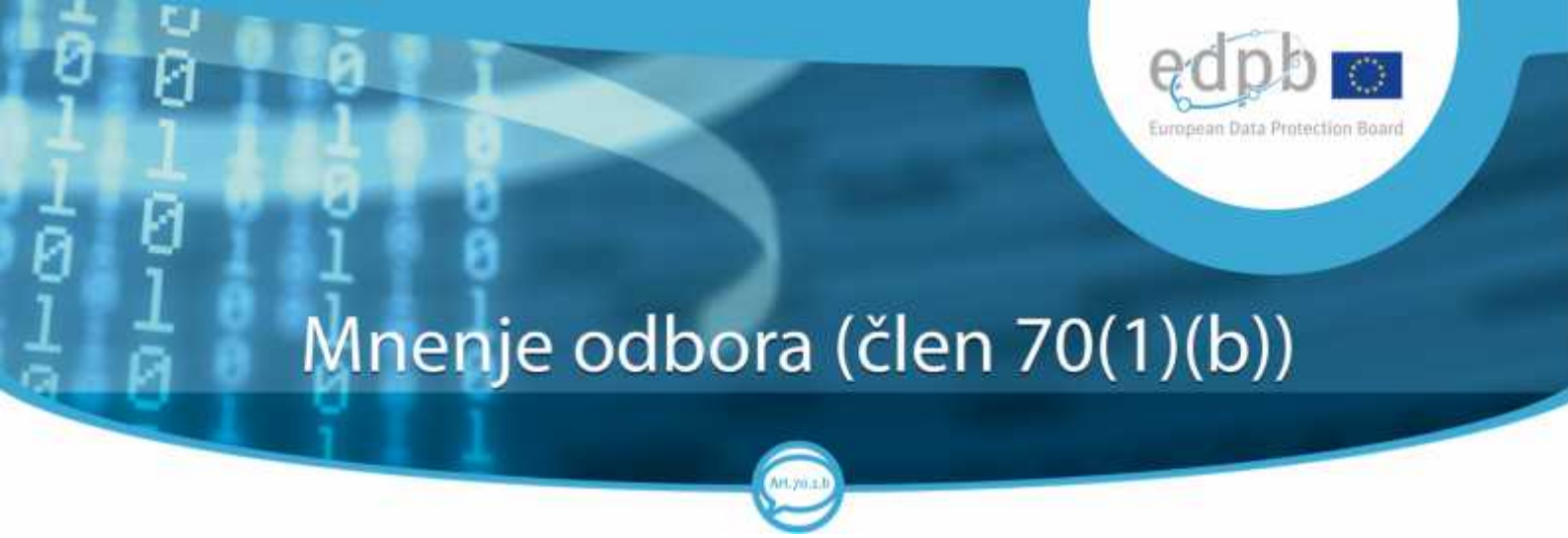

Mnenje št. 28/2018

o osnutku izvedbenega sklepa Evropske komisije

o ustreznem varstvu osebnih podatkov na Japonskem

Sprejeto 5. decembra 2018

Kazalo

1 POVZETEK 4

1.1 Področja, o katerih je doseženo soglasje 5

1.2 Splošni izzivi 5

1.3 Posebni trgovinski vidiki 6

1.3.1 Pomisleki EOVP glede ključnih načel varstva podatkov 6

1.3.2 Potreba po pojasnilu 7

1.4 O dostopu javnih organov do podatkov, prenesenih na Japonsko 7

1.5 Sklep 7

2 UVOD 8

2.1 Japonski okvir varstva podatkov 8

2.2 Obseg ocene EOVP 9

2.3 Splošne pripombe in pomisleki 10

2.3.1 Posebnosti tovrstnega sklepa o ustreznosti 10

2.3.2 Zanesljivost prevodov 10

2.3.3 Sektorska ustreznost 11

2.3.4 Zavezujoča narava dopolnilnih pravil in smernic komisije za varstvo osebnih podatkov 11

2.3.5 Redni pregled ugotovitve o ustreznosti 12

2.3.6 Mednarodne zaveze, ki jih je sprejela Japonska 12

2.3.7 Pooblastila organov za varstvo podatkov za vložitev tožb v zvezi z veljavnostjo sklepa o ustreznosti na sodišču 13

3 TRGOVINSKI VIDIKI 13

3.1 Vsebinska načela 13

3.1.1 Pojmi 13

3.1.2 Razlogi za zakonito in pošteno obdelavo podatkov za zakonite namene 16

3.1.3 Načelo preglednosti 17

3.1.4 Omejitve nadaljnjih prenosov 18

3.1.5 Neposredno trženje 21

3.1.6 Avtomatizirano sprejemanje odločitev in oblikovanje profilov 21

3.2 Postopkovni mehanizmi in mehanizmi za izvrševanje 22

3.2.1 Pristojni neodvisni nadzorni organ 22

3.2.2 Sistem varstva podatkov mora zagotavljati dobro raven skladnosti 23

3.2.3 Sistem varstva podatkov mora zagotavljati podporo in pomoč posameznikom, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic in ustreznih pravnih sredstev 24

4 O DOSTOPU JAVNIH ORGANOV DO PODATKOV, PRENESENIH NA JAPONSKO 25
4.1 Dostop organov pregona do podatkov 26
4.1.1 Postopki za dostop do podatkov na področju kazenskega prava 26
4.1.2 Nadzor na področju kazenskega prava 28
4.1.3 Pravna sredstva na področju kazenskega prava 31
4.2 Dostop za namene nacionalne varnosti 36
4.2.1 Obseg nadzora 36
4.2.2 Prostovoljno razkritje v primeru nacionalne varnosti 38
4.2.3 Nadzor 39
4.2.4 Mehanizem pravnega varstva 41

Evropski odbor za varstvo podatkov je –

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 nadaljnjem besedilu: splošna uredba o varstvu podatkov),

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

ob upoštevanju členov 12 in 22 svojega poslovnika z dne 25. maja 2018 –

SPREJEL NASLEDNJE MNENJE:

1 POVZETEK

1. Evropska komisija je osnutek izvedbenega sklepa o ustreznem varstvu osebnih podatkov, ki ga v skladu s Splošno uredbo o varstvu podatkov zagotavlja Japonska, potrdila [1] 5. septembra 2018[2]. Evropska komisija je po tem začela postopek za njegov uradni sprejem.

2. Evropska komisija je 25. septembra 2018 za mnenje zaprosila Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: EOVP)[3]. Komisija je morala EOVP predložiti vso potrebno dokumentacijo glede te države, vključno z morebitno ustrezno korespondenco z vlado Japonske.

3. Evropska komisija je ob upoštevanju razprav z EOVP osnutek svojega sklepa o ustreznosti dvakrat spremenila in zadnjo različico poslala 13. novembra 2018[4]. To mnenje EOVP temelji na zadnji različici osnutka izvedbenega sklepa (v nadaljnjem besedilu: osnutek sklepa o ustreznosti).

4. EOVP je raven varstva, zagotovljeno s sklepom Komisije o ustreznosti, ocenil na podlagi proučitve samega sklepa kot tudi analize dokumentacije, ki jo je dala na voljo[5] Komisija[6].

5. EOVP se je osredotočil na oceno tako trgovinskih vidikov osnutka sklepa o ustreznosti kot tudi na dostop vlade do osebnih podatkov, prenesenih iz EU za namene preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj in nacionalne varnosti, vključno s pravnimi sredstvi, ki jih imajo na voljo posamezniki iz EU. Ocenil je tudi, ali so zaščitni ukrepi, ki jih zagotavlja japonski pravni okvir, vzpostavljeni in učinkoviti.

[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.
[2] Glej sporočilo za javnost, dostopno na spletnem naslovu http://europa.eu/rapid/press-release_IP-18-5433_sl.htm.
[3] V skladu s členom 70(1)(s) Splošne uredbe o varstvu podatkov.
[4] Za posodobljeno različico osnutka izvedbenega sklepa Evropske komisije glej Prilogo I k Mnenju EOVP.
[5] Analiza EOVP je temeljila na prevodih, ki so jih zagotovili japonski organi, Evropska komisija pa jih je preverila.
[6] Za seznam dokumentov, ki jih Evropska komisija EOVP ni poslala EOVP, glej Prilogo II k Mnenju EOVP.

6. Pri tem delu je kot glavno izhodišče za svoje delo uporabil referenčni dokument o ustreznosti[7], ki ga je sprejel februarja 2018.

1.1 Področja, o katerih je doseženo soglasje

7. Poglavitni cilj EOVP je bil, da Evropski komisiji poda mnenje o ravni varstva, zagotovljenega posameznikom v japonskem okviru. Pomembno je poudariti, da EOVP ne pričakuje, da bo japonski pravni okvir posnemal zakonodajo EU o varstvu osebnih podatkov.

8. Vendar EOVP opozarja, da tako sodna praksa Sodišča Evropske unije kot člen 45 Splošne uredbe o varstvu podatkov zahtevata, da mora biti zakonodaja tretje države usklajena z bistvom temeljnih načel iz navedene uredbe, da bi se lahko štelo, da zagotavlja ustrezno raven varstva. EOVP na področjih varstva podatkov nadalje ugotavlja, da so med okvirom Splošne uredbe o varstvu podatkov in japonskim okvirom ključna področja približevanja glede nekaterih temeljnih določb, kot so točnost in najmanjši obseg podatkov, omejitev hrambe, varnost podatkov, omejitev namena ter neodvisni nadzorni organ, tj. Komisija za varstvo osebnih podatkov.

9. Poleg tega je EOVP izrazil odobravanje glede prizadevanj Evropske komisije in japonskih organov za to, da bi Japonska zagotavljala ustrezno raven varstva, podobno tisti, zagotovljeni s Splošno uredbo o varstvu podatkov, zlasti z zapolnitvijo vrzeli med navedeno uredbo in japonskim okvirom za varstvo podatkov na način, da bi Komisija za varstvo osebnih podatkov sprejela dodatna pravila, ki bi se uporabljala samo za osebne podatke, prenesene iz EU na Japonsko, t. i. dopolnilna pravila. EOVP na primer ugotavlja, da se je Komisija za varstvo osebnih podatkov strinjala, da bo kot občutljive podatke obravnavala dodatne kategorije podatkov (v skladu z japonsko zakonodajo med občutljive podatke niso vključeni podatki o spolni usmerjenosti in podatki o članstvu v sindikatu). Dopolnilna pravila poleg tega zagotavljajo, da se bodo pravice posameznika, na katerega se nanašajo osebni podatki, uporabljale za vse osebne podatke, prenesene iz EU, ne glede na obdobje njihove hrambe (japonski pravni sistem namreč zagotavlja, da se pravice posameznika, na katerega se nanašajo osebni podatki, ne uporabljajo za osebne podatke, ki bi se morali v šestih mesecih izbrisati).

10. EOVP opaža tudi, da si je Evropska komisija v odziv na njegove pomisleke prizadevala okrepiti sklep o ustreznosti.

1.2 Splošni izzivi

11. Izzivi vseeno ostajajo in EOVP predlaga naslednja glavna področja, ki bi jih bilo treba v japonskem sistemu okrepiti in pazljivo spremljati.

12. Prvi izziv je povezan s spremljanjem te nove zgradbe ustreznosti, ki združuje obstoječi pravni okvir in posebna dopolnilna pravila, da se zagotovi, da bo to trajnosten in zanesljiv sistem, ki ne bo odpiral **praktičnih vprašanj v zvezi s konkretno in učinkovito skladnostjo** japonskih subjektov niti vprašanj Komisije za varstvo osebnih podatkov med izvajanjem.

13. EOVP je seznanjen tudi z večkrat izraženimi zavezami in zagotovili Evropske komisije in japonskih organov glede zavezujoče in izvršljive narave dopolnilnih pravil, hkrati pa Evropsko komisijo poziva, naj **njihovo zavezujočo naravo in učinkovito uporabo na Japonskem stalno spremlja**, saj je njihova pravna veljavnost nujno potrebni element ustreznosti med EU in Japonsko. Meni tudi, da bi bilo glede smernic Komisije za varstvo osebnih podatkov koristno v osnutek sklepa o ustreznosti dodati pojasnila v zvezi z **njihovo zavezujočo naravo, in Komisijo poziva, naj ta vidik pozorno spremlja**[8].

[7] Delovni dokument WP254, referenčni dokument o ustreznosti, 6. februar 2018.
[8] Za več informacij glej razdelek 1.3.4 tega mnenja.

1.3 Posebni trgovinski vidiki

14. EOVP ima nekaj posebnih pomislekov na področju trgovinskih vidikov osnutka sklepa o ustreznosti med EU in Japonsko ter želi pojasnila o nekaterih pomembnih vprašanjih.

1.3.1 Pomisleki EOVP glede ključnih načel varstva podatkov

15. EOVP odobrava, da se z dopolnilnimi pravili izključuje nadaljnji prenos osebnih podatkov, prenesenih iz EU, v tretjo državo na podlagi Skupine za azijsko-pacifiško gospodarsko sodelovanje – sistema o pravilih o varovanju zasebnosti pri čezmejnem prenosu podatkov (v nadaljnjem besedilu: sistem CBPR skupine APEC). Poleg tega ugotavlja, da se je Evropska komisija v novem osnutku sklepa o ustreznosti zavezala, da bo sklep o ustreznosti začasno prenehala izvajati, če nadaljnji prenosi ne bodo več zagotavljali neprekinjenega varstva.

16. V skladu z japonsko zakonodajo je ena od pravnih podlag za nadaljnje prenose priznanje, da je raven varstva v tretji državi skladna z ravnijo, ki jo zagotavlja Japonska. Vendar se zdi, da japonska ocena tretje države kot ustrezne ne vključuje posebnih dopolnilnih pravil, dogovorjenih s pogajanji med Evropsko komisijo in Komisijo za varstvo osebnih podatkov in ki se uporabljajo le za osebne podatke iz EU, da bi se zagotovila raven varstva, ki je v osnovi enakovredna standardom iz Splošne uredbe o varstvu podatkov. Iz tega izhaja, da osebni podatki iz EU, preneseni iz Japonske v drugo tretjo državo, za katero se na podlagi japonske ustreznosti ne priznava, da je njen okvir za varstvo podatkov v osnovi enakovreden Splošni uredbi o varstvu podatkov, ne bodo več nujno uživali posebnega varstva, ki velja za osebne podatke iz EU.

17. **Vendar je treba upoštevati, da se lahko nadaljnji prenosi osebnih podatkov opravijo v tretje države, za katere se začne uporabljati morebitni poznejši japonski sklep o ustreznosti. Te tretje države lahko niso bile predmet prejšnje ocene ali ugotovitve o ustreznosti EU. Na tej točki bi morala Komisija prevzeti vlogo spremljanja in zagotoviti, da se ohrani raven varstva podatkov iz EU, ali razmisliti o začasni odložitvi izvajanja navedenega sklepa o ustreznosti.**

18. EOVP ima poleg tega pomisleke v zvezi s **privolitvijo in obveznostmi glede preglednosti** upravljavcev podatkov (poslovni subjekti, ki ravnajo z osebnimi podatki). Te elemente je pozorno preveril, saj ima v japonskem pravnem sistemu, v nasprotju z zakonodajo EU o varstvu podatkov, osrednjo vlogo uporaba privolitve kot podlage za obdelavo in prenose. Pomisleke ima na primer glede same opredelitve pojma privolitev, saj ta ni opredeljena tako, da bi vključevala pravico do preklica privolitve, ki je v skladu z zakonodajo EU bistveni element, ki posamezniku, na katerega se nanašajo osebni podatki, zagotavlja resnični nadzor nad lastnimi osebnimi podatki. V zvezi z obveznostmi glede preglednosti poslovnih subjektov, ki ravnajo z osebnimi podatki, obstajajo pomisleki glede tega, ali so posameznikom, na katere se nanašajo osebni podatki, zagotovljene proaktivne informacije.

19. Ker Komisija za varstvo osebnih podatkov zagotavlja podporo prek telefonske linije za pomoč strankam in le v japonščini, EOVP izraža zaskrbljenost, da posamezniki iz EU, ki potrebujejo podporo ali želijo vložiti pritožbo, morda težko dostopajo do **japonskega sistema pravnih sredstev**. Enaka težava se pojavlja pri storitvi mediacije, ki jo zagotavlja Komisija za varstvo osebnih podatkov, saj sistem na angleški različici spletne strani te komisije ni objavljen, medtem ko so pomembni informativni dokumenti, kot so pogosto zastavljena vprašanja o zakonu o varstvu osebnih podatkov, na voljo le v japonščini. V zvezi s tem bi EOVP pozdravil prizadevanja Komisije, da bi s Komisijo za varstvo osebnih podatkov razpravljala o možnosti vzpostavitve spletne storitve, podobne tisti, ki je predvidena v Prilogi II k temu sklepu o ustreznosti, ki bi bila vsaj v angleščini ter bi bila namenjena zagotavljanju pomoči posameznikom iz EU in obravnavanju njihovih pritožb. Evropska komisija bo morala prav tako pozorno spremljati tudi učinkovitost sankcij in ustreznih pravnih sredstev.

1.3.2 Potreba po pojasnilu

20. EOVP bi pozdravil zagotovila glede nekaterih vidikov osnutka sklepa o ustreznosti, ki jih je še vedno treba dodatno pojasniti.

21. To se na primer nanašajo na nekatere ključne pojme japonske zakonodaje. Premalo je pojasnjen **status t. i. skrbnika**, tj. pojem, podoben pojmu obdelovalca podatkov v skladu s Splošno uredbo o varstvu podatkov, katerega sposobnost za določanje in spreminjanje namenov in sredstev obdelave osebnih podatkov ostaja nejasna.

22. EOVP bi zaradi pomanjkanja ustreznih dokumentov potreboval zagotovila tudi o tem, ali so **omejitve pravic posameznikov** (zlasti pravic do dostopa, popravka in ugovora) v demokratični družbi potrebne in sorazmerne ter ali spoštujejo bistvo temeljnih pravic.

23. EOVP pričakuje tudi, da bo Evropska komisija pozorno spremljala učinkovito varstvo **osebnih podatkov, prenesenih iz EU na Japonsko, na podlagi osnutka sklepa o ustreznosti, v njihovem celotnem življenjskem ciklu**, čeprav je v japonski zakonodaji določena obveznost vodenja evidenc o izvoru podatkov za največ tri leta.

1.4 O dostopu javnih organov do podatkov, prenesenih na Japonsko

24. EOVP je za japonske vladne subjekte analiziral tudi pravni okvir pri dostopu do osebnih podatkov, prenesenih iz EU na Japonsko za namene preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ali nacionalne varnosti. Čeprav je priznal zagotovila japonske vlade, kot so navedena v Prilogi II k osnutku sklepa o ustreznosti, je opredelil številne vidike, ki jih je treba pojasniti in v zvezi s katerimi obstajajo pomisleki, med katerimi je treba izpostaviti, kot sledi.

25. Na področju preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj EOVP ugotavlja, da se pravna načela, ki se uporabljajo za dostop do podatkov, pogosto zdijo podobna pravilom v EU, kolikor so na voljo. Vendar je zaradi pomanjkanja ustreznih prevodov številnih pravnih besedil in zadevne sodne prakse težko sklepati, da so vsi postopki za dostop do podatkov potrebni in sorazmerni ter da se navedena načela uporabljajo na način, ki je „v osnovi enakovreden“ pravu EU.

26. EOVP na področju nacionalne varnosti ugotavlja, da je japonska vlada znova izjavila, da se lahko informacije pridobijo le iz prosto dostopnih virov ali jih podjetja prostovoljno razkrijejo in da ne zbira informacij o širši javnosti. Vendar se zaveda pomislekov, izraženih s strani strokovnjakov in medijev ter se zavzema, da bi japonski vladni subjekti dodatno pojasnili nadzorne ukrepe.

27. EOVP izraža odobravanje, da sta se Evropska komisija in japonska vlada v zvezi s pravnimi sredstvi posameznikov iz EU na področju preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter nacionalne varnosti s pogajanji dogovorili o dodatnem mehanizmu za posameznike iz EU, da se jim zagotovijo dodatna pravna sredstva, s čimer se razširijo tudi pristojnosti japonskega organa za varstvo podatkov. Vendar ostaja pomislek, da se s tem novim mehanizmom ne nadomeščajo popolnoma pomanjkljivosti nadzornih in pritožbenih mehanizmov v skladu z japonskim pravom. EOVP si torej prizadeva dobiti dodatna pojasnila, da bi ta novi mehanizem popolnoma nadomestil te pomanjkljivosti.

