Mnenje št. 32/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu osebnih podatkov v Republiki Koreji

Različica 1.0

Sprejeto 24. septembra 2021

KAZALO

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1), točka (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 (**Splošna uredba o varstvu podatkov**),

ob upoštevanju Sporazuma o Evropskem gospodarskem prostoru (**EGP**) ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE MNENJE:

1. POVZETEK

1. Evropska komisija je 16. junija 2021 začela formalni postopek za sprejetje osnutka izvedbenega sklepa (**osnutek sklepa**) o ustreznem varstvu osebnih podatkov v Republiki Koreji, in sicer na podlagi zakona o varstvu osebnih podatkov v skladu s Splošno uredbo o varstvu podatkov[2].

2. Istega dne je Evropska komisija za mnenje zaprosila Evropski odbor za varstvo podatkov (**EOVP**)[3]. EOVP je ustreznost ravni varstva, zagotovljene v Republiki Koreji, ocenil na podlagi proučitve osnutka sklepa in analize dokumentacije, ki jo je dala na voljo[4] Evropska komisija.

3. EOVP se je osredinil na oceno tako splošnih vidikov osnutka sklepa v skladu s Splošno uredbo o varstvu podatkov kot tudi dostopa javnih organov do osebnih podatkov, prenesenih iz EGP, za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter državne varnosti, vključno s pravnimi sredstvi, ki so na voljo posameznikom v EGP. Ocenil je tudi, ali so zaščitni ukrepi, zagotovljeni v skladu z južnokorejskim pravnim okvirom, vzpostavljeni in učinkoviti.

4. EOVP je kot glavni vir za to delo uporabil svoj referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov[5], sprejet februarja 2018, in svoja Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe[6].

1.1. Področja, o katerih je doseženo soglasje

5. Glavni cilj EOVP je Evropski komisiji podati mnenje o ustreznosti ravni varstva podatkov, kot se zagotavlja posameznikom, katerih osebni podatki se prenesejo v Republiko Korejo. Pomembno je poudariti, da EOVP ne pričakuje, da bo južnokorejski okvir za varstvo podatkov posnemal zakonodajo EU o varstvu osebnih podatkov.

---

[1] Sklicevanje na **države članice** v tem mnenju je treba razumeti kot sklicevanje na države članice EGP.
[2] Glej Sporočilo za javnost na spletnem naslovu https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Prav tam.
[4] EOVP je svojo analizo oprl na uradne prevode, ki jih je pripravila vlada Republike Koreje.
[5] WP254, Referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, 6. februar 2018 (ki ga je potrdil EOVP, glej https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Glej EOVP, Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, sprejeta 10. novembra 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

6. Vendar EOVP opozarja, da se v členu 45 Splošne uredbe o varstvu podatkov in sodni praksi Sodišča Evropske unije zahteva, da mora biti zakonodaja tretje države usklajena z bistvom temeljnih načel iz navedene uredbe, da bi se lahko štelo, da zagotavlja ustrezno raven varstva podatkov. V tem smislu je južnokorejski okvir za varstvo podatkov zelo podoben okviru EU za varstvo podatkov, saj ima en glavni zakonodajni akt, ki zajema javni in zasebni sektor ter je dopolnjen s sektorskimi zakonodajnimi akti.

7. EOVP glede vsebine ugotavlja ključna področja usklajevanja med okvirom Splošne uredbe o varstvu podatkov in južnokorejskim okvirom za varstvo podatkov v zvezi z nekaterimi ključnimi določbami, kot so na primer koncepti (na primer osebni podatki, obdelava, posameznik, na katerega se nanašajo osebni podatki), razlogi za zakonito in pošteno obdelavo podatkov za zakonite namene, omejitev namena, kakovost in sorazmernost podatkov, hramba podatkov, varnost in zaupnost, preglednost in posebne vrste podatkov.

8. Poleg tega EOVP odobrava prizadevanja Evropske komisije in južnokorejskih organov, s katerimi zagotavljajo, da Republika Koreja zagotavlja ustrezno raven varstva podatkov v primerjavi s Splošno uredbo o varstvu podatkov, pri čemer južnokorejski nadzorni organ sprejme uradna obvestila (ta se ne uporabljajo le za osebne podatke, prenesene iz EGP v Republiko Korejo), da bi zapolnili vrzeli med Splošno uredbo o varstvu podatkov in južnokorejskim okvirom za varstvo podatkov. Glede tega želi EOVP poudariti pomen teh uradnih obvestil za oceno ustreznosti Republike Koreje, pri čemer na primer ugotavlja, da zagotavljajo ustrezna pojasnila o nekaterih pomembnih zaščitnih ukrepih, med drugim v zvezi s področjem uporabe izvzetij iz zakona o varstvu osebnih podatkov za obdelavo psevdonimiziranih osebnih podatkov v znanstvene, raziskovalne in statistične namene, nadaljnjih prenosih in predpisih, ki se uporabljajo v okviru dostopa javnih organov do podatkov.

1.2. Izzivi

9. EOVP je ugotovil, da so številni vidiki južnokorejskega okvira za varstvo podatkov načelno enakovredni okviru EU za varstvo podatkov, vendar tudi, da bi bilo morda treba nekatere vidike podrobneje proučiti in pojasniti. Natančneje, meni, da bi bilo treba naslednje elemente dodatno oceniti, da bi zagotovili, da je dosežena načelno enakovredna raven varstva, in da bi jih morala Evropska komisija pozorno spremljati.

1.2.1. Splošno

10. EOVP ugotavlja, da ima uradno obvestilo št. 2021-1 *status upravnega predpisa s pravno zavezujočim učinkom za upravljavca osebnih podatkov v smislu, da se lahko vsaka kršitev uradnega obvestila šteje za kršitev zadevnih določb zakona o varstvu osebnih podatkov*[7]. Vendar EOVP, glede na to, da uradno obvestilo ne vključuje dodatnih pravil, temveč le pojasnila o tem, kako je treba ob pravilnem razumevanju uporabljati pravno besedilo zakona o varstvu osebnih podatkov, in glede na njegov splošni pomen, zlasti v zvezi z določbami o psevdonimizaciji v okviru omenjenega zakona, ki so po razumevanju EOVP predmet potekajočih sodnih postopkov, Evropsko komisijo poziva, naj zagotovi dodatne informacije o zavezujoči naravi, izvršljivosti in veljavnosti uradnega obvestila št. 2021-1, poleg tega priporoča pozorno spremljanje spoštovanja tega uradnega obvestila v praksi, še posebno, kako ga uporabljajo južnokorejski nadzorni organ in sodišča, zlasti kadar enakovredna raven pravnega varstva, ki ga zagotavlja južnokorejski pravni okvir, temelji na pojasnilih iz navedenega uradnega obvestila.

1.2.2. Splošni vidiki varstva podatkov

11. EOVP glede področja uporabe sklepa o ustreznosti ugotavlja, da bo zajemal prenose iz pravnega okvira EGP k javnim in zasebnim upravljavcem osebnih podatkov, ki spadajo na področje uporabe zakona o varstvu osebnih podatkov. EOVP razume, da ta izraz zajema subjekte, ki delujejo kot obdelovalci v

[7] Glej oddelek I Priloge I k osnutku sklepa.

smislu Splošne uredbe o varstvu podatkov, vendar da bi se izognili nesporazumom, Evropsko komisijo poziva, naj pojasni, da bo sklep o ustreznosti zajemal tudi prenose obdelovalcem v Republiki Koreji.

12. Pomemben vidik, na katerega želi EOVP opozoriti, se nanaša na koncept psevdonimiziranih podatkov v južnokorejskem okviru za varstvo podatkov. V skladu z južnokorejskim pravom za obdelavo psevdonimiziranih osebnih podatkov veljajo izjeme od številnih ustreznih določb, vključno s tistimi o pravicah posameznikov, na katere se nanašajo osebni podatki, in o hrambi podatkov. Po mnenju Evropske komisije to velja le, kadar se psevdonimizirani osebni podatki obdelujejo za namene statistike, znanstvenih raziskav ali arhiviranja v javnem interesu. Vendar to trditev podpira predvsem uradno obvestilo št. 2021-1, zaradi česar je v tem kontekstu zelo pomembna že omenjena potreba po dodatnih informacijah o tem uradnem obvestilu ter spremljanju njegove zavezujoče narave, izvršljivosti in veljavnosti. Poleg tega EOVP Evropsko komisijo poziva, naj dodatno oceni učinek psevdonimizacije v južnokorejski zakonodaji ter, kar je najpomembnejše, kako lahko vpliva na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki in katerih osebni podatki se na podlagi sklepa o ustreznosti prenesejo v Republiko Korejo. Natančneje, Evropsko komisijo poziva, naj dodatno oceni odstopanja iz člena 28(7) zakona o varstvu osebnih podatkov in člena 40(3) zakona o uporabi in varstvu kreditnih informacij ter pozorno spremlja njihovo uporabo in ustrezno sodno prakso, da se zagotovi, da pravice posameznikov, na katere se nanašajo osebni podatki, niso neupravičeno omejene, kadar se osebni podatki, preneseni na podlagi sklepa o ustreznosti, obdelujejo v te namene.

13. Poleg tega EOVP ugotavlja, da v skladu z južnokorejsko zakonodajo pravica do preklica privolitve obstaja le v posebnih okoliščinah, zato Evropsko komisijo poziva, naj dodatno oceni učinek tega, da ni splošne pravice do preklica privolitve, in priskrbi dodatna zagotovila, da bo bistvena raven varstva podatkov vedno zagotovljena, po potrebi tudi s pojasnitvijo vloge pravice do začasnega preklica v skladu z zakonom o varstvu osebnih podatkov, če ni splošne pravice do preklica privolitve.

14. Glede nadaljnjih prenosov EOVP potrjuje, da se bo informirana privolitev posameznika, na katerega se nanašajo osebni podatki, na splošno uporabljala kot podlaga za prenose podatkov od upravljavca osebnih podatkov s sedežem v Republiki Koreji k prejemniku, ki ima sedež v tretji državi, in da je v uradnem obvestilu št. 2021-1 predvideno, da morajo biti posamezniki obveščeni, v katero tretjo državo bodo preneseni njihovi podatki. Ob tem EOVP Evropsko komisijo poziva, naj zagotovi, da informacije, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, vključujejo tudi informacije o možnih tveganjih pri prenosih, ki so posledica tega, da ni ustreznega varstva v tretji državi niti ustreznih zaščitnih ukrepov. Poleg tega bi EOVP v sklepu o ustreznosti odobraval zagotovila, da južnokorejski upravljavci osebnih podatkov teh ne bodo poslali v tretjo državo v nobenem primeru, v katerem v skladu s Splošno uredbo o varstvu podatkov ne bi bilo mogoče zagotoviti veljavne privolitve, na primer zaradi neravnovesja moči.

15. Glede imenovanja članov južnokorejskega nadzornega organa bi EOVP, čeprav bi bil uradni postopek v skladu s Splošno uredbo o varstvu podatkov in bi zato izpolnjeval preizkus enakovrednosti s pravnim okvirom EGP, odobraval odločitev Evropske komisije, da spremlja razvoj dogodkov, ki bi lahko vplivali na neodvisnost članov južnokorejskega nadzornega organa.

16. Kar zadeva proračun, tudi v tem primeru na podlagi informacij, ki jih je zagotovila Evropska komisija, niso navedena specifična vloga osebja, dodeljenega odboru za varstvo osebnih podatkov, niti finančna sredstva, ki so mu na voljo. EOVP bi zato v osnutku sklepa odobraval dodatne informacije o teh dveh pomembnih temah.

1.2.3. O dostopu javnih organov do podatkov, prenesenih v Republiko Korejo

17. EOVP je južnokorejski pravni okvir proučil tudi v zvezi z dostopom vlade do osebnih podatkov, prenesenih iz EGP v Republiko Korejo, za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter državne varnosti. Ob tem, ko se je seznanil z izjavami in zagotovili južnokorejske vlade, kot

je navedeno v Prilogi II k osnutku sklepa, je ugotovil še, da je treba številne vidike pojasniti ali da ti vzbujajo pomisleke.

18. EOVP ugotavlja, da se določbe zakona o varstvu osebnih podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uporabljajo brez omejitev. Ob tem ugotavlja še, da pa za obdelavo podatkov na področju državne varnosti velja bolj omejen sklop določb omenjenega zakona.

19. Glede prostovoljnega razkritja osebnih podatkov s strani ponudnikov telekomunikacijskih storitev organom za državno varnost je EOVP zaskrbljen, da razmerje med oddelkom 3 Priloge I k osnutku sklepa, v katerem je navedeno, da morajo ponudniki načeloma obvestiti zadevnega posameznika, kadar prostovoljno izpolnijo zahtevo, in členom 58(1), točka 2, zakona o varstvu osebnih podatkov, tj. delno izvzetje za namene državne varnosti, ni povsem jasno. Zaradi tega bi lahko zahteve po obveščanju postale neučinkovite, kar bi posameznikom, na katere se nanašajo osebni podatki, precej otežilo uveljavljanje njihovih pravic do varstva podatkov, zlasti v zvezi s sodnim varstvom.

20. Čeprav v osnutku sklepa to ni izrecno navedeno, EOVP na podlagi pojasnil Evropske komisije razume, da južnokorejski pravni okvir ne omogoča množičnega prestrezanja telekomunikacijskih podatkov. Zato nedavna sodna praksa Evropskega sodišča za človekove pravice o ureditvah množičnega prestrezanja ne bi bila neposredno relevantna za oceno ravni varstva podatkov v Republiki Koreji.

21. Osnutek sklepa ne vsebuje nobenih informacij o pravnem okviru za nadaljnje prenose na področju državne varnosti. EOVP je razumel, da so po mnenju Evropske komisije nadaljnji prenosi za namene državne varnosti zadovoljivo urejeni s splošnimi zaščitnimi ukrepi in načeli, ki izhajajo iz ustavnega okvira in zakona o varstvu osebnih podatkov, vendar je zaskrbljen, ali se lahko šteje, da to izpolnjuje zahteve po natančnosti in jasnosti zakonodaje ter vključuje učinkovite in izvršljive zaščitne ukrepe. Zaščitni ukrepi, na katere se sklicuje Evropska komisija, so zelo splošni in s pravnega vidika ne obravnavajo specifičnih okoliščin niti pogojev, v skladu s katerimi se lahko izvedejo nadaljnji prenosi za namene državne varnosti. Glede tega EOVP ugotavlja še, da Evropska komisija ni upoštevala obstoja mednarodnih sporazumov, sklenjenih med Republiko Korejo in tretjimi državami ali mednarodnimi organizacijami, v katerih bi bile navedene specifične določbe za mednarodni prenos osebnih podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in/ali obveščevalnih služb v tretje države. EOVP meni, da bo sklenitev dvostranskih ali večstranskih sporazumov s tretjimi državami za namene sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali sodelovanja med obveščevalnimi službami verjetno vplivala na južnokorejski pravni okvir za varstvo podatkov, kot je bil ocenjen.

22. EOVP ugotavlja, da nadzor nad organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter za državno varnost zagotavlja kombinacija različnih notranjih in zunanjih organov, zlasti odbora za varstvo osebnih podatkov, ki ima zadostna izvršilna pooblastila.

23. Za učinkovita pravna sredstva in sodno varstvo je potrebno, da se lahko posamezniki, na katere se nanašajo osebni podatki, obrnejo na pristojni organ, ki izpolnjuje zahteve iz člena 47 Listine Evropske unije o temeljnih pravicah, tj. ki je pristojen za ugotavljanje, ali se podatki obdelujejo, za preverjanje zakonitosti obdelave in ki ima izvršljiva pooblastila za odpravo nepravilnosti, če je obdelava podatkov nezakonita. Glede na to EOVP Evropsko komisijo poziva, naj pojasni, ali za pritožbo, predloženo odboru za varstvo osebnih podatkov, ali katero koli tožbo pred sodiščem veljajo vsebinske in/ali postopkovne zahteve, kot je dokazno breme, in ali bi posamezniki v EGP lahko izpolnili tak prvi pogoj.

1.3. Sklep

24. EOVP meni, da je ta sklep o ustreznosti izjemno pomemben tudi ob upoštevanju, da bo – z izjemami, poudarjenimi v mnenju – zajemal prenose v javnem in zasebnem sektorju.

25. EOVP odobrava prizadevanja Evropske komisije in južnokorejskih organov, da bi se južnokorejski pravni okvir uskladil z okvirom EU. Izboljšave, ki naj bi jih uvedlo uradno obvestilo št. 2021-1 za

premostitev razlik med obema okviroma, so zelo pomembne in dobro sprejete. Vendar EOVP ugotavlja, da so še vedno številni pomisleki, tudi v zvezi z uradnim obvestilom št. 2021-1, skupaj s potrebo po dodatnih pojasnilih o drugih vprašanjih, in Evropski komisiji priporoča, naj obravnava pomisleke in zahteve za pojasnila, ki jih je izrazil EOVP, ter zagotovi dodatne informacije in pojasnila v zvezi z vprašanji iz tega mnenja.

2. UVOD

2.1. Južnokorejski okvir za varstvo podatkov

26. Glavni zakonodajni akt, ki ureja varstvo podatkov v Republiki Koreji, je zakon o varstvu osebnih podatkov (zakon št. 10465 z dne 29. marca 2011, nazadnje spremenjen z zakonom št. 16930 z dne 4. februarja 2020). Dopolnjuje ga uredba o izvajanju (predsedniška uredba št. 23169 z dne 29. septembra 2011, nazadnje spremenjena s predsedniško uredbo št. 30892 z dne 4 avgusta 2020, uredba o izvajanju zakona o varstvu osebnih podatkov), ki je pravno zavezujoča in izvršljiva.

27. Južnokorejski okvir za varstvo podatkov poleg zakona o varstvu osebnih podatkov vključuje tudi regulativna uradna obvestila, ki jih je izdal južnokorejski nadzorni organ, tj. odbor za varstvo osebnih podatkov, in zagotavljajo nadaljnja pravila o razlagi in uporabi navedenega zakona. Odbor za varstvo osebnih podatkov je nedavno sprejel uradno obvestilo št. 2021-1 z dne 21. januarja 2021 (to je spremenilo prejšnje uradno obvestilo št. 2020-10 z dne 1. septembra 2020; v nadaljevanju: uradno obvestilo št. 2021-1) o razlagi, uporabi in izvajanju nekaterih določb zakona o varstvu osebnih podatkov. Natančneje, navedeno uradno obvestilo je nastalo na podlagi razprav o ustreznosti med južnokorejskimi organi in Evropsko komisijo. Vsebuje pojasnila o uporabi specifičnih določb zakona o varstvu osebnih podatkov, tudi glede obdelave osebnih podatkov, prenesenih v Republiko Korejo na podlagi predvidenega sklepa o ustreznosti[8], in *ima status upravnega predpisa s pravno zavezujočo močjo za upravljavca osebnih podatkov v smislu, da se lahko vsaka kršitev uradnega obvestila šteje za kršitev ustreznih določb zakona o varstvu osebnih podatkov*[9]. Glede tega želi EOVP opozoriti, da čeprav je v osnutku sklepa omenjeno kot „dodatno pravilo“, uradno obvestilo ne vključuje dodatnih pravil, temveč le pojasnila o tem, kako je treba ob pravilnem razumevanju uporabljati pravno besedilo zakona o varstvu osebnih podatkov, zlasti v zvezi s podatki, prenesenimi iz EGP. Glede na to EOVP priporoča pozorno spremljanje spoštovanja uradnega obvestila št. 2021-1 v praksi, še posebno, kako ga uporabljajo odbor za varstvo osebnih podatkov in sodišča, zlasti kadar enakovredna raven pravnega varstva, ki ga zagotavlja južnokorejski pravni okvir, temelji na pojasnilih iz navedenega uradnega obvestila.

