatkov²⁴⁶. Poleg tega priznava vlogo posebnih odvetnikov, predvidenih v novem mehanizmu pravnega varstva, ki vključuje zagovarjanje interesov pritožnika v zadevi²⁴⁷. Vendar ima v luči zgoraj navedenih posledic sodne prakse Sodišča in ESČP ter ob upoštevanju, da se na odločbo sodišča za presojo varstva podatkov ni mogoče pritožiti, temveč je dokončna²⁴⁸, pomisleke glede splošne uporabe standardnega odgovora sodišča za presojo varstva podatkov. Opozarja tudi, da bo PCLOB neodvisno pregledal delovanje novega mehanizma pravnega varstva, in poziva Komisijo, naj v prihodnjih pregledih sklepa, če bo sprejet, temu vprašanju namenijo posebno pozornost, vključno s kakršno koli oceno tega vidika s strani PCLOB.

4 IZVAJANJE IN SPREMLJANJE OSNUTKA SKLEPA

242. EOVP v zvezi s spremljanjem in pregledom osnutka sklepa ugotavlja, da mora v skladu s sodno prakso Sodišča „glede na to, da se raven varstva, ki jo zagotavlja tretja država, lahko spremeni, [...] Komisija po sprejetju odločbe na podlagi [člena 45 Splošne uredbe o varstvu podatkov] redno preverjati, ali je ugotovitev v zvezi z ustrezno ravni varstva, ki ga zagotavlja zadevna tretja država, še zmeraj dejansko in pravno utemeljena. Vsekakor je taka preveritev potrebna, kadar je na podlagi indicev mogoče o tem dvomiti“²⁴⁹.
243. EOVP poleg tega ugotavlja, da dopis ministrstva za trgovino zagotavlja, da se bodo ministrstvo za trgovino in druge agencije ZDA, kot je primerno, redno sestajali s Komisijo, zainteresiranimi organi EU za varstvo podatkov in ustreznimi predstavniki EOVP²⁵⁰.
244. EOVP meni, da bo treba pri naslednjih rednih pregledih posebno pozornost nameniti varstvu državnih zakonov v zvezi z dostopom organov kazenskega pregona, odstopanju za začasno množično zbiranje glede na ciljno zbiranje s strani nacionalnih varnostnih organov ZDA, uporabi novo uvedenih načel nujnosti in sorazmernosti v praksi, tudi v okviru programa UPSTREAM, medsebojnemu vplivu Odredbe št. 14086 in različnih pravnih instrumentov ZDA, ki ameriškim obveščevalnim agencijam omogočajo zbiranje in nadaljnjo obdelavo osebnih podatkov, izvedbenim notranjim politikam in postopkom, temu,

²⁴² Sodba Sodišča v zadevi *Kadi II*, točka 128.

²⁴³ Sodba Sodišča v zadevi *Kadi II*, točka 129.

²⁴⁴ Sodba ESČP v zadevi *Big Brother Watch*, točka 359.

²⁴⁵ Uredba pravosodnega ministra, člen 201.9 (g).

²⁴⁶ Odredba št. 14086, člen 3(d)(v).

²⁴⁷ Uredba pravosodnega ministra, člen 201.8 (g).

²⁴⁸ Uredba pravosodnega ministra, člen 201.9 (g).

²⁴⁹ Sodba Sodišča v zadevi *Schrems I*, točka 76. Glej tudi osnutek sklepa, člen 3(4).

²⁵⁰ Osnutek sklepa, Priloga III.

kako se bodo ti zaščitni ukrepi upoštevali tudi v okviru nadzora, ki ga izvaja FISC, in kako bo mehanizem pravnega varstva deloval učinkovito, ter vprašanju nadaljnjih prenosov avtomatiziranemu sprejemanju odločitev, vsebinskemu in učinkovitemu nadzoru, uveljavljanju načel DPF ter učinkovitim pravnim sredstvom.

245. EOVP ugotavlja, da bo pregled ugotovitve ustreznosti opravljen po enem letu od datuma, ko se države članice obvesti o sklepu o ustreznosti, in nato najmanj vsaka štiri leta²⁵¹. Da bi se dodatno okrepilo stalno spremljanje sklepa o ustreznosti, EOVP poziva Komisijo, naj nadaljnje preglede izvede vsaj vsaka tri leta.
246. Kar zadeva praktično sodelovanje EOVP in njegovih predstavnikov pri pripravi in izvajanju prihodnjih rednih pregledov, EOVP vnovič poudarja, da bi mu bilo treba dovolj zgodaj pred pregledi pisno predložiti vso ustrezno dokumentacijo, vključno s korespondenco. EOVP priporoča, naj Komisija, administracija ZDA in EOVP, najpozneje tri mesece pred pregledom določijo načine pregleda in se o njih dogovorijo, kot pri pregledih, izvedenih v okviru zasebnostnega ščita.
247. Poleg tega ugotavlja in pozdravlja dejstvo, da so v uvodni izjavi 212 osnutka sklepa navedeni primeri sprememb, ki ogrožajo raven varstva in v katerih bi se lahko upravičeno sprožil „izredni postopek razveljavitve“, ki se osredinja na spremembe, do katerih bi lahko prišlo v zvezi z Odredbo št. 14086 in z njo povezano uredbo pravosodnega ministra.

Za Evropski odbor za varstvo podatkov

predsednica

(Andrea Jelinek)

²⁵¹ Osnutek sklepa, člen 3(4).