1.5 Sklepna ugotovitev

28. Po mnenju EOVP je ta sklep o ustreznosti ključnega pomena. Kot prvi sklep o ustreznosti, sprejet po začetku veljavnosti Splošne uredbe o varstvu podatkov, bo **precedenčni primer tako za prihodnje vloge za ugotovitev ustreznosti kot tudi za pregled sklepov o ustreznosti, sprejetih na podlagi**

Direktive 95/46/ES[9]. Pomembno je poudariti tudi, da se posamezniki čedalje bolj zavedajo vpliva globalizacije na njihovo zasebnost in pri nadzornih organih poizvedujejo, ali so ob prenosu njihovih osebnih podatkov v tujino vzpostavljena ustrezna zagotovila. EOVP je glede na te posledice prepričan, da bi morala Evropska komisija zagotoviti, da pri varstvu, ki ga zagotavlja ustreznost med EU in Japonsko, ni pomanjkljivosti ter da je ta posebna vrsta ustreznosti usklajena z zahtevami iz člena 45 Splošne uredba o varstvu podatkov.

29. EOVP odobrava prizadevanja Evropske komisije in japonske Komisije za varstvo osebnih podatkov, da bi se japonski pravni okvir čim bolj uskladil z okvirom EU. **Izboljšave**, uvedene z dopolnilnimi pravili za premostitev razlik med obema okviroma, so zelo pomembne in dobro sprejete.

30. Vendar EOVP po temeljiti analizi osnutka sklepa Komisije o ustreznosti ter japonskega okvira za varstvo podatkov opaža, da **ostajajo številni pomisleki, skupaj s potrebo po dodatnih pojasnilih**. Pri tej posebni vrsti ustreznosti, ki združuje veljavni nacionalni okvir in dodatna podrobna pravila, se zastavljajo tudi vprašanja o njenem operativnem izvajanju. Glede na navedeno EOVP priporoča, da Evropska komisija obravnava pomisleke in zahteve za pojasnila, ki jih je navedel, ter v zvezi z obravnavanimi vprašanji predloži dodatne dokaze in pojasnila. Evropsko komisijo poziva še, naj opravi pregled te ugotovitve o ustreznosti (vsaj) vsaki dve leti, ne vsaka štiri leta, kot je predlagano v sedanjem osnutku sklepa o ustreznosti.

2 UVOD

2.1 Pravni okvir Japonske za varstvo podatkov

31. Japonski pravni okvir za varstvo podatkov je bil posodobljen pred kratkim, in sicer leta 2017. Ta okvir zajema več stebrov, v njihovem središču pa je splošno zakonsko pravo, tj. Zakon o varstvu osebnih podatkov (v nadaljnjem besedilu: ZVOP). Še en pomemben zakonodajni akt je odredba kabineta predsednika vlade o uveljavitvi ZVOP (v nadaljnjem besedilu: odredba kabineta), v kateri so podrobno opredeljena nekatera temeljna načela ZVOP.

32. Komisija za varstvo osebnih podatkov ima na podlagi sklepa kabineta, sprejetega 12. junija 2018[10], in člena 6 ZVOP pooblastilo, da *sprejme potrebne ukrepe za premostitev razlik med sistemi in operacijami med Japonsko in zadevnimi tujimi državami, da se zagotovi ustrezno ravnanje z osebnimi podatki, ki jih prejme od vsake države*[11]. V sklepu kabineta je predlagano še, da so pravila, ki jih je sprejela Komisija za varstvo osebnih podatkov in ki dopolnjujejo ali presegajo pravila iz ZVOP, za japonske nosilce dejavnosti zavezujoča in izvršljiva[12].

33. Skladno s tem je Komisija za varstvo osebnih podatkov začela pogajanja z Evropsko komisijo in junija 2018 sprejela pravila, strožja od pravil v ZVOP in odredbi kabineta, ki bi jih bilo treba uporabljati za podatke, prenesene iz EU. To so dopolnilna pravila v skladu z Zakonom o varstvu osebnih podatkov za ravnanje z osebnimi podatki, prenesenimi iz EU, ki temelji na sklepu o ustreznosti (v nadaljnjem

[9] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.
[10] EOVP ugotavlja, da je bil glede na osnutek sklepa o ustreznosti ta sklep kabineta sprejet 12. junija 2018. Vendar mu je bil poslan le osnutek sklepa kabineta iz aprila 2018.
[11] Sklep kabineta z dne 25. aprila 2018.
[12] Za več informacij glej razdelek 1.3.4 v nadaljevanju.

besedilu: dopolnilna pravila)[13]. Ta dopolnilna pravila so tudi priložena osnutku izvedbenega sklepa Komisije, objavljenega julija 2018.

34. Opozoriti je treba, da se dopolnilna pravila uporabljajo le za osebne podatke, ki se iz Evropske unije na Japonsko prenašajo na podlagi sklepa o ustreznosti, in da je njihov namen izboljšati veljavno varstvo teh podatkov. Kot taka se ne uporabljajo za osebne podatke posameznikov na Japonskem ali posameznikov iz držav, ki niso države EGP.

35. EOVP želi opozoriti še na dejstvo, da je začel spremenjeni ZVOP veljati 30. maja 2017 in da je bila Komisija za varstvo osebnih podatkov v sedanji obliki ustanovljena leta 2016. Poleg tega dopolnilna pravila, o katerih se je Komisija za varstvo osebnih podatkov dogovorila na pogajanjih z Evropsko komisijo, še niso začela veljati, saj bo to odvisno od tega, ali bo Evropska komisija Japonsko priznala kot sodno pristojnost, ki ustreza sodni pristojnosti v EU.

2.2 Obseg ocene EOVP

36. Osnutek sklepa Evropske komisije o ustreznosti varstva podatkov je rezultat ocene japonskih pravil o varstvu podatkov, čemur so sledila pogajanja z japonskimi organi. Izid teh pogajanj je viden zlasti v dveh prilogah k osnutku sklepa o ustreznosti: prva določa dodatne zaščitne ukrepe, ki jih bodo morali japonski poslovni subjekti uporabljati pri obdelavi osebnih podatkov, prenesenih iz EU, druga pa vsebuje zagotovila in zaveze japonske vlade v zvezi z dostopom javnih organov do podatkov.

37. EOVP je proučil japonski okvir za varstvo podatkov, dopolnilna pravila, o katerih se je pogajala Evropska komisija, ter zagotovila in zaveze japonske vlade. Pričakuje se, da bo pripravil neodvisno mnenje o ugotovitvah Evropske komisije, opredelil morebitne pomanjkljivosti v okviru ustreznosti in si prizadeval predlagati spremembe ali popravke za njihovo odpravo.

38. Kot je navedeno v referenčnem dokumentu o ustreznosti EOVP, *bi morale biti informacije, ki jih zagotovi Evropska komisija, izčrpne in EOVP omogočati, da izvede lastno oceno o ravni varstva podatkov v tretji državi[14].*

39. Kljub temu je EOVP večino dokumentov prejel prevedenih v angleščino, na katere so navedeni sklici v osnutku sklepa o ustreznosti in ki so ključni del japonskega pravnega sistema. Zato to mnenje pripravlja na podlagi analize razpoložljivih dokumentov v angleščini. EOVP je upošteval veljavni okvir varstva podatkov v Evropski uniji, vključno s členom 8 Evropske konvencije o človekovih pravicah (v nadaljnjem besedilu: EKČP) o varstvu pravice do zasebnega in družinskega življenja ter členi 7, 8 in 47 Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina) o varstvu pravice do zasebnega in družinskega življenja, pravice do varstva osebnih podatkov oziroma pravice do učinkovitega pravnega sredstva in nepristranskega sojenja. Poleg navedenega je proučil tudi zahteve iz Splošne uredbe o varstvu podatkov in pregledal ustrezno sodno prakso.

40. S tem je nameraval zagotoviti, da bi bil japonski okvir za varstvo podatkov v osnovi enakovreden okviru Evropske unije. Sodišče Evropske unije je še dodatno razvilo pojem ustrezne ravni varstva, ki je obstajal že na podlagi Direktive 95/46/ES. Opozoriti je treba na standard, ki ga je Sodišče Evropske unije določilo v zadevi Schrems, in sicer da mora biti raven varstva v tretji državi „v bistvenem enakovredna“ varstvu, zagotovljenem v EU – „[...] so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva,

[13] Dopolnilna pravila, Priloga I k Izvedbenemu sklepu Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan septembra 2018.

[14] Delovni dokument WP254, str. 3.

lahko drugačna od sredstev, uporabljenih znotraj [Unije]“[15]. Cilj torej ni, da bi se zakonodaja EU odražala od točke do točke, temveč da bi se določile bistvene in temeljne zahteve zakonodaje, ki se pregleduje. Ustreznost je mogoče doseči s kombinacijo pravic za posameznike, na katere se nanašajo osebni podatki, in obveznosti tistih, ki obdelujejo podatke ali izvajajo nadzor nad takšno obdelavo, ter nadzora, ki ga izvajajo neodvisni organi. Vendar so pravila za varstvo podatkov učinkovita le, če so izvršljiva in se jim v praksi sledi. Zato je treba upoštevati ne le vsebino pravil, ki se uporabljajo za osebne podatke, prenesene v tretjo državo ali mednarodno organizacijo, temveč tudi vzpostavljeni sistem, ki zagotavlja učinkovitost takih pravil. Učinkoviti mehanizmi izvajanja[16] so bistvenega pomena za učinkovitost pravil o varstvu podatkov.

2.3 Splošne pripombe in pomisleki

2.3.1 Posebnosti tovrstnega sklepa o ustreznosti

41. Ustreznost med EU in Japonsko je prva, ki jo je treba proučiti glede na novo pravno podlago Splošne uredbe o varstvu podatkov. Zaradi tega je delo EOVP še toliko pomembnejše, pri čemer je treba upoštevati učinke tega osnutka sklepa o ustreznosti za prihodnje vloge za ugotovitev ustreznosti.

42. Ustreznost med EU in Japonsko bi bila tudi prva medsebojna ustreznost. Ko in če bo EU ugotovila, da Japonska zagotavlja raven varstva, ki je v osnovi enakovredna tisti iz Splošne uredbe o varstvu podatkov, bo tudi Japonska izdala svoj sklep o ustreznosti v skladu s členom 24 ZVOP, s čimer bo potrdila, da EU zagotavlja ustrezno raven varstva v skladu z japonskim okvirom za varstvo podatkov. Zato je ta predvidena ustreznost med EU in Japonsko posebna, kar je EOVP upošteval pri svoji oceni. Kot je bilo navedeno zgoraj, se je japonska Komisija za varstvo osebnih podatkov na pogajanjih z Evropsko komisijo dogovorila o posebnih, strožjih pravilih, ki se uporabljajo le za osebne podatke, prenesene iz EU. Ta strožja pravila so zavezujoča in izvršljiva v skladu s sklepom kabineta in jih morajo pri obdelavi osebnih podatkov iz EU v skladu s tem osnutkom sklepa o ustreznosti upoštevati vsi poslovni subjekti.

43. Evropska komisija se pri svoji ugotovitvi o ustreznosti tako ni oprla le na veljavni splošni japonski okvir za varstvo podatkov, temveč tudi na ta posebna pravila. Dejstvo, da so bila za dopolnitev ZVOP potrebna dopolnilna pravila, kaže na to, da Evropska komisija potrjuje, da japonska zakonodaja o varstvu osebnih podatkov sama po sebi ni v osnovi v bistvenem enakovredna Splošni uredbi o varstvu podatkov.

44. **EOVP glede na navedeno Evropsko komisijo poziva, naj zagotovi, da bo ta nova zgradba ustreznosti, ki naj bi bila prva, ki bo sprejeta v skladu s Splošno uredbo o varstvu podatkov in bo temeljila na dopolnilnih pravilih, trajnosten in zanesljiv sistem, v okviru katerega se ne bodo odpirala praktična vprašanja o konkretni in učinkoviti skladnosti japonskih subjektov ali o uveljavljanju s strani Komisije za varstvo osebnih podatkov .**

2.3.2 Zanesljivost prevodov

45. Delo EOVP je tako kot delo Evropske komisije temeljilo na angleških prevodih, zagotovljenih s strani japonskih organov[17]. EOVP Evropsko komisijo poziva, naj pojasni, da je osnutek sklepa o ustreznosti utemeljila na prejetih angleških prevodih, ter naj redno preverja kakovost in zanesljivost teh prevodov.

[15] Sodba Sodišča z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, točki 73 in 74.
[16] Delovni dokument WP254, str. 3.
[17] Evropska komisija je te prevode preverila.

2.3.3 Sektorska ustreznost

46. Ugotovitev ustreznosti tega osnutka sklepa o ustreznosti je omejena na varstvo osebnih podatkov, ki ga v smislu ZVOP zagotavljajo poslovni subjekti, ki ravnajo z osebnimi podatki. To pomeni, da je ustreznost sektorska, saj se uporablja le za zasebni sektor, pri čemer so z njenega področja uporabe izključeni prenosi osebnih podatkov med javnimi organi in telesi. Evropska komisija za zdaj bežno omenja to posebnost področja uporabe ustreznosti v uvodni izjavi 10 osnutka sklepa o ustreznosti.

47. **EOVP Evropsko komisijo poziva, naj sektorsko naravo te ugotovitve o ustreznosti izrecno omeni v naslovu izvedbenega sklepa in v členu 1 navedenega sklepa v skladu s členom 45(3) Splošne uredbe o varstvu podatkov.**

2.3.4 Zavezujoča narava dopolnilnih pravil in smernic Komisije za varstvo osebnih podatkov

48. V členu 6 ZVOP je navedeno, da *vlada [...] sprejme potrebne zakonodajne in druge ukrepe, da bi lahko sprejela diskretne ukrepe za varstvo osebnih podatkov, pri katerih je treba zaradi boljšega varstva pravic in interesov posameznika zlasti zagotoviti natančno izvajanje njihove primerne obdelave, ter v sodelovanju z vladami drugih držav sprejme potrebne ukrepe za vzpostavitev mednarodno primernega sistema v zvezi z osebnimi podatki, tako da spodbuja sodelovanje z mednarodno organizacijo in drugim mednarodnim okvirom*. Čeprav ta člen ZVOP vlado jasno opredeljuje kot pristojno za sprejemanje takih pravnih ukrepov, ne vsebuje neposrednega sklica na Komisijo za varstvo osebnih podatkov kot pristojni organ za sprejemanje posebnih pravil[18]. Zaradi časovnih omejitev EOVP na tej točki ni mogel zbrati, pregledati in proučiti obstoječih dokazov.

49. **EOVP je ob upoštevanju pomena tega vprašanja seznanjen s ponavljajočimi zavezami in zagotovili Evropske komisije in japonskih organov glede zavezujoče in izvršljive narave dopolnilnih pravil. Evropsko komisijo poziva, naj njihovo zavezujočo naravo in učinkovito uporabo na Japonskem stalno spremlja, saj je njihova pravna veljavnost bistven element ustreznosti med EU in Japonsko.**

50. Poleg tega se Evropska komisija v več poglavjih osnutka sklepa o ustreznosti sklicuje na smernice Komisije za varstvo osebnih podatkov (v nadaljnjem besedilu: smernice).

51. Čeprav Evropska komisija v uvodni izjavi 16 osnutka sklepa o ustreznosti pojasnjuje, da smernice zagotavljajo verodostojno razlago ZVOP, se v isti uvodni izjavi sklicuje na zavezujočo naravo teh smernic: „Glede na informacije, prejete od Komisije za varstvo osebnih podatkov, se te smernice obravnavajo kot zavezujoča pravila, ki so sestavni del pravnega okvira, ter jih je treba brati skupaj z besedilom ZVOP, odredbo kabineta, pravili o varstvu osebnih podatkov in sklopom vprašanj in odgovorov, ki jih je pripravila Komisija za varstvo osebnih podatkov“[19].

52. Vendar EOVP na podlagi istih informacij, ki jih je poslala komisija za varstvo osebnih podatkov, razume, da smernice niso pravno zavezujoče. Zagotavljajo pa verodostojno razlago zakona. Komisija za varstvo osebnih podatkov trdi, da smernice v praksi upoštevajo poslovni subjekti, ki obdelujejo osebne podatke, uporablja pa jih Komisija za varstvo osebnih podatkov pri izvajanju zakonodaje proti tem subjektom in sodišča pri sprejemanju sodb. Vendar ti elementi niso zadostni dokaz, da smernice predstavljajo pravno zavezujoče norme.

[18] Pravno zavezujoča narava dopolnilnih pravil je bila glede na članek, objavljen julija 2018, ko so bila ta pravila šele na stopnji priprave osnutka, verjetno predmet notranje razprave v državi. Glej Fujiwara, S., Comparison between the EU and Japan’s Data Protection Legal Frameworks’, revija Jurist, zvezek 1521 (julij 2018), str. 19.

[19] Uvodna izjava 16 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

53. **EOVP meni, da bi bilo koristno v sklep o ustreznosti dodati pojasnila v zvezi z zavezujočo naravo smernic Komisije za varstvo osebnih podatkov, in Evropsko komisijo poziva, naj ta vidik pozorno spremlja.**

54. Komisija za varstvo osebnih podatkov navaja, da se smernice v praksi vseeno upoštevajo, saj gre za lokalno navado. Po njenih navedbah japonska sodišča uporabljajo te smernice pri sprejemanju sodb, ko uporabljajo pravila ZVOP. Za zagotovitev dokaza, da se japonska sodišča pri svojih ugotovitvah opirajo na smernice, je Evropska komisija navedla sklic na sodno odločbo[20] iz leta 2006. Čeprav EOVP ta sodna odločba ni bila predložena, bi bil hvaležen, če bi mu lahko Evropska komisija poslala novejšo sodno odločbo, če je na voljo, bodisi s področja varstva podatkov bodisi iz drugega sektorja, v katerem so japonska sodišča kot podlago za svojo odločitev uporabila smernice Komisije za varstvo osebnih podatkov ali druge podobne smernice.

2.3.5 Redni pregled ugotovitve o ustreznosti

55. V členu 45(3) Splošne uredbe o varstvu podatkov je določeno, da je treba vsaj vsaka štiri leta izvesti redni pregled. V skladu z referenčnim dokumentom[21] o ustreznosti EOVP je to splošni časovni okvir, ki ga je treba prilagoditi posamezni tretji državi ali mednarodni organizaciji i s sklepom o ustreznosti. Glede na posebne obravnavane okoliščine je lahko upravičen krajši cikel pregledov. Potreba po pregledu, ki se izvede prej od predvidenega, se lahko pojavi tudi zaradi izrednih dogodkov ali drugih informacij o pravnem okviru ali sprememb tega okvira v zadevni tretji državi ali mednarodni organizaciji. Poleg tega se zdi primerno, da se prvi pregled povsem novega sklepa o ustreznosti izvede dokaj kmalu, pogostnost pregledov pa se potem postopoma prilagodi glede na rezultat.

56. **EOVP Evropsko komisijo poziva, naj pregled te ugotovitve o ustreznosti izvede (vsaj) vsaki dve leti, ne vsaka štiri leta, kot je predlagano v sedanjem osnutku sklepa o ustreznosti**, pri čemer upošteva številne dejavnike, vključno z dejstvi, da je ZVOP začel veljati leta 2017, da je bila Komisija za varstvo osebnih podatkov ustanovljena leta 2016 in da še ni informacij ali dokazov o praktični uporabi dopolnilnih pravil.

2.3.6 Mednarodne zaveze, ki jih je sprejela Japonska

57. Evropska komisija mora pri ocenjevanju ustreznosti ravni varstva tretje države v skladu s členom 45(2)(c) Splošne uredbe o varstvu podatkov in referenčnim dokumentom o ustreznosti[22] med drugim upoštevati mednarodne zaveze, ki jih je sprejela tretja država, ali druge obveznosti, ki izhajajo iz sodelovanja tretje države v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov, ter izvajanje takih zavez. Poleg tega bi bilo treba upoštevati zlasti pristop tretje države h Konvenciji Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (t. i. Konvencija 108+) [23] in Dodatnemu protokolu h Konvenciji.