28. Pravila za obdelavo osebnih podatkov v specifičnih industrijskih sektorjih določajo drugi ustrezni zakoni o varstvu podatkov v južnokorejskem zakonodajnem okviru, kot na primer:

- zakon o uporabi in varstvu kreditnih informacij, vključno z uredbo o njegovem izvajanju (**uredba o izvajanju zakona o uporabi in varstvu kreditnih informacij**), v katerem so opredeljena specifična pravila, ki se uporabljajo za poslovne subjekte in specializirane subjekte (kot so bonitetne agencije in finančne institucije), kadar obdelujejo osebne kreditne informacije, potrebne za ugotavljanje kreditne sposobnosti strank v finančnih ali poslovnih transakcijah,
- zakon o spodbujanju uporabe informacijskih in komunikacijskih omrežij ter varstvu podatkov (**zakon o omrežjih**) in

[8] Glej oddelek I Priloge I k osnutku sklepa.
[9] Prav tam.

- zakon o varstvu zasebnosti v komunikacijah.

29. Na področju vladnega dostopa je EOVP poleg zadevnih določb iz zakonov o varstvu osebnih podatkov in zasebnosti v komunikacijah obravnaval še nekatere druge zakonodajne akte, tj. zakon o kazenskem postopku, zakon o telekomunikacijskih podjetjih, zakon o poročanju in uporabi specifičnih informacij o finančnih transakcijah in zakon o državni obveščevalni službi.

2.2. Obseg ocene EOVP

30. Osnutek sklepa Evropske komisije je nastal na podlagi ocene južnokorejskega okvira za varstvo podatkov, ki so ji sledile razprave z južnokorejsko vlado. V skladu s členom 70(1), točka (s), Splošne uredbe o varstvu podatkov se od EOVP pričakuje, da bo pripravil neodvisno mnenje o ugotovitvah Evropske komisije, opredelil morebitne pomanjkljivosti v okviru ustreznosti in si prizadeval pripraviti predloge za njihovo odpravo.

31. Da bi se izognil ponavljanju in da bi pomagal pri oceni južnokorejskega pravnega okvira, se je EOVP odločil, da se bo osredinil na nekatere specifične točke, navedene v osnutku sklepa, ter o njih predložil svojo analizo in mnenje, pri čemer se je vzdržal ponavljanja večine dejanskih ugotovitev in ocen, za katere nima izhodišča za domnevo, da zakonodaja Republike Koreje ne bi bila v bistvenem enakovredna zakonodaji v EGP. Poleg tega v skladu s sodno prakso Sodišča Evropske unije zelo pomemben del analize zajema pravno ureditev dostopa služb za državno varnost do osebnih podatkov, prenesenih v Republiko Korejo, in prakso njenega državnega varnostnega aparata.

32. EOVP je v svoji oceni upošteval veljavni okvir EU za varstvo podatkov, vključno s členi 7, 8 in 47 Listine Evropske unije o temeljnih pravicah, ki varujejo pravico do zasebnega in družinskega življenja, pravico do varstva osebnih podatkov oziroma pravico do učinkovitega pravnega sredstva in poštenega sojenja, ter členom 8 EKČP, ki varuje pravico do zasebnega in družinskega življenja. Poleg tega je proučil zahteve iz Splošne uredbe o varstvu podatkov in ustrezno sodno prakso.

33. Cilj tega postopka je Evropski komisiji zagotoviti mnenje o oceni ustreznosti ravni varstva v Republiki Koreji. 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 I, 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, lahko drugačna od sredstev, uporabljenih znotraj Unije“[10]. 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 osebne 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. Za učinkovitost pravil za varstvo podatkov so poglavitni učinkoviti mehanizmi izvajanja[11].

[10] C-362/14, *Maximilian Schrems/Data Protection Commissioner*, 6. oktober 2015, ECLI:EU:C:2015:650, točki 73 in 74.
[11] WP254, str. 2.

2.3. Splošne pripombe in pomisleki

2.3.1. Mednarodne zaveze, ki jih je sprejela Republika Koreja

34. Evropska komisija pri ocenjevanju ustreznosti ravni varstva tretje države v skladu s členom 45(2), točka (c), Splošne uredbe o varstvu podatkov in referenčnim dokumentom o ustreznosti v skladu s Splošno uredbo o varstvu podatkov[12] med drugim upošteva mednarodne zaveze, ki jih je sprejela tretja država, ali druge obveznosti, ki izhajajo iz sodelovanja tretje države v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov, ter izvajanje takih zavez.

35. Republika Koreja je pogodbenica številnih mednarodnih sporazumov, ki zagotavljajo pravico do zasebnosti, kot so Mednarodni pakt o državljanskih in političnih pravicah (člen 17), Konvencija o pravicah invalidov (člen 22) in Konvencija o otrokovih pravicah (člen 16). Poleg tega kot članica Organizacije za gospodarsko sodelovanje in razvoj spoštuje okvir te organizacije za zagotavljanje zasebnosti, zlasti smernice, ki urejajo varstvo zasebnosti in čezmejni pretok osebnih podatkov.

36. EOVP je seznanjen tudi s sodelovanjem Republike Koreje kot države opazovalke pri delu posvetovalnega odbora Konvencije Sveta Evrope št. 108(+), čeprav se še ni odločila, ali bo k njej pristopila.

2.3.2. Področje uporabe sklepa o ustreznosti

37. V skladu z uvodno izjavo 5 osnutka sklepa Evropska komisija ugotavlja, da Republika Koreja zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih z upravljavca ali obdelovalca v Uniji k upravljavcem osebnih podatkov (na primer fizičnim ali pravnim osebam, organizacijam in javnim ustanovam), ki spadajo na področje uporabe zakona o varstvu osebnih podatkov, z izjemo obdelave osebnih podatkov za misijonarske dejavnosti s strani verskih organizacij in za imenovanje kandidatov s strani političnih strank[13] ali obdelave osebnih kreditnih informacij v skladu z zakonom o uporabi in varstvu kreditnih informacij s strani upravljavcev, ki jih nadzira Komisija za finančne storitve.

38. EOVP ugotavlja, da bo sklep o ustreznosti zajemal prenose iz pravnega okvira EGP k javnim in zasebnim upravljavcem osebnih podatkov, ki spadajo na področje uporabe zakona o varstvu osebnih podatkov. EOVP razume, da izraz „upravljavec osebnih podatkov“ zajema tudi subjekte, ki delujejo kot obdelovalci v smislu Splošne uredbe o varstvu podatkov, glede na to, da se bo zakon o varstvu osebnih podatkov enako uporabljal tudi zanje in da veljajo specifične obveznosti, kadar upravljavec osebnih podatkov (ki najame zunanjega izvajalca) za obdelavo osebnih podatkov najame tretjo osebo (najeti zunanji izvajalec), vendar EOVP v izogib nesporazumom Evropsko komisijo poziva, naj zagotovi, da bo sklep o ustreznosti zajemal tudi prenose k obdelovalcem podatkov v Republiki Koreji in da raven varstva osebnih podatkov, prenesenih iz EGP, tudi v teh primerih ne bo ogrožena.

39. Ob upoštevanju, da sklep o ustreznosti zajema tudi prenose osebnih podatkov med javnimi organi, EOVP razume še, da bo to zajemalo tudi prenose med nadzornimi organi za varstvo podatkov, zato zaradi jasnosti Evropsko komisijo poziva, naj to vprašanje obravnava posebej.

40. Poleg tega želi EOVP glede subjektov, ki so izključeni s področja uporabe sklepa o ustreznosti, poudariti, da bi bilo za sklep o ustreznosti koristno jasneje opredeliti poslovne organizacije, ki so predmet nadzora odbora za varstvo osebnih podatkov (člen 45(3) zakona o uporabi in varstvu kreditnih informacij), tako da bi lahko upravljavci in obdelovalci s sedežem v EGP pred prenosom podatkov subjektom, ki spadajo na področje uporabe navedenega zakona, zlahka ocenili, ali tudi

[12] WP254, str. 2.

[13] Za več informacij glej oddelek 3.1.2 tega mnenja v nadaljevanju.

uvoznik spada na področje uporabe sklepa o ustreznosti, ali bi bili vsaj opozorjeni na potrebo po oceni tega vidika.

41. Glede področja uporabe sklepa o ustreznosti je EOVP iz dodatnih pojasnil Evropske komisije razbral, da je s področja uporabe izključena tudi južnokorejska finančnoobveščevalna enota, ki je ustanovljena v okviru komisije za finančne storitve in nadzoruje preprečevanje pranja denarja in financiranja terorizma v skladu z zakonom o poročanju in uporabi specifičnih informacij o finančnih transakcijah[14], saj je pristojna le za finančne institucije, na katere se osnutek sklepa ne nanaša. Člen 1(2), točka (c), osnutka sklepa s svojega področja uporabe izključuje le tiste upravljavce osebnih podatkov, ki so pod nadzorom komisije za finančne storitve in obdelujejo osebne kreditne informacije v skladu z zakonom o uporabi in varstvu kreditnih informacij. Glede na to EOVP Evropsko komisijo poziva, naj pojasni, ali se osnutek sklepa nanaša tudi na južnokorejsko finančnoobveščevalno enoto in njene dejavnosti obdelave podatkov.

3. SPLOŠNI VIDIKI VARSTVA PODATKOV

3.1. Vsebinska načela

42. Poglavje 3 referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov je namenjeno vsebinskim načelom. Sistem tretje države jih mora vsebovati, da bi se lahko štelo, da je zagotovljena raven varstva v bistvenem enakovredna tisti, ki jo zagotavlja zakonodaja EU.

43. Čeprav pravica do varstva osebnih podatkov ni izrecno zapisana v južnokorejski ustavi, je priznana kot temeljna pravica, ki izhaja iz ustavnih pravic do človekovega dostojanstva in prizadevanja za srečo (člen 10), do zasebnega življenja (člen 17) in do zasebnosti komunikacij (člen 18). To sta potrdila vrhovno sodišče in ustavno sodišče, kot je navedeno v osnutku sklepa Evropske komisije[15]. EOVP je seznanjen s to potrditvijo, saj iz nje izhaja, da se varstvo podatkov kot temeljna pravica v skladu s členom 37 južnokorejske ustave *lahko omeji le z zakonom in kadar je to potrebno zaradi državne varnosti, vzdrževanja javnega reda in miru ali javne blaginje* in da *tudi če so take omejitve uvedene, ne smejo vplivati na bistvo svobode ali pravice*.

44. Po navedbah Evropske komisije[16] je ustavno sodišče presodilo, da temeljne pravice veljajo tudi za tuje državljane. V skladu z uradnimi navedbami južnokorejske vlade[17] je med strokovnjaki splošno sprejeto, da členi 12–22 ustave določajo pravice ljudi, čeprav sodna praksa doslej ni izrecno obravnavala pravice do zasebnosti ljudi, ki niso državljani Republike Koreje. Poleg tega je Republika Koreja sprejela številne zakone na področju varstva podatkov, ki zagotavljajo zaščitne ukrepe za vse posameznike, ne glede na njihovo državljanstvo, kot je na primer zakon o varstvu osebnih podatkov. V zvezi s tem je EOVP seznanjen s členom 6(2) ustave, ki določa, da je status tujih državljanov zagotovljen v skladu z mednarodnim pravom in pogodbami ter sodno prakso, navedeno v osnutku sklepa, v skladu s katero temeljne pravice veljajo tudi za tujca. Glede na pomembnost priznanja pravice do varstva podatkov tujim državljanom EOVP Evropsko komisijo opozarja, da je treba še naprej spremljati sodno prakso v zvezi z varstvom podatkov kot temeljno pravico, priznano ne le južnokorejskim državljanom, temveč vsem posameznikom, na katere se nanašajo osebni podatki, da se zagotovi, da raven varstva posameznikov, ki jo zagotavlja Splošna uredba o varstvu podatkov, pri prenosu osebnih podatkov v Republiko Korejo na podlagi sklepa o ustreznosti ne bo ogrožena.

[14] Glej oddelek 2.2.3.1 Priloge II.
[15] Glej uvodno izjavo 8 osnutka sklepa in ustrezno sodno prakso, navedeno v opombi 10 osnutka sklepa, za katerega so na voljo samo angleški povzetki.
[16] Glej uvodno izjavo 9 osnutka sklepa.
[17] Oddelek 1.1 Priloge II k osnutku sklepa.

3.1.1. Pojmi

45. Na podlagi referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov bi morali biti v pravnem okviru tretje države temeljni pojmi in/ali načela o varstvu podatkov. Čeprav ni treba, da bi odražali izrazje Splošne uredbe o varstvu podatkov, bi morali izražati pojme iz zakonodaje EU o varstvu podatkov in biti skladni z njimi. Splošna uredba o varstvu podatkov na primer zajema naslednje pomembne pojme: osebni podatki, obdelava osebnih podatkov, upravljavec podatkov, obdelovalec podatkov, uporabnik in občutljivi podatki[18].

46. Zakon o varstvu osebnih podatkov zajema številne opredelitve, kot so med drugim opredelitve pojmov osebni podatki, obdelava in posameznik, na katerega se nanašajo osebni podatki, te opredelitve so zelo podobne ustreznim pojmom iz Splošne uredbe o varstvu podatkov.

3.1.1.1. *Pojem psevdonimiziranih podatkov*

47. Med opredelitvami v zakonu o varstvu osebnih podatkov je v njegovem členu 2(1) osebni podatek opredeljen zlasti kot kateri koli od naslednjih podatkov, ki se nanašajo na živečega posameznika: (a) informacije, ki določajo posameznika z njegovim polnim imenom, matično številko rezidenta, sliko itd., in (b) informacije, ki jih je mogoče zlahka združiti z drugimi informacijami za identifikacijo zadevnega posameznika, čeprav same po sebi zadevnega posameznika ne identificirajo. V zadnjenavedenem primeru se to, ali je kombinacija enostavna ali ne, opredeli z razumnim upoštevanjem časa, stroškov, tehnologije itd., uporabljenih za identifikacijo posameznika, kot je verjetnost, da je mogoče pridobiti druge informacije.

48. Poleg tega se v skladu s členom 2(1), točka (c), zakona o varstvu osebnih podatkov tudi psevdonimizirani podatki štejejo za osebne podatke. Psevdonimizirani podatki so opredeljeni kot podatki iz zgornje točke (a) ali (b), ki so psevdonimizirani v skladu s podtočko 1-2, in tako z njimi ni mogoče identificirati zadevnega posameznika brez uporabe ali kombinacije podatkov za vrnitev v prvotno stanje. Podatki, ki so v celoti anonimizirani, so izključeni s področja uporabe zakona o varstvu osebnih podatkov. V skladu s členom 58(2) zakona o varstvu osebnih podatkov se zakon ne uporablja za podatke, ki v kombinaciji z drugimi podatki ne omogočajo več identifikacije zadevnega posameznika, pri čemer se razumno upoštevajo čas, stroški, tehnologija itd.

49. Evropska komisija v uvodni izjavi 17 svojega osnutka sklepa navaja, da to ustreza stvarnemu področju uporabe Splošne uredbe o varstvu podatkov in njenim pojmom osebni podatki, psevdonimizacija in anonimizirani podatki.

50. Vendar se v skladu s členom 28(7) ter členi 20, 21 in 27, členom 34(1), členi 35 do 37 ter členom 39(3), (4), (6) do (8) zakona o varstvu osebnih podatkov ne uporabljajo za psevdonimizirane osebne podatke.

51. Evropska komisija v osnutku svojega sklepa navaja, da se člen 28(7) zakona o varstvu osebnih podatkov za psevdonimizirane osebne podatke uporablja samo, kadar se ti obdelujejo za namene statistike, znanstvenih raziskav ali arhiviranja v javnem interesu[19]. Vendar to ne izhaja neposredno iz črke zakona, temveč iz pojasnil v uradnem obvestilu št. 2021-1[20]. EOVP potrjuje, da je mogoče na podlagi strukture in utemeljitve zakona o varstvu osebnih podatkov trditi, da je treba njegov člen 28(2) razumeti in logično razlagati tako, da se uporablja tudi za njegov člen 28(7) ob upoštevanju pomena uradnega obvestila št. 2021-1 v mnenju Evropske komisije o ustreznosti ravni varstva osebnih podatkov v Republiki Koreji, poleg tega v izogib kakršnim koli dvomom Evropsko komisijo poziva, naj zagotovi

[18] WP254, str. 4.
[19] Glej med drugim uvodno izjavo 82 osnutka sklepa.
[20] Oddelek 4 Priloge I k osnutku sklepa.

dodatne informacije o zavezujoči naravi, izvršljivosti in veljavnosti uradnega obvestila št. 2021-1 ter spremlja njegovo uporabo v tem specifičnem kontekstu.

52. Glede tega želi EOVP opozoriti, da se psevdonimizacija v skladu s Splošno uredbo o varstvu podatkov razume kot priporočeni varnostni ukrep. Z drugimi besedami, v skladu s Splošno uredbo o varstvu podatkov psevdonimizirani podatki ostajajo osebni podatki, za katere se v celoti uporablja Splošna uredba o varstvu podatkov. Na podlagi tega ima EOVP pomisleke, da bi lahko bila raven varstva psevdonimiziranih osebnih podatkov v skladu s Splošno uredbo o varstvu podatkov pri prenosu osebnih podatkov v Republiko Korejo ogrožena. EOVP zato Evropsko komisijo poziva, naj dodatno oceni učinek psevdonimizacije na podlagi zakona o varstvu osebnih podatkov in, kar je najpomembnejše, kako lahko vpliva na temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki in katerih osebni podatki bi se na podlagi sklepa o ustreznosti prenesli v Republiko Korejo. Zato EOVP Evropsko komisijo poziva, naj zagotovi, da se raven varstva osebnih podatkov posameznikov, na katere se nanašajo osebni podatki, v EGP po prenosu v Republiko Korejo ne bo okrnila, tudi če so preneseni osebni podatki psevdonimizirani.