58. **EOVP v zvezi s tem opozarja, da je Japonska opazovalka posvetovalnega odbora Konvencije 108+.**

[20] Opomba 16 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018, na strani 5; sodba okrajnega sodišča v Osaki z dne 19. maja 2006 v zadevi Hanrei Jiho, zvezek 1948, str. 122.

[21] Delovni dokument WP254, str. 3.

[22] Delovni dokument WP254, str. 3.

[23] Konvencija o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Konvencija 108+, 18. maj 2018.

2.3.7 Pooblastila nadzornih organov za varstvo podatkov[24] za vložitev tožb v zvezi z veljavnostjo sklepa o ustreznosti na sodišču

59. EOVP poudarja, da čeprav so v uvodni izjavi 179 osnutka sklepa o ustreznosti navedeni le primeri, v katerih nadzorni organ za varstvo podatkov prejme pritožbo, v kateri je izražen dvom o združljivosti sklepa o ustreznosti s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, je treba to izjavo razumeti kot primer okoliščin, ko lahko nadzorni organ za varstvo podatkov zadevo predloži nacionalnemu sodišču, kar bi lahko bilo mogoče tudi brez pritožbe, ne pa kot omejitev pooblastil nadzornih organov za varstvo podatkov v skladu s Splošno uredbo o varstvu podatkov in nacionalno zakonodajo držav članic na tem področju. V določbe Splošne uredbe o varstvu podatkov sta dejansko vključeni pooblastili za začasno ustavitev prenosov podatkov, tudi če temeljijo na sklepu o ustreznosti, in za vložitev tožbe v zvezi z veljavnostjo sklepa o ustreznosti, ki nista omejeni na zadeve, v katerih je bila prejeta pritožba, če bi jim njihova nacionalna zakonodaja dovoljevala, da to storijo bolj na splošno in neodvisno od pritožbe v skladu z ustreznimi določbami Splošne uredbe o varstvu podatkov.

60. **EOVP Evropsko komisijo poziva, naj v osnutku sklepa o ustreznosti pojasni, da je pooblastilo nadzornih organov, da na podlagi pritožbe vložijo tožbo proti veljavnosti sklepa o ustreznosti, le prikaz širših pooblastil organov za varstvo podatkov na podlagi Splošne uredbe o varstvu podatkov, med katere sta vključeni pooblastili za začasno ustavitev prenosov in za vložitev tožbe v zvezi z veljavnostjo sklepa o ustreznosti, kadar pritožba ni bila vložena, če je tako določeno v njihovi nacionalni zakonodaji.**

3 TRGOVINSKI VIDIKI

3.1 Vsebinska načela

61. Poglavje 3 referenčnega dokumenta o ustreznosti je namenjeno vsebinskim načelom. Sistem tretje države ali mednarodne organizacije jih mora vsebovati, da bi se lahko štelo, da je zagotovljena raven varstva v osnovi enakovredna tisti, ki jo zagotavlja zakonodaja EU. EOVP se zaveda, da se pristop japonskega pravnega sistema pri uveljavljanju pravice do zasebnosti razlikuje od pristopa Splošne uredbe o varstvu podatkov. Čeprav pravica do zasebnosti sama po sebi ni vključena v japonsko ustavo, je bila kot ustavna pravica priznana skozi sodno prakso, kot je navedeno tudi v sklepu Evropske komisije[25].

62. Zaradi precejšnjih razlik med japonskim in evropskim pristopom je treba zlasti pozorno opazovati, ali posamezni vidiki in sistem kot celota nazadnje zagotavljajo „bistveno enakovredno“ raven varstva. To pomeni, da se lahko morebitne pomanjkljivosti, ki se nanašajo na eno vsebinsko načelo, nadomestijo z nekaterimi drugimi vidiki, ki zagotavljajo ustrezna preverjanja in ravnovesja.

3.1.1 Pojmi

63. Na podlagi referenčnega dokumenta o ustreznosti bi morali v pravnem okviru tretje države obstajati temeljni pojmi in/ali načela varstva podatkov. Čeprav ni treba, da bi odražali terminologijo Splošne uredbe o varstvu podatkov, bi morali izražati pojme iz zakonodaje EU o varstvu podatkov ali biti skladni z njimi. Splošna uredba o varstvu podatkov na primer zajema naslednje pomembne pojme: osebni

[24] Sodba Sodišča z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14.

[25] EOVP ni prejel angleškega prevoda te sodne odločbe. Glej opombo 9 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

podatki, obdelava osebnih podatkov, upravljavec podatkov, obdelovalec podatkov, uporabnik in občutljivi podatki[26].

64. Tudi ZVOP vsebuje številne opredelitve pojmov, kot so med drugim osebni podatki in poslovni subjekt, ki ravna z osebnimi podatki. **Vendar se zdi, da ZVOP ne vsebuje opredelitve pojma ravnanje z osebnimi podatki, ki je podoben pojmu obdelava osebnih podatkov.**

65. Komisija za varstvo osebnih podatkov je glede opredelitve pojma ravnanje z osebnimi podatki pisno odgovorila na vprašanje EOVP v zvezi s to opredelitvijo. Evropska komisija je ta odgovor navedla v osnutku sklepa Komisije: „*Čeprav se v ZVOP pojem obdelava ne uporablja, se nanaša na enakovreden pojem ravnanje, ki glede na informacije, ki jih prejme Komisija za varstvo osebnih podatkov, zajema kakršno koli dejanje v zvezi z osebnimi podatki, vključno s pridobivanjem, vnosom, zbiranjem, organizacijo, shranjevanjem, urejanjem/obdelavo, obnovitvijo, iznosom, ponovnim potrjevanjem, uporabo ali zagotavljanjem osebnih podatkov.“*[27]

66. Vendar ker EOVP besedilo te opredelitve ni bilo predloženo, **Evropsko komisijo poziva, naj pozorno spremlja, ali se opredelitev navedenega pojma, kot jo je poslala Komisija za varstvo osebnih podatkov, dejansko spoštuje v praksi**.

3.1.1.1 Pojem obdelovalca podatkov in obveznosti skrbnika

67. Kot je bilo navedeno zgoraj, bi morali na podlagi referenčnega dokumenta o ustreznosti v pravnem okviru tretje države obstajati temeljni pojmi in/ali načela varstva podatkov.

68. V ZVOP je opredeljen pojem poslovni subjekt, ki ravna z osebnimi podatki, ki po navedbah Evropske komisije obsega oba pojma, upravljavec podatkov in obdelovalec podatkov, kot sta določena v Splošni uredbi o varstvu podatkov, in ne razlikuje med njima[28]. Vendar je v člen 22 ZVOP vključen pojem skrbnik, ki je v nekaterih pogledih podoben pojmu obdelovalec podatkov v skladu s Splošno uredbo o varstvu podatkov.

69. Kot je Komisija za varstvo osebnih podatkov pojasnila v svojih odgovorih, poslanih EOVP, in kot je navedeno v osnutku sklepa Evropske komisije o ustreznosti, se skrbnik šteje za enakovrednega obdelovalcu podatkov na podlagi Splošne uredbe o varstvu podatkov, saj mu poslovni subjekt, ki ravna z osebnimi podatki, zaupa ravnanje z osebnimi podatki. Skrbnik ima enake obveznosti in pravice kot kateri koli poslovni subjekt, ki ravna z osebnimi podatki, vključno s tistimi iz dopolnilnih pravil za osebne podatke, prenesene iz EU. Poslovni subjekt, ki ravna z osebnimi podatki, ki skrbniku zaupa ravnanje z osebnimi podatki, mora nad skrbnikom *izvajati potreben in ustrezen nadzor*[29].

70. **EOVP Evropsko komisijo poziva, naj pojasni status in obveznosti skrbnika, kadar ta spremeni namene in sredstva obdelave, ter pojasni, ali privolitev posameznika, na katerega se nanašajo osebni podatki, ostaja nujen pogoj za takšno spremembo namena ali določitev sredstev[30].**

---

[26] Delovni dokument WP254, str. 4.

[27] Uvodna izjava 17 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

[28] Uvodna izjava 35 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

[29] Člen 22 spremenjenega zakona o varstvu osebnih podatkov, ki je začel veljati 30. maja 2017.

[30] Člen 23(5)(i) ZVOP. Glej tudi razdelek o načelu preglednosti v nadaljevanju.

3.1.1.2 Pojem shranjenih osebnih podatkov

71. ZVOP vsebuje pojem shranjeni osebni podatki, ki se šteje kot podkategorija osebnih podatkov. V skladu z ZVOP se določbe o pravicah posameznika, na katerega se nanašajo osebni podatki[31], uporabljajo le za shranjene osebne podatke. Opredelitev pojma shranjeni osebni podatki je vključena v člen 2(7) ZVOP.

72. Shranjeni osebni podatki so osebni podatki, razen tistih, (i) ki jih je treba izbrisati v največ šestih mesecih[32] ali (ii) ki spadajo med izjeme iz člena 4 odredbe kabineta in lahko škodijo javnim ali drugim interesom, če je njihova prisotnost ali odsotnost znana.

73. V dopolnilnem pravilu 2 je določeno, da *se osebni podatki, prejeti iz EU na podlagi sklepa o ustreznosti, obravnavajo kot shranjeni osebni podatki ne glede na obdobje, v katerem je treba podatke izbrisati*.

74. Vendar z osebnimi podatki, za katere veljajo izjeme iz člena 4 odredbe kabineta, ne bo treba ravnati kot s shranjenimi osebnimi podatki, pravice posameznikov, na katere se nanašajo osebni podatki, pa se ne bodo uporabljale.

75. V členu 23 Splošne uredbe o varstvu podatkov je tako kot v členu 4 odredbe kabineta določeno, da lahko pravo Unije ali pravo države članice, ki velja za upravljavca/obdelovalca podatkov, omeji obseg obveznosti, ki se uporabljajo zanj, in pravic, ki jih ima posameznik, na katerega se nanašajo osebni podatki. To se lahko stori z zakonodajnim ukrepom. Te omejitve morajo spoštovati bistvo temeljnih pravic in svoboščin ter biti potreben in sorazmeren ukrep v demokratični družbi.

76. EOVP v zvezi z vsebino izjem iz člena 4 odredbe kabineta ni prejel zadostne dokumentacije o teh omejitvah ali dodatnih elementov za pojasnitev področja uporabe teh določb[33]. EOVP ne more oceniti, ali so te omejitve pravic posameznikov, na katere se nanašajo osebni podatki, omejene na to, kar bi se štelo za nujno potrebno in sorazmerno v skladu z zakonodajo EU, in bi bilo zato v osnovi enakovredno pravicam posameznikov iz EU, na katere se nanašajo osebni podatki.

77. **EOVP bi zaradi pomanjkanja nekaterih ustreznih dokumentov pozdravil zagotovila Evropske komisije tudi o tem, ali so omejitve pravic posameznikov (zlasti pravice dostopa ter pravic do popravka in ugovora) v demokratični družbi potrebne in sorazmerne ter ali spoštujejo bistvo temeljnih pravic.**

78. Bistvena zahteva v skladu s Splošno uredbo o varstvu podatkov je, da so osebni podatki zaščiteni v njihovem celotnem življenjskem ciklu.

79. Ob upoštevanju dejstva, da se dopolnilna pravila uporabljajo le za osebne podatke, prenesene iz EU, bi EOVP želel prejeti dodatne informacije o tem, kako poslovni subjekti, ki ravnajo z osebnimi podatki, ta pravila izvajajo v praksi, zlasti kadar se ti podatki po prvem prenosu na Japonsko posredujejo naprej drugemu poslovnemu subjektu, ki ravna z osebnimi podatki.

80. Evropska komisija je v uvodni izjavi 15 osnutka sklepa o ustreznosti pojasnila, da bodo poslovni subjekti, ki ravnajo z osebnimi podatki, ki sprejemajo in/ali dodatno obdelujejo osebne podatke iz EU, pravno zavezani k spoštovanju dopolnilnih pravil, zaradi česar bodo morali zagotoviti, da bo take osebne podatke mogoče identificirati v njihovem celotnem življenjskem ciklu.

---

[31] Členi 27–30 ZVOP.

[32] Člen 5 spremembe odredbe kabineta predsednika vlade o izvajanju zakona o varstvu osebnih podatkov, ki je začel veljati 30. maja 2017.

[33] EOVP niso bile poslane odločitve vrhovnega sodišča iz uvodne izjave 53 osnutka sklepa o ustreznosti.

81. Komisija za varstvo osebnih podatkov[34] je v odgovorih pojasnila, da bo taka identifikacija izvedena s tehničnimi (označevanje) ali organizacijskimi metodami (shranjevanje podatkov iz EU v namensko podatkovno zbirko).

82. Evropska komisija v opombi 14 osnutka sklepa o ustreznosti pojasnjuje, da morajo poslovni subjekti, ki ravnajo z osebnimi podatki, podatke o izvoru podatkov iz EU shranjevati tako dolgo, kot je to potrebno, da bo mogoče zagotoviti skladnost z dopolnilnimi pravili. To je zapisano tudi v členu 26(1), (3) in (4) ZVOP, v katerem je navedeno, da mora poslovni subjekt, ki ravna z osebnimi podatki, potrditi in evidentirati vir teh podatkov ter vse okoliščine v zvezi s pridobivanjem teh podatkov.

83. Vendar EOVP ugotavlja, da člen 18 Pravil o varstvu osebnih podatkov[35] določa, da so obveznosti za vodenje evidenc poslovnih subjektov, ki ravnajo z osebnimi podatki, omejene na največ tri leta za primere, ki ne spadajo na področje uporabe posebnih metod vodenja evidenc, opisanih v členu 16 Pravil o varstvu osebnih podatkov (uporaba pisnega dokumenta, elektromagnetnega zapisa ali mikrofilma). To je navedla tudi Evropska komisija v uvodni izjavi 71 osnutka sklepa o ustreznosti: „Kot je določeno v členu 18 Pravil o varstvu osebnih podatkov, je treba te evidence hraniti od enega do treh let, odvisno od okoliščin.“

84. Čeprav – kot je navedla Evropska komisija v opombi 14 osnutka sklepa o ustreznosti, poslovnim subjektom, ki ravnajo z osebnimi podatki – ni prepovedano voditi evidence o izvoru podatkov za obdobje, daljše od treh let, da bi lahko izpolnili svoje obveznosti v skladu z dopolnilnim pravilom 2, to ni jasno izraženo niti v japonski zakonodaji niti v dopolnilnih pravilih. EOVP meni, da obstaja tveganje, da bodo poslovni subjekti, ki ravnajo z osebnimi podatki, zahteve iz člena 18 Pravil o varstvu osebnih podatkov, dejansko izpolnjevali tudi pri obdelavi podatkov, ki izvirajo iz EU. Glede na razumevanje EOVP in na podlagi razpoložljivih dokumentov je tako predvsem zato, ker za zdaj ni določbe, ki bi poslovnim subjektom, ki ravnajo z osebnimi podatki, namesto tega nalagala tako obveznost o upoštevanju dopolnilnih pravil. To bi privedlo do tega, da podatki, preneseni iz EU, ne bi bili več zaščiteni z dodatnimi varovalkami, vključenimi v dopolnilna pravila.

85. **EOVP Evropsko komisijo poziva, naj pozorno spremlja učinkovito varstvo osebnih podatkov, prenesenih iz EU na Japonsko, na podlagi osnutka sklepa o ustreznosti, v njihovem celotnem življenjskem ciklu, čeprav je v japonski zakonodaji določena obveznost vodenja evidenc o izvoru podatkov za največ tri leta.**

3.1.2 Razlogi za zakonito in pošteno obdelavo podatkov za zakonite namene

86. V skladu z referenčnim dokumentom o ustreznosti in na podlagi Splošne uredbe o varstvu podatkov je treba podatke obdelovati zakonito, pošteno in legitimno[36]. Pravno podlago, v skladu s katero se lahko osebni podatki zakonito, pošteno in legitimno obdelujejo, je treba dovolj jasno določiti. Evropski okvir priznava več takih zakonitih podlag, vključno z na primer določbami v nacionalni zakonodaji, privolitvijo posameznika, na katerega se nanašajo osebni podatki, izvajanjem pogodbe ali zakonitim interesom upravljavca podatkov ali tretje osebe, ki ne prevlada nad interesi posameznika.

87. V skladu z ZVOP ima v japonskem pravnem sistemu za varstvo podatkov privolitev osrednjo vlogo. Privolitev je osrednja pravna podlaga za obdelavo osebnih podatkov na Japonskem in tudi ena od glavnih pravnih podlag za prenose osebnih podatkov iz Japonske v tretjo državo. Poleg tega je privolitev potrebna tudi za spremembo namena obdelave.

[34] Priloga III k temu mnenju.
[35] Člen 16 pravil o izvajanju zakona o varstvu osebnih podatkov (v nadaljnjem besedilu: pravila o varstvu osebnih podatkov), ki je začel veljati 30. maja 2017.
[36] Delovni dokument WP254, str. 4.

88. V skladu z dopolnilnim pravilom 3 bo pravna podlaga za obdelavo osebnih podatkov, prenesenih iz EU na Japonsko, tista pravna podlaga, glede na katero se podatki prenesejo na Japonsko. Če želi poslovni subjekt, ki ravna z osebnimi podatki, te podatke nadalje obdelovati za drug namen, mora predhodno pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki.

89. Po mnenju EOVP mora biti kakovost privolitve, zlasti zaradi njene osrednje vloge v japonskem pravnem okviru, skladna s temeljnimi zahtevami pojma privolitve, tj. v skladu s pravom EU „prostovoljno, specifično, informirano in nedvoumno ravnanje [...], iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki [...]“. Posameznik, na katerega se nanašajo osebni podatki, lahko svojo privolitev kadar koli prekliče, kar je ključni zaščitni ukrep za zagotovitev njegove svobodne volje[37]. Zdi se, da v japonskem pravnem okviru kot obvezni element privolitve manjka pravica do preklica privolitve. V skladu s smernicami Komisije za varstvo osebnih podatkov[38] je preklic privolitve dejansko le zaželen ter pogojen z značilnostmi, velikostjo in statusom poslovnih dejavnosti.

3.1.3 Načelo preglednosti

90. Preglednost je na podlagi člena 5 Splošne uredbe o varstvu podatkov temeljno načelo sistema EU za varstvo podatkov[39]. V referenčnem dokumentu o ustreznosti je preglednost navedena kot eno od vsebinskih načel, ki jih je treba upoštevati pri ocenjevanju bistveno enakovredne ravni varstva, ki jo zagotavlja tretja država. Z načeloma preglednosti in pravičnosti se prizadeva, da bi imel posameznik, na katerega se nanašajo osebni podatki, nadzor nad svojimi podatki in da bi se mu informacije v ta namen praviloma zagotavljale proaktivno. V primeru zasebnostnega ščita se je Delovna skupina iz člena 29[40] v Mnenju št. 1/2016 sklicevala na prilogi II in II.1.b k sporazumu o zasebnostnem ščitu (obvestilo posamezniku) ter navedla, da bi morala organizacija posameznika, na katerega se nanašajo osebni podatki, uradno obvestiti, ko organizacija v zasebnostnem ščitu evidentira podatke, če se podatki ne zbirajo neposredno (razdelek 2.2.1.a). Dodatno merilo je javno dostopna politika zasebnosti (glej razdelek 2.2.1.b). Že v skladu z Direktivo 95/46/ES se je neposredno obveščanje posameznika, na katerega se nanašajo osebni podatki, torej štelo za potrebno.

91. Pojavljajo se pomisleki glede načina zagotavljanja informacij posamezniku, na katerega se nanašajo osebni podatki, v skladu z ZVOP. Poslovni subjekt, ki ravna z osebnimi podatki, mora v skladu s členom 27(1) ZVOP zagotoviti informacije iz tega člena tako, da jih pretvori v obliko, v kateri je pooblastitelj lahko z njimi seznanjen. Vendar to besedilo ne pojasnjuje, v kakšnem obsegu mora poslovni subjekt, ki ravna z osebnimi podatki, sprejeti pozitivne ukrepe za dejansko obveščanje posameznika, na katerega se nanašajo osebni podatki.

---

[37] Glej člen 4(11) splošne uredbe o varstvu podatkov. Za več informacij glej tudi ustrezne smernice EOVP o privolitvi, delovni dokument WP259, 10. april 2018.

[38] Data Protection Legal and Technical Research and Analysis Consortium (DPC) (Konzorcij za pravne in tehnične raziskave in analize varstva podatkov), An assessment of the level of protection of personal data, provided under Japan law (Ocena ravni varstva osebnih podatkov, zagotovljenih v skladu z japonskim pravom), str. 46: Z vidika varstva pravic in interesov pooblastiteljev, kot so potrošniki, je zaželeno, da se v primeru pooblastiteljeve zahteve za shranjene osebne podatke nanjo nadalje odzove tako, da se ustavi itd. neposredna pošta ali prostovoljno izpolnjevanje obrazca za prenehanje uporabe itd., pri čemer se upoštevajo značilnosti, velikost in status poslovnih dejavnosti.

[39] Delovni dokument WP254, točka 7 poglavja 3, str. 5; glej tudi uvodno izjavo 39 Splošne uredbe o varstvu podatkov.

[40] Ta delovna skupina je bila ustanovljena v skladu s členom 29 Direktive 95/46/ES. Je neodvisni nadzorni organ za varstvo podatkov in zasebnost. Njene naloge so navedene v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES. Iz Delovne skupine iz člena 29 je zdaj nastal Evropski odbor za varstvo podatkov.

92. **EOVP Komisijo poziva, naj pojasni pomen izraza „je lahko seznanjen“ in ali ZVOP praviloma določa obveznost dejanskega obveščanja posameznikov, na katere se nanašajo osebni podatki.**

93. Poleg tega lahko glede na referenčni dokument o ustreznosti obstajajo omejitve glede informacij, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, podobno kot v členu 23 Splošne uredbe o varstvu podatkov. Člen 14(5) Splošne uredbe o varstvu podatkov podobno določa izjemo od pravice do obveščenosti, kadar bi informacije lahko onemogočile ali resno ovirale uresničevanje obdelave. Vendar upravljavec tudi v tem primeru zagotovi neke vrste informacij, na primer tako, da javno objavi posplošene informacije. Ob prenehanju obstoja tveganja je posameznik, na katerega se nanašajo osebni podatki, o tem obveščen[41]. Ti vidiki so pomembni za zagotovitev temeljnega načela pravičnosti.

94. Poslovni subjekt, ki ravna z osebnimi podatki, mora v skladu s členom 23 ZVOP posamezniku, na katerega se nanašajo osebni podatki, na splošno vnaprej zagotoviti informacije o posredovanju njegovih podatkov tretji osebi, bodisi implicitno ob pridobitvi privolitve ali pa izrecno z obvestilom o zavrnitvi privolitve. Po razumevanju EOVP posamezniki, na katere se nanašajo osebni podatki, ne prejmejo obvestila s sporočilom o tem, da njihovi podatki niso shranjeni osebni podatki v skladu z ZVOP, ker spadajo med izjeme iz člena 4 odredbe kabineta. Zato ne bodo mogli v celoti izkoristiti svojih pravic. Posamezniki, na katere se nanašajo osebni podatki, niso obveščeni tudi v primerih iz člena 18(4) ZVOP.

95. **EOVP priznava, da so pravice lahko omejene zaradi zakonitih ciljev poslovnega subjekta, ki ravna z osebnimi podatki, in državnih organov. Hkrati pa meni, da bi bilo treba vnaprej zagotoviti vsaj splošne informacije o možnosti omejitve pravic za cilje, na katere se sklicuje zakon, in da bi bilo treba ob prenehanju obstoja tveganj, za katera so te informacije omejene, o tem obvestiti posameznika, na katerega se nanašajo osebni podatki.**

96. Drugi vidiki preglednosti so nadalje razviti v nadaljevanju. Nanašajo se na tveganja, ki jih povzroča prenos v tretjo državo[42], in informacije o logiki obdelave v okviru samodejnega sprejemanja odločitev, vključno z oblikovanjem profilov[43].

3.1.4 Omejitve nadaljnjih prenosov

97. EOVP odobrava prizadevanja japonskih organov in Evropske komisije za izboljšanje ravni varstva pri nadaljnjih prenosih v dopolnilnem pravilu 4, ki izključuje, da se osebni podatki, preneseni iz EU, nato prenesejo v tretjo državo na podlagi sistema CBRS skupine APEC. Poleg tega ugotavlja, da se je Evropska komisija v uvodnih izjavah 177 in 184 novega osnutka sklepa o ustreznosti zavezala, da bo sklep o ustreznosti začasno prenehala izvajati, če nadaljnji prenosi ne bodo več zagotavljali neprekinjenega varstva. Glede prenosov osebnih podatkov iz EU iz Japonske v tretje države pa želi EOVP poudariti dve točki.

98. **Uporaba privolitve kot podlage za prenose podatkov iz Japonske v tretjo državo v japonskem pravnem sistemu vzbuja pomisleke, saj informacije, ki se posamezniku, na katerega se nanašajo osebni podatki, zagotovijo pred privolitvijo, po mnenju EOVP očitno niso popolne.**

99. Člen 24 ZVOP prepoveduje prenos osebnih podatkov tretji osebi zunaj ozemlja Japonske brez predhodne privolitve zadevnega posameznika. V dopolnilnem pravilu 4 je navedeno, da je treba

[41] Sodbi Sodišča z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, ZOdl., točka 121, in z dne 8. aprila 2014, Digital Rights Ireland, C-293/12 in C-594/12, ZOdl., točke 54–62.
[42] Glej razdelek 2.1.4.
[43] Glej razdelek 2.1.6.

posameznikom iz EU, na katere se nanašajo osebni podatki, zagotoviti informacije o okoliščinah v zvezi s prenosom, ki so potrebne za odločitev o privolitvi.

100. Evropska komisija je v osnutku sklepa o ustreznosti ugotovila, da dopolnilno pravilo 4 zagotavlja, da je privolitev posameznika iz EU, na katerega se nanašajo osebni podatki, posebej dobro informirana[44], saj bo obveščen o prenosu podatkov v tujino in o posebni namembni državi. Tako bo lahko posameznik, na katerega se nanašajo osebni podatki, ocenil tveganje za zasebnost, povezano s prenosom.

101. V skladu z načelom preglednosti iz referenčnega dokumenta o ustreznosti se pri obveščanju posameznikov zagotovi določena stopnja poštenosti. Za zagotovitev take ustrezne stopnje poštenosti bi bilo treba v okviru nadaljnjih prenosov, ki temeljijo na privolitvi, po mnenju EOVP posameznike, na katere se nanašajo osebni podatki, pred privolitvijo izrecno obvestiti o morebitnih tveganjih pri takih prenosih, ki izhajajo iz odsotnosti ustreznega varstva v tretji državi, in o neobstoju ustreznih zaščitnih ukrepov. Tako obvestilo bi moralo vključevati na primer informacije, da tretja država morda nima nadzornega organa in/ali da tretja država ne zagotavlja načel obdelave podatkov in/ali pravic posameznikov, na katere se nanašajo osebni podatki[45]. Po mnenju EOVP je zagotavljanje teh informacij bistveno za to, da lahko posameznik, na katerega se nanašajo osebni podatki, da privolitev na podlagi popolnega poznavanja teh konkretnih dejstev v zvezi s prenosom[46].

102. Informirana privolitev je pomembna tudi glede sektorskih izjem. Sklep o ustreznosti ne zajema nekaterih določenih vrst obdelave, ki jih izvajajo zadevni organi, kot so univerze, zaradi obdelave osebnih podatkov za akademske namene. Pomislek EOVP v zvezi s tem se nanaša na poseben scenarij, ko se podatki, preneseni iz EU v okviru sklepa o ustreznosti, na primer podatki o človeških virih študentov Erasmus na Japonskem, s privolitvijo posameznika, na katerega se nanašajo osebni podatki, uporabijo v drugačne namene, ki ne spadajo v področje uporabe sklepa o ustreznosti (npr. raziskovalne namene), zaradi česar niso več zajeti z dodatnim varstvom, ki ga zagotavljajo dopolnilna pravila.

103. Evropska komisija je v uvodni izjavi 38 osnutka sklepa o ustreznosti navedla, da bo tak scenarij spadal v okvir nadaljnjih prenosov in da mora poslovni subjekt, ki ravna z osebnimi podatki, posamezniku, na katerega se nanašajo osebni podatki, kadar se to zgodi, zagotoviti vse potrebne informacije pred pridobitvijo njegove privolitve, vključno s tem, da osebni podatki ne bodo zaščiteni s pravili ZVOP.

104. Dopolnilno pravilo 4 vsebuje le zahtevo, da mora poslovni subjekt, ki ravna z osebnimi podatki, pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki, po tem ko so mu zagotovljene informacije o okoliščinah v zvezi s prenosom, ki so potrebne za odločitev o privolitvi.

105. **EOVP poziva Evropsko komisijo, naj zagotovi, da bodo informacije, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, „o okoliščinah v zvezi s prenosom“ vključevale informacije o morebitnih tveganjih pri prenosih, ki izhajajo iz odsotnosti ustreznega varstva v tretji državi, in o neobstoju ustreznih zaščitnih ukrepov, v primeru sektorskih izjem pa tudi o neobstoju zaščitnih ukrepov v zvezi z dopolnilnimi pravili in ZVOP.**

106. **Nadaljnji prenosi osebnih podatkov se lahko opravijo v tretje države, za katere se začne uporabljati morebitni poznejši japonski sklep o ustreznosti.**

[44] Uvodna izjava 76 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

[45] Smernice EOVP št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679, 25. maj 2018, str. 8.

[46] Smernice EOVP št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679, 25. maj 2018, str. 7.

107. Brez poseganja v odstopanja iz člena 23(1) ZVOP se lahko podatki, ki so bili sprva preneseni iz EU na Japonsko, nato brez privolitve prenesejo iz Japonske v tretjo državo v dveh primerih:

- Če sta poslovni subjekt, ki ravna z osebnimi podatki, in tretji prejemnik s pogodbo, drugimi oblikami zavezujočih sporazumov ali zavezujočimi sporazumi v skupini podjetij skupaj izvedla ukrepe, ki zagotavljajo raven varstva, enakovredno ravni iz ZVOP, branega skupaj z dopolnilnimi pravili[47].
- Če je Komisija za varstvo osebnih podatkov v skladu s členom 24 ZVOP in členom 11 Pravil o varstvu osebnih podatkov[48] priznala tretjo državo kot državo, ki zagotavlja enakovredno raven varstva, kot jo zagotavlja Japonska.

108. EOVP ocenjuje, da je člen 24 ZVOP kot bolj podrobno pravilo, ki vsebuje odstopanje od splošnega pravila v skladu s členom 23 ZOVP. Zato se ne strinja z oceno Evropske komisije v novem zadnjem stavku uvodne izjave 78 osnutka sklepa o ustreznosti, v kateri je navedeno, da tudi v teh primerih pri prenosu tretji osebi še vedno velja zahteva po pridobitvi privolitve v skladu s členom 23(1) ZVOP.

109. V skladu s členom 11(1) pravil o varstvu osebnih podatkov so za sklep o ustreznosti, ki ga izda Komisija za varstvo osebnih podatkov, potrebni vsebinski standardi, enakovredni ZVOP, katerih izvajanje je zagotovljeno v tretji državi in ki jih učinkovito nadzoruje neodvisni izvršni organ. Poleg tega lahko Komisija za varstvo osebnih podatkov v skladu s členom 11(2) Pravil o varstvu osebnih podatkov določi potrebne pogoje za varstvo pravic in interesov posameznikov na Japonskem.

110. V dopolnilnem pravilu 4 je navedeno, da se lahko osebni podatki EU prenesejo v tretjo državo, za katero je bil sprejet japonski sklep o ustreznosti brez dodatnih omejitev. Vendar člen 44 Splošne uredbe o varstvu podatkov določa, da mora vsak prenos osebnih podatkov v tretjo državo izpolnjevati pogoje iz poglavja V Splošne uredbe o varstvu podatkov, vključno z nadaljnjimi prenosi iz tretje države v drugo tretjo državo. Pri nadaljnjih prenosih se ne sme ogroziti raven varstva posameznikov, katerih osebni podatki se prenašajo[49]. Čeprav se s to razlago načeloma strinja tudi Evropska komisija v osnutku sklepa o ustreznosti[50], se zdi, da je ne upošteva v celoti. Evropska komisija se je pogajala o prepovedi prenosa podatkov, ki izvirajo iz EU, v tretjo državo na podlagi sistema CBPR skupine APEC. Glede na orodje za primerjavo, razvito leta 2014 v okviru direktive EU, med zavezujočimi poslovnimi pravili in sistemom CBPR, ki kaže zahteve obeh sistemov, njune skupne točke in razlike (Mnenje Delovne skupine iz člena 29 št. 02/2014), ima EOVP pomisleke glede uporabe sistema CBPR kot orodja za nadaljnje prenose osebnih podatkov, ki se prenašajo iz EU v države zunaj Japonske.

111. Nasprotno pa se zdi, da Evropska komisija sprejema nadaljnje prenose osebnih podatkov, prenesenih iz EU na Japonsko na podlagi japonskega sklepa o ustreznosti, pri čemer Komisija za varstvo osebnih podatkov dopolnilnih pravil ne more naložiti kot pogojev za varstvo pravic in interesov posameznikov iz EU, če je to potrebno. EOVP iz člena 44 Splošne uredbe o varstvu podatkov sklepa, da je treba okrepljeno varstvo podatkov, ki se prenašajo iz EU na Japonsko in so predvideni v dopolnilnih pravilih, vedno podaljšati, kadar se osebni podatki, preneseni iz EU na Japonsko, prenesejo naprej v tretjo

[47] Dopolnilno pravilo 4(ii).

[48] Pravila o izvajanju zakona o varstvu osebnih podatkov, 30. maj 2017. Evropska komisija je EOVP poslala angleški prevod novega člena 11, vendar ta člen še ni bil objavljen.

[49] Delovni dokument WP254, str. 5.

[50] Uvodna izjava 75 Izvedbenega sklepa Komisije z dne XXXX v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov, ki ga zagotavlja Japonska, kot je bil EOVP poslan 13. novembra 2018.

državo, če okvir varstva podatkov v tej državi ni priznan kot v osnovi enakovreden Splošni uredbi o varstvu podatkov.

112. **Zato EOVP Evropsko komisijo poziva, naj prevzame nadzorno vlogo in zagotovi, da se raven varstva podatkov iz EU ohrani ali da razmisli o začasni odložitvi izvajanja te odločitve o ustreznosti, če se osebni podatki, preneseni iz EU na Japonsko, prenesejo naprej v tretje države, za katere se začne uporabljati morebitni poznejši japonski sklep o ustreznosti, če te tretje države niso bile predmet predhodnih ocen ali ugotovitev o ustreznosti EU.**

3.1.5 Neposredno trženje

113. V skladu z dopolnilnim pravilom 3 poslovni subjekt, ki ravna z osebnimi podatki, teh podatkov ne sme obdelovati za namen neposrednega trženja, če so bili iz Evropske unije preneseni za drug namen in če posameznik iz EU, na katerega se nanašajo osebni podatki, ni dal privolitve za spremembo namena uporabe.

114. Če se podatki obdelujejo za namen neposrednega trženja, bi moral imeti posameznik, na katerega se nanašajo osebni podatki, v skladu z referenčnim dokumentom o ustreznosti možnost, da kadar koli brezplačno ugovarja obdelavi svojih podatkov, obdelanih za take namene. V skladu s členom 16 ZVOP lahko poslovni subjekt, ki ravna z osebnimi podatki, osebne podatke obdeluje le, če posameznik, na katerega se nanašajo osebni podatki, poda privolitev. Preklic privolitve bi lahko pripeljal do enakega rezultata kot prednostna pravica do ugovora neposrednemu trženju.

115. Japonski okvir varstva podatkov ne zagotavlja prednostne pravice do ugovora in, kot je pojasnjeno zgoraj v razdelku o privolitvi, je preklic privolitve v skladu s smernicami Komisije za varstvo osebnih podatkov zgolj zaželen in pogojen ter se zato ne more enačiti s pravico, da se temu kadar koli ugovarja, kot se zahteva v skladu z referenčnim dokumentom o ustreznosti. **EOVP poziva Evropsko komisijo, naj da ponovna zagotovila o pravici do preklica privolitve in spremlja primere v zvezi z neposrednim trženjem.**

3.1.6 Avtomatizirano sprejemanje odločitev in oblikovanje profilov

116. Odločitve, ki temeljijo zgolj na avtomatizirani obdelavi (avtomatizirano sprejemanje posameznih odločitev), vključno z oblikovanjem profilov, ki imajo pravne učinke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali nanj znatno vplivajo, se lahko v skladu z referenčnim dokumentom o ustreznosti izvedejo le pod določenimi pogoji, opredeljenimi v pravnem okviru tretje države. Zato je vsakič, ko se v navedenih okoliščinah izvedeta avtomatizirano sprejemanje odločitev in oblikovanje profilov, potrebna pravna podlaga.

117. Pogoji za avtomatizirano sprejemanje odločitev v evropskem okviru vključujejo na primer potrebo po pridobitvi izrecne privolitve[51] posameznika, na katerega se nanašajo osebni podatki, ali potrebe po taki odločitvi za sklenitev pogodbe. Če odločitev ni skladna s pogoji, določenimi v pravnem okviru tretje države, bi moral imeti posameznik, na katerega se nanašajo osebni podatki, pravico, da zanj ne velja. Poleg tega bi moralo pravo tretje države v vsakem primeru zagotoviti potrebne zaščitne ukrepe, vključno s pravico do obveščenosti o posebnih razlogih, na katerih temelji odločitev, in razlogih za popravljanje netočnih ali nepopolnih informacij ter izpodbijanje odločitve, kadar je bila sprejeta na napačni dejanski podlagi.

[51] Za kritične pripombe k pojmu privolitve v japonskem pravnem okviru za varstvo podatkov glej: 2.1 Splošno in 2.2.8 Neposredno trženje

118. Sklep Komisije se nanaša le na bančni sektor, v katerem se uporabljajo sektorska pravila[52] o avtomatiziranih odločitvah. V celovitih smernicah za nadzor večjih bank, navedenih v uvodni izjavi 93 osnutka sklepa o ustreznosti, je navedeno, da je treba zadevnemu posamezniku posebej pojasniti razloge za zavrnitev zahteve za sklenitev posojilne pogodbe.

119. Zdi se (na primer), da Evropska komisija pri svojih utemeljitvah, ki se nanašajo na osnutek sklepa o ustreznosti (uvodna izjava 94), glede tega, da ni verjetno, da bi odsotnost podrobnih pravil o avtomatiziranem sprejemanju odločitev v okviru ZVOP vplivala na raven varstva, ne upošteva primera, v katerem osebne podatke, prenesene iz EU, naknadno obdela drug japonski upravljavec podatkov (ki ni prvotni japonski uvoznik podatkov).

120. Zato se zdi, da na Japonskem ne obstajajo splošna pravila, ki bi se uporabljala v različnih sektorjih in bi urejala avtomatizirano sprejemanje odločitev in oblikovanje profilov.

121. **EOVP poziva Evropsko komisijo, naj spremlja primere v zvezi z avtomatiziranim sprejemanjem odločitev in oblikovanjem profilov.**

3.2 Postopkovni mehanizmi in mehanizmi za izvrševanje

122. EOVP je na podlagi meril iz referenčnega dokumenta o ustreznosti analiziral naslednje vidike japonskega varstva podatkov in pravnega okvira, kot so zajeti v osnutku sklepa o ustreznosti: obstoj in učinkovito delovanje neodvisnega nadzornega organa; obstoj sistema, ki zagotavlja dobro raven skladnosti ter sistema za dostop do ustreznih pravnih sredstev, ki posameznikom iz EU zagotavlja sredstva za uveljavljanje pravic in pravnih sredstev, ne da bi pri tem naleteli na zapletene ovire za upravno in sodno varstvo.

123. EOVP na podlagi parametrov, ki jih je Sodišče Evropske unije določilo v zadevi Schrems[53], ter parametrov iz uvodne izjave 104 in člena 45 Splošne uredbe o varstvu podatkov ugotavlja, da čeprav na Japonskem obstaja sistem, ki je skladen z evropskim sistemom, posamezniki iz EU, katerih podatki se bodo v skladu s tem sklepom o ustreznosti prenesli, v praksi do njega mogoče težko dostopajo zaradi jezikovnih in institucionalnih ovir.