3.1.1.2. *Pojem upravljavca osebnih podatkov*

53. Člen 2(5) zakona o varstvu osebnih podatkov vsebuje opredelitev pojma upravljavec osebnih podatkov, ki pomeni javno institucijo, pravno osebo, organizacijo ali posameznika itd., ki osebne podatke obdeluje neposredno ali posredno za upravljanje zbirk osebnih podatkov v okviru svojih dejavnosti. Vendar je v dodatnih zaščitnih ukrepih iz uradnega obvestila št. 2021-1 izraz upravljavec osebnih podatkov opredeljen kot javna institucija, pravna oseba, organizacija, posameznik itd., ki osebne podatke obdeluje neposredno ali posredno za upravljanje zbirk osebnih podatkov za poslovne namene. Namesto tega je v opombi 272 osnutka sklepa o pojmu upravljavca osebnih podatkov navedeno: *Kot je navedeno v členu 2 zakona o varstvu osebnih podatkov, javna institucija, pravna oseba, organizacija, posameznik itd., ki osebne podatke neposredno ali posredno obdeluje za upravljanje zbirk osebnih podatkov za uradne ali poslovne namene.*

54. EOVP potrjuje, da so te nedoslednosti morda posledica prevodov izvirnega besedila, kot so jih zagotovili južnokorejski organi, in Evropsko komisijo poziva, naj redno preverja kakovost in zanesljivost prevodov. Ob tem EOVP poudarja, da je za oceno bistvene enakovrednosti ravni varstva podatkov južnokorejskega pravnega okvira potrebno jasno razumevanje namenov obdelave, ki spadajo na vsebinsko področje uporabe zakona o varstvu osebnih podatkov. Poleg tega v zvezi s tem ugotavlja, da se v zakonu o varstvu osebnih podatkov ne uporablja enako izrazje kot v Splošni uredbi o varstvu podatkov v zvezi s pojmoma upravljavec in obdelovalec, ter Evropsko komisijo poziva, naj pojasni pravilno opredelitev in področje uporabe pojma upravljavec osebnih podatkov ter izrecno obravnava, ali ta pojem zajema tudi obdelovalce v smislu Splošne uredbe o varstvu podatkov, saj to neposredno vpliva na področje uporabe sklepa o ustreznosti[21].

3.1.2. Delna izvzetja iz zakona o varstvu osebnih podatkov

55. Člen 58(1) zakona o varstvu osebnih podatkov izključuje uporabo delov navedenega zakona (tj. členov 15 do 57) v zvezi s štirimi kategorijami obdelave osebnih podatkov, kot je opisano v nadaljevanju. Natančneje, izjeme se nanašajo na določbe zakona o varstvu osebnih podatkov o specifičnih razlogih za obdelavo, nekaterih obveznostih glede varstva podatkov, podrobnih pravilih za uresničevanje pravic posameznikov ter pravilih, ki urejajo reševanje sporov. Vendar EOVP ugotavlja, da se še vedno uporabljajo nekatere splošne določbe zakona o varstvu osebnih podatkov, na primer tiste, ki se nanašajo na načela varstva podatkov (člen 3) in pravice posameznikov (člen 4). Poleg tega

[21] Glej tudi točko 38 zgoraj.

člen 58(4) zakona o varstvu osebnih podatkov določa specifične obveznosti za navedene štiri kategorije obdelave podatkov.

56. Prvič, delno izvzetje zajema osebne podatke, zbrane v skladu z zakonom o statistiki, pri čemer podatke obdelujejo javne institucije. Evropska komisija v uvodni izjavi 27 svojega osnutka sklepa navaja, da se glede na pojasnila, prejeta od južnokorejske vlade, osebni podatki, ki se obdelujejo v tem okviru, običajno nanašajo na južnokorejske državljane ter lahko le izjemoma vključujejo informacije o tujcih, in sicer v primeru statistike o vstopu na ozemlje in izstopu z njega ali o tujih naložbah. Vendar se v skladu z osnutkom sklepa tudi v teh primerih taki podatki običajno ne prenesejo od upravljavcev oziroma obdelovalcev v EGP, ampak bi jih neposredno zbrali javni organi v Republiki Koreji.

57. EOVP je seznanjen z utemeljitvijo Evropske komisije o izjemnosti uporabe zakona o statistiki za obdelavo osebnih podatkov, prenesenih na podlagi sklepa o ustreznosti, vendar bi pozdravil dodatne informacije in zagotovila o posebnih zaščitnih ukrepih, ki bi se uporabljali, kadar bi se osebni podatki, preneseni iz EGP, v skladu z zakonom o statistiki dodatno zbirali, da bi jih obdelovale javne institucije, zlasti v zvezi z uresničevanjem pravic posameznikov, tj posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 89(2) Splošne uredbe o varstvu podatkov, če ni verjetno, da bi take pravice onemogočile ali resno ovirale doseganja specifičnih namenov, in če taka odstopanja niso potrebna za uresničitev teh namenov.

58. S tega vidika se zdi, da uporaba člena 4 zakona o varstvu osebnih podatkov tudi za to vrsto obdelave zagotavlja zagotovila, vendar bi EOVP v sklepu o ustreznosti pozdravil dodatne informacije in pojasnila o specifičnih obveznostih, ki so v skladu s členom 58(4) zakona o varstvu osebnih podatkov naložene za te dejavnosti obdelave, in sicer v zvezi z najmanjšim obsegom podatkov, omejenim rokom hrambe podatkov, varnostnimi ukrepi ter reševanjem pritožb.

59. Drugič, delno izvzetje zajema osebne podatke, ki so zbrani ali se zanje zahteva, da se predložijo, za analizo informacij, povezanih z državno varnostjo. EOVP se zaveda, da imajo države v zadevah državne varnosti široko polje proste presoje, ki ga priznava Evropsko sodišče za človekove pravice. EOVP ugotavlja še, da v skladu s členom 37(2) južnokorejske ustave nobena omejitev svoboščin in pravic, na primer kadar je potrebna za zagotavljanje državne varnosti, ne sme kršiti bistvenega vidika zadevne svoboščine ali pravice. Poleg tega je EOVP seznanjen z zaščitnimi ukrepi iz oddelka 6 uradnega obvestila št. 2021-1 v zvezi z obdelavo osebnih podatkov za namene državne varnosti, vključno s preiskovanjem kršitev in izvrševanjem. Vendar EOVP glede tega Evropsko komisijo poziva, naj dodatno pojasni obseg izvzetij, saj ima pomisleke, ali so vsa izvzetja iz člena 58(1), točka 2, zakona o varstvu osebnih podatkov (poglavja od III do VII) pomembna za delo obveščevalnih služb in ali zagotavljajo enakovrednost z načeloma nujnosti in sorazmernosti. Natančneje, EOVP Evropsko komisijo poziva, naj podrobneje pojasni, v katerih okoliščinah se lahko obveščevalna služba sklicuje na izvzetja. EOVP meni, da je treba pozorno spremljati učinek teh omejitev v praksi, zlasti na učinkovito uresničevanje in izvrševanje pravic posameznikov, na katere se nanašajo osebni podatki.

60. Tretjič, delno izvzetje se uporablja za *osebne podatke, ki se začasno obdelujejo, kadar je to nujno potrebno za javno varnost in zaščito, javno zdravje itd.* V skladu z uvodno izjavo 29 osnutka sklepa Evropske komisije se v zakonu o varstvu osebnih podatkov ta kategorija razlaga ozko in se uporablja samo v nujnih primerih, v katerih je potrebno nujno ukrepanje, na primer za sledenje povzročiteljem okužb ali za reševanje in pomoč žrtvam naravnih nesreč.

61. EOVP poudarja še, da je treba vsa odstopanja od ravni varstva osebnih podatkov razlagati ozko. Hkrati ugotavlja, da določba ni ozko opredeljena in ne vsebuje izčrpnega seznama primerov, v katerih bi se obdelava osebnih podatkov lahko štela za *nujno potrebno*. EOVP je na primer zaskrbljen, ali bi v obseg tega izvzetja spadali tudi mednarodni prenosi zdravstvenih podatkov med potekajočo pandemijo covida-19. Glede na zgoraj navedeno EOVP Evropsko komisijo poziva, naj zagotovi dodatna pojasnila o obsegu tega izvzetja ter v celoti spremlja uporabo in področje uporabe, da se zagotovi, da se raven

varstva osebnih podatkov po prenosu teh iz EGP v Republiko Korejo na podlagi sklepa o ustreznosti ne okrni.

62. Nazadnje, delno izvzetje velja za osebne podatke, ki se zberejo ali uporabljajo za namene medijskega poročanja, misijonarskih dejavnosti verskih organizacij in imenovanja kandidatov s strani političnih strank[22]. Glede obdelave osebnih podatkov s strani tiskanih medijev za novinarske dejavnosti Evropska komisija v uvodni izjavi 31 svojega osnutka sklepa navaja, da je ravnovesje med svobodo izražanja in drugimi pravicami, vključno s pravico do zasebnosti, zagotovljeno z zakonom o arbitraži in pravnih sredstvih itd. za škodo, povzročeno z novinarskimi prispevki (v nadaljevanju: zakon o tisku), in zagotavlja specifične zaščitne ukrepe, ki izhajajo iz zakona o tisku. Vendar EOVP Evropsko komisijo poziva, naj v celoti spremlja to izvzetje in ustrezno sodno prakso, da bi zagotovila, da se enakovredna raven varstva podatkov zagotavlja tudi v praksi v južnokorejskem pravnem okviru.

3.1.3. Razlogi za zakonito in pošteno obdelavo podatkov za zakonite namene

63. Na podlagi referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov in na podlagi Splošne uredbe o varstvu podatkov je treba podatke obdelovati zakonito, pošteno in legitimno. Pravno podlago, v skladu s katero se lahko osebni podatki zakonito, pošteno in legitimno obdelujejo, je treba dovolj jasno določiti. Okvir EU potrjuje številne take zakonite podlage, vključno z na primer določbami v nacionalni zakonodaji, privolitvijo posameznika, na katerega se nanašajo osebni podatki, izvajanjem pogodbe ali zakonitimi interesi upravljavca podatkov ali tretje osebe, ki ne prevladajo nad interesi posameznika.

64. Po podobni strukturi, kot je v Splošni uredbi o varstvu podatkov, zakon o varstvu osebnih podatkov na začetku najprej uvede načelo zakonitosti, pravičnosti in preglednosti (člen 3(1) in (2)), nato pa opredeli posebna pravila za njegovo uporabo (členi 15 do 19). Natančneje, člen 15 zakona o varstvu osebnih podatkov zajema zbir pravnih podlag, na katerih lahko upravljavci osebnih podatkov utemeljijo zbiranje osebnih podatkov in jih uporabijo v okviru zbiranja za zadevni namen. Te pravne podlage so: (1) informirana privolitev posameznika, na katerega se nanašajo osebni podatki, (2) zakonsko dovoljenje ali nujnost za izpolnitev pravne obveznosti, (3) nujnost za opravljanje nalog javne institucije, (4) nujnost za sklenitev ali izvajanje pogodbe s posameznikom, na katerega se nanašajo osebni podatki, (5) nujnost za zaščito življenja, telesnih ali lastninskih interesov posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo (in ni mogoče pridobiti predhodne privolitve), (6) nujnost za dosego upravičenega interesa upravljavca osebnih podatkov, ki pretehta interes posameznika, na katerega se nanašajo osebni podatki.

65. Poleg tega so v členu 17 zakona o varstvu osebnih podatkov navedene pravne podlage, ki se uporabljajo za izmenjavo osebnih podatkov s tretjo osebo in so med drugim: (1) informirana privolitev posameznika, na katerega se nanašajo osebni podatki, (2) zakonsko dovoljenje ali nujnost za izpolnitev pravne obveznosti, (3) nujnost za opravljanje nalog javne institucije in (4) nujnost za zaščito življenja, telesnih ali lastninskih interesov posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe pred neposredno nevarnostjo (in predhodne privolitve ni mogoče pridobiti). Tudi če posameznik, na katerega se nanašajo osebni podatki, ne da privolitve, je izmenjava osebnih podatkov dovoljena, če se to zgodi v obsegu, ki je razumno povezan z nameni, za katere so bili osebni podatki prvotno zbrani (člen 17(4) zakona o varstvu osebnih podatkov).

66. Člen 18 zakona o varstvu osebnih podatkov določa specifična pravila za uporabo in izmenjavo osebnih podatkov, kadar to ne spada na področje uporabe prvotnega namena zbiranja ali zagotavljanja. Med drugim je tudi tu eno od takih pravil v zvezi z dovoljenjem privolitev.

[22] V skladu s tem sta s področja uporabe sklepa o ustreznosti izključeni tudi obdelava osebnih podatkov, ki jo izvajajo verske organizacije za svoje misijonarske dejavnosti, in obdelava osebnih podatkov, ki jo izvajajo politične stranke v okviru imenovanja kandidatov. Glej tudi točko 37 v oddelku 2.3.2 zgoraj.

67. EOVP potrjuje precejšnjo podobnost južnokorejske zakonodaje s Splošno uredbo o varstvu podatkov glede načela zakonitosti in obstoja splošne pravice do začasne prekinitve obdelave osebnih podatkov (člen 37 zakona o varstvu osebnih podatkov), na katero se je mogoče sklicevati tudi, kadar se osebni podatki obdelujejo na podlagi privolitve, vendar želi opozoriti, da v zakonu o varstvu osebnih podatkov ni splošne pravice do preklica privolitve[23]. Glede na pomen privolitve kot pravne podlage v vseh zgoraj opisanih scenarijih in ob upoštevanju vloge pravic posameznika v pravnem sistemu varstva podatkov za namene varstva temeljnih pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, EOVP Evropsko komisijo poziva, naj dodatno oceni učinek pomanjkanja splošne pravice do preklica privolitve v skladu z južnokorejsko zakonodajo in priskrbi dodatna zagotovila za zagotavljanje, da je bistvena raven varstva podatkov, kot je navedena v Splošni uredbi o varstvu podatkov, vedno zagotovljena, tudi v posebnih okoliščinah, in sicer tudi s pojasnitvijo vloge začasnega preklica, kadar je to potrebno.

3.1.4. Načelo omejitve namena

68. V referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov in na podlagi Splošne uredbe o varstvu podatkov je treba osebne podatke obdelovati za določen namen in jih pozneje uporabljati le, če to ni nezdružljivo z namenom obdelave.

69. V skladu s členom 3(1) in (2) zakona o varstvu osebnih podatkov upravljavci osebnih podatkov podrobno opredelijo in izrecno navedejo namene obdelave ter zagotovijo, da je obdelava združljiva z navedenimi nameni. Čeprav je to načelo potrjeno v drugih določbah (tj. v členu 15(1), členu 18(1) in členu 19(1) zakona o varstvu osebnih podatkov), so v nekaterih okoliščinah dovoljeni obdelava za razumno povezane namene (glej člen 17(4) zakona o varstvu osebnih podatkov)[24] ter nenamenska uporaba in zagotavljanje osebnih podatkov (glej člena 18 in 19 zakona o varstvu osebnih podatkov)[25].

70. EOVP razume, da v primeru prenosov osebnih podatkov iz EGP v Republiko Korejo na podlagi sklepa o ustreznosti namen, za katerega podatke zbirajo upravljavci s sedežem v EGP, pomeni namen, za katerega se podatki prenesejo, in namen za obdelavo, ki jo izvaja upravljavec osebnih podatkov s sedežem v Republiki Koreji, ki jih prejema. Upravljavcu s sedežem v Republiki Koreji je sprememba namena dovoljena le, kot je navedeno v členu 18(2), točke 1–3, zakona o varstvu osebnih podatkov, *če bi to lahko nepravično posegalo v interese posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe*[26]. V tem okviru EOVP pritrjuje navedbi Evropske komisije v uvodni izjavi 55 osnutka sklepa, da morajo zakoni, kadar so v skladu z njimi dovoljene spremembe namena, spoštovati temeljno pravico do zasebnosti in varstva podatkov. Vendar ob tem ugotavlja, da niso bile predložene nobene specifične informacije, ki bi potrjevale to izrecno navedbo, na primer ni naveden noben sklic na člen 37 (južnokorejske) ustave. Zato Evropsko komisijo poziva, naj v osnutku sklepa zagotovi dodatna zagotovila in jamstva, da se za vse zakone, v skladu s katerimi je dovoljena sprememba namena

[23] Čeprav lahko posamezniki, na katere se nanašajo osebni podatki, v nekaterih okoliščinah zavrnejo privolitev, glej na primer člen 18(3), točka (5), zakona o varstvu osebnih podatkov. Nasprotno pa se zdi, da pravica do preklica privolitve obstaja le v specifičnih primerih; v skladu s členom 27(1), točka 2, zakona o varstvu osebnih podatkov imajo posamezniki, na katere se nanašajo osebni podatki, pravico do preklica privolitve, kadar ne želijo, da se njihovi osebni podatki prenesejo tretji osebi zaradi prenosa dela ali celotnega poslovanja upravljavca osebnih podatkov, združitve itd., v skladu s členom 39(7) navedenega zakona pa lahko uporabniki pri ponudniku informacijskih in komunikacijskih storitev kadar koli prekličejo privolitev za zbiranje, uporabo in zagotavljanje osebnih podatkov itd., poleg tega lahko v skladu s členom 37 zakona o uporabi in varstvu kreditnih informacij posamezni subjekt, na katerega se nanašajo kreditne informacije, prekliče privolitev, dano ponudniku oziroma uporabniku kreditnih informacij.

[24] Pri tem je treba združljivost z namenom predhodno preveriti na podlagi meril iz člena 14-2 uredbe o izvajanju zakona o varstvu osebnih podatkov.

[25] Glej tudi točko 66 zgoraj.

[26] Člen 18(2) zakona o varstvu osebnih podatkov.

obdelave, zahteva, da se z njimi spoštujejo temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, v zvezi z zasebnostjo in varstvom podatkov.

3.1.5. Načelo kakovosti in sorazmernosti podatkov

71. V referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov je navedeno, da morajo biti podatki točni in po potrebi posodobljeni. Podatki morajo biti ustrezni, relevantni in ne čezmerni glede na namene, za katere se obdelujejo.

72. V skladu z zakonom o varstvu osebnih podatkov morajo upravljavci osebnih podatkov zagotoviti, da so osebni podatki točni, popolni in posodobljeni, kolikor je to potrebno v zvezi z nameni, za katere se osebni podatki obdelujejo (člen 3(3) zakona o varstvu osebnih podatkov). Upravljavci osebnih podatkov morajo zbirati le toliko osebnih podatkov, kot je potrebno za dosego zadevnega namena. Glede tega sami nosijo dokazno breme (člen 16(1) zakona o varstvu osebnih podatkov).

73. Glede na to se EOVP strinja z mnenjem Evropske komisije glede take bistvene enakovrednosti ravni varstva po zakonu o varstvu osebnih podatkov v primerjavi s Splošno uredbo o varstvu podatkov.