124. V nadaljnjih razdelkih bodo najprej proučeni navedeni vidiki japonskega okvira, nato pa bo poudarjenih nekaj priporočil za Komisijo.

3.2.1 Pristojni neodvisni nadzorni organ

125. Komisija za varstvo osebnih podatkov je bila ustanovljena 1. januarja 2016 po spremembah ZVOP iz leta 2015 in je nadomestila svojo predhodnico – Posebno komisijo za varstvo osebnih podatkov (ustanovljeno leta 2013 z Zakonom o moji številki). Čeprav je Komisija za varstvo osebnih podatkov mlada ustanova, si je od svoje ustanovitve zelo prizadevala za gradnjo potrebne infrastrukture, ki bi omogočila izvajanje spremenjenega ZVOP. Med prizadevanji so omembe vredni določitev Pravil komisije za varstvo osebnih podatkov, Smernice komisije za varstvo osebnih podatkov za zagotavljanje navodil poslovnim subjektom, ki ravnajo z osebnimi podatki, o razlagi ZVOP, objava dokumenta z vprašanji in odgovori Komisije za varstvo osebnih podatkov[54] ter vzpostavitev telefonske linije za svetovanje poslovnim subjektom in državljanom v zvezi z določbami o varstvu podatkov in storitve mediacije za obravnavo pritožb.

[52] EOVP teh sektorskih predpisov ni prejel.

[53] Sodba Sodišča z dne 6. oktobra 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, točki 73 in 74.

[54] Evropska komisija tega dokumenta EOVP ni predložila v angleščini.

126. Ustanovitev in delovanje Komisije za varstvo osebnih podatkov je urejeno v poglavju V ZVOP. Čeprav je Komisija za varstvo osebnih podatkov v pristojnosti predsednika vlade, je v členu 62 določeno, da svoje naloge izvaja neodvisno. EOVP odobrava pojasnilo Evropske komisije v spremenjenem osnutku sklepa o ustreznosti, razposlanem 13. novembra 2018, z nadaljnjim opisom stopnje neodvisnosti Komisije za varstvo osebnih podatkov od notranjih in zunanjih vplivov.

3.2.2 Sistem varstva podatkov mora zagotavljati dobro raven skladnosti

127. Osnutek sklepa o ustreznosti vsebuje zavezo o celovitem pregledu pooblastil, ki jih ima Komisija za varstvo osebnih podatkov v skladu s členi 40, 41 in 42 ZVOP, za zagotavljanje spremljanja in izvajanja zakonodaje. Člen 40 pooblašča Komisijo za varstvo osebnih podatkov, da od poslovnih subjektov, ki ravnajo z osebnimi podatki, zahteva predložitev poročila in dokumentacije v zvezi s postopki obdelave ter da izvaja inšpekcijske preglede na kraju samem. Če Komisija za varstvo osebnih podatkov ugotovi, da je to potrebno za varstvo posameznih pravic ali v primeru kršitve določb zakonodaje, ima v skladu s členom 42 pooblastilo za izdajanje priporočil, če se ta ne upoštevajo, pa poslovnim subjektom, ki ravnajo z osebnimi podatki, odredi prekinitev dejanja kršitve ali sprejem potrebnih ukrepov za odpravo kršitve.

128. Enega svojih prvih ukrepov v skladu s členom 41 spremenjenega ZVOP je Komisija za varstvo osebnih podatkov sprejela oktobra 2018 in izdala „smernice“ za poslovni subjekt, ki ravna z osebnimi podatki, v katerih mu je svetovala, naj okrepi svoje varnostne ukrepe in učinkovito nadzoruje ponudnike aplikacij, hkrati pa uporabnikom jasno in razumljivo pojasni, kako se uporabljajo njihovi osebni podatki, ter pridobi predhodno privolitev, kadar se podatki izmenjujejo s tretjo osebo, ter se ustrezno odzove na zahtevo uporabnikov po izbrisu njihovih podatkov. V odgovorih, ki jih je prejel EOVP[55], so uradniki Komisije za varstvo osebnih podatkov opozorili, da jih je poslovni subjekt obvestil, da namerava sodelovati, če pa tega ne bo storil, mu bo Komisija izdala „priporočilo“ v skladu s členom 42(1) ZVOP.

129. Preiskava, ki jo je v zvezi z zgoraj navedenim poslovnim subjektom, ki ravna z osebnimi podatki, izvedla Komisija za varstvo osebnih podatkov, je zelo pozitiven kazalnik prizadevanj japonskega nadzornega organa za zagotovitev dobre ravni skladnosti v državi.

130. Čeprav so bile v primerjavi z okvirom, vzpostavljenim pred spremembami iz leta 2015, uvedene izboljšave, EOVP ugotavlja, da ima Komisija za varstvo osebnih podatkov manj pooblastil kot evropski organ za varstvo podatkov v skladu s Splošno uredbo o varstvu podatkov, zlasti v zvezi z **izvajanjem**. Upravne globe[56] so na primer precej nizke. V uvodni izjavi 108 sklepa Evropske komisije je poudarjeno, da so v primerih neskladnosti ali nekaterih kršitev ZVOP uvedene kazenske sankcije in da lahko predsednik te komisije zadeve posreduje državnemu tožilcu. Vendar sklep Evropske komisije ne upošteva dejstva, da je javno tožilstvo na Japonskem diskrecijsko in včasih predmet dolgotrajnih postopkov pregleda[57]. Poleg tega je kazen zapora (z delom v splošno korist ali brez njega), povezano s kršitvami ZVOP v skladu z določbami iz poglavja VII, morda težko izvršiti, saj je namenjena fizičnim osebam in v nobenem primeru ne kaznuje poslovnega subjekta, ki ravna z osebnimi podatki, kot pravne osebe, ki ne izpolnjuje svojih obveznosti glede načela odgovornosti.

[55] Priloga III

[56] Te so določene v poglavju VII ZVOP. Najvišja kazen je določena v členu 83 (zagotavljanje ali prikrita uporaba podatkovne zbirke osebnih podatkov za lasten nezakonit dobiček ali nezakonit dobiček tretje osebe) in je enakovredna bodisi enoletni kazni zapora z delom v splošno korist ali globo, ki ne presega 500 000 jenov (približno 3 900 EUR). Po pojasnilih, ki jih je predložila Komisija, se globe za posamezno kršitev seštevajo. Čeprav to morda drži, EOVP ugotavlja, da bo, tudi če se globe seštejejo, skupni znesek v primerjavi z evropskimi standardi verjetno ostal precej nizek.

[57] Oda, H., Japanese Law, Oxford University Press (III. izdaja), 2009, strani 439–440.

131. **EOVP glede na navedeno poziva Evropsko komisijo, naj pozorno spremlja učinkovitost sankcij in ustreznih pravnih sredstev v japonskem sistemu varstva podatkov.**

3.2.3 Sistem varstva podatkov mora zagotavljati podporo in pomoč posameznikom, na katere se nanašajo osebni podatki, ter jim pomagati pri uresničevanju njihovih pravic in ustreznih pravnih sredstev

132. Na spletišču Komisije za varstvo osebnih podatkov so zagotovljene obsežne informacije in smernice, katerih namen je ozaveščati poslovne subjekte, ki ravnajo z osebnimi podatki, o njihovih obveznostih in odgovornostih na podlagi okvira za varstvo podatkov, ter telefonska številka za pomoč, na kateri se japonskim državljanom zagotavljajo informacije in podpora v zvezi z njihovimi posameznimi pravicami v skladu z ZVOP. Na spletišču je tudi razdelek, imenovan soba za ˇotrokeˇ, izrecno namenjen otrokom in mladim. EOVP ugotavlja, da so te informacije – skupaj s telefonsko številko za pomoč, smernicami ter dokumentom z vprašanji in odgovori – na voljo v japonščini[58]. Zato je trdno prepričan, da bi bilo koristno, če bi lahko Komisija za varstvo osebnih podatkov na angleški različici svojega spletišča zagotovila posebno stran z informacijami za posameznike iz EU, katerih podatki bodo v skladu s sklepom Evropske komisije o ustreznosti preneseni na Japonsko, o njihovih osebnih pravicah na podlagi japonskega okvira za varstvo podatkov in dopolnilnih pravil.

133. EOVP pozdravlja pojasnila Evropske komisije v uvodni izjavi 104 spremenjenega osnutka sklepa o ustreznosti, razposlanega 13. novembra 2018, glede storitve mediacije, ki jo v skladu s členom 61(ii) ZVOP upravlja Komisija za varstvo osebnih podatkov. Vendar je želel v zvezi s tem opozoriti na tri točke. Prvič, storitev mediacije ni objavljena na angleški različici spletišča Komisije za varstvo osebnih podatkov. Drugič, storitev je dostopna le prek telefona in je na voljo le v japonščini. Tretjič, mediacija je zgolj spodbujevalni postopek, ki ne vodi do zavezujočega sporazuma med strankama, kar vpliva na učinkovitost možnosti uveljavljanja pravnih sredstev, ki so na voljo posameznikom, na katere se nanašajo osebni podatki[59].

134. EOVP nazadnje ugotavlja, da osnutek sklepa o ustreznosti poudarja pravna sredstva, ki so na voljo na podlagi civilne tožbe in kazenskih postopkov, ne priznava pa obstoja **institucionalnih ovir pri reševanju sporov** na Japonskem, kot so stroški postopka (odvetniške nagrade se enakomerno razdelijo med tožnika in toženca, ne glede na to, katera stranka uspe v sodnem postopku[60]), pomanjkanje odvetnikov v državi[61], dejstvo, da tuji odvetniki ne smejo opravljati odvetniškega poklica na področju nacionalnega prava, ter zahteve o dokaznem bremenu v skladu z odškodninskim pravom. EOVP se boji, da bi lahko ti dejavniki (v praksi) ovirali dostop posameznikov do pravnega varstva ter ogrozili njihovo pravico, da bi pravna sredstva uveljavljali hitro in brez pretiranih stroškov.

135. Ob upoštevanju navedenega **EOVP izraža zaskrbljenost glede obstoja tveganja, da imajo lahko posamezniki iz EU težave pri dostopu do upravnega in sodnega varstva**, zato bi bilo dobrodošlo, če bi Evropska komisija lahko s Komisijo za varstvo osebnih podatkov razpravljala o možnosti vzpostavitve spletne storitve, vsaj v angleščini, **ki bi bila namenjena zagotavljanju podpore in obravnavanju**

[58] https://www.ppc.go.jp/en/contactus/piinquiry/.

[59] Kojima, T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; in Menkel-Meadow, C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003) (izd.).

[60] Wagatsuma (2012), Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure v: Reimann (ur.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice, zvezek 11, str. 195–200.

[61] Po zadnjih podatkih je na Japonskem 38 980 odvetnikov (približno 290 odvetnikov na milijon ljudi [po podatkih japonske odvetniške zbornice] (2017), Bela knjiga o odvetnikih, str. 8–9).

pritožb[62] **posameznikov iz EU**. Poleg tega bi se EOVP zdelo koristno, če bi lahko organi za varstvo podatkov iz EU delovali kot posredniki za pritožbe med posamezniki iz EU, na katere se nanašajo osebni podatki, ter organizacijami, ki delujejo na Japonskem, in Komisijo za varstvo osebnih podatkov.

4 O DOSTOPU JAVNIH ORGANOV DO PODATKOV, PRENESENIH NA JAPONSKO

136. Namen Komisije je, da s sklepom o ustreznosti prizna, da „Japonska zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenesejo poslovnim subjektom, ki ravnajo z osebnimi podatki, na Japonskem“, kot je navedeno v členu 1 osnutka sklepa o ustreznosti. Komisija je v skladu s členom 45(2) Splošne uredbe o varstvu podatkov analizirala tudi omejitve in zaščitne ukrepe v zvezi z dostopom javnih organov do osebnih podatkov. To poglavje je osredotočeno na oceno dostopa organov kazenskega pregona in drugih vladnih subjektov do osebnih podatkov za namene nacionalne varnosti. Analiza EOVP temelji na osnutku sklepa o ustreznosti, njegovi Prilogi II, v kateri je japonska vlada predstavila pregled ustreznega pravnega okvira, in japonskih pravnih besedilih v obsegu, v katerem mu jih je predložila Komisija. V posebnem okviru te ocene je EOVP upošteval elemente, ki se nanašajo na japonsko zakonodajo in ne izhajajo iz ugotovitev Evropske komisije, vendar so pomembni za oceno pogojev in zaščitnih ukrepov, v skladu s katerimi lahko japonski javni organi dostopajo do osebnih podatkov, prenesenih iz Evropske unije.

[62] Podobno kot je predvideno v Prilogi II k temu sklepu o ustreznosti za pritožbe prebivalcev EU v zvezi z dostopom japonskih javnih organov do njihovih podatkov.

4.1 Dostop organov kazenskega pregona do podatkov

4.1.1 Postopki za dostop do podatkov na področju kazenskega prava

137. V osnutku sklepa o ustreznosti so predstavljeni trije načini, na katere lahko organi kazenskega pregona v skladu z japonsko zakonodajo dostopajo do podatkov na Japonskem:

4.1.1.1 Zahteve za dostop s sodnim nalogom

138. V osnutku sklepa o ustreznosti je navedeno, da na Japonskem za dostop vlada in zlasti organi kazenskega pregona pri zahtevah za dostop do elektronskih dokazov v okviru kazenskih preiskav vedno potrebujejo nalog, razen če uporabijo postopek prostovoljnega razkritja – glej v nadaljevanju.

4.1.1.1.1 Zahteva „zadostnega razloga“, potrebnosti in sorazmernosti nalogov

139. EOVP priznava, da mora v skladu z japonsko ustavo vsako zbiranje osebnih podatkov z obveznimi sredstvi temeljiti na sodnem nalogu. Natančneje, v osnutku sklepa o ustreznosti je navedeno, da je treba v vseh primerih „preiskav in zasegov“ izdati sodni nalog zaradi „zadostnega razloga“, za katerega vrhovno sodišče meni, da obstaja samo, če naj bi zadevni posameznik (osumljenec ali obtoženec) storil kaznivo dejanje ter sta preiskava in zaseg potrebna za kazensko preiskavo. Komisija se pri tem sklicuje na sodbo vrhovnega sodišča z dne 18. marca 1969 v zadevi N. 100 (1968(Shi)). EOVP opozarja, da lahko v skladu s sodno prakso Sodišča Evropske unije[63] zbiranje podatkov zlasti o promet in lokaciji odobri le sodišče, ne pa na primer tožilci.

140. EOVP prav tako ob upoštevanju sodne prakse Sodišča Evropske unije, v skladu s katero je lahko dostop do podatkov predmet naloga, kot v zadevi Tele2, obžaluje, da niso bile zagotovljene dodatne informacije za proučitev, kako se v praksi uporabljajo merila za oceno nujnosti naloga – teža kaznivega dejanja in način, na katerega je bilo storjeno, vrednost in pomen zaseženih materialov kot dokazov, verjetnost skrivanja in uničenja zaseženih materialov, obseg nevšečnosti, ki jih je povzročil zaseg, drugi s tem povezani pogoji – in pojem „zadostnega razloga“, ki izhaja iz Ustave. Zato poziva Komisijo, naj spremlja, ali se v praksi pri izdaji nalogov izpolnjujejo merila, ki jih je v svoji praksi določilo Sodišče Evropske unije.

4.1.1.1.2 Vrste kaznivih dejanj, za katere se lahko izdajo nalogi

141. Postopek izdaje naloga se uporablja le ob izvedbi obveznih preiskav. Načeloma se lahko nalogi izdajo le v primerih kršitev prava. V zvezi s tem EOVP ugotavlja, da je bil 15. junija 2017 v okviru pristopa Japonske h Konvenciji Združenih narodov proti mednarodnemu organiziranemu kriminalu (UNTOC) sprejet Zakon o kaznovanju organiziranega kriminala in nadzoru premoženjske koristi, pridobljene s kaznivim dejanjem[64]. Ker ta zakon ni na voljo v angleškem jeziku, v skladu z zakonodajo EU pa obstaja zahteva, da se nekateri podatki zbirajo le v okviru preiskovanja, odkrivanja ali pregona hudih kaznivih dejanj[65], ter ker je več poročevalcev, vključno s posebnim poročevalcem ZN Josephom Cannatacijem[66], izrazilo pomisleke glede širokega področja uporabe, ki se nanaša na opredelitev organizirane kriminalne združbe, ki naj bi bila nejasna in preširoka, EOVP ne more ugotoviti, da je dostop do elektronskih dokazov v skladu z ustrezno japonsko zakonodajo omejen na pragove, določene v zakonodaji EU.

[63] Glej sodbi Sodišča Evropske unije v zadevi C-203/15 in združenih zadevah C-293/12 in C-594/12.
[64] Glej https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[65] Glej združeni zadevi C-293/12 in C-594/12 ter zadevo C-203/15.
[66] Posebni poročevalec Združenih narodov za pravico do zasebnosti in Graham Greenlist, raziskovalec pravne fakultete UNSW Law iz Sydneyja.

142. Opozoriti je treba tudi na to, da je za nekatere vrste kaznivih dejanj pristojna prefekturna policija, ki ima posebne policijske odloke. EOVP ni prejel notranjih pravil, ki se uporabljajo za prefekturno policijo .

143. V skladu z osnutkom sklepa o ustreznosti je za zbiranje elektronskih informacij na področju preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj odgovorna prefekturna policija.

4.1.1.2 Nalogi za prisluškovanje telefonskim pogovorom

144. V Prilogi II k osnutku sklepa o ustreznosti je navedeno, da so posebnosti prestrezanja komunikacij določene v Zakonu o prisluškovanju telefonskim pogovorom zaradi preiskovanja kaznivih dejanj. Ta zakonodajni akt je bil poslan zelo pozno, zato ga ni bilo mogoče poglobljeno analizirati. Čeprav se zdi, da so v tem pravnem okviru določeni številni zaščitni ukrepi, EOVP ne more oceniti, ali so pogoji iz tega zakonodajnega akta obdani z jamstvi, ki so bistveno enakovredna tistim, ki se v EU zahtevajo tako z Listino, kot jo razlaga Sodišče Evropske unije, kot tudi z EKČP, kot jo razlaga Evropsko sodišče za človekove pravice v Strasbourgu.

4.1.1.3 Postopek prostovoljnega razkritja, ki temelji na obrazcu za poizvedbo

145. Ta neobvezna oblika sodelovanja omogoča javnim organom, da upravljavce (razen telekomunikacijskih operaterjev) zaprosijo podatke, ki jih imajo na voljo. Neizpolnitve zahtevka ni mogoče izvršiti. Nejasno ostaja, kateri organi lahko uporabijo tovrstni postopek, vendar se zdi, da je omejen na tiste, ki preiskujejo kazniva dejanja.

4.1.1.3.1 Pogoji za izdajo obrazcev za poizvedbo

146. EOVP priznava, da je japonsko vrhovno sodišče s sklicevanjem na ustavo določilo, da se omejitve uporabljajo pri „prostovoljnih razkritjih“[67]. Iz osnutka sklepa o ustreznosti je razvidno, da lahko „prostovoljno razkritje“ zahtevajo le pristojni organi z izdajo “obrazca za poizvedbo“. Pošiljanje takega “obrazca za poizvedbo“ naj bi bilo dovoljeno le v okviru preiskave kaznivega dejanja, tako da naj bi vedno obstajal konkreten sum, da je bilo kaznivo dejanje že storjeno. Take preiskave običajno izvaja prefekturna policija , pri kateri veljajo omejitve v skladu s členom 2(2) Zakona o policiji, kar pomeni, da bi to moralo biti pomembno za policijske dejavnosti. Vendar EOVP zahteva dodatno pojasnilo glede konkretne oblike meril, na podlagi katerih je mogoče izdati “obrazec za poizvedbo“ (kot je sodna praksa, ki kaže uporabo teh meril), ter odnosa med postopkom prostovoljnega razkritja in zasegom podatkov na podlagi naloga. Dejansko se zdi, da tudi če podatkov ni bilo mogoče pridobiti s prostovoljnim postopkom, bi jih bilo še vedno mogoče pridobiti z nalogom, če bi bilo to za preiskovalne organe nujno potrebno[68].

4.1.1.3.2 Razpoložljiva sodna praksa o omejitvah uporabe prostovoljnega razkritja

147. Primeri, navedeni v osnutku sklepa o ustreznosti[69], s katerimi je ponazorjena omejitev uporabe postopkov prostovoljnega razkritja, se nanašajo na primere, ko je obdolženca na javnem prostoru fotografirala ali posnela neposredno policija, zaradi česar omejeno kažejo okoliščine, v katerih lahko pristojni organi upravljavca zaprosijo za razkritje podatkov, zlasti v zvezi z merili iz Priloge II v zvezi z „ustreznostjo metod“, za katere se zdi, da se nanašajo na oceno tega, ali je prostovoljna preiskava „ustrezna“ ali razumna za dosego namena preiskave. Enako je mogoče trditi glede splošnih meril o tem, ali se lahko v skladu z družbeno sprejetimi konvencijami šteje za razumno, da se oceni zakonitost prostovoljnih preiskav. Poleg tega je Nacionalna policijska agencija, ki je zvezni organ, pristojen za vse zadeve v zvezi s kriminalistično policijo, prefekturni policiji izdala navodila za pravilno uporabo, kadar

[67] Glej Prilogo II, stran 8.
[68] Glej Prilogo II, stran 7.
[69] Glej Prilogo II, str. 8 – dve sodbi vrhovnega sodišča z dne 24. decembra 1969 (1965 (A) št. 1187) in 15. aprila 2008 (2007 (A) št. 839).

se v preiskovalnih zadevah uporabljajo pisne poizvedbe. Glavni raziskovalec mora med drugim pridobiti notranjo odobritev od visokega uradnika. EOVP nima podatkov, ali so ta navodila zavezujoča. Kljub temu navaja, da mora biti uporaba tega postopka sorazmerna ali potrebna.

4.1.1.3.3 Pravice in obveznosti upravljavcev v okviru prostovoljnega razkritja

148. Poleg tega morajo upravljavci privoliti v zagotavljanje podatkov (vendar jim očitno ni treba zaprositi za privolitev oseb, na katere se nanašajo osebni podatki, ali jih obvestiti), če te zahteve niso v nasprotju z drugimi pravnimi obveznostmi (kot so obveznosti glede zaupnosti). Poročilo, ki ga je predložila Komisija, kaže na to, da so upravljavci po visoki stopnji skladnosti začeli upoštevati varstvo podatkov svojih strank in so zato začeli manj pogosto odgovarjati na te zahteve.

149. Prav tako ostaja nejasno, ali imajo upravljavci kakršne koli spodbude za izpolnjevanje zahtev (na primer, ali imajo prednost, če izpolnjujejo zahteve, ali so izvzeti iz kazenskega pregona itd.). Zlasti ni omenjeno nobeno načelo, kot na primer načelo privilegija zoper samoobtožbo.

150. EOVP bi pozdravil dodatne informacije, če so na voljo, podatke o številu in vrstah zahtev ter odgovorih, ki so jih zagotovili zaprošeni upravljavci. Zaradi neobstoja sodne prakse in podatkov poziva Komisijo, naj spremlja učinkovitost in dejansko uporabo tega postopka v praksi.

151. Vendar EOVP nima na voljo sodne prakse in podatkov o tem postopku za določitev teh elementov. Zato ne more oceniti učinkovitosti in konkretne uporabe tega postopka brez nadaljnjih elementov o tej praksi.

4.1.1.4 Sklep o postopkih za dostop do podatkov za namene preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj

152. EOVP sklepno priznava, da načelo, po katerem je obvezen dostop pristojnih organov do osebnih podatkov mogoč le, če je to potrebno in sorazmerno namenu ter če temelji na nalogu, ustreza glavnim bistvenim jamstvom, zagotovljenim z zakonodajo EU in EKČP. V skladu z navedenimi ugotovitvami EOVP Komisijo poziva, naj spremlja področje uporabe teh ukrepov, področje uporabe postopka prostovoljnega razkritja in kako prefekturne policije in sodišča uporabljajo to načelo v zadevni sodni praksi, poleg tega naj spremlja tudi, ali japonski pravni okvir zagotavlja bistvena jamstva, ki jih dajeta Sodišče Evropske unije na podlagi Listine in Evropsko sodišče za človekove pravice na podlagi Konvencije.

4.1.2 Nadzor na področju kazenskega prava

153. V osnutku sklepa o ustreznosti in Prilogi II so predstavljene štiri vrste nadzora, ki se izvaja nad policijo, ministrstvi in javnimi agencijami.

4.1.2.1 Sodni nadzor

4.1.2.1.1 V primerih, ko se elektronske informacije zbirajo z obveznimi sredstvi (preiskava in zaseg)

154. V skladu z osnutkom sklepa o ustreznosti mora policija v vseh primerih, ko se elektronske informacije zbirajo z obveznimi sredstvi (preiskava in zaseg), pridobiti predhodni sodni nalog. Vendar obstaja izjema od tega pravila[70]. V skladu s členom 220(1) Zakonika o kazenskem postopku lahko javni tožilec, njegov pomočnik ali uradnik sodne policije ob odvzemu prostosti osumljenca preišče ali zaseže elektronske informacije na kraju odvzema prostosti. V takem primeru lahko sodnik izključi te podatke kot dokaze.

[70] Glej Prilogo II.

155. EOVP se zaveda, da podobne izjeme obstajajo tudi v zakonodaji EU. Ugotavlja, da se sodni nadzor ne izvaja v vseh primerih, ko se elektronske informacije zbirajo z obveznimi sredstvi, kot je določeno v osnutku sklepa o ustreznosti. V tem okviru navaja sodno prakso ESČP o naknadnih sodnih preverjanjih.[71]

4.1.2.1.2 V primeru zahtev za prostovoljno razkritje

156. V skladu z osnutkom sklepa o ustreznosti sodnik ne more opraviti predhodnega preverjanja v primeru zahtev za prostovoljno razkritje. V takem primeru prefekturna policija deluje pod nadzorom javnega tožilca. V osnutku sklepa o ustreznosti sta navedena člen 192(1) in člen 246 o vzajemnem sodelovanju in usklajevanju tožilcev, prefekturnih komisij za javno varnost in uradnikov sodne policije ter izmenjavi informacij med njimi. Vsebuje tudi sklic na člen 193(1), v skladu s katerim lahko državni tožilec sodni policiji daje potrebna navodila in določi standarde za pošteno preiskavo. V njem je omenjen člen 194 o disciplinskih ukrepih proti sodni policiji zaradi nespoštovanja javnih tožilcev, ki ga sprejeme nacionalna ali prefekturna komisija za javno varnost.

157. EOVP potrjuje vzpostavitev predhodnih ukrepov in izvedbo nadzora, ki ga v sodni policiji izvajata nacionalna in prefekturna komisija za javno varnost (glej v nadaljevanju).

4.1.2.2 Nadzor policije, ki ga izvajata komisiji za javno varnost

158. Nadzor policije v skladu s Prilogo II k osnutku sklepa o ustreznosti izvajata dve vrsti komisij. Namen obeh je zagotavljati demokratično upravljanje in politično nevtralnost policijske uprave.

4.1.2.2.1 Nadzor, ki ga izvaja nacionalna komisija za javno varnost

159. V Prilogi II k osnutku sklepa o ustreznosti je omenjen nadzor, ki ga nad Nacionalno policijsko agencijo izvaja nacionalna komisija za javno varnost. Zakon o policiji vsebuje seznam nalog te komisije, iz katerih izhajajo njena nadzorna pooblastila (glej člen 5).

160. V skladu s členom 4 Zakona o policiji je nacionalna komisija za javno varnost ustanovljena pod pristojnostjo predsednika vlade, sestavljajo pa jo predsednik in pet članov. Člen 7 določa nekatere omejitve glede imenovanja članov komisije. Člani komisije imajo petletni mandat, ki se lahko le enkrat podaljša, kot je določeno v členu 8. Poleg tega se zdi, da ima parlament veliko moč pri imenovanju in razrešitvi člana komisije, kar nacionalni komisiji za javno varnost zagotavlja neodvisnost.

161. Take zakonske določbe povečujejo politično nevtralnost nacionalne komisije za javno varnost.

4.1.2.2.2 Nadzor, ki ga izvajajo prefekturne komisije za javno varnost

162. Prefekturna policija je pod nadzorom prefekturnih komisij za javno varnost, ustanovljenih v vsaki prefekturi. V skladu s členom 2 in členom 36(2) Zakona o policiji so za varstvo pravic in svoboščin posameznika pristojne prefekturne komisije za javno varnost. V členih 38 in 42 Zakona o policiji so navedene dolžnosti prefekturnih komisij za javno varnost. Namen teh komisij je tudi zagotavljati demokratično upravljanje in politično nevtralnost policijske uprave, kot je navedeno v členu 43(2), in sicer s sprožitvijo posameznih zadev proti prefekturni policiji , če menijo, da je to potrebno v okviru inšpekcijskega pregleda dejavnosti prefekturne policije ali kršitve, ki so jo storili njeni zaposleni.

163. Ni pa jasno, ali imajo te komisije druga pooblastila, razen nadzora ravnanja policije. EOVP se sprašuje, ali je v pojem "kršitev" vključen nezakonit dostop do podatkov in ali lahko te komisije v takem primeru odredijo izbris podatkov ali ne.

[71] Sodba ESČP v zadevi Modestou proti Grčiji, št.°51693/13.

164. Kar zadeva nevtralnost in neodvisnost prefekturnih komisij za javno varnost, so, kot je navedeno v osnutku sklepa o ustreznosti[72], te komisije ustanovljene pod pristojnostjo guvernerja prefekture, ki mora imenovati člane komisije in pri tem dobiti soglasje skupščine prefekture. Člani prefekturne komisije za javno varnost imajo triletni mandat, ki se lahko do dvakrat podaljša. Člen 39 Zakona o policiji določa omejitve v zvezi z imenovanjem članov. V osnutku sklepa o ustreznosti je omenjen tudi nadzor, ki ga nad prefekturno policijo izvaja lokalna skupščina, pri čemer je naveden sklic na člen 100 Zakona o lokalni avtonomiji. Vendar EOVP ta akt ni bil poslan[73].

165. Poleg tega je v členu 42(2) in (3) Zakona o policiji navedeno, da noben član komisije ne postane obenem član skupščine ali osebja, ki v lokalnih javnih organih opravlja delo s polnim ali krajšim delovnim časom, kot je določeno v določbi iz odstavka 1 člena 28(5) Zakona o lokalni javni službi.

166. EOVP se glede na navedene elemente in ob upoštevanju sodelovanja med prefekturnimi komisijami za javno varnost in nacionalno komisijo za javno varnost strinja z osnutkom sklepa o ustreznosti ter pozdravlja nevtralnost in neodvisnost članov prefekturnih komisij za javno varnost. Glede na njegovo razumevanje imajo prefekturne komisije za javno varnost le pooblastilo za preiskovanje ravnanja policije, nimajo pa drugih nadzornih pooblastil , vključno z izbrisom podatkov, ki jih je zbrala prefekturna policija . Zato se zdi, da je potrebno dodatno pojasnilo o tem, ali nadzor, ki s ga izvajajo prefekturne komisije za javno varnost, zadostuje standardom, določenim v okviru prava EU.

4.1.2.2.3 Nadzor, ki ga izvaja parlament

167. Osnutek sklepa o ustreznosti[74] in Priloga II[75] vsebujeta nekatere informacije o nadzoru, ki ga v zvezi z vlado izvaja parlament, tudi glede zakonitosti zbiranja podatkov s strani policije. V obeh je sklic na člen 62 ustave, v skladu s katerim lahko parlament zahteva predložitev dokumentov in zaslišanje prič. V obeh so omenjene tudi pravne določbe Zakona o parlamentu, zlasti člen 104 o pooblastilih parlamenta in člen 74 o predložitvi pisnih poizvedb, na katere mora kabinet pisno odgovoriti v sedmih dneh, kot je določeno v členu 75. V osnutku sklepa o ustreznosti je dodano še, da je "vloga parlamenta pri nadzoru izvršilne oblasti podprta z obveznostmi poročanja, na primer v skladu s členom 29 Zakona o prisluškovanju telefonskim pogovorom".

168. EOVP priznava vključenost parlamenta pri nadzoru vlade in policije, ki se nanaša na zakonitost zbiranja podatkov.

4.1.2.2.4 Nadzor, ki ga izvaja izvršilna oblast

169. Po eni strani je za nadzor in izvajanje, ki temeljita na podlagi japonskega zakona o varstvu osebnih podatkov v lasti upravnih organov (Act on the Protection of Personal Information Held by Administrative Organs, v nadaljnjem besedilu: zakon APPIHAO), v skladu s Prilogo II k osnutku sklepa o ustreznosti pristojen minister ali predstojnik posameznega ministrstva ali agencije[76]. Po drugi strani ima minister za notranje zadeve in komunikacije preiskovalna pooblastila v zvezi s tem, kako vsa druga ministrstva, vključno z ministrom za pravosodje in policijo, izvajajo zakon APPIHAO, kot je navedeno v osnutku sklepa o ustreznosti[77].

170. Minister lahko od predstojnika upravnega organa na podlagi člena 50 zakona APPIHAO zahteva predložitev gradiva in pojasnil o tem, kako zadevni upravni organ obdeluje osebne podatke v skladu s členom 50 zakona APPIHAO. V primeru suma kršitve ali neustreznega učinkovanja tega zakona lahko

[72] Glej osnutek sklepa o ustreznosti, str. 31.
[73] Glej osnutek sklepa o ustreznosti, str. 33.
[74] Glej osnutek sklepa o ustreznosti, str. 30.
[75] Glej Prilogo II, str. 12.
[76] Glej Prilogo II, str. 10.
[77] Glej Prilogo II, str. 11.

zahteva revizijo ukrepov ter izdaja mnenja v zvezi s tem, kako zadevni upravni organ obdeluje osebne podatke, skladno s členoma 50 in 51 zakona APPIHAO.

171. V osnutku sklepa o ustreznosti in Prilogi II je navedeno tudi, da je bilo ustanovljenih 51 celovitih informacijskih centrov, ki "zagotavljajo nemoteno izvajanje tega zakona" v skladu s členom 47 zakona APPIHAO. EOVP ugotavlja, da v zakonu APPIHAO niso nadalje pojasnjene vloga in pooblastila teh informacijskih centrov, nekaj podrobnosti pa vsebuje osnutek sklepa o ustreznosti.

172. Zato EOVP odobrava dejstvo, da minister za notranje zadeve in komunikacije izvaja izvršilni nadzor nad tem, kako ministrstva in upravni organi spoštujejo zakon APPIHAO.

173. Nazadnje, zakonodaja EU in EKČP v sodni praksi svojih ustreznih sodišč vzpostavljata standarde in jamstva, v skladu s katerimi mora biti nadzor popoln, nevtralen in neodvisen. EOVP ugotavlja, da Komisija za varstvo osebnih podatkov nima nadzornih pooblastil v zadevah, povezanih s preprečevanjem, odkrivanjem, preiskovanjem in pregonom kaznivih dejanj. Čeprav se zdi, da je nadzor, ki ga izvajajo parlament, nacionalna in prefekturna komisija za javno varnost nevtralen in neodvisen, je treba dodatno pojasniti nadzorna pooblastila prefekturnih komisij za javno varnost.

4.1.3 Pravna sredstva na področju kazenskega prava

174. V osnutku sklepa o ustreznosti, dopolnjenem s Prilogo II, je predstavljenih več možnosti, prek katerih lahko posamezniki vložijo pritožbe pri neodvisnih organih in sodnikih.

175. V nadaljevanju so na podlagi razpoložljive dokumentacije predstavljeni te možnosti in glavni elementi teh postopkov, in sicer po kratkem pregledu razpoložljivih pravic, da se pojasni, kaj lahko posamezniki, na katere se nanašajo osebni podatki, pričakujejo od javnih organov v okviru obdelave podatkov na področju kazenskih postopkov.

4.1.3.1 Razpoložljive pravice posameznikov, na katere se nanašajo osebni podatki, v okviru kazenskih postopkov

176. Da bi lahko posamezniki, na katere se nanašajo osebni podatki, pridobili pravno varstvo, morajo v skladu z zakonodajo najprej imeti pravice, da lahko vložijo pritožbe zaradi nespoštovanja teh pravic. Zato je EOVP tudi ocenil razpoložljive pravice v okviru kazenskih postopkov, predstavljene v osnutku sklepa o ustreznosti.

4.1.3.1.1 Splošne omejitve pravic posameznikov, na katere se nanašajo osebni podatki, v skladu z zakonom APPIHAO

177. Komisija se v osnutku sklepa o ustreznosti sklicuje in opira na splošna načela varstva podatkov, ki jih morajo spoštovati javni organi, potem ko zberejo osebne podatke. Ta načela so podrobneje opisana tudi v Prilogi II, zato se je EOVP odločil, da tudi v zvezi z njimi navede pripombe.

178. EOVP glede razpoložljivih pravic ugotavlja, da v skladu s Prilogo II osnutka sklepa o ustreznosti nekatere splošne pravice, zagotovljene posameznikom, na katere se nanašajo osebni podatki, v zvezi s podatki, ki jih obdelujejo upravni organi, ostanejo na voljo tudi v okviru kazenskih preiskav. Vendar iz zakona APPIHAO izhajajo tudi dodatne omejitve glede zbiranja in nadaljnjega ravnanja z osebnimi podatki v tem okviru.

179. Te omejitve, ki veljajo tako za podatke, zbrane na podlagi naloga, kot za podatke, zbrane na podlagi poizvedbe v okviru prostovoljnega razkritja, vzbujajo pomisleke v zvezi z več vidiki.

180. Čeprav se od upravnih organov glede načela omejitve namena načeloma zahteva, da določijo namen, zaradi katerega hranijo osebne podatke, in čeprav hramba teh podatkov ne sme presegati tistega, kar

je potrebno za doseganje določenega namena uporabe, lahko namen spremenijo, če se lahko "razumno šteje, da se ustrezno nanaša na prvotni namen".

181. V zakonu APPIHAO je določeno tudi načelo nerazkritja, v skladu s katerim zaposleni pridobljenih osebnih podatkov ne sme razkriti drugi osebi brez utemeljenega razloga ali takih podatkov uporabiti za nepravičen namen. Niso pa zagotovljene dodatne informacije o tem, kaj bi lahko zajemal "utemeljen razlog" ali "neupravičen namen", tako da bi bila za oceno potrebna dodatna pojasnila.

182. Člen 8(1) zakona APPIHAO določa tudi prepoved uporabe ali razkritja podatkov, "razen če ni v zakonih in predpisih določeno drugače". Čeprav ta določba načeloma ni v nasprotju s stopnjo varstva, zagotovljeno v skladu z zakonodajo EU, EOVP manjkajo dodatni elementi o tem, v kolikšni meri se nadzor ali pregledi izvajajo, kadar je razkritje določeno z zakoni ali predpisi. Poleg tega se v skladu s členom 8(2) za to pravilo uporabljajo dodatne izjeme, če "ni verjetno, da bi takšno izredno razkritje povzročilo neupravičeno škodo pravicam in interesom posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe". Brez nadaljnjih elementov v zvezi s tem je treba to izjemo, ki se nanaša na nejasen pojem "neupravičene škode", dodatno pojasniti, če je to dovolj ozko.

183. V členu 9 zakona APPIHAO so določene dodatne omejitve namena ali metode uporabe ali katere koli druge omejitve, ki jih naloži predstojnik upravnega organa, ko se shranjeni osebni podatki zagotavljajo drugi osebi. Ker sta zvezi "katere koli druge potrebne omejitve" in "zagotavljajo drugi osebi" zelo široki, te dodatne omejitve pravic posameznikov, na katere se nanašajo osebni podatki, vzbujajo pomisleke, ne da bi se dodatno pojasnilo področje uporabe te določbe.

184. Čeprav se EOVP v celoti zaveda, da so pravice dostopa in druga načela varstva podatkov v kazenskih postopkih omejeni tudi v skladu z zakonodajo EU i, so zagotovljeni dodatni zaščitni ukrepi, tudi v smislu nadzora, pregleda in pravnih sredstev, kadar so take omejitve predvidene. Ker ni na voljo ustrezne sodne prakse o teh omejitvah ali dodatnih elementov za pojasnitev področja uporabe teh določb, EOVP ne more oceniti, ali so te omejitve pravic posameznikov, na katere se nanašajo osebni podatki, omejene na to, kar bi se štelo za nujno potrebno in sorazmerno v skladu z zakonodajo EU ter bi bilo zato bistveno enakovredno pravicam posameznikov iz EU, na katere se nanašajo osebni podatki.