3.1.6. Načelo hrambe podatkov

74. Na podlagi referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov se morajo podatki na splošno hraniti le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo. V skladu s členom 21(1) zakona o varstvu osebnih podatkov to načelo velja tudi v južnokorejski zakonodaji. V skladu z zakonom o varstvu osebnih podatkov morajo upravljavci osebnih podatkov nemudoma uničiti osebne podatke, ko ti postanejo nepotrebni po izteku obdobja hrambe ali po tem, ko je dosežen predvideni namen obdelave, razen če se uporabljajo zakonsko določeni roki hrambe.

75. EOVP pa je zaskrbljen, ker se člen 21(1) zakona o varstvu osebnih podatkov ne uporablja za psevdonimizirane osebne podatke. Seznanjen je, da v skladu z oddelkom 4(iii) uradnega obvestila št. 2021-1, *kadar upravljavec osebnih podatkov obdeluje psevdonimizirane podatke za namene zbiranja statističnih podatkov, znanstvenih raziskav, vzdrževanja javnih evidenc itd. in če psevdonimizirani podatki niso bili uničeni, ko je bil zadevni namen obdelave uresničen, v skladu s členom 37 ustave in členom 3 (načela varstva osebnih podatkov) zakona, upravljavec osebnih podatkov v skladu s členom 58(2) zakona o varstvu osebnih podatkov podatke anonimizira in tako zagotovi, da na podlagi teh podatkov ni več mogoče identificirati zadevnega posameznika, in to samo na podlagi teh podatkov ali v kombinaciji z drugimi podatki, pri čemer se razumno upoštevajo čas, stroški, tehnologija itd.* Tudi v tem primeru zaradi pomembnosti uradnega obvestila št. 2021-1 in zaradi pravne varnosti glede enakovrednosti ravni varstva osebnih podatkov, prenesenih v Republiko Korejo na podlagi sklepa o ustreznosti, EOVP Evropsko komisijo znova poziva, naj zagotovi dodatne informacije, zlasti o tem, kako je uradno obvestilo št. 2021-1 postalo zavezujoče ter kako sta zagotovljeni njegovi izvršljivost in veljavnost[27].

3.1.7. Načelo varnosti in zaupnosti podatkov

76. Kot je opisano v referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, se po načelu varnosti in zaupnosti od subjektov, ki obdelujejo podatke, zahteva, da zagotovijo, da se osebni podatki obdelujejo tako, da se zagotavlja njihovo varovanje, kar zajema tudi zaščito pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem, z uporabo ustreznih tehničnih ali organizacijskih ukrepov. Raven varnosti bi morala upoštevati najsodobnejšo tehnologijo in zadevne stroške.

[27] Glede splošnih pomislekov EOVP v zvezi z učinkom psevdonimizacije v južnokorejski zakonodaji glej tudi točko 51 v oddelku 3.1.1.1 tega mnenja in točko 52.

77. Evropska komisija je podobno načelo varnosti podatkov prepoznala v členu 3(4) zakona o varstvu osebnih podatkov, to načelo pa je v tem zakonu podrobneje opredeljeno še v členu 29. Poleg tega se določbe o varnosti podatkov uporabljajo tudi, kadar upravljavec osebnih podatkov najame zunanjega izvajalca. Varnost obdelave je treba zagotoviti s tehničnimi in upravljavskimi zaščitnimi ukrepi, ki morajo biti vključeni tudi v zavezujočo pogodbo o obdelavi podatkov (člen 26 zakona o varstvu osebnih podatkov in člen 28 uredbe o izvajanju zakona o varstvu osebnih podatkov). Poleg tega v skladu z zakonom o varstvu osebnih podatkov v primeru kršitve varstva podatkov veljajo specifične obveznosti, vključno z obveznostjo obveščanja prizadetih posameznikov, na katere se nanašajo osebni podatki, in nadzornega organa, kadar število prizadetih posameznikov, na katere se nanašajo osebni podatki, presega veljavni prag (člen 34 zakona o varstvu osebnih podatkov v povezavi s členom 39 uredbe o izvajanju zakona o varstvu osebnih podatkov), razen kadar so zadevni podatki psevdonimizirani osebni podatki, ki se obdelujejo za namene statistike, znanstvenih raziskav ali arhiviranja v javnem interesu (člen 28(7) zakona o varstvu osebnih podatkov). Tudi glede tega[28] je EOVP zaskrbljen zaradi zelo obsežnih izjem za psevdonimizirane podatke in Evropsko komisijo znova poziva, naj dodatno oceni ta vidik in zagotovi, da bo v južnokorejski zakonodaji zagotovljena v bistvenem enakovredna raven varstva[29].

78. Ne glede na to je EOVP na splošno zadovoljen z oceno in sklepom Evropske komisije glede v bistvenem enakovredne južnokorejske zakonodaje v zvezi z načelom varnosti in zaupnosti.

3.1.8. Načelo preglednosti

79. Preglednost je na podlagi člena 5(1), točka (a), Splošne uredbe o varstvu podatkov temeljno načelo sistema EU za varstvo podatkov. V uvodni izjavi 39 Splošne uredbe o varstvu podatkov je opisana ključna funkcija tega načela, in sicer: „Načini zbiranja, uporabe, pregledovanja ali drug način obdelave ter obseg obdelave ali prihodnje obdelave osebnih podatkov, ki se nanašajo na posameznike, bi morali za posameznike biti pregledni. [...] Posameznike bi bilo treba opozoriti na tveganja, pravila, zaščitne ukrepe in pravice v zvezi z obdelavo njihovih osebnih podatkov ter na to, kako lahko uresničujejo njihove pravice v zvezi s tako obdelavo.“

80. V referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov je preglednost navedena kot eno od vsebinskih načel, ki jih je treba upoštevati pri presoji v bistvenem enakovredne ravni varstva, ki jo zagotavlja tretja država. Natančneje, določa, da *mora biti vsak posameznik obveščen o vseh glavnih elementih obdelave njegovih osebnih podatkov v jasni, lahko dostopni, jedrnati, pregledni in razumljivi obliki. Takšne informacije bi morale vključevati namen obdelave, identiteto upravljavca podatkov, pravice, ki so mu na voljo, in druge informacije, če je to potrebno za zagotovitev poštenosti. Pod nekaterimi pogoji so možne tudi nekatere izjeme od te pravice do obveščenosti, na primer za zagotavljanje kazenskih preiskav in državne varnosti, za varstvo neodvisnosti sodstva in sodnega postopka ali za zagotavljanje drugih pomembnih ciljev v splošnem javnem interesu, kot je navedeno v členu 23 Splošne uredbe o varstvu podatkov.*

81. Podobno kot v Splošni uredbi o varstvu podatkov tudi v zakonu o varstvu osebnih podatkov velja splošno načelo preglednosti, po katerem se od upravljavcev osebnih podatkov zahteva, da javno objavijo svojo politiko zasebnosti in druge zadeve, povezane z obdelavo osebnih podatkov (člen 3(5) zakona o varstvu osebnih podatkov). Specifične obveznosti obveščanja veljajo, kadar upravljavci osebnih podatkov poskušajo od posameznikov, na katere se nanašajo osebni podatki, pridobiti privolitev za zbiranje in obdelavo osebnih podatkov (člen 15(2) zakona o varstvu osebnih podatkov), za posredovanje osebnih podatkov tretji osebi (člen 17(2) zakona o varstvu osebnih podatkov) in za nenamensko obdelavo (člen 18(3) zakona o varstvu osebnih podatkov). Opozoriti je treba, da se te

[28] Kot je že navedeno v točkah 51 in 52 zgoraj in v oddelku 3.1.1.1 tega mnenja.
[29] Glej tudi oddelka 3.1.6 in 3.1.10 tega mnenja.

obveznosti obveščanja smiselno uporabljajo tudi za zunanjega izvajalca (člen 26(7) zakona o varstvu osebnih podatkov).

82. EOVP potrjuje in odobrava dodatne zaščitne ukrepe v oddelku 3(i) in (ii) uradnega obvestila št. 2021-1[30] v zvezi z informacijami, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, kadar subjekt iz EGP njihove podatke prenese, ob upoštevanju, da so v skladu s členom 20(1) zakona o varstvu osebnih podatkov posamezniki, na katere se nanašajo osebni podatki, kadar podatki niso bili pridobljeni od posameznika, na katerega se nanašajo osebni podatki, obveščeni le na zahtevo, splošna pravica do obveščenosti pa je v skladu s členom 20(2) navedenega zakona priznana le, kadar zadevni postopki obdelave presegajo pragove, navedene v uredbi o izvajanju zakona o varstvu osebnih podatkov (člen 15(2)).

83. Na splošno je EOVP prepričan, da je raven varstva v južnokorejski zakonodaji glede načela preglednosti v bistvenem enakovredna tisti, ki je zagotovljena s Splošno uredbo o varstvu podatkov.

3.1.9. Posebne vrste osebnih podatkov

84. Da bi se lahko za sistem varstva podatkov tretje države potrdilo, da zagotavlja raven varstva osebnih podatkov, ki je v bistvenem enakovredna ravni varstva iz Splošne uredbe o varstvu podatkov, morajo biti vzpostavljeni specifični zaščitni ukrepi, kadar gre za posebne vrste osebnih podatkov v smislu členov 9 in 10 Splošne uredbe o varstvu podatkov.

85. V skladu z zakonom o varstvu osebnih podatkov za obdelavo tako imenovanih občutljivih podatkov veljajo specifične določbe, ti podatki vključujejo osebne podatke, ki razkrivajo ideologijo, prepričanje, članstvo v sindikatu ali politični stranki ali prenehanje tega članstva, politično mnenje, podatke v zvezi z zdravjem, podatke v zvezi s spolnim življenjem in druge osebne podatke, ki lahko izrazito ogrozijo zasebnost katerega koli posameznika, na katerega se nanašajo osebni podatki, ter – s sklicevanjem na uredbo o izvajanju zakona o varstvu osebnih podatkov – podatke o DNK, pridobljene z genetskimi testi, podatke, iz katerih je razvidna predkaznovanost, osebne podatke, ki izhajajo iz specifične tehnične obdelave podatkov v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika za namene edinstvene identifikacije tega posameznika, in osebne podatke, ki razkrivajo rasno ali etnično poreklo.

86. Podobno kot Splošna uredba o varstvu podatkov tudi južnokorejska zakonodaja o varstvu podatkov prepoveduje obdelavo občutljivih podatkov, razen če veljajo specifične izjeme, ki vključujejo (1) obveščanje posameznika, na katerega se nanašajo osebni podatki, in pridobitev specifične privolitve ter (2) pravne določbe, ki dovoljujejo obdelavo (člen 23(2) zakona o varstvu osebnih podatkov).

87. Na podlagi tega se EOVP načeloma strinja z ugotovitvijo Evropske komisije o bistveni enakovrednosti južnokorejske zakonodaje glede obdelave posebnih vrst osebnih podatkov. Vendar želi EOVP opozoriti, da ni prejel pravilnika o izvajanju zakona o varstvu osebnih podatkov niti pojasnil odbora za varstvo osebnih podatkov v zvezi z razlago pojma „spolno življenje“, ki zajema tudi posameznikovo spolno usmerjenost ali želje, kar ni bilo vključeno v uradno obvestilo št. 2021-1. EOVP zato Evropsko komisijo poziva, naj zagotovi te informacije, da bi jih lahko neodvisno ocenili. Poleg tega EOVP Evropsko komisijo poziva še, naj izrecno navede, v katerih dokumentih je mogoče najti informacije, na katere se sklicuje o tej temi.

3.1.10. Pravice dostopa, popravka, izbrisa in ugovora

88. V južnokorejskem pravnem okviru so pravice posameznikov, na katere se nanašajo osebni podatki, priznane v členu 3(5) zakona o varstvu osebnih podatkov – v skladu s tem upravljavec osebnih podatkov zagotavlja pravice posameznikov, na katere se nanašajo osebni podatki, navedene v členu 4

[30] Priloga I k osnutku sklepa.

zakona o varstvu osebnih podatkov in podrobneje opredeljene v členih 35 do 37, 39 in členu 39(2) navedenega zakona, glede osebnih kreditnih informacij (tj. kreditnih informacij, ki so potrebne za opredelitev kreditne sposobnosti strank pri finančnih ali poslovnih transakcijah, glej uvodno izjavo 3 osnutka sklepa) pa v členih 37, 38 in členu 38(3) zakona o uporabi in varstvu kreditnih informacij.

89. EOVP ugotavlja, da se lahko pravica dostopa (ter pravici do popravka in do izbrisa, ki ju lahko uresničuje *„posameznik, na katerega se nanašajo osebni podatki in ki je dostopal do svojih osebnih podatkov v skladu s členom 35*“ zakona o varstvu osebnih podatkov) omeji ali zavrne, *„če je dostop prepovedan ali omejen z zakoni*, *če bi dostop lahko povzročil škodo za življenje ali telo tretje osebe ali bi neupravičeno kršil lastninsko pravico in posegel v druge interese katere koli druge osebe*,“ za javne institucije pa tudi, če bi odobritev dostopa *povzročila resne težave* pri opravljanju nekaterih nalog, ki so podrobneje opredeljene v členu 35(4) zakona o varstvu osebnih podatkov[31]. Podobne določbe vsebuje tudi člen 37 zakona o varstvu osebnih podatkov glede pravice do začasne prekinitve obdelave osebnih podatkov.

90. Člen 23 Splošne uredbe o varstvu podatkov dovoljuje, da pravo Unije ali države članice omeji pravice posameznika, kadar taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi, in predvideva take omejitve za med drugim zagotavljanje varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih ter za zagotavljanje „spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti v primerih iz točk (a) do (e) in (g)“ navedenega člena.

91. Glede na to bi EOVP pozdravil splošna zagotovila v osnutku sklepa o tem, da mora vsak zakon ali zakonski predpis, ki omejuje pravice posameznikov, na katere se nanašajo osebni podatki, izpolnjevati zahteve južnokorejske ustave, da se lahko temeljna pravica omeji le, če je to potrebno za državno varnost ali vzdrževanje javnega reda in miru za javno dobrobit, in da ta omejitev ne sme vplivati na bistvo zadevne svoboščine ali pravice (člen 37(2) južnokorejske ustave).

92. Poleg tega glede izjeme, ki se nanaša na *„neupravičeno kršitev lastninske pravice ali poseg v druge interese drugih oseb*,“ EOVP potrjuje, da to *„pomeni, da je treba vzpostaviti ravnovesje med ustavno varovanimi pravicami in svoboščinami posameznika na eni strani ter drugih oseb na drugi strani*“[32], ob tem pa Evropsko komisijo poziva, naj v celoti spremlja uporabo te izjeme in ustrezno sodno prakso, da bi zagotovila, da se enakovredna raven varstva pravic posameznikov, na katere se nanašajo osebni podatki, zagotavlja tudi v praksi na podlagi južnokorejskega pravnega okvira.

93. Iz istega razloga bi EOVP pozdravil pozorno spremljanje uporabe izjeme za javne organe, zlasti glede primerov, v katerih bi odobritev dostopa pomenila *„resne težave*“ pri opravljanju njihovih nalog, saj se zdi, da je ta izraz širši od tistega, ki se uporablja v drugih določbah zakona o varstvu osebnih podatkov, na primer v členu 18(2), točka 5[33], zato je to treba razlagati ozko, da se prepreči neupravičeno omejevanje pravic posameznikov, na katere se nanašajo osebni podatki.

94. Poleg tega je EOVP zaskrbljen, ali so izjeme, v skladu s katerimi se določbe o preglednosti na zahtevo (člen 20 zakona o varstvu osebnih podatkov) in pravicah posameznikov (členi 35 do 37 zakona o varstvu osebnih podatkov) – ter podobne določbe, ki se nanašajo na zahteve za ponudnike informacijskih in komunikacijskih storitev (člen 39(2), (6) do (8) zakona o varstvu osebnih podatkov) in tiste iz zakona o uporabi in varstvu kreditnih informacij (glej izjeme, predvidene v členu 40(3)) – ne

[31] Enaki pogoji in izjeme od pravic dostopa in do popravka, ki ju predvideva zakon o varstvu osebnih podatkov, veljajo tudi za pravici dostopa in do popravka, kot to za osebne kreditne informacije predvideva zakon o uporabi in varstvu kreditnih informacij (opomba 135 v osnutku sklepa).

[32] Uvodna izjava 76 osnutka sklepa.

[33] V zvezi z izjemami od omejitve nenamenske uporabe in zagotavljanja osebnih podatkov so v členu 18(2), točka 5, zakona o varstvu osebnih podatkov navedeni primeri, v katerih je javnim institucijam *onemogočeno*, da bi opravljale svoje naloge.

uporabljajo v zvezi s psevdonimiziranimi podatki, kadar se ti obdelujejo za namene statistike, znanstvenih raziskav ali arhiviranja v javnem interesu (člen 28(7) zakona o varstvu osebnih podatkov), v skladu z zaščitnimi ukrepi iz pravnega okvira EU.

95. Zdi se, da te določbe uvajajo splošno odstopanje za tako obdelavo, Splošna uredba o varstvu podatkov pa predvideva, da se lahko, kadar se osebni podatki (vključno s psevdonimiziranimi osebnimi podatki) obdelujejo v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene, v pravu Unije ali države članice določijo odstopanja od pravic posameznika, na katerega se nanašajo osebni podatki, vendar le, „*kolikor je verjetno, da bi te pravice onemogočile ali resno ovirale doseganje posebnih namenov in kolikor so takšna odstopanja nujna za uresničitev teh namenov*“, pri čemer je psevdonimizacija le eden od tehničnih in organizacijskih ukrepov, ki jih je treba sprejeti, da se zagotovi spoštovanje načela najmanjšega obsega podatkov (člen 89(1) Splošne uredbe o varstvu podatkov).

96. Evropska komisija meni, da je odstopanje, predvideno v členu 28(7) zakona o varstvu osebnih podatkov, upravičeno tudi glede na njegov člen 28(5), s katerim je upravljavcu osebnih podatkov izrecno prepovedano obdelovati psevdonimizirane podatke za namen identifikacije zadevnega posameznika, in se sklicuje na pristop iz člena 11(2) Splošne uredbe o varstvu podatkov (v povezavi z njeno uvodno izjavo 57) za obdelavo, ki ne zahteva identifikacije[34].

97. V skladu s členom 11 Splošne uredbe o varstvu podatkov upravljavec namreč ni zavezan „*ohraniti, pridobiti ali obdelati dodatnih informacij, da bi identificiral posameznika, na katerega se nanašajo osebni podatki*“, in sicer izključno za namen izpolnjevanja Splošne uredbe o varstvu podatkov, če lahko za predvidene namene obdeluje osebne podatke, ki ne zahtevajo ali ne zahtevajo več identifikacije posameznika, na katerega se nanašajo osebni podatki, v takih primerih, ko lahko upravljavec dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki, se pravice posameznika, na katerega se nanašajo osebni podatki, ne uporabljajo. Kot potrjuje Evropska komisija[35], Splošna uredba o varstvu podatkov zato v takih primerih zahteva praktično nezmožnost za upravljavca podatkov in v skladu z načelom najmanjšega obsega podatkov, poleg tega zaradi Splošne uredbe o varstvu podatkov ni treba obdelovati dodatnih podatkov.

98. Vendar EOVP meni, da se ta položaj razlikuje od položaja, v katerem lahko upravljavec praktično identificira posameznika, na katerega se nanašajo osebni podatki, vendar tega ne dovoljuje zakonska določba, kot je tista iz člena 28(5) zakona o varstvu osebnih podatkov. V zvezi s tem EOVP odobrava pojasnila odbora za varstvo osebnih podatkov v uradnem obvestilu št. 2021-1[36], ki potrjujejo, da se oddelek 3 zakona o varstvu osebnih podatkov (vključno s členom 28(7)) in izjema iz člena 40(3) zakona o uporabi in varstvu kreditnih informacij uporabljata le, kadar se psevdonimizirani podatki obdelujejo za znanstvene raziskave, statistiko ali arhiviranje v javnem interesu. Vendar se – poleg že omenjenih pomislekov glede učinkovite zavezujoče narave uradnega obvestila št. 2021-1[37] – EOVP še vedno sprašuje, ali bi bilo mogoče odstopanja, predvidena v členu 28(7) zakona o varstvu osebnih podatkov in členu 40(3) zakona o uporabi in varstvu kreditnih informacij, šteti za potrebna in sorazmerna v demokratični družbi, kolikor omejujejo pravice posameznikov, na katere se nanašajo osebni podatki, v vseh primerih, kadar se psevdonimizirani podatki obdelujejo za take namene, tj. tudi tedaj, kadar upravljavec osebnih podatkov praktično ne more identificirati posameznika, na katerega se nanašajo

[34] Opozoriti je treba, da enaka utemeljitev ne bi veljala za izjemo, ki jo predvideva člen 40(3) zakona o uporabi in varstvu kreditnih informacij za obdelavo psevdonimiziranih kreditnih informacij, saj člen 40(2), točka (6), predvideva, da: „*Družba za dajanje kreditnih informacij itd. ne obdeluje psevdonimiziranih podatkov na način, ki bi omogočal identifikacijo zadevnega posameznika za katere koli pridobitne ali nepoštene namene*,“ tako bi lahko bila omogočena vnovična identifikacija za pošten namen, kot je izpolnitev zahteve posameznika, na katerega se nanašajo osebni podatki.

[35] Glej uvodno izjavo 82 osnutka sklepa.

[36] Oddelek 4 Priloge I k osnutku sklepa.

[37] Glej oddelek 3.1.1.1 zgoraj.

osebni podatki, in ni verjetno, da bi pravice onemogočile ali resno ovirale uresničevanje posebnih namenov.

99. EOVP je zlasti zaskrbljen, da ta odstopanja ne bi bila upravičena in bi jih bilo treba dodatno proučiti, zlasti če bi jih uporabil upravljavec osebnih podatkov, ki podatke psevdonimizira „*za statistične namene, znanstvenoraziskovalne namene in namene arhiviranja v javnem interesu itd.*," v skladu s členom 28(2) zakona o varstvu osebnih podatkov „*brez privolitve posameznikov, na katere se nanašajo osebni podatki*" (in brez zagotavljanja informacij, predvidenih v členu 20 zakona o varstvu osebnih podatkov)[38], če ta upravljavec ohrani podatke, ki omogočajo vnovično identifikacijo. V skladu s Splošno uredbo o varstvu podatkov bi morali imeti posamezniki možnost uresničevati svoje pravice v zvezi z vsemi informacijami, na podlagi katerih jih je mogoče identificirati ali izpostaviti, tudi če se podatki štejejo za psevdonimizirane, razen če se uporablja že omenjeni člen 11 Splošne uredbe o varstvu podatkov. Glede tega EOVP ugotavlja, da le, kadar se ti podatki zagotovijo tretji osebi za iste statistične in znanstvenoraziskovalne namene in namene arhiviranja, podatki, na podlagi katerih je mogoče identificirati zadevnega posameznika, ne bi smeli biti vključeni, zato le upravljavec osebnih podatkov, ki se mu v skladu s členom 28-2(2) zakona o varstvu osebnih podatkov zagotovijo psevdonimizirani podatki, brez dodatnih podatkov verjetno praktično ne bi mogel identificirati posameznika, na katerega se nanašajo osebni podatki.

100. Na kratko, glede na to, da se, kot je potrdila Evropska komisija, „*zakon o varstvu osebnih podatkov ne zanaša na psevdonimizacijo kot možni zaščitni ukrep, ampak jo določa kot predpogoj za izvajanje nekaterih dejavnosti obdelave za namene statistike, znanstvenih raziskav in arhiviranja v javnem interesu (na primer za obdelavo podatkov brez privolitve ali združevanje različnih naborov podatkov)*"[39], vendar za take primere predvideva pomembne omejitve pravic posameznikov, na katere se podatki nanašajo, EOVP Evropsko komisijo poziva, naj dodatno oceni odstopanja iz člena 28(7) zakona o varstvu osebnih podatkov in člena 40(3) zakona o uporabi in varstvu kreditnih informacij ter pozorno spremlja njihovo uporabo in ustrezno sodno prakso[40], da se zagotovi, da pravice posameznikov, na katere se nanašajo osebni podatki, ne bodo neupravičeno omejene, kadar se osebni podatki, preneseni na podlagi sklepa o ustreznosti, obdelujejo za te namene, ob upoštevanju, da te pravice v številnih primerih pomagajo tudi upravljavcu, da zagotovi kakovost obdelanih podatkov.

3.1.11. Omejitve nadaljnjih prenosov podatkov

101. V referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov je pojasnjeno, da nadaljnji prenos podatkov ne sme ogroziti ravni varstva posameznikov, katerih osebni podatki se prenesejo na podlagi sklepa o ustreznosti, zato bi moral biti vsak nadaljnji prenos podatkov „*dovoljen le, kadar za nadaljnjega prejemnika (tj. prejemnika nadaljnjega prenosa) veljajo pravila (vključno s pogodbenimi pravili), ki zagotavljajo ustrezno raven varstva, in pri obdelavi podatkov v imenu upravljavca podatkov upošteva ustrezna navodila"*.

102. Kar zadeva nadaljnje prenose podatkov zunanjim izvajalcem (tj. obdelovalcem) s sedežem v drugih tretjih državah, EOVP ugotavlja, da v južnokorejskem pravnem okviru ni posebnih pravil za te primere in da mora, kot meni Evropska komisija[41], južnokorejski upravljavec osebnih podatkov s pravno zavezujočim instrumentom zagotoviti skladnost z določbami zakona o varstvu osebnih podatkov o

[38] Glej člen 28(7) zakona o varstvu osebnih podatkov, kot je pojasnjeno v uradnem obvestilu št. 2021-1, v skladu s katerim se nekateri zaščitni ukrepi iz zakona o varstvu osebnih podatkov, tj. *v členih 20, 21, 27, členu 34(1), členih 35 do 37 ter členu 39(3), (4), (6) do (8)*, ne uporabljajo za psevdonimizirane podatke, ki se obdelujejo za namene zbiranja podatkov za statistiko, znanstvene raziskave, vzdrževanja javnih evidenc itd.

[39] Uvodna izjava 42 osnutka sklepa.

[40] Glej na primer ustavne izzive Open Neta (informacije na naslovu https://opennet.or.kr/19909 so na voljo samo v korejščini).

[41] Uvodna izjava 87 osnutka sklepa.

zunanjem izvajanju (člen 26) in bo odgovoren za osebne podatke, ki so bili preneseni v zunanje izvajanje (člen 26).

103. Glede nadaljnjih prenosov podatkov tretjim osebam (tj. drugim upravljavcem osebnih podatkov) mora južnokorejski upravljavec osebnih podatkov v skladu s členom 17(3) zakona o varstvu osebnih podatkov posameznike, na katere se nanašajo osebni podatki, obvestiti o prenosih podatkov v tujino in pridobiti njihovo privolitev za te prenose podatkov ter „*ne sme skleniti pogodbe o čezmejnem prenosu osebnih podatkov v nasprotju z zakonom o varstvu osebnih podatkov*“. EOVP ugotavlja, da bo ta zadnja določba zagotovila – kot meni Evropska komisija[42] –, da nobena pogodba za čezmejne prenose podatkov ne bo vsebovala obveznosti, ki bi bile v nasprotju z zahtevami, ki jih upravljavcu osebnih podatkov nalaga zakon o varstvu osebnih podatkov, in bi se zato lahko štela kot zaščitni ukrep, vendar ne nalaga nobene obveznosti uvedbe zaščitnih ukrepov za zagotovitev, da bo prejemnik podatkov zagotovil enako raven varstva, kot jo zagotavlja zakon o varstvu osebnih podatkov. Zato EOVP potrjuje, da se bo informirana privolitev posameznika, na katerega se nanašajo osebni podatki, na splošno uporabljala kot podlaga za prenos podatkov od upravljavca osebnih podatkov s sedežem v Republiki Koreji prejemniku s sedežem v tretji državi.

104. Glede tega so dobrodošla dodatna pojasnila odbora za varstvo osebnih podatkov v uradnem obvestilu št. 2021-1 v zvezi z obveznostjo obveščanja posameznikov o tem, v katero tretjo državo bodo preneseni njihovi podatki[43], saj bi to – kot je poudarila Evropska komisija[44] – posameznikom, na katere se nanašajo osebni podatki, v EGP pomagalo sprejeti popolnoma informirano odločitev o tem, ali dajo privolitev za prenos podatkov v tujino ali ne.

105. Vendar je treba, kot je bilo obravnavano tudi v Mnenju št. 28/2018 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na Japonskem, poudariti, da je treba v skladu s Splošno uredbo o varstvu podatkov posameznike, na katere se nanašajo osebni podatki, pred privolitvijo izrecno obvestiti o možnih tveganjih takih prenosov podatkov, ki so posledica tega, da ni ustreznega varstva v tretji državi in da ni ustreznih zaščitnih ukrepov. Tako obvestilo bi lahko vključevalo na primer informacije, da morda v tretji državi ni nadzornega organa in/ali 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 informirano privolitev na podlagi popolnega poznavanja teh konkretnih dejstev v zvezi s prenosom[46]. Zato je EOVP zaskrbljen zaradi ugotovitev Evropske komisije v osnutku sklepa o ustreznosti v zvezi s to posebno vrsto prenosov podatkov. Posamezniki, na katere se nanašajo osebni podatki, običajno niso seznanjeni z okvirom varstva podatkov v tretjih državah. Zato ni mogoče sklepati, da lahko posameznik, na katerega se nanašajo osebni podatki, oceni tveganje prenosa podatkov samo na podlagi poznavanja zadevne namembne države. Preden posameznik, na katerega se nanašajo osebni podatki, da privolitev, je treba zagotoviti jasne informacije o specifičnih tveganjih takega prenosa osebnih podatkov v državo zunaj ozemlja Republike Koreje.

106. Zato EOVP Evropsko komisijo poziva, naj zagotovi, da informacije, ki jih je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, „*o okoliščinah v zvezi s prenosom*“ vključujejo tudi informacije o možnih tveganjih pri prenosu podatkov, ki so posledica tega, da ni ustreznega varstva v tretji državi niti ustreznih zaščitnih ukrepov. To je pomembno za EOVP, da lahko oceni, ali so zahteve glede privolitve v bistvenem enakovredne Splošni uredbi o varstvu podatkov.

107. Poleg tega bi, glede na to, da mora biti privolitev dana prostovoljno, ozaveščeno, specifično in nedvoumno, EOVP v sklepu o ustreznosti odobraval zagotovila, da južnokorejski upravljavci osebnih

[42] Uvodna izjava 88 osnutka sklepa.
[43] Prav tam.
[44] Prav tam.
[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.

podatkov teh ne bodo poslali tretji osebi v tretji državi v nobenem primeru, v katerem v skladu s Splošno uredbo o varstvu podatkov ne bi bilo mogoče zagotoviti veljavne privolitve, na primer zaradi neravnovesja moči.

108. V zvezi s primeri, v katerih lahko upravljavec osebnih podatkov te prenese tretji osebi v tujini brez privolitve posameznika, na katerega se nanašajo osebni podatki, tj. (1) če se osebni podatki zagotovijo v obsegu, ki je razumno povezan s prvotnim namenom zbiranja v skladu s členom 17(4) zakona o varstvu osebnih podatkov, in (2) če se lahko osebni podatki tretji osebi zagotovijo v izjemnih primerih iz člena 18(2) zakona o varstvu osebnih podatkov, je EOVP seznanjen s pojasnili odbora za varstvo osebnih podatkov v oddelku 2 uradnega obvestila št. 2021-1 (in pozdravlja predvideno obveznost, naloženo upravljavcu s sedežem v Republiki Koreji in prejemniku v tujini, da s pravno zavezujočim instrumentom (na primer s pogodbo) zagotovita raven varstva, enakovredno zakonu o varstvu osebnih podatkov, tudi v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki).

3.1.12. Neposredno trženje

109. V skladu s členom 21(2) in (3) Splošne uredbe o varstvu podatkov in referenčnim dokumentom o ustreznosti v skladu s Splošno uredbo o varstvu podatkov mora imeti posameznik, na katerega se nanašajo osebni podatki, vedno možnost, da brez kakršnih koli stroškov ugovarja obdelavi podatkov za namene oblikovanja profilov in neposrednega trženja.

110. Glede pravice do začasne prekinitve obdelave osebnih podatkov, predvidene v členu 37 zakona o varstvu osebnih podatkov, EOVP potrjuje mnenje Evropske komisije, da ta pravica velja tudi, kadar se podatki uporabljajo za namene neposrednega trženja[47]. Vendar bi EOVP v osnutku sklepa pozdravil dodatne informacije in pojasnila v zvezi s to oceno in zlasti o praktični uporabi pravice do začasne prekinitve obdelave osebnih podatkov v okviru neposrednega trženja (na primer sklicevanja na ustrezno sodno prakso itd.). Glede tega želi EOVP poudariti še, da je pravica posameznika, da od ponudnika oziroma uporabnika kreditnih informacij zahteva, da preneha vzpostavljati stik z njim za namene predstavitve ali nagovarjanja k nakupu blaga ali storitev, izrecno navedena v zakonu o uporabi in varstvu kreditnih informacij (člen 37(2)).

111. Poleg tega je, kot potrjuje Evropska komisija[48], v južnokorejskem pravnem okviru za takšno obdelavo na splošno potrebna specifična (dodatna) privolitev posameznika, na katerega se nanašajo osebni podatki (glej člen 15(1), točka 1, in člen 17(2), točka 1, zakona o varstvu osebnih podatkov).

112. Ker ni mogoče izključiti, da se osebni podatki, preneseni iz EGP, v Republiki Koreji obdelujejo za take namene, bi EOVP v sklepu o ustreznosti pozdravil tudi pojasnila o obstoju pravice posameznika, na katerega se nanašajo osebni podatki, da prekliče privolitev[49], in pravice, da se njegovi osebni podatki izbrišejo in se ne obdelujejo več, kadar obdelava temelji na privolitvi (na primer v primeru obdelave za namene trženja) ter jo je posameznik, na katerega se nanašajo osebni podatki, preklical.

3.1.13. Avtomatizirano sprejemanje odločitev in oblikovanje profilov

113. Kot Evropska komisija navaja v svojem osnutku sklepa[50], zakon o varstvu osebnih podatkov niti njegova uredba o izvajanju ne vsebujeta splošnih določb, ki bi obravnavale vprašanje odločitev, ki vplivajo na posameznika, na katerega se nanašajo osebni podatki, in temeljijo izključno na avtomatizirani obdelavi

[47] Uvodna izjava 79 osnutka sklepa.
[48] Prav tam.
[49] Glej tudi točko 67 zgoraj: v zakonu o uporabi in varstvu kreditnih informacij je možnost preklica privolitve jasno predvidena v členu 37(1), v zakonu o varstvu osebnih podatkov pa je omenjena le dvakrat za specifične posebne okoliščine: v členu 27(1), točka 2, in členu 39(7).
[50] Glej uvodno izjavo 81 osnutka sklepa.

osebnih podatkov. Vendarle pa južnokorejski pravni sistem takšno pravico predvideva v zakonu o uporabi in varstvu kreditnih informacij, ki vsebuje pravila o avtomatiziranem sprejemanju odločitev (člen 36(2)), čeprav se zdi, da je njihova uporaba zunaj področja nadzora odbora za varstvo osebnih podatkov (in zunaj področja uporabe tega osnutka sklepa, o področju uporabe osnutka sklepa glej oddelek 2.3.2 zgoraj).

114. Kot je Delovna skupina iz člena 29[51] že proučila v svojem Mnenju št. 1/2016 o ustreznosti zasebnostnega ščita in je EOVP obravnaval v svojem prejšnjem mnenju o sklepu o ustreznosti v zvezi z Japonsko[52], bi bilo treba zaradi čedalje večjega pomena avtomatiziranega sprejemanja odločitev, oblikovanja profilov in umetne inteligence glede tega sprejeti bolj zaščitni pristop. V nasprotju z argumenti Evropske komisije[53], v skladu s katerimi odsotnost specifičnih pravil o avtomatiziranem sprejemanju odločitev v zakonu o varstvu osebnih podatkov verjetno ne bo vplivala na raven varstva v zvezi z osebnimi podatki, ki so bili zbrani v Uniji (saj bi vsako odločitev na podlagi avtomatizirane obdelave običajno sprejel upravljavec v Uniji, ki je v neposrednem odnosu z zadevnim posameznikom, na katerega se nanašajo osebni podatki), EOVP meni, da ni mogoče izključiti, da bi lahko upravljavec osebnih podatkov s sedežem v Republiki Koreji uporabil avtomatizirano sprejemanje odločitev v primeru podatkov, prenesenih na podlagi sklepa o ustreznosti (na primer v okviru zaposlitve, za ocenjevanje uspešnosti pri delu, zanesljivosti, vedenja itd.).

115. Razvoj novih tehnologij podjetjem omogoča, da lažje izvajajo ali razmišljajo o izvajanju sistemov avtomatiziranega sprejemanja odločitev, kar lahko posledično oslabi položaj posameznikov. Kadar odločitve, ki jih sprejmejo izključno ti avtomatizirani sistemi, vplivajo na pravni položaj posameznikov ali jih pomembno prizadenejo (na primer z uvrstitvijo na črni seznam in s tem onemogočanjem pravic posameznikom), je ključno, da se zagotovijo zadostni zaščitni ukrepi, vključno s pravico do obveščenosti o specifičnih razlogih za odločitev in zadevni logiki, do popravka netočnih ali nepopolnih informacij ter do izpodbijanja odločitve, če je bila ta sprejeta na napačni dejanski podlagi[54].

116. Glede tega ima EOVP pomisleke zaradi pomanjkanja pravnih določb o avtomatiziranem sprejemanju odločitev v zakonu o varstvu osebnih podatkov, zato Evropsko komisijo poziva, naj obravnava ta pomislek in še naprej spremlja razvoj južnokorejskega zakonodajnega okvira v zvezi s tem.