4.1.3.1.2 Dodatne omejitve v zvezi s pravicami iz zakona APPIHAO, ki izhajajo iz Zakonika o kazenskem postopku in odlokov prefekturne policije

185. Čeprav se zdi, da se zakon APPIHAO uporablja pri vseh obdelavah, ki jih izvajajo upravni organi na Japonskem, EOVP ugotavlja, da iz določenih zakonodajnih aktov izhajajo nekatere pomembne omejitve pravic posameznikov, na katere se nanašajo osebni podatki. V členu 53(2) Zakonika o kazenskem postopku[78] je posebej navedeno, da so "osebni podatki, evidentirani v dokumentih, ki se nanašajo na sodne postopke in zasežene predmete", izvzeti s področja uporabe posameznih pravic iz poglavja IV zakona APPIHAO. EOVP zato konkretno razume, da posamezniki, na katere se nanašajo osebni podatki, v okviru kazenskih postopkov nimajo koristi od pravic do seznanitve, dostopa, popravka ali izbrisa osebnih podatkov, evidentiranih v dokumentih, ki se nanašajo na sojenja in zasežene predmete.

186. Glede na razumevanje EOVP se te omejitve uporabljajo za podatke, zbrane na podlagi nalogov, in tudi za podatke, zbrane na podlagi obrazca za poizvedbo v okviru prostovoljnega razkritja (glej v nadaljevanju). Dejansko se zdi, da se kot pravna podlaga obeh postopkov za dostop do podatkov (na podlagi naloga in na podlagi obrazca za poizvedbo) iz Zakonika o kazenskem postopku uporablja člen 53(2) tega zakonika in velja za obe vrsti zbiranja podatkov. Ker se člen 53(2) nanaša na zasežene

[78] Na voljo na povezavi http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 in navedeno v opombi 25 Priloge II k osnutku sklepa o ustreznosti.

predmete, bi se lahko pojasnilo, ali se omejitve pravic, predvidene s to določbo uporabljajo tudi v okviru prostovoljnega razkritja.

187. EOVP obžaluje, da mu niso bili poslani odloki prefekturne policije , s katerimi naj bi se osebni podatki, pravice in obveznosti varovali enako kot z zakonom APPIHAO. EOVP se ob upoštevanju nejasnosti v zvezi z razlago zakona APPIHAO in nerazpoložljivosti odlokov prefekturne policije sprašuje, ali pravice, zagotovljene posameznikom v tem okviru, ter dodatni nadzorni in/ali mehanizmi pravnih sredstev zadostujejo za nadomestitev odsotnosti pravic.

4.1.3.2 Pravno varstvo s pravnimi sredstvi neodvisnih organov

4.1.3.2.1 Upravno varstvo

188. EOVP ugotavlja, da so upravni organi, ki zbirajo podatke, kot je prefekturna policija , pristojni za obravnavanje prošenj posameznikov glede njihovih – omejenih – pravic v zvezi s podatki, zbranimi v okviru kazenskih preiskav (glej zgoraj o pravicah, ki so na voljo), za katere se zdi, da vključujejo tako zbiranje podatkov na podlagi naloga kot na podlagi obrazcev za poizvedbo. Te pravice se konkretno zdijo omejene na splošna načela, kot so potreba po hrambi podatkov v zvezi z namenom (glej člen 3(1) zakona APPIHAO), načelo omejitve namena (člen 4) ali točnosti podatkov (člen 5), medtem ko so posamezne pravice, kot so pravica do seznanitve, dostopa, popravka ali izbrisa, izključene za osebne podatke, evidentirane v dokumentih, ki se nanašajo na sojenja in zasežene predmete[79]. Čeprav teh organov ni mogoče obravnavati kot neodvisnih in zato kot takih, ki zagotavljajo neodvisna pravna sredstva ali nadzor, EOVP pozdravlja to možnost. Vendar poudarja, da pritožbe, vložene v zvezi s tem, ostajajo omejene na zelo malo pravic posameznikov, na katere se nanašajo osebni podatki, glede na omejitve pravic iz zakona APPIHAO.

189. Ker so osebni podatki, evidentirani v dokumentih, ki se nanašajo na sojenja in zasežena predmete, v skladu s členom 53(2) Zakonika o kazenskem postopku izključeni s področja uporabe individualnih pravic iz poglavja IV zakona APPIHAO, so možnosti za zahtevanje dostopa do osebnih podatkov prav tako omejene na postopke, predvidene z drugimi določbami tega zakonika o kazenskem postopku. Zdi se, da lahko v tem okviru ukrepajo le žrtve, osumljenci ali obdolženci in še to odvisno od faze kazenskega postopka. Zato EOVP izraža zaskrbljenost, da v okviru japonske zakonodaje na področju kazenskega postopka posameznikom, na katere se nanašajo osebni podatki, ni na voljo nobena splošna pravica do dostopa in/ali popravka ali izbrisa podatkov ter da vsa razpoložljiva pravna sredstva vključujejo bodisi žrtev (v tem primeru bi oseba verjetno vedela, da so bili njeni podatki zbrani) ali osumljenca ali obdolženca ali dokaz škode, medtem ko bi morali imeti tudi posamezniki, na katere se nanašajo osebni podatki, pravico dostopa do svojih podatkov in po možnosti pravico do njihovega popravka ali izbrisa, če (morda še) niso utrpeli škode in/ali če niso žrtev, osumljenec ali obtoženec, ampak na primer priča.

4.1.3.2.2 Upravno varstvo prek prefekturnih komisij za javno varnost

190. Poleg tega so za obravnavo pritožb očitno pristojne prefekturne komisije za javno varnost. Na podlagi člena 79 Zakona o policiji, navedenega v osnutku sklepa o ustreznosti, se lahko posamezniki pritožijo proti kakršnemu koli nezakonitemu ali nepravilnemu ravnanju policista pri opravljanju njegove dolžnosti.

191. EOVP želi pojasnilo, ali kakršnakoli “nezakonita“ obdelava osebnih podatkov izpolnjuje pogoje za “nezakonito ali nepravilno ravnanje policista“ in o dokazovanju škode, ki se zahteva od posameznika, na katerega se nanašajo osebni podatki. V obvestilu, ki ga je Nacionalna policijska agencija izdala policiji

[79] Glej zgoraj navedene omejitve v zvezi z zakonom APPIHAO in glej zlasti člen 53(2) Zakonika o kazenskem postopku (ni zagotovljen, vendar je naveden v opombi 25 Priloge II k osnutku sklepa o ustreznosti).

in prefekturnim komisijam za javno varstvo, o ustreznem obravnavanju pritožb, ki se nanašajo na to, kako policijski uradniki opravljajo njihove dolžnosti, so pritožbe omejene na konkretne zahtevke za "popravo kakršne koli škode, povzročene zaradi nezakonitega ali neprimernega ravnanja ali če policijski uradnik pri opravljanju svojih dolžnosti ne sprejme potrebnih ukrepov", in "možnost vložitve pritožbe/izražanja nezadovoljstva glede neustreznega načina, kako policijski uradnik opravlja svoje dolžnosti". Izrecno je pojasnjeno, da se "pritožbe, ki se nanašajo na neizpolnjevanje obveznosti policijskega uradnika o kateri koli zadevi, ki spada med njegove dolžnosti, ter tudi tiste, ki izražajo splošno mnenje ali predlog in ne vplivajo neposredno na stranko pritožnico samo, izključijo".

192. EOVP v zvezi s postopkovnimi zahtevami pri vložitvi pritožbe, čeprav jih je treba vložiti v pisni obliki, ugotavlja, da je v skladu z japonsko zakonodajo v tem okviru zagotovljena pomoč pri pisanju pritožb, tudi za tujce. Poleg tega se zdi, da je japonska vlada Komisiji za varstvo osebnih podatkov naložila tudi obveznost, da posameznikom iz EU, na katere se nanašajo osebni podatki, zagotavlja pomoč pri obravnavi in reševanju pritožb na tem področju, kar EOVP pozdravlja. Kot razume EOVP, bo Komisija za varstvo osebnih podatkov v tem okviru delovala le kot kontaktna točka med posamezniki iz EU, na katere se nanašajo osebni podatki, in pristojnimi organi na Japonskem.

193. Uradno obveščanje o rezultatih pritožbe pri prefekturni komisiji za javno varnost se ne izvede v zadevah iz člena 79(2) Zakona o policiji, kar vključuje tudi primere, v katerih trenutno "prebivališče pritožnika ni znano". EOVP ugotavlja, da sklicevanje na prebivališče ne pomeni, da bodo posamezniki iz EU, na katere se nanašajo osebni podatki, zato v vseh primerih izključeni iz uradnega obvestila o rezultatih njihovih pritožb, ker ne prebivajo na Japonskem.

4.1.3.2.3 Posebni mehanizem, ki vključuje Komisijo za varstvo osebnih podatkov

194. Glede na navedene ugotovitve EOVP izraža odobravanje glede tega, da sta japonska vlada in Evropska komisija sklenili dodatni mehanizem pravnega varstva, ki posameznikom iz EU zagotavlja dodatne možnosti pravnih sredstev na Japonskem, s katerimi lahko posamezniki uveljavijo tudi pravna sredstva proti nezakonitim in nepravilnim preiskavam s strani javnih organov. Prav tako ugotavlja in odobrava, da se zahtevki lahko vložijo pri Komisiji za varstvo osebnih podatkov in ne pri drugem vladnem uradu, s čimer se obseg pristojnosti te komisije razširi na področje preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter na področje nacionalne varnosti.

195. Pri analizi novega mehanizma je bil EOVP usmerjen na razumevanje pooblastil, ki jih ima Komisija za varstvo osebnih podatkov v tem okviru.

196. Čeprav jezik ni povsem jasen, EOVP razume, da dodatni mehanizem pravnega varstva ne zahteva "procesnega upravičenja" v smislu, da vložniku ni treba dokazati, da je japonski organ verjetno nadzoroval njegove osebne podatke. EOVP še vedno želi potrditev Komisije.

197. EOVP v skladu s svojo oceno mehanizma varuha človekovih pravic, ustvarjenega v okviru zasebnostnega ščita, poudarja potrebo po učinkovitih pooblastilih naslovnika zahtevka, v tem primeru Komisije za varstvo osebnih podatkov, da bi se mehanizem pravnega varstva obravnaval kot bistveno enakovreden učinkovitemu pravnemu sredstvu v smislu člena 47 Listine o temeljnih pravicah.

198. Japonska vlada se pri razlagi mehanizma pravnega varstva sklicuje na člen 6, člen 61(ii) in člen 80 ZVOP ter določa ta pooblastila v Prilogi II. EOVP razume, da postopek, kot je opisan v Prilogi II, podrobneje določa ali razširja pooblastila Komisije za varstvo osebnih podatkov, saj je besedilo člena 6, člena 61(ii) in člena 80 ZVOP precej nejasno in splošno. Kolikor so v Prilogi II določena ali razširjena pooblastila Komisije za varstvo osebnih podatkov, želi EOVP dobiti pojasnilo, ali zavezujejo tudi druge agencije japonske vlade.

199. EOVP na podlagi postopka iz Priloge II ugotavlja, da morajo pristojni javni organi na Japonskem sodelovati s Komisijo za varstvo osebnih podatkov, "vključno s tem, da ji zagotavljajo potrebne informacije in ustrezno gradivo, tako da komisija lahko oceni, ali je zbiranje ali nadaljnja uporaba osebnih podatkov potekala v skladu z veljavnimi pravili". Da bi se ocenila učinkovitost sistema, se je torej treba znova sklicevati na pooblastila teh navedenih pristojnih organov, s katerimi sodeluje Komisija za varstvo osebnih podatkov. Kot razume EOVP, se ta pooblastila z zagotovili iz Priloge II ne bi razširila.

200. EOVP ugotavlja še, da če je bila ugotovljena kršitev pravil, "sodelovanje zadevnih javnih organov s Komisijo za varstvo osebnih podatkov vključuje obveznost odprave kršitve", kar izrecno vključuje izbris podatkov, zbranih v nasprotju z veljavnimi pravili. Razume, da obveznosti pristojnega organa izhajajo iz sodelovanja s Komisijo za varstvo osebnih podatkov in ne iz odločitve te komisije.

201. Komisija za varstvo osebnih podatkov bo vložnika obvestila o "rezultatu ocenjevanja, vključno z morebitnimi popravnimi ukrepi, ki se po potrebi sprejmejo". Obvestila ga bo tudi o "možnosti, da zahteva potrditev rezultatov od pristojnega javnega organa in organu, pri katerem se taka zahteva za potrditev vloži".

202. Poleg tega se je Komisija za varstvo osebnih podatkov zavezala, da bo vložniku pomagala pri vlaganju nadaljnjih pravnih sredstev v skladu z japonsko zakonodajo, če vložnik ni zadovoljen z izidom postopka.

203. EOVP se ob upoštevanju potrebe po učinkovitem mehanizmu pravnega varstva, ki je v osnovi enakovreden standardom EU, kljub temu sprašuje, ali ima Komisija za varstvo osebnih podatkov kakšna posebna pooblastila, razen tistih za ocenjevanje tega, ali je bilo zbiranje ali poznejša uporaba osebnih podatkov izvedeno v skladu z veljavnimi pravili, ter pristojne organe poziva, naj uporabijo svoja pooblastila in obravnavajo pritožbe, ki jim jih je posredovala komisija. Če bi komisija delovala le kot kontaktna točka za posameznike iz EU, po mnenju EOVP to ne bi zadostovalo za zagotovitev učinkovitih pravnih sredstev, bistveno enakovrednim standardom EU. EOVP zato Komisijo poziva, naj navede pojasnila o točkah iz tega podpoglavja, zlasti o tem, ali in kako mehanizem razširja obveznosti pristojnih organov, kako jih zavezuje ter kako lahko Komisija za varstvo osebnih podatkov učinkovito zagotavlja skladnost in ne deluje le kot kontaktna točka za posameznike iz EU.

4.1.3.3 Sodno varstvo

4.1.3.3.1 Mehanizem za neprave pritožbe

204. Tako imenovani "postopek neprave pritožbe" omogoča ukrepanje proti obveznemu zbiranju podatkov na podlagi naloga, da se prekliče ali spremeni nezakonit zaseg.

205. Ta možnost pomeni, da se posameznik zaveda, da so bili podatki zaseženi. Vendar EOVP razume, da posameznik, na katerega se nanašajo osebni podatki, ni uradno obveščen o postopku zbiranja podatkov na podlagi naloga. Prav tako razume, da prostovoljno razkritje ne pomeni, da morajo družbe, ki so jim bile poslane zahteve, obvestiti posameznike, na katere se nanašajo osebni podatki, o prejetih in izpolnjenih zahtevah. Čeprav je v Prilogi II poudarjeno, da se "lahko tak poziv vloži, ne da bi moral posameznik počakati na zaključek zadeve", se v praksi zdi, da je ta možnost razen nalogov, ki dovoljujejo prisluškovanje telefonskim pogovorom in za katere je navedeno, da je v zakonodaji določena obveznost uradnega obveščanja[80], dejansko na voljo šele, ko se posameznik, na katerega se nanašajo osebni podatki, seznani z zbiranjem prek tožbe, vložene zoper njega.

[80] Člen 23 Zakona o prisluškovanju telefonskim pogovorom je naveden na strani 33 osnutka sklepa o ustreznosti, vendar EOVP to besedilo ni bilo poslano, zato ne more oceniti, v kakšnem obsegu se obveznost uradnega obveščanja uporablja in v katerih primerih se lahko omeji.

4.1.3.3.2 Sodna prepoved

206. Poleg tega lahko posamezniki na sodišču vložijo civilne tožbe, da bi dosegli izbris podatkov, zbranih na podlagi kazenskega postopka (t. i. sodna prepoved), ali uveljavljali odškodnino za škodo.

207. EOVP glede nadomestila ugotavlja, da se postopek zdi omejen na primere, v katerih je javni uslužbenec pri opravljanju svojih nalog nezakonito in napačno (namerno ali iz malomarnosti) povzročil škodo zadevnemu posamezniku. EOVP razume, da škoda vključuje moralno škodo. Vendar ni nadalje podrobneje določeno, kaj mora dokazati posameznik, ki je utrpel škodo. EOVP ni mogel oceniti sodne prakse v zvezi z dodelitvijo nadomestila in zato ne more oceniti, ali ta možnost zagotavlja učinkovito pravno sredstvo v primeru škode.

208. EOVP v zvezi s "sodno prepovedjo" ugotavlja tudi, da mora biti posameznik, da bi lahko vložil pritožbo, najprej seznanjen s tem, da so bili njegovi podatki zbrani in da se še vedno hranijo. Glede na omejeno pravico do obveščenosti in pravico dostopa posameznikov v okviru kazenskih preiskav in postopkov se zato zdi, da je precej omejena tudi učinkovitost postopka.

4.1.3.4 Splošna ocena možnosti pravnih sredstev

209. Po oceni vseh možnosti pravnih sredstev, ki so na voljo posameznikom v skladu z japonsko zakonodajo ter posameznikom iz EU, na katere se nanašajo osebni podatki, pri Komisiji za varstvo osebnih podatkov, EOVP odobrava začasni mehanizem za reševanje sporov, v katerega je vključena Komisija za varstvo osebnih podatkov. Za posameznike iz EU, na katere se nanašajo osebni podatki, ima dodano vrednost, zlasti zato, ker jim omogoča razumeti, katere možnosti imajo na voljo za pridobitev pravnega varstva in/ali uveljavljanje odškodnine ter za predstavitev svojih zahtevkov v skladu z veljavnimi postopkovnimi zahtevami japonske zakonodaje. Vseeno pa so potrebna dodatna pojasnila, zlasti o tem, ali in kako mehanizem razširja obveznosti pristojnih organov, kako jih zavezuje ter kako lahko Komisija za varstvo osebnih podatkov učinkovito zagotavlja skladnost, da bi lahko ta mehanizem pomenil učinkovito pravno varstvo.

210. Ta ocena kaže, da se zdi, da noben mehanizem pravnega varstva v japonski zakonodaji ne omogoča dostopa, popravka ali izbrisa podatkov z posameznikom, na katere se nanašajo osebni podatki, ki niso žrtve, osumljenci ali obtoženci v okviru kazenskega postopka, na primer za odpravo nezakonitega zbiranja ali hrambe njihovih podatkov. Poleg tega kaže, da vsi mehanizmi pravnega varstva in odškodnin ter postopki, ki so v skladu z japonsko zakonodajo na voljo žrtvam, osumljencem ali obdolžencem, pomenijo seznanitev z zbiranjem podatkov, za katerega se zdi, da je v praksi omejeno, saj zanje veljajo omejene pravice dostopa in pravice do obveščenosti. Poleg tega se zdi potrebno dodatno pojasnilo o dokazovanju nezakonitega ravnanja s strani organov, zlasti o tem, ali takšno ravnanje vključuje kakršno koli nezakonito obdelavo osebnih podatkov ali škodo, ki jo je utrpel posameznik.

211. Ker EOVP nima dodatne dokumentacije in elementov, izraža zaskrbljenost glede tega, ali je pravno varstvo v skladu z japonsko zakonodajo in osnutkom sklepa o ustreznosti dovolj učinkovito v primerjavi s standardi zakonodaje EU.

4.2 Dostop za namene nacionalne varnosti

4.2.1 Obseg nadzora

212. V osnutku sklepa o ustreznosti je poglavje o "dostopu in uporabi japonskih javnih organov za namene nacionalne varnosti" uvedeno s splošno izjavo, kar je skladno z zagotovilom japonske vlade iz Priloge II, po katerem noben japonski zakon ne bi določal in s tem omogočal "obveznih zahtev za informacije ali prisluškovanje upravnim telefonskim pogovorom zunaj kazenskih preiskav". Kot sklep je navedeno, da se "lahko podatki zaradi nacionalne varnosti pridobijo le iz vira informacij, do katerega lahko vsakdo

prosto dostopa, ali s prostovoljnim razkritjem“. To izključuje vse tajne nadzorne dejavnosti na tem področju. Poslovni subjekti, ki jim je poslana prošnja za prostovoljno sodelovanje (v obliki razkritja elektronskih informacij), niso pravno zavezani k zagotavljanju takih informacij[81].