3.1.14. Odgovornost

117. Južnokorejski pravni okvir vsebuje številna pravila, katerih cilj je zagotoviti, da upravljavci osebnih podatkov uvedejo ustrezne tehnične in organizacijske ukrepe za učinkovito izpolnjevanje svojih obveznosti glede varstva podatkov in da lahko to izpolnjevanje med drugim dokažejo pristojnemu nadzornemu organu. Natančneje, EOVP pozdravlja vzpostavljena pravila, ki predvidevajo sprejetje notranjega načrta upravljanja (člen 29 zakona o varstvu osebnih podatkov), obveznost izvedbe t. i. ocene učinka na zasebnost za primere, v katerih obdelava pomeni večje tveganje morebitnih kršitev zasebnosti (člen 33(1) zakona o varstvu osebnih podatkov in člen 35 uredbe o izvajanju zakona o varstvu osebnih podatkov), pravila o usposabljanju in nadzoru osebja (člen 28 zakona o varstvu osebnih podatkov) ter obveznost imenovanja pooblaščene osebe za varstvo zasebnosti (člen 31 zakona o varstvu osebnih podatkov v povezavi s členom 32 uredbe o izvajanju zakona o varstvu osebnih podatkov).

[51] 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.

[52] Mnenje št. 28/2018 o osnutku izvedbenega sklepa Evropske komisije o ustreznem varstvu osebnih podatkov na Japonskem, sprejeto 5. decembra 2018.

[53] Uvodna izjava 81 osnutka sklepa.

[54] WP 254, str. 7.

118. EOVP se strinja s stališčem Evropske komisije glede v bistvenem enakovrednega varstva, ki ga zagotavljajo – tudi v primerih, v katerih se zdi, da se pravila razmeroma razlikujejo od tistih v Splošni uredbi o varstvu podatkov, na primer ni določbe, ki bi določala, da mora biti pooblaščena oseba za varstvo zasebnosti neodvisna, vendar pa je jasno določeno, da mora poročati vodstvu upravljavca osebnih podatkov (člen 31(4) zakona o varstvu osebnih podatkov) in da zaradi opravljanja teh nalog ne sme imeti neupravičeno negativnih posledic (člen 31(5) zakona o varstvu osebnih podatkov) –, in Evropski komisiji predlaga, da pri pregledu sklepa o ustreznosti spremlja dejansko uporabo teh določb, da se oceni njihovo učinkovito izvajanje.

3.2. Postopkovni mehanizmi in mehanizmi za izvrševanje

119. EOVP je na podlagi meril iz referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov analiziral naslednje vidike južnokorejskega okvira za varstvo podatkov, kot so zajeti v osnutku sklepa: obstoj in učinkovito delovanje neodvisnega nadzornega organa, obstoj sistema, ki zagotavlja dobro raven skladnosti ter sistema za dostop do ustreznih pravnih sredstev, ki posameznikom v EGP zagotavlja sredstva za uresničevanje pravic in pravnih sredstev, ne da bi pri tem naleteli na zapletene ovire za upravno in sodno varstvo.

120. V skladu s poglavjem VI Splošne uredbe o varstvu podatkov in poglavjem 3 referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov mora biti vzpostavljen eden ali več neodvisnih nadzornih organov, katerih naloga je spremljanje, zagotavljanje in uveljavljanje skladnosti z določbami o varstvu podatkov in zasebnosti v tretji državi, da se zagotovi raven varstva, enakovredna ravni varstva v EGP.

121. V tem okviru mora nadzorni organ tretje države pri opravljanju svojih nalog in izvajanju pooblastil delovati popolnoma neodvisno in nepristransko ter pri tem ne sme niti zahtevati niti sprejemati navodil. Poleg tega mora imeti nadzorni organ vsa potrebna in razpoložljiva pooblastila ter naloge za zagotavljanje skladnosti s pravicami do varstva podatkov in spodbujanje ozaveščenosti. Upoštevati je treba tudi osebje in proračun nadzornega organa. Nadzorni organ mora imeti tudi možnost, da postopek začne na svojo pobudo.

3.2.1. Pristojni neodvisni nadzorni organ

122. V Republiki Koreji je neodvisni organ, pristojen za spremljanje in izvajanje zakona o varstvu osebnih podatkov, odbor za varstvo osebnih podatkov. Navedeni odbor sestavljajo predsednik, podpredsednik in sedem članov odbora. Predsednika in podpredsednika odbora imenuje predsednik na predlog predsednika vlade. Po dva člana odbora sta imenovana na predlog predsednika odbora in na predlog predstavnikov politične stranke, katere član je predsednik, preostali trije člani odbora pa so imenovani na predlog predstavnikov drugih političnih strank (člen 7-2(2) zakona o varstvu osebnih podatkov). Odboru za varstvo osebnih podatkov pomaga sekretariat (člen 7-13), za obravnavo manjših kršitev in ponavljajočih se zadev pa lahko ustanovi pododbore (sestavljene iz po treh članov odbora) (člen 7-12 zakona o varstvu osebnih podatkov).
123. V tem smislu EOVP potrjuje, da je kljub nedavni reorganizaciji, ki je močno spremenila njegov status in pristojnosti, odbor za varstvo osebnih podatkov vložil veliko prizadevanj v vzpostavitev potrebne infrastrukture za izvajanje zakona o varstvu osebnih podatkov in njegovih najnovejših sprememb. Med temi prizadevanji je mogoče omeniti vzpostavitev pravil odbora za varstvo osebnih podatkov, pripravo smernic za zagotavljanje navodil za razlago zakona o varstvu osebnih podatkov in vzpostavitev telefonske številke za pomoč poslovnim subjektom in posameznikom glede določb o varstvu podatkov ter storitve mediacije za obravnavo pritožb. Naloge odbora za varstvo osebnih podatkov vključujejo zlasti svetovanje o zakonih in drugih predpisih, povezanih z varstvom podatkov, pripravo politik in smernic za varstvo podatkov, preiskovanje kršitev pravic posameznikov, obravnavanje pritožb in reševanje sporov z mediacijo, uveljavljanje skladnosti z zakonom o varstvu osebnih podatkov,

zagotavljanje izobraževanja in promocije na področju varstva podatkov ter izmenjavo in sodelovanje z organi tretjih držav za varstvo podatkov[55].

124. Imenovanje in sestava odbora za varstvo osebnih podatkov sta opredeljena v členu 7-2 zakona o varstvu osebnih podatkov. Čeprav je odbor za varstvo osebnih podatkov v pristojnosti predsednika vlade (predsednika in podpredsednika odbora pa imenuje predsednik na predlog predsednika vlade), pravni okvir članom odbora nalaga, da svoje naloge opravljajo neodvisno, v skladu z zakonom in svojo vestjo. EOVP je seznanjen z institucionalnimi in postopkovnimi jamstvi, ki jih vsebuje zakon o varstvu osebnih podatkov, zlasti členi 7-4 do 7-7. Kljub temu EOVP Evropsko komisijo poziva, naj spremlja vse dogodke, ki bi lahko vplivali na neodvisnost članov južnokorejskega nadzornega organa.

125. Poleg tega osnutek sklepa še ne zajema analize proračuna odbora za varstvo osebnih podatkov, vključno z viri financiranja in preglednostjo proračuna. EOVP meni, da je treba ta element, ki je omenjen tako v členu 56(1) Splošne uredbe o varstvu podatkov kot tudi v procesnih in izvršilnih načelih ter mehanizmih varstva podatkov, ki jih je treba upoštevati v okviru referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov pri proučevanju sistema države ali mednarodne organizacije, temeljito upoštevati, saj je kazalnik gospodarskih in človeških virov, ki so nadzornemu organu na voljo za neodvisno izvajanje zakonskih obveznosti in nalog v zvezi z varstvom podatkov, zato Evropski komisiji svetuje, naj ga v osnutku sklepa podrobneje upošteva.

3.2.2. Obstoj sistema varstva podatkov, ki zagotavlja dobro raven skladnosti

126. Na področju izvrševanja je EOVP seznanjen z raznovrstnimi izvršilnimi pooblastili in sankcijami odbora za varstvo osebnih podatkov, kot jih opredeljujeta zakona o varstvu osebnih podatkov ter o uporabi in varstvu kreditnih informacij, poleg tega je seznanjen s pojasnili iz uradnega obvestila št. 2021-1, po katerih se bodo pogoji iz člena 64(1) zakona o varstvu osebnih podatkov in člena 45(4) zakona o uporabi in varstvu kreditnih informacij[56] uporabljali, kadar koli bodo kršena katera koli načela, pravice in dolžnosti, vključene v zakon o varstvu osebnih podatkov. Vendar Evropski komisiji priporoča, naj pozorno spremlja izvajanje pooblastil odbora za varstvo osebnih podatkov v praksi, da kršitelju odredi ukrep, za katerega meni, da je ustrezen v skladu z ukrepi iz člena 64(1) zakona o varstvu osebnih podatkov ali člena 45(4) zakona o uporabi in varstvu kreditnih informacij.

127. Poleg tega je v zvezi s korektivnimi ukrepi iz člena 64(1) zakona o varstvu osebnih podatkov v primeru neupoštevanja korektivnega ukrepa odbor za varstvo osebnih podatkov pooblaščen, da naloži globo v najvišjem znesku 50 milijonov južnokorejskih vonov (člen 75(2), točka 13, zakona o varstvu osebnih podatkov). Ta znesek je enakovreden znesku 36.564 evrov. EOVP meni in ima pomisleke, da tako omejen obseg denarnih sankcij morda ne bo imel posebno močnega odvračilnega učinka na kršitelje, kot je predvideno z zakonom, da bi se zagotovilo izvajanje pravil o varstvu podatkov, saj se ne zdi ustrezno zadosten za odvračanje, zlasti v primeru velikih organizacij ali podjetij s precejšnjimi finančnimi sredstvi.

128. Glede možnosti, da lahko odbor za varstvo osebnih podatkov zahteva, da vodja osrednje agencije za upravni nadzor izvede preiskavo v zvezi z upravljavcem osebnih podatkov ali skupaj z njim sodeluje pri preiskavi kršitev zakona o varstvu osebnih podatkov in celo naloži korektivne ukrepe v zvezi z upravljavci osebnih podatkov v njihovi pristojnosti (člen 63(4) in (5) zakona o varstvu osebnih podatkov), EOVP ugotavlja, da čeprav so bile nekatere informacije navedene v uvodni izjavi 122 osnutka sklepa, na splošno narava teh drugih agencij in njihova pravna razmerja z odborom za varstvo osebnih podatkov ostajajo precej nejasna. Poleg tega se člen 68(1) zakona o varstvu osebnih podatkov

[55] Naloge in pooblastila odbora za varstvo osebnih podatkov so navedeni predvsem v členih 7-8, 7-9 in 61 do 66 zakona o varstvu osebnih podatkov.

[56] Tj. šteje se, *„da kršitev zakona verjetno krši pravice in svoboščine posameznikov v zvezi z osebnimi podatki in da bo zaradi opustitve ukrepanja verjetno nastala težko popravljiva škoda“.*

sklicuje na številne subjekte, na katere bi bilo mogoče prenesti pooblastila odbora za varstvo osebnih podatkov. Čeprav se zdi, da je bila ta določba uporabljena samo v zvezi z južnokorejsko agencijo za internet in varnost[57], bi EOVP pozdravil pojasnila v zvezi z naravo možnih interakcij med temi subjekti in pozorno spremljanje uporabe te določbe v prihodnosti, da se zagotovi neodvisnost subjektov, ki so zadolženi za uporabo pravil o varstvu podatkov.

129. Kar zadeva sankcije, se zdi, da južnokorejski sistem združuje različne vrste sankcij, od korektivnih ukrepov in upravnih glob do kazenskih sankcij, ki imajo verjetno močan odvračilni učinek, južnokorejski organi pa so predstavili več primerov glob, ki jih je pred kratkim naložil odbor za varstvo osebnih podatkov, med drugim globo v znesku 6,7 milijarde južnokorejskih vonov, ki je bila decembra 2020 naložena podjetju zaradi kršenja številnih določb zakona o varstvu osebnih podatkov, in še eno globo v znesku 103,3 milijona južnokorejskih vonov, ki je bila 28. aprila 2021 naložena podjetju AI Technology zaradi kršenja pravil o zakonitosti obdelave, zlasti pravil o privolitvi, in obdelave psevdonimiziranih podatkov.

130. Čeprav imata lahko zgoraj navedena zneska odvračilni učinek, bi EOVP pozdravil dodatne informacije o načinu, ki ga odbor za varstvo podatkov uporablja za izračun višine upravnih glob, na primer v zvezi z globami, naloženimi zaradi neupoštevanja korektivnega ukrepa, izdanega v skladu s členom 64(1) zakona o varstvu osebnih podatkov (glej člen 75(2), točka 13, zakona o varstvu osebnih podatkov). To je pomembno zlasti v zvezi s kazenskimi sankcijami in uporabo (južnokorejskega) zakona o kazenskem postopku.

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

131. Glede pravnih sredstev se zdi, da južnokorejski sistem omogoča različne možnosti za zagotavljanje ustreznega varstva in zlasti uresničevanje pravic posameznikov z učinkovitimi upravnimi in sodnimi pravnimi sredstvi, vključno z odškodnino za škodo.

132. Južnokorejski sistem omogoča tudi alternativne mehanizme, na katere se lahko posamezniki poleg upravnih in sodnih poti obrnejo za pridobitev pravnega varstva, kot je pojasnjeno v uvodnih izjavah 132 in 133 osnutka sklepa, ki se nanašata na klicni center za pomoč glede zasebnosti oziroma na odbor za reševanje sporov z mediacijo. Ker gre za dodatna pravna sredstva, bi EOVP pozdravil podrobnejša pojasnila o tem, kako dopolnjujejo možnosti pravnih sredstev pred odborom za varstvo osebnih podatkov in sodišči za posameznike, na katere se nanašajo osebni podatki in katerih osebni podatki se prenesejo v Republiko Korejo na podlagi sklepa o ustreznosti.

4. DOSTOP DO OSEBNIH PODATKOV, PRENESENIH IZ EVROPSKE UNIJE, IN NJIHOVA UPORABA S STRANI JAVNIH ORGANOV V JUŽNI KOREJI

133. Glede ocene ravni varstva podatkov na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter državne varnosti je Evropska komisija v svojem osnutku sklepa in prilogah, ki so na voljo, zagotovila izčrpne informacije. Zato se EOVP v tem mnenju vzdržuje ponavljanja večine dejanskih ugotovitev in ocen.

134. Evropska komisija ugotavlja, da je na zgoraj navedenih področjih vzpostavljena taka raven varstva podatkov, ki ustreza zahtevam iz sodne prakse Sodišča Evropske unije in jo je zato mogoče šteti za v bistvenem enakovredno ravni varstva podatkov v Evropski uniji.

[57] Glej uvodno izjavo 117 osnutka sklepa in člen 62 uredbe o izvajanju zakona.

135. Na splošno želi EOVP poudariti, da je treba tudi v primerih, v katerih se zdi ali Evropska komisija trdi, da zadevna južnokorejska zakonodaja verjetno ne bo vplivala na podatke, prenesene iz Evropske unije v Južno Korejo, oceniti ustreznost južnokorejske ravni varstva podatkov v zvezi s takimi primeri. Njihovo pomembnost dokazuje tudi dejstvo, da jih je Evropska komisija sama obravnavala v osnutku sklepa.

4.1. Splošni okvir za varstvo podatkov v okviru vladnega dostopa

136. Ko gre za dostop javnih organov do osebnih podatkov, je treba za oceno ravni varstva pravice do zasebnosti in varstva osebnih podatkov oceniti raznovrstne južnokorejske predpise. EOVP najprej ugotavlja, da se zakon o varstvu osebnih podatkov kot ključni zakon o varstvu osebnih podatkov uporablja zelo široko. Vendar se ta zakon v celoti uporablja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, njegova uporaba za obdelavo podatkov za namene državne varnosti pa je omejena. V skladu s členom 58(1), točka 2, zakona o varstvu osebnih podatkov, se njegova poglavja III do VII ne uporabljajo za obdelavo osebnih podatkov za namene državne varnosti. Ob tem pa se njegova poglavja I, II, IX in X še naprej uporabljajo za namene državne varnosti. Tako se za dostop do osebnih podatkov in njihovo uporabo s strani organov za državno varnost uporabljajo temeljna načela zakona o varstvu osebnih podatkov, temeljna jamstva za pravice posameznikov, na katere se nanašajo osebni podatki, in določbe o nadzoru, izvrševanju in pravnih sredstvih.

137. Tudi južnokorejska ustava vsebuje bistvena načela varstva podatkov, in sicer načela zakonitosti, nujnosti in sorazmernosti. Ta načela se uporabljajo tudi za dostop do osebnih podatkov s strani južnokorejskih javnih organov na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in državne varnosti[58].

138. Na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj lahko policija, tožilstvo, sodišča in drugi javni organi zbirajo osebne podatke na podlagi specifične zakonodaje, tj. na podlagi zakona o kazenskem postopku, zakona o varstvu zasebnosti v komunikacijah, zakona o telekomunikacijskih podjetjih in zakon o poročanju in uporabi specifičnih informacij o finančnih transakcijah, ki se uporablja za pregon in preprečevanje pranja denarja ter financiranja terorizma. Ti specifični zakoni opredeljujejo dodatne omejitve, zaščitne ukrepe in izjeme.

139. Na področju državne varnosti lahko državna obveščevalna služba na podlagi zakona o državni obveščevalni službi in nadaljnjih zakonih o državni varnosti[59] zbira osebne podatke ter prestreza komunikacije. EOVP razume, da mora državna obveščevalna služba pri izvajanju svojih pooblastil ravnati v skladu z zgoraj navedenimi zakonskimi določbami in zakonom o varstvu osebnih podatkov.

140. EOVP Komisijo poziva, naj pojasni, ali v Republiki Koreji poleg državne obveščevalne službe delujejo še drugi organi, ki so odgovorni za državno varnost, saj Evropska komisija v oddelku 6 Priloge I daje vtis, da je državna obveščevalna služba primer agencije za državno varnost.

4.2. Varstvo in zaščitni ukrepi za podatke o potrditvi komunikacij v okviru vladnega dostopa za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

141. Na podlagi zadevnega zakona, tj. zakona o varstvu zasebnosti v komunikacijah, lahko organi kazenskega pregona sprejmejo dve vrsti ukrepov za dostop do podatkov o komunikacijah. Zakon o varstvu zasebnosti v komunikacijah razlikuje med ukrepi za omejevanje komunikacije, ki zajemajo tako zbiranje vsebine navadne pošte kot tudi neposredno prestrezanje vsebine telekomunikacij[60], in

[58] Glej uvodno izjavo 145 osnutka sklepa.
[59] Zakonodaja na področju državne varnosti vključuje na primer zakon o varstvu zasebnosti v komunikacijah, zakon o boju proti terorizmu za zaščito državljanov in javne varnosti ter zakon o telekomunikacijskih podjetjih.
[60] Člen 3(2) ter člen 2(6) in (7) zakona o varstvu zasebnosti v komunikacijah.

zbiranjem tako imenovanih podatkov o potrditvi komunikacij. Zadnjenavedeni vključujejo datum telekomunikacij, čas njihovega začetka in konca, število odhodnih in dohodnih klicev ter naročniško številko druge strani, pogostost uporabe, dnevniške datoteke o uporabi telekomunikacijskih storitev in podatke o lokaciji[61].

142. EOVP ugotavlja, da za podatke o potrditvi komunikacij očitno ne veljajo enaki zaščitni ukrepi kot za podatke, zbrane z ukrepi za omejevanje komunikacije, tj. podatke o vsebini. Dejansko EOVP ugotavlja, da je za zbiranje vsebine na voljo več zaščitnih ukrepov kot za zbiranje podatkov o potrditvi komunikacij za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj: prvič, v nasprotju z zbiranjem podatkov o vsebini zbiranje podatkov o potrditvi komunikacij ni omejeno na preiskovanje nekaterih hudih kaznivih dejanj, ampak se lahko izvede, kadar je to potrebno za izvedbo „katere koli preiskave ali za izvršitev katere koli kazni“ (člen 13(1) zakona o varstvu zasebnosti v komunikacijah). Drugič, zbiranje podatkov o potrditvi komunikacij načeloma ni zasnovano kot skrajni ukrep in se uporabi le, kadar je drugače težko preprečiti storitev kaznivega dejanja, prijeti storilca ali zbrati dokaze[62]. Podatki o potrditvi komunikacij se lahko zbirajo, kadar tožilec ali pravosodni policist „meni, da je to potrebno“ za preiskavo kaznivega dejanja ali izvršitev kazni. Vendar glede tega velja izjema za podatke o sledenju v realnem času in podatke o potrditvi komunikacij v zvezi s specifično bazno postajo v skladu s členom 13(2) zakona o varstvu zasebnosti v komunikacijah. Tretjič, organi kazenskega pregona, ki zbirajo vsebino komunikacije, morajo to prenehati nemudoma, ko se šteje, da nadaljnji dostop ni več potreben[63]. V zvezi s podatki o potrditvi komunikacij to ni izrecno določeno v zakonu o varstvu zasebnosti v komunikacijah ali njegovi uredbi o izvajanju.

143. EOVP upošteva, da se lahko podatki o potrditvi komunikacij zbirajo le na podlagi sodnega naloga. Poleg tega zakon o varstvu zasebnosti v komunikacijah zahteva, da se tako v zahtevku za izdajo sodnega naloga kot tudi v zadevnem nalogu navedejo podrobne informacije[64]. Taka predhodna sodna odobritev je dejansko že omejitev diskrecijske pravice organov kazenskega pregona pri uporabi zakona in preverjanju, ali so v posameznem primeru zadostni razlogi za zbiranje podatkov o potrditvi komunikacij. EOVP je seznanjen še, da se za zakonodajo Republike Koreje ne zdi, da ta opredeljuje splošno in neselektivno hrambo podatkov o potrditvi komunikacij. Tako se vladni dostop do takih podatkov vedno nanaša na podatke, ki se še vedno hranijo za namene zaračunavanja in zagotavljanja dejanskih komunikacijskih storitev.

144. Vendar EOVP poudarja, da je Sodišče Evropske unije podvomilo, da so podatki o prometu manj občutljivi kot drugi, zlasti podatki o vsebini[65]. Ob upoštevanju, da je za podatke o potrditvi komunikacij v več pogledih zagotovljena nižja raven varstva kot za podatke o vsebini, EOVP Evropsko komisijo poziva, naj pozorno spremlja, ali zaščitni ukrepi, ki jih za to vrsto osebnih podatkov zagotavlja južnokorejska zakonodaja, zagotavljajo v bistvenem enakovredno raven varstva, kot jo zagotavlja zakonodaja EU, zlasti glede sorazmernosti in predvidljivosti prava.

---

[61] Člen 2(11) zakona o varstvu zasebnosti v komunikacijah.

[62] To velja za podatke o vsebini v skladu s členoma 3(2) in 5(1) zakona o varstvu zasebnosti v komunikacijah.

[63] Člen 2 uredbe o izvajanju zakona o varstvu zasebnosti v komunikacijah.

[64] Glej uvodno izjavo 156 osnutka sklepa.

[65] Glej sodbo Sodišča Evropske unije z dne 6. oktobra 2020, Privacy International, C-623/17, EU:C:2020:790, točka 71: „*Poseg, ki ga pomeni prenos podatkov o prometu in podatkov o lokaciji varnostnim in obveščevalnim agencijam, v pravico, določeno v členu 7 Listine Evropske unije o temeljnih pravicah, je treba obravnavati kot posebno resen, zlasti ob upoštevanju občutljivosti informacij, ki jih lahko zagotovijo ti podatki, in še posebej možnosti, da se na njihovi podlagi ugotovi profil zadevnih oseb, saj so take informacije prav tako občutljive kot sama vsebina sporočil. Poleg tega lahko ta poseg pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje (glej po analogiji sodbi z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 27 in 37, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 99 in 100).*“

4.3. Dostop južnokorejskih javnih organov do komunikacijskih informacij za namene državne varnosti

145. V zvezi s pravnim okvirom za dostop organov za državno varnost do komunikacijskih informacij, prenesenih iz EGP v Republiko Korejo, je EOVP ugotovil dve skrb vzbujajoči točki, pri čemer se obe nanašata na ureditev dostopa do komunikacij med državljani, ki niso državljani Republike Koreje, ki spadajo v specifični sklop primerov uporabe (glej točko 29). V teh primerih se v zvezi s podatki o potrditvi komunikacij in podatki o vsebini ne uporabljajo nekateri zaščitni ukrepi, ki so sicer zagotovljeni. Z drugimi besedami, v teh specifičnih primerih za te podatke ne veljajo enaki zaščitni ukrepi kot za podatke, sporočene, kadar je v komunikaciji udeležen vsaj en južnokorejski državljan.

4.3.1. Ni obveznosti obveščanja posameznikov o vladnem dostopu do komunikacij med tujimi državljani

146. Kot je navedeno zgoraj, tj. kadar nobena od strank v komunikaciji ni južnokorejski državljan, organi za državno varnost posameznikov niso dolžni obvestiti o zbiranju in obdelavi njihovih podatkov. EOVP je seznanjen, da to velja le v nekaterih primerih. Prvič, kot je bilo že poudarjeno, kadar je v komunikacijo vključen vsaj en južnokorejski državljan, zahteve za obveščanje iz zakona o varstvu zasebnosti v komunikacijah veljajo za vse stranke v komunikaciji ne glede na njihovo državljanstvo[66]. Drugič, za zbiranje osebnih podatkov, ki izhajajo iz komunikacij izključno med tujimi državljani, velja specifični sklop primerov uporabe. Pravica do dostopa v takih primerih zajema zlasti komunikacijo v primerih a) držav, sovražnih do Republike Koreje, b) tujih agencij, skupin ali državljanov, za katere se sumi, da sodelujejo v dejavnostih proti Republiki Koreji[67], ali c) članov skupin, ki delujejo na Korejskem polotoku, vendar dejansko zunaj suverenosti Republike Koreje, in njihovih krovnih skupin s sedežem v tujih državah. Komunikacije med posamezniki iz Evropske unije, ki se iz EGP prenesejo v Republiko Korejo, se torej lahko za namene državne varnosti zbirajo le, če spadajo v eno od treh zgoraj navedenih skupin[68]. EOVP je iz dodatnih pojasnil Evropske komisije razbral, da kot dodatni omejitveni dejavnik veljavni pravni okvir ne predvideva prestrezanja podatkov, ki se prenašajo zunaj Republike Koreje.

147. Zato se lahko kritičnost pomanjkanja zahteve po uradnem obveščanju z vidika njenih praktičnih učinkov šteje za omejeno. Vendar EOVP poudarja pomen (naknadnega) obvestila o vladnem dostopu, zlasti glede zagotavljanja učinkovitih pravnih sredstev. Sodišče Evropske unije je menilo, da je ta obvestitev *„nujna, da te osebe lahko uveljavljajo pravice, ki zanje izhajajo iz členov 7 in 8 Listine, da lahko zahtevajo dostop do svojih osebnih podatkov, ki so predmet teh ukrepov, in po potrebi njihov popravek ali izbris, ter da lahko v skladu s členom 47, prvi odstavek, Listine vložijo učinkovito pravno sredstvo pred sodiščem“*[69]. Vladni dostop za namene državne varnosti pogosto vključuje tajne nadzorne ukrepe, kar pomeni, da posamezniki, na katere se podatki nanašajo, niso seznanjeni z obdelavo svojih podatkov. Tako *„je načeloma za zadevnega posameznika malo možnosti za pravno sredstvo pred sodišči, razen če je seznanjen z ukrepi, ki so bili sprejeti brez njegove vednosti, in tako lahko izpodbija njihovo zakonitost za nazaj, ali pa, če lahko vsaka oseba, ki sumi, da se njene komunikacije prestrezajo ali da so se prestrezale, zahteva sodno varstvo pred sodišči, tako da sodna pristojnost ni odvisna od obvestitve posameznika, da so bile njegove komunikacije prestrežene“*[70]. V

---

[66] Glej uvodno izjavo 192 osnutka sklepa.

[67] Glej opombo 244 v Prilogi II, v skladu s katero se pojem dejavnosti proti Republiki Koreji nanaša na dejavnosti, ki ogrožajo obstoj in varnost države, demokratični red ali preživetje in svobodo ljudi.

[68] Glej uvodno izjavo 187 osnutka sklepa.

[69] Sodba Sodišča Evropske unije z dne 6. oktobra 2020, La Quadrature du Net in drugi, združene zadeve C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 190.

[70] Sodbi Evropskega sodišča za človekove pravice z dne 25. maja 2021, *Big Brother Watch in drugi proti Združenemu kraljestvu*, ECLI:CE:ECHR:2021:0525JUD005817013, točka 337; in z dne 4. decembra 2015, *Roman Zakharov proti Rusiji*, ECLI:CE:ECHR:2015:1204JUD004714306, točka 234.

tem kontekstu in skladno s tem je EOVP večkrat izrazil zaskrbljenost glede učinkovitih pravnih sredstev v primerih nadzora. EOVP poudarja, da tajnost vladnih ukrepov ne sme povzročiti, da bi bili ti ukrepi dejansko neizpodbojni. Glede na to je treba vprašanje, ali to, da ni zahteve po obvestitvi za komunikacije med tujimi državljani, vpliva na raven varstva podatkov, kot je ocenjena v osnutku sklepa, proučiti kot del splošne ocene s specifičnim upoštevanjem mehanizmov nadzora in pravnih sredstev, ki jih zagotavlja južnokorejska zakonodaja (glej točki 4.7 in 4.8).

148. Poleg tega EOVP glede tega ugotavlja, da se zakonodaja nanaša na precej široko opredeljene pojme, kot so dejavnosti proti Republiki Koreji ali protidržavne dejavnosti[71], in da je težko predvideti, kako se ti pojmi razlagajo v južnokorejskem pravu. EOVP Evropsko komisijo poziva, naj spremlja, kako so ti pojmi opredeljeni v južnokorejskem pravu in ali njihova uporaba v praksi izpolnjuje zahteve sorazmernosti, ki izhajajo iz prava Evropske unije.

4.3.2. Brez predhodne neodvisne odobritve za zbiranje informacij o komunikaciji med tujimi državljani

149. V primerih, v katerih je treba osebne podatke iz EGP, ki izhajajo iz komunikacije med državljani, ki niso državljani Republike Koreje (in spadajo v enega od zgoraj navedenih primerov uporabe), obdelati v Republiki Koreji za namene državne varnosti, za zbiranje takih podatkov ni potrebna predhodna odobritev neodvisnega organa (kot v primeru komunikacije, v kateri je vsaj eden od zadevnih posameznikov južnokorejski državljan)[72].

150. Zlasti glede na nedavni sodbi Evropskega sodišča za človekove pravice v zadevah *Big Brother Watch in drugi proti Združenemu kraljestvu* ter *Centrum för Rättvisa proti Švedski* EOVP meni, da je treba proučiti, ali to pomeni kritično pomanjkljivost južnokorejskega okvira za varstvo podatkov. Glede tega EOVP opozarja, da, kot je poudarjeno v njegovih posodobljenih priporočilih glede evropskih temeljnih jamstev za nadzorne ukrepe[73], člen 6(3) Pogodbe o Evropski uniji določa, da temeljne pravice, vsebovane v Evropski konvenciji o človekovih pravicah, pomenijo splošna načela prava EU, Sodišče Evropske unije pa v svoji sodni praksi opozarja, da dokler Evropska unija ne postane njena pogodbenica, ta ni pravni instrument, ki bi bil formalno vključen v pravni red Evropske unije[74]. Tako mora biti raven varstva temeljnih pravic, ki jo zahteva člen (45) Splošne uredbe o varstvu podatkov, določena na podlagi določb navedenega predpisa, v povezavi s temeljnimi pravicami, navedenimi v Listini Evropske unije o temeljnih pravicah. Glede na navedeno imajo v skladu s členom 52(3) Listine Evropske unije o temeljnih pravicah pravice iz Listine, ki ustrezajo pravicam, zagotovljenim z EKČP, enak pomen in področje uporabe kot pravice, določene v navedeni konvenciji. Zato je treba sodno prakso Evropskega sodišča za človekove pravice v zvezi s pravicami, ki so predvidene tudi v Listini Evropske unije o temeljnih pravicah upoštevati kot minimalno raven varstva za razlago ustreznih pravic v Listini, tj. kolikor Listina, kot jo razlaga Sodišče Evropske unije, ne zagotavlja višje ravni varstva[75].

151. EOVP ugotavlja, da čeprav predhodna (neodvisna) odobritev nadzornih ukrepov velja za pomembni zaščitni ukrep pred arbitrarnostjo, te odobritve iz sodne prakse Sodišča Evropske unije ni mogoče izpeljati kot absolutne zahteve za sorazmernost nadzornih ukrepov. Vendar je Evropsko sodišče za človekove pravice zdaj izrecno določilo zahtevo po predhodni neodvisni odobritvi za množično

[71] Evropska komisija je pojasnila, da se po pojasnilih južnokorejske vlade to nanaša na dejavnosti, ki ogrožajo obstoj in varnost države, demokratični red ali preživetje in svobodo ljudi, glej tudi opombo 319 v osnutku sklepa o ustreznosti.

[72] Glej uvodno izjavo 190 osnutka sklepa.

[73] Glej EOVP, Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, točki 10 in 11.

[74] Glej sodbo Sodišča Evropske unije z dne 16. julija 2020, Data Protection Commissioner/Facebook Ireland Limited in Maximilian Schrems, C-311/18, EU:C:2020:559 (v nadaljevanju: Schrems II), točka 98.

[75] Sodba Sodišča Evropske unije z dne 6. oktobra 2020, La Quadrature du Net in drugi, združene zadeve C-511/18, C-512/18 in C-520/18, točka 124.

prestrezanje[76]. Čeprav v osnutku sklepa to ni izrecno navedeno, EOVP razume, da pravni okvir Republike Koreje ne predvideva množičnega prestrezanja, temveč le ciljno prestrezanje telekomunikacij[77]. Evropska komisija je to razumevanje potrdila.

152. Glede na navedeno zgoraj navedene sodbe Evropskega sodišča za človekove pravice v skladu s sodno prakso Sodišča Evropske unije[78] in predhodno sodno prakso Evropskega sodišča za človekove pravice[79] znova dokazujejo pomen celovitega nadzora, ki ga izvajajo neodvisni nadzorni organi. EOVP poudarja, da je neodvisen nadzor na vseh stopnjah postopka vladnega dostopa za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter državne varnosti pomemben zaščitni ukrep pred samovoljnimi nadzornimi ukrepi in s tem za oceno ustrezne ravni varstva podatkov. Zagotovilo neodvisnosti nadzornih organov v smislu člena 8(3) Listine Evropske unije o temeljnih pravicah naj bi zagotovilo učinkovito in zanesljivo spremljanje skladnosti s pravili o varstvu posameznikov v zvezi z obdelavo osebnih podatkov. To velja zlasti v okoliščinah, v katerih posameznik zaradi narave tajnega opazovanja ne more zahtevati pregleda ali neposredno sodelovati v katerem koli postopku pregleda pred ali med izvajanjem nadzornega ukrepa.

153. To, da ni predhodne neodvisne odobritve, samo po sebi ne more veljati za bistveno pomanjkljivost južnokorejskega prava v zvezi z oceno v bistvenem enakovredne ravni varstva podatkov. Ocena ustreznosti je znova odvisna od vseh okoliščin zadeve, zlasti od učinkovitosti naknadnega nadzora in pravnih sredstev, kot je navedeno v južnokorejskem pravnem okviru (glej še točki 4.7 in 4.8).

4.4. Prostovoljna razkritja

154. V skladu s členom 83(3) zakona o telekomunikacijskih podjetjih lahko ponudniki telekomunikacijskih storitev tako imenovane podatke o naročnikih[80] na zahtevo prostovoljno predložijo organom za državno varnost in organom kazenskega pregona. Čeprav EOVP ugotavlja, da je verjetno malo zadev, ki vključujejo osebne podatke, prenesene iz EGP v Republiko Korejo, jih je kljub temu treba proučiti, da bi ocenili raven varstva podatkov, kot je že navedeno zgoraj.

155. EOVP razume, da se v teh primerih uporabljajo zaščitni ukrepi za varstvo podatkov iz zakona o varstvu osebnih podatkov ter da morajo javni organi in ponudniki telekomunikacijskih storitev izpolnjevati te zahteve[81] ter da so lahko oboji odgovorni za morebitno kršitev pravic in svoboščin zadevnih posameznikov, na katere se nanašajo osebni podatki[82]. Poleg tega EOVP razume, da ponudnikom telekomunikacijskih storitev ni treba izpolnjevati takih zahtevkov.

156. Vendar glede koncepta dostopa državnih organov do podatkov o naročnikih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter še zlasti za namene državne varnosti na

[76] Sodba Evropskega sodišča za človekove pravice z dne 25. maja 2021, *Big Brother Watch in drugi proti Združenemu kraljestvu*, ECLI:CE:ECHR:2021:0525JUD005817013, točka 351: „*Množično prestrezanje bi moralo biti že na začetku predmet neodvisne odobritve*, *množično prestrezanje bi moral odobriti neodvisni organ, tj. organ, ki je neodvisen od izvršilne oblasti*."

[77] Le oddelek 3.2 Priloge II vsebuje izrecno izjavo za namene državne varnosti, pri čemer je določeno, da omejitve in zaščitni ukrepi „*zagotavljajo, da sta zbiranje in obdelava informacij omejena na to, kar je nujno potrebno za dosego zakonitega cilja. To izključuje kakršno koli množično in neselektivno zbiranje osebnih podatkov za namene državne varnosti.*"

[78] Glej na primer sodbo Sodišča Evropske unije, Tele2 Sverige AB in drugi, združeni zadevi C-203/15 in C-698/15, EU:C:2016:970.

[79] Glej na primer sodbo Evropskega sodišča za človekove pravice z dne 4. decembra 2015, *Roman Zakharov proti Rusiji*, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Zadevni nabori podatkov bi bili: ime, matična številka prebivalca, naslov in telefonska številka uporabnikov, datumi, ko se uporabniki naročijo ali prekinejo naročnino, ter identifikacijske kode uporabnikov (ki se uporabljajo za identifikacijo zakonitega uporabnika računalniških sistemov ali komunikacijskih omrežij).

[81] Glej uvodni izjavi 164 in 194 osnutka sklepa.

[82] Glej uvodno izjavo 166 osnutka sklepa.

podlagi prostovoljnega razkritja telekomunikacijskih operaterjev obstaja pomislek zaradi povečanega tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zlasti v zvezi z njihovo pravico do obveščenosti.

157. V skladu s členom 58(1), točka 2, zakona o varstvu osebnih podatkov, se določbe njegovih poglavij III do VII ne uporabljajo za katere koli osebne podatke, katerih predložitev se zahteva za namene državne varnosti. V tem smislu se za take zahtevke ne uporabljajo na primer določbe členov 18 (Omejitev nenamenske uporabe in zagotavljanja osebnih podatkov) in 20 (Obvestilo o virih itd. osebnih podatkov, zbranih od tretjih oseb) zakona o varstvu osebnih podatkov. V primerih, v katerih zahtevek vloži organ za državno varnost, se na eni strani postavlja vprašanje, ali člen 58(1), točka 2, nasprotuje uporabi zakona o varstvu osebnih podatkov tudi za ponudnike telekomunikacijskih storitev. Po drugi strani pa se postavlja vprašanje, ali izključitev uporabe člena 20 zakona o varstvu osebnih podatkov v takih primerih velja tudi za ustrezno določbo iz oddelka 3 Priloge I (Obvestilo v zvezi s podatki, kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se nanašajo (člen 20 zakona)). Če bi bilo tako in če bi se člen 58(1), točka 2, nanašal tudi na ponudnike telekomunikacijskih storitev, bi glede na informacije, ki so na voljo, obstajalo tveganje, da ne bi bilo zakonske obveznosti, da se posameznike, na katere se nanašajo osebni podatki, obvesti o prostovoljnem razkritju.

158. EOVP je zato zaskrbljen zaradi učinka, da bi lahko zahteve po obveščanju postale neučinkovite, saj bi posameznikom, na katere se nanašajo osebni podatki, pomembno otežilo, da uresničijo svoje pravice do varstva podatkov, zlasti v zvezi s sodnimi pravnimi sredstvi. Glede tega EOVP Evropsko komisijo poziva, naj pojasni področje uporabe zadevnih določb.

4.5. Nadaljnja uporaba podatkov

159. Načelo omejitve namena je temeljna pravna zahteva za varstvo podatkov. Zahteva, da se osebni podatki zbirajo le za določene, izrecne in zakonite namene ter da se ne smejo dodatno obdelovati na način, ki ni združljiv s temi nameni. Poleg tega smejo javni organi v skladu z zakonodajo EU obdelovati osebne podatke za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, tudi če so bili ti podatki prvotno pridobljeni za drug namen, če imajo ti organi pravno podlago za obdelavo takih podatkov v skladu z ustrezno zakonodajo in če nadaljnja obdelava ni nesorazmerna[83].

160. V skladu s tem EOVP ugotavlja, da južnokorejski okvir za varstvo podatkov opredeljuje podobne zaščitne ukrepe in omejitve, kot jih opredeljuje zakonodaja Evropske unije, v zvezi z nadaljnjo uporabo podatkov, zbranih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in državne varnosti, na primer načelo omejitve namena iz člena 3(1) in (2) zakona o varstvu osebnih podatkov.

4.6. Nadaljnji prenosi in izmenjava obveščevalnih podatkov

161. Člen 44 Splošne uredbe o varstvu podatkov določa, da se prenosi in nadaljnji prenosi osebnih podatkov izvedejo le, če ni ogrožena raven varstva, ki jo zagotavlja navedena uredba. Tako se raven varstva, zagotovljena za osebne podatke, prenesene iz EGP v Republiko Korejo, z nadaljnjim prenosom prejemnikom v tretji državi ne sme okrniti, tj. nadaljnji prenosi smejo biti dovoljeni le, če je zagotovljena stalna raven varstva, ki je v bistvenem enakovredna tisti, ki jo zagotavlja zakonodaja Evropske unije. Zato je treba pri ocenjevanju, ali tretja država zagotavlja ustrezno raven varstva podatkov, upoštevati pravni okvir zadevne države za nadaljnje prenose. To je nesporno in v skladu s stališčem Evropske komisije[84] in EOVP.

[83] Glej člen 4(2) direktive o varstvu posameznikov pri obdelavi osebnih podatkov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.
[84] Glej uvodno izjavo 84 in naslednje osnutka sklepa.

162. V tem smislu EOVP ugotavlja, da je Evropsko sodišče za človekove pravice v svojih nedavnih sodbah v zadevah *Big Brother Watch in drugi proti Združenemu kraljestvu* ter *Centrum för Rättvisa proti Švedski* zagotovilo smernice[85] glede previdnostnih ukrepov v zvezi z varstvom podatkov, ki jih morajo države pogodbenice upoštevati pri sporočanju osebnih podatkov drugim osebam za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in državne varnosti v primerih množičnega zbiranja: *„Najprej, v notranjem pravu je treba jasno določiti okoliščine, v katerih se lahko opravi tak prenos. Drugič, država, ki podatke prenese, mora zagotoviti, da ima država prejemnica pri ravnanju s podatki vzpostavljene zaščitne ukrepe, s katerimi je mogoče preprečiti zlorabo in nesorazmerno poseganje. Država prejemnica mora zlasti zagotoviti varno hrambo gradiva in omejiti njegovo nadaljnje razkritje. [...] Tretjič, poostreni zaščitni ukrepi bodo potrebni, kadar je jasno, da se prenaša gradivo, za katero je potrebna posebna zaupnost – na primer zaupno novinarsko gradivo.“*[86]

163. Pri uporabi teh standardov je Evropsko sodišče za človekove pravice v zadevi *Centrum för Rättvisa proti Švedski* ugotovilo, da to, da ni izrecne pravne zahteve v ureditvi prestrezanja, da se ocenita nujnost in sorazmernost izmenjave obveščevalnih podatkov zaradi njenega morebitnega vpliva na pravico do zasebnosti, pomeni kršitev člena 8 EKČP. Evropsko sodišče za človekove pravice je bilo kritično, da je mogoče zaradi splošne ravni prava prestrezano gradivo na splošno poslati v tujino, kadar koli se šteje, da je to v nacionalnem interesu, ne glede na to, ali tuji prejemnik zagotavlja sprejemljivo minimalno raven zaščitnih ukrepov[87].

164. Ob priznavanju, da pravni okvir Južne Koreje ne omogoča množičnega prestrezanja, še vedno glede na posledice sodne prakse Evropskega sodišča za človekove pravice, kot je opisano zgoraj, EOVP meni, da je treba poleg zahtev, ki izhajajo iz prava EU, kot ga razlaga Sodišče Evropske unije, pri ocenjevanju, ali pravni okvir za nadaljnje prenose v tretjo državo zagotavlja ustrezne standarde varstva podatkov, upoštevati tudi argumente Evropskega sodišča za človekove pravice.

4.6.1. Veljavni pravni okvir za nadaljnje prenose s strani organov kazenskega pregona

165. V zvezi z nadaljnjimi prenosi s strani pristojnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj EOVP iz pojasnil Evropske komisije razume, da se oddelek 2 Priloge I k osnutku sklepa o omejitvi nadaljnjih prenosov uporablja tudi, kadar se prenos opravi na podlagi zakona, ki ni zakon o varstvu osebnih podatkov. V skladu s tem pravilom, *„če se osebni podatki zagotovijo tretji osebi v tujini, zaradi razlik v sistemih varstva osebnih podatkov v različnih državah morda ne bodo deležni ravni varstva, ki jo zagotavlja južnokorejski zakon o varstvu osebnih podatkov. Tako se takšni primeri štejejo za primere, v katerih se lahko posamezniku, na katerega se nanašajo osebni podatki, povzroči škoda iz točke 4 člena 17 zakona ali za primere, v katerih se nepošteno krši interes posameznika, na katerega se nanašajo osebni podatki, ali tretje osebe iz točke 2 člena 18 zakona in člena 14(2) uredbe o izvajanju navedenega zakona. Za izpolnitev zahtev teh določb morata upravljavec osebnih podatkov in tretja oseba zato izrecno zagotoviti raven varstva, enakovredno tisti v zakonu, vključno z zagotovitvijo uresničevanja pravic posameznika, na katerega se nanašajo osebni podatki, v pravno zavezujočih dokumentih, kot so pogodbe, tudi po prenosu osebnih podatkov v tujino“*[88].

---

[85] Naslednji elementi so bili opredeljeni na podlagi zadev *Big Brother Watch* in *Centrum för Rättvisa*, ki se nanašata na ureditve množičnega prestrezanja. Zahteva po previdnostnih ukrepih, ki jih je treba sprejeti pri prenosu gradiva drugim osebam, je že bila del meril, ki jih je Evropsko sodišče za človekove pravice oblikovalo v okviru ciljno usmerjenega prestrezanja, in je Evropsko sodišče za človekove pravice ni dodatno opredelilo (glej sodbo v zadevi *Big Brother Watch in drugi proti Združenemu kraljestvu*, točki 335 in 362).

[86] Sodba Evropskega sodišča za človekove pravice z dne 25. maja 2021, *Big Brother Watch in drugi proti Združenemu kraljestvu*, ECLI:CE:ECHR:2021:0525JUD005817013, točka 362.

[87] Glej sodbo Evropskega sodišča za človekove pravice z dne 25. maja 2021, *Centrum för Rättvisa proti Švedski*, ECLI:CE:ECHR:2021:0525JUD003525208, točka 326.

[88] Osnutek sklepa, Priloga I, str. 7.

166. EOVP pozdravlja to določbo, ki ob predpostavki, da je raven varstva podatkov v Republiki Koreji ustrezna za ta namen, zagotavlja kontinuiteto ravni varstva, kot jo v bistvenem zagotavlja zakonodaja Evropske unije za nadaljnje prenose. Komisija je potrdila, da je razumevanje EOVP pravilno, in sicer da se ta oddelek Priloge I uporablja za vse nadaljnje prenose s strani pristojnih organov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Vendar EOVP poudarja, da je treba zagotoviti, da ta predpis v praksi zagotavlja stalno raven varstva, saj lahko obstaja negotovost glede tega, katere pogodbene zaščitne ukrepe in obveznosti ali druge podobne mehanizme je mogoče uporabiti za doseganje take ravni varstva v primeru obdelave za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Glede tega bi bilo treba dodatno navesti, na primer, da se osebni podatki lahko delijo le z ustreznimi pristojnimi organi v tretji državi.

167. Glede na zgoraj zahtevano pojasnilo, ali se osnutek sklepa nanaša na južnokorejsko finančnoobveščevalno enoto, EOVP ugotavlja, da je v uradnem pojasnilu o vladnem dostopu[89] pojasnjeno, da lahko pooblaščena oseba južnokorejske finančnoobveščevalne enote v skladu s členom 8(1) zakona o poročanju in uporabi specifičnih informacij o finančnih transakcijah tujim finančnim obveščevalnim službam zagotovi specifične informacije o finančnih transakcijah, če se to šteje za potrebno za uresničitev namena navedenega zakona[90]. Člen 8 zakona o poročanju in uporabi specifičnih informacij o finančnih transakcijah ne določa obveznosti ugotavljanja, ali tuja država omogoča ustrezne zaščitne ukrepe za varstvo podatkov, in zagotavljanja teh ukrepov. Priloga II se v glede tega ne sklicuje na novi oddelek Priloge I. Zato EOVP Evropsko komisijo poziva, naj pojasni medsebojno povezanost ustreznega oddelka Priloge I o omejitvi nadaljnjih prenosov in pravne podlage za nadaljnje prenose v skladu z zakonom o poročanju in uporabi specifičnih informacij o finančnih transakcijah.

4.6.2. Veljavni pravni okvir za nadaljnje prenose za namene državne varnosti

168. Osnutek sklepa ne vsebuje nobenih informacij o pravnem okviru za nadaljnje prenose na področju državne varnosti. Zato EOVP razume, da se v nasprotju z namenom za preprečevanja, odkrivanja in preiskovanja kaznivih dejanj oddelek 2 Priloge I ne uporablja za nadaljnje prenose za namene državne varnosti. Člena 17 in 18 zakona o varstvu osebnih podatkov, ki sta predmet zadevnega oddelka Priloge I, sta del poglavja III navedenega zakona, ki pa se ne uporablja za obdelavo osebnih podatkov za namene državne varnosti (člen 58(1) navedenega zakona).

169. Vendar EOVP predpostavlja, da Republika Koreja morda mora prenašati osebne podatke tujim obveščevalnim službam za namene državne varnosti in jih tudi dejansko prenaša, na primer zaradi sodelovanja v boju proti čezmejnim grožnjam državni varnosti, za opozarjanje tujih vlad o takih grožnjah ali za njihovo pomoč pri njihovem prepoznavanju.

170. EOVP je razumel, da so po mnenju Evropske komisije nadaljnji prenosi v južnokorejskem pravu zadovoljivo urejeni z zaščitnimi ukrepi, ki izhajajo iz splošnega ustavnega okvira, zlasti z načeloma nujnosti in sorazmernosti ter s temeljnimi načeli varstva podatkov, ki jih ureja zakon o varstvu osebnih podatkov, kot so zakonitost in poštenost obdelave, omejitev namena, najmanjšega obsega podatkov, varnost in splošne obveznosti za preprečevanje zlorabe ter napačne uporabe osebnih podatkov.

171. EOVP potrjuje splošno uporabnost teh ključnih načel (varstva podatkov) in je seznanjen s tem, vendar izraža zaskrbljenost, da so ti zaščitni ukrepi zelo splošni in se v pravni podlagi ne nanašajo specifično

[89] Glej osnutek sklepa, Priloga II.

[90] Glej osnutek sklepa, oddelek 2.2.3.2 Priloge II. Čeprav je taka izmenjava mogoča le, če tuja služba podatkov ne sme uporabiti za druge namene, kot je bil prvotni namen razkritja, zlasti pa ne za kazensko preiskavo ali sojenje (člen 8(2) zakona o poročanju in uporabi specifičnih informacij o finančnih transakcijah), lahko pooblaščena oseba južnokorejske finančnoobveščevalne enote po prejemu zahtevka tuje države ob predhodnem soglasju ministra za pravosodje da privolitev za uporabo takih podatkov za kazensko preiskavo ali sojenje zaradi kaznivih dejanj (člen 8(3) zakona o poročanju in uporabi specifičnih informacij o finančnih transakcijah).

na posebne okoliščine in pogoje za nadaljnje prenose podatkov, prenesenih iz EGP, za namene državne varnosti ali jih ne obravnavajo. Čeprav so ta splošna in krovna načela široko uporabna, se EOVP sprašuje, ali se lahko šteje, da to izpolnjuje merila jasnih in natančnih pravil ter da so zadovoljivo zapisani učinkoviti in izvršljivi zaščitni ukrepi. Zlasti kadar se vladni dostop do osebnih podatkov in njihova obdelava izvajata v tajnosti in so sklepi, ki bi jih bilo mogoče izpeljati iz podatkov, še posebej strogi, so nujna jasna in podrobno opredeljena pravila. V zakonu bi morala biti dovolj jasno navedena obseg morebitne diskrecijske pravice, dodeljene pristojnim organom, in način njenega izvajanja, da se posamezniku zagotovi ustrezno varstvo. Sodišče Evropske unije v sodbi v zadevi *Schrems II* opozarja, da mora pravna podlaga, ki omogoča poseganje v temeljne pravice, za izpolnitev zahtev načel nujnosti in sorazmernosti sama opredeliti obseg omejitve uresničevanja zadevne pravice ter določiti jasna in natančna pravila, ki urejajo področje uporabe in uporabo zadevnega ukrepa, ter uvesti minimalne zaščitne ukrepe[91]. EOVP je zato zaskrbljen, da ne zadostuje, da so taki zaščitni ukrepi na splošno zapisani v zakonodaji višje stopnje, ne da bi bil pojem na primer sorazmernosti izrecno vključen v zadevno pravno podlago.

172. Te pomisleke podpira zgoraj navedena sodba Evropskega sodišča za človekove pravice, v kateri je sodišče ugotovilo, da splošno pravilo brez izrecne zahteve po oceni nujnosti in sorazmernosti ali upoštevanju pomislekov glede zasebnosti ni združljivo s pravico do zasebnosti na podlagi člena 8 Evropske konvencije o človekovih pravicah. Glede tega EOVP ugotavlja, da v pravni podlagi zadevne zadeve (in v pravu Republike Koreje) obstajata krovni (ustavno zagotovljeni) načeli nujnosti in sorazmernosti, na primer v skladu z Listino Evropske unije o temeljnih pravicah in s pristopom k Evropski konvenciji o človekovih pravicah.

173. EOVP Evropsko komisijo poziva, naj pojasni pravno podlago, kako, v kakšnem obsegu in pod katerimi specifičnimi pogoji morajo obveščevalne službe upoštevati pomisleke glede zasebnosti in zaščitnih ukrepov za varstvo podatkov, preden tujim partnerjem razkrijejo osebne podatke za namene državne varnosti. Če taka obveznost izhaja neposredno iz ustavnih načel, naj Evropska komisija dodatno oceni zahteve po natančnosti in jasnosti zadevne zakonodaje ter potrdi, da se splošna ustavna načela in načela varstva podatkov ustrezno uporabljajo in izvajajo.

4.6.3. Mednarodni sporazumi

174. EOVP ugotavlja, da Evropska komisija v okviru svoje ocene ustreznosti ni upoštevala mednarodnih sporazumov, sklenjenih med Republiko Korejo in tretjimi državami ali mednarodnimi organizacijami, ki bi lahko vsebovali specifične določbe za mednarodni prenos osebnih podatkov s strani organov kazenskega pregona in/ali obveščevalnih služb tretjim državam. Meni, da bo sklenitev dvostranskih ali večstranskih sporazumov s tretjimi državami za namene sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali sodelovanja med obveščevalnimi službami verjetno vplivala na pravni okvir Republike Koreje za varstvo podatkov, kot je bil ocenjen.

175. EOVP zato Evropsko komisijo poziva, naj pojasni, ali taki sporazumi obstajajo in pod katerimi pogoji se lahko sklenejo, in oceni, ali