213. V okviru teh omejitev so navedeni štirje vladni subjekti, ki so pooblaščeni za zbiranje elektronskih informacij japonskih poslovnih subjektov zaradi nacionalne varnosti. V zvezi z Ministrstvom za obrambo, kot enim od teh štirih subjektov, je navedeno, da “ima le pooblastilo za zbiranje (elektronskih) informacij na podlagi prostovoljnih razkritij[82].

214. EOVP želi pri oceni splošne sheme za zbiranje podatkov za namene nacionalne varnosti opozoriti na prvo od štirih tako imenovanih “bistvenih jamstev“, v skladu s katerim mora obdelava temeljiti na jasnih, natančnih in dostopnih pravilih“[83]. ESČP je natančneje zelo jasno opredelilo, da so programi nadzora „določeni z zakonom“ le, če imajo nadzorni ukrepi „določeno podlago v nacionalnem pravu“. Sodišče je pojasnilo, da mora biti zakon, ki dovoljuje ukrep, zaradi združljivosti z načelom vladavine prava dostopen in predvidljiv glede svojih učinkov. Sodišče je ob sklicevanju na tveganje samovoljnega ravnanja zahtevalo „jasna, podrobna pravila o ukrepih tajnega nadzora“, ki bi bila „dovolj jasna, da bi se državljanom zagotovila ustrezna navedba okoliščin, v katerih, in pogojev, v skladu s katerimi so javni organi pooblaščeni za uporabo takega ukrepa“[84].

215. EOVP se pri uporabi teh bistvenih jamstev za pravni sistem Japonske ne zaveda le dejstva, da imajo države pri vprašanjih na področju nacionalne varnosti široko diskrecijsko pravico, ki jo priznava Evropsko sodišče za človekove pravice. Iz pristojnosti na področju nacionalne varnosti so razvidne tudi zgodovinske izkušnje narodov. EOVP se torej zaveda, da so imele japonske nacionalne obveščevalne službe po drugi svetovni vojni, kot je poudarila japonska vlada, bolj omejena pooblastila kot v drugih državah.

216. Glede na obravnavo EOVP osnutek sklepa o ustreznosti skupaj z zagotovilom japonske vlade kaže, da japonski vladni subjekti ne izvajajo programov, ki strateško spremljajo ali na splošno nadzorujejo (internetno) komunikacijo. Kot je navedeno zgoraj, je japonska vlada v dopisu, ki ga je podpisal minister za pravosodje, zagotovila, da „se lahko podatki zaradi nacionalne varnosti pridobijo le iz vira informacij, do katerega lahko vsakdo prosto dostopa, ali s prostovoljnim razkritjem“.

217. EOVP glede pravne podlage Ministrstva za obrambo ugotavlja, da osnutek sklepa o ustreznosti vključuje splošne informacije o njegovih pooblastilih in kot njegovo nalogo navaja „opravljanje takih zadev, povezanih s tem, da bi se zagotovil nacionalni mir in neodvisnost ter varnost naroda“. Vendar EOVP ni prejel angleškega prevoda pravne podlage.

218. Hkrati se EOVP zaveda poročil, objavljenih v različnih medijih, ki kažejo na to, da programe nadzora izvaja Direktorat za obveščevalne dejavnosti pri zaznavanju signalov pri japonskem Ministrstvu za obrambo[85]. V poročilu je tudi navedeno, da japonsko Ministrstvo za obrambo, čeprav ni želelo razpravljati o podrobnostih poročila, „priznava, da ima Japonska „urade po vsej državi“, ki prestrezajo komunikacijo, ter da bi moralo biti to „usmerjeno na vojaške dejavnosti“ in „kibernetske grožnje“, ne

[81] Odstavek 151 sklepa o ustreznosti varstva.

[82] Odstavek 153 sklepa o ustreznosti varstva.

[83] Delovna skupina iz člena 29, delovni dokument WP237: Delovni dokument št. 01/2016 o utemeljenosti posegov v temeljne pravice do zasebnosti in varstva podatkov z ukrepi nadzora pri prenosu osebnih podatkov (temeljna zagotovila EU).

[84] Glej na primer sodbo ESČP v zadevi Big Brother Watch in drugi proti Združenemu kraljestvu, točka 305.

[85] Na spletišču za objavo novic organizacije „The Intercept“ je bilo maja 2018 objavljeno poročilo z naslovom „The untold story of Japan’s secret spy agency“ (Nerazkrita zgodba o japonski skrivni vohunski agenciji).

pa na „zbiranje informacij splošne javnosti“. Zadnja izjava (da Ministrstvo za obrambo ne zbira informacij o splošni javnosti) je sestavni del ponovne izjave japonske vlade.

219. To pomeni, da je japonska vlada v pismu, ki ga je podpisal minister za pravosodje, ponovno zatrdila, da Ministrstvo za obrambo ne zbira informacij o splošni javnosti.

220. EOVP nima naloge, da bi izdelal splošno oceno morebitnih zmogljivosti za nadzor japonske vlade. Te dejavnosti so pomembne le pri njegovi oceni, ali se nanašajo na prenos osebnih podatkov med EU in Japonsko. V zvezi s tem želi EOVP ponovno potrditi svoj pristop, ki ga je že sprejel njegov predhodnik, ko je bil zaprošen za mnenje o zasebnostnem ščitu EU-ZDA. Delovna skupina iz člena 29 je pri pripravi mnenja o zasebnostnem ščitu v svojo analizo vključila pooblastila in omejitve ZDA za izvajanje nadzora podatkov “na poti“ v ZDA[86]. EOVP, ki uporablja enak standard za sklep o ustreznosti za Japonsko, meni, da so informacije o pooblastilih japonskih organov za nadzor podatkov “na poti“ na Japonsko pomembne. Če ta pooblastila za nadzor obstajajo, se zdi, da odločitev ESČP v zadevi Big Brother Watch kaže, da bi bilo treba taka pooblastila urediti v skladu s standardi, ki jih določa ESČP.

221. Posledica tega je, da če so bila prestrezanja omejena “na pomoč pri vojaškem ukrepanju“, morda niso pomembna za oceno sklepa o ustreznosti. Zato si želi EOVP prejeti pojasnila o nadzornih ukrepih japonskih vladnih subjektov. Taka pojasnila bi bila v zvezi s tem dobrodošla, da se ugotovi, ali lahko do podatkov, ki se prenašajo v skladu s tem okvirom ustreznosti, dostopajo japonski pristojni organi na tem področju za namene nacionalne varnosti.

4.2.2 Prostovoljno razkritje v primeru nacionalne varnosti

222. V osnutku sklepa o ustreznosti je navedeno, da so za zbiranje (elektronskih) informacij s prostovoljnim razkritjem pooblaščeni le štirje vladni subjekti. V skladu z osnutkom sklepa in Prilogo II obstajajo nekatere omejitve v zvezi z zakonskimi razlogi, kar pomeni, da je zbiranje podatkov omejeno na to, kar je potrebno za izvajanje nalog subjektov.

223. Kot je navedeno v razdelku o preprečevanju, odkrivanju, preiskovanju in pregonu kaznivih dejanj, je prostovoljno razkritje na področju kazenskega prava dovoljeno le v okviru preiskave kaznivega dejanja, pri čemer se torej domneva o utemeljenem sumu kaznivega dejanja, ki je bilo že storjeno. Preiskave na področju nacionalne varnosti se razlikujejo od preiskav na področju preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj. EOVP priznava, da se v skladu s Prilogo II osrednji načeli “potrebe po preiskavi“ in “ustreznosti metode“ podobno uporabljata na področju nacionalne varnosti in da je treba zagotoviti skladnost z njima ter pri tem upoštevati posebne okoliščine posamezne zadeve[87]. Obžaluje, da uporaba ni nadalje pojasnjena, tudi z nadaljnjim sklicevanjem na sodno prakso. Kljub temu navaja, da mora biti uporaba tega postopka sorazmerna ali potrebna.

224. Ko se osebni podatki zberejo (pridobijo), je ravnanje z njimi v skladu z osnutkom sklepa urejeno z zakonom APPIHAO, razen za prefekturno policijo [88]. V Prilogi II je navedeno, da je način, kako prefekturna policija ravna z osebnimi podatki, urejen s prefekturnimi odloki, ki določajo načela za

[86] Glej delovni dokument WP255, EU-U.S. Privacy Shield –First annual joint review (Zasebnostni ščit EU-ZDA – prvi letni skupni pregled), sprejet 28. novembra 2017, str. 16: Delovna skupina iz člena 29 meni, da analiza zakonodaje tretje države, katere ustreznost se proučuje, ne bi smela biti omejena na pravo in prakso, ki omogoča nadzor znotraj fizičnih meja te države, temveč bi morala vključevati tudi analizo pravne podlage v zakonodaji te tretje države, ki ji omogoča izvajanje nadzora zunaj njenega ozemlja, kar zadeva podatke EU. Kot je že bilo poudarjeno v njenem prejšnjem mnenju, bi moralo biti jasno, da se bodo načela zasebnostnega ščita uporabljala od trenutka prenosa podatkov, kar pomeni tudi za podatke na poti do te države.

[87] Glej Prilogo II, str. 23.

[88] Odstavka 118 in 157 sklepa o ustreznosti.

varstvo osebnih podatkov, pravic in obveznosti, ki so enakovredne tistim iz zakona APPIHAO[89]. Ker prevodi teh odlokov v angleščino niso na voljo, EOVP ne more oceniti, ali so načela enakovredna načelom iz navedenega zakona.

225. Pri drugih pripombah v zvezi s prostovoljnim razkritjem je naveden sklic na razdelek o preprečevanju, odkrivanju, preiskovanju in pregonu kaznivih dejanj.

4.2.3 Nadzor

4.2.3.1 Splošne točke

226. Štirje vladni subjekti, pooblaščeni za zbiranje elektronskih informacij japonskih poslovnih subjektov zaradi nacionalne varnosti, so: (I) obveščevalna in raziskovalna agencija kabineta, (ii) Ministrstvo za obrambo, (iii) policija (nacionalna policijska agencija[90] in prefekturna policija) in (iv) obveščevalna agencija za javno varnost.

227. Te vladne subjekte v skladu z osnutkom sklepa o ustreznosti nadzorujejo tri veje oblasti [91] na več ravneh. EOVP ugotavlja obstoj mehanizma za nadzor v zakonodajni veji (japonski parlament) in izvršilni veji oblasti (urad generalnega inšpektorja za pravno skladnost, prefekturne komisije za javno varnost in komisija za preiskave na področju javne varnosti). EOVP poudarja, da bi morala Komisija pojasniti sodni nadzor (po uradni dolžnosti /jamstvo C iz delovnega dokumenta WP237; v zvezi s pravnim varstvom obstaja posebno poglavje v osnutku sklepa in dodatno jamstvo iz delovnega dokumenta WP237) navedenih vladnih organov, saj ni jasno, ali obstaja takšen sodni nadzor na področju zbiranja osebnih podatkov za namene nacionalne varnosti brez obveznih sredstev.

4.2.3.2 Pregled, ki ga izvaja japonski parlament

228. EOVP ugotavlja, da lahko japonski parlament izvaja preiskave v zvezi z dejavnostmi javnih organov, torej tudi za vse navedene vladne subjekte. Poleg tega lahko zahteva tudi predložitev dokumentov in zaslišanje prič (*člen 62 japonske ustave, člen 104 Zakona o parlamentu*). EOVP navaja še, da lahko poslanci v skladu s *členoma 74 in 75 Zakona o parlamentu* kabinetu pošiljajo pisna vprašanja, na katera lahko ta odgovori (*člen 75 Zakona o parlamentu*). Nazadnje je treba opozoriti, da mora na primer obveščevalna agencija za javno varnost upoštevati posebne obveznosti poročanja (člen 36 zakona SAPA/člen 31 zakona ACO), in sicer v obliki letnega poročila parlamentu. EOVP takega poročila ni prejel.

4.2.3.3 Nadzor, ki ga izvaja urad generalnega inšpektorja za pravno skladnost

229. EOVP ugotavlja, da obstaja nadzorni organ za Ministrstvo za obrambo, ki se imenuje urad generalnega inšpektorja za pravno skladnost. EOVP ni prejel zakona o ustanovitvi Ministrstva za obrambo, temveč le njegov opis v Prilogi II k osnutku sklepa. Urad generalnega inšpektorja za pravno skladnost je glede na Prilogo II neodvisen urad v okviru Ministrstva za obrambo, ki je pod neposrednim nadzorom tega ministra v skladu s členom 29 Zakona o ustanovitvi Ministrstva za obrambo. Ta urad ima pooblastila za izvajanje pregledov skladnosti z zakoni in predpisi, ki jih v okviru celotnega ministrstva, vključno s samoobrambnimi silami, izvajajo uradniki Ministrstva za obrambo (t. i. pregledi na področju obrambe).

230. Ta urad glede na Prilogo II izvaja svoje naloge neodvisno od operativnih oddelkov na Ministrstvu za obrambo. Odbor EOVP ugotavlja, da je urad generalnega inšpektorja za pravno skladnost *notranji* nadzorni organ.

---

[89] Glej Prilogo II, str. 3.

[90] Vendar je glede na prejete informacije glavna vloga nacionalne policijske agencije usklajevanje preiskav različnih oddelkov prefekturne policije , njene dejavnosti zbiranja informacij pa so omejene na izmenjave s tujimi organi.

[91] Glej Prilogo II, str. 39.

231. Pri preiskavah se navedejo ugotovitve in, z namenom zagotovitve skladnosti, ukrepi, o katerih se neposredno poroča ministru za obrambo. Minister za obrambo lahko na podlagi poročila urada generalnega inšpektorja za pravno skladnost izda odredbe o izvajanju ukrepov, potrebnih za izboljšanje stanja. Za izvajanje teh ukrepov je pristojen namestnik ministra za obrambo, ki mora ministru za obrambo poročati o stanju izvajanja.

232. EOVP z analizo Priloge II, ne da bi mu bile predložene pravne določbe (Zakon o ustanovitvi Ministrstva za obrambo) za te premisleke, pozdravlja možnost odreditve potrebnih ukrepov za zagotovitev skladnosti, da se izboljša stanje. Vendar ima pomisleke glede neodvisnosti urada generalnega inšpektorja za pravno skladnost, saj gre za urad v okviru Ministrstva za obrambo, ki je pod neposrednim nadzorom ministra za obrambo v skladu s Prilogo II (v delovnem dokumentu WP237 je navedeno, da funkcionalna neodvisnost sama po sebi ne zadostuje za zaščito tega nadzornega organa pred vsemi zunanjimi vplivi).

233. Generalni inšpektor lahko zaradi usklajevanja s sodno prakso ESČP in *delovnim dokumentom WP237* glede na pomisleke iz Priloge II zahteva poročila od zadevnega urada (dokumenti, lokacije, pojasnila). Po mnenju EOVP je treba pojasniti, ali mora zadevni urad upoštevati te zahteve ali ne in ali zahtevani dokumenti vključujejo zaprto gradivo, kot so omembe v *delovnem dokumentu WP237*, ali ne.

234. Čeprav EOVP odobrava, da so na čelu urada generalnega inšpektorja za pravno skladnost vodilni pravni strokovnjaki (nekdanji glavni tožilec), je treba pojasniti način imenovanja tega nadzornega organa.

4.2.3.4 Nadzor, ki ga izvaja komisija za preiskave na področju javne varnosti

235. Obveščevalna agencija za javno varnost glede na Prilogo II (stran 25) izvaja redne in posebne preglede dejavnosti posameznih oddelkov in uradov (obveščevalni urad za javno varnost, obveščevalni uradi in poduradi za javno varnost itd.). Za redne preglede se kot inšpektorja imenujeta pomočnik generalnega direktorja in/ali direktor. Ti pregledi bi se morali nanašati tudi na upravljanje osebnih podatkov.

236. Komisija za preiskave na področju javne varnosti v skladu z uvodno izjavo 163 osnutka sklepa deluje kot neodvisen organ za predhodni nadzor obveščevalne agencije za javno varnost za zadeve, ki se nanašajo na zakona ACO[92] in SAPA[93]. EOVP to odobrava.

237. Čeprav spletišče japonskega ministrstva za pravosodje vsebuje nekaj informacij[94], EOVP ne more natančno dodatno oceniti neodvisnosti komisije za preiskave na področju javne varnosti, saj mu niso bili predloženi akt o ustanovitvi komisije za preiskave na področju javne varnosti[95] niti predpisi navedene komisije[96].

---

[92] Zakon o nadzoru organizacij, ki so storile dejanja množičnih umorov brez izbire cilja (zakon št. 147 z dne 7. decembra 1999).

[93] Zakon o preprečevanju subverzivnih dejavnosti (št. 240 z dne 21. julija 1952).

[94] Glej spletišče http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (september 2018): zunajministrski organ *je sestavljen iz predsednika in šestih članov. Izbirajo se med osebami dobrega značaja, ki lahko pošteno presodijo o nadzoru nad organizacijami, ter osebami, ki imajo dovolj znanja in izkušenj na področju prava in družbe. Imenuje jih predsednik vlade in jih morata potrditi oba domova parlamenta. Kar zadeva uporabo navedenih zakonov (SAPA/ACO), člani svoje naloge opravljajo povsem samostojno, ne da bi jih pri tem usmerjal ali nadzoroval predsednik vlade ali minister za pravosodje.*

[95] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (september 2018).

[96] Člen 28 ACO.

4.2.3.5 Nadzor, ki ga izvajajo nacionalna komisija za javno varnost, prefekturne komisije za javno varnost in zakon APPIHAO (izvršna oblast)

238. Glej razdelke 3.1.2.2.1 (nacionalna komisija za javno varnost), 3.1.2.2.2 (prefekturne komisije za javno varnost) in 3.1.2.2.4 (izvršilna oblast).

4.2.3.6 Nadzor, ki ga izvaja Komisija za varstvo osebnih podatkov

239. EOVP Komisijo poziva, naj v uvodni izjavi 164 navede, da Komisija za varstvo osebnih podatkov ni nadzorni organ za navedene vladne subjekte in da je pristojna le za pravno varstvo posameznikov, ali odlomek besedila o tej komisiji iz uvodne izjave 164 premakne v razdelek o individualnih pravnih sredstvih.

4.2.4 Mehanizem pravnega varstva

240. Pri analizi mehanizma pravnega varstva, ki je bil nedavno dosežen s pogajanji, je naveden sklic na razdelek o preprečevanju, odkrivanju, preiskovanju in pregonu kaznivih dejanj.

241. Poleg tega je treba omeniti, da japonska zakonodaja določa posebne možnosti za individualna pravna sredstva, ki so na voljo na področju nacionalne varnosti. EOVP razume, da lahko vsi posamezniki, vključno s posamezniki iz EU, od upravnih organov na splošno zahtevajo razkritje, popravek (vključno z izbrisom) ali začasno prekinitev uporabe podatkov, tudi če se obdelujejo za namene nacionalne varnosti. Če je taka zahteva zavrnjena, ker se šteje, da zadevnih informacij ni mogoče razkriti, se lahko vloži vloga za ponovno proučitev in posvetovati se je treba z odborom za ponovno proučitev razkritja podatkov in varstvo osebnih podatkov. Odbor sestavljajo člani, ki jih imenuje predsednik vlade s soglasjem obeh domov parlamenta in imajo preiskovalna pooblastila ter za zadevnega posameznika sprejmejo pisno poročilo, ki ni pravno zavezujoče, vendar se skoraj vedno upošteva[97]. V skladu s Prilogo II je upravni organ le pri dveh od 2 000 zadev sprejel sklep, ki se je razlikoval od sklepov odbora[98].

242. Iz pojasnila izhaja, da ponovna proučitev ni na voljo, kadar je podatke mogoče razkriti, posameznik pa ni zadovoljen z izidom. EOVP priznava to možnost uporabe pravnih sredstev, vendar želi dodatno pojasniti zadnji vidik, s čimer bi se znatno omejilo njeno področje uporabe.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

[97] Priloga II, str. 25 in 26. Členi 4, 9 in 11 Zakona o ustanovitvi odbora za ponovno proučitev razkritja podatkov in varstvo osebnih podatkov.
[98] Priloga II, opomba 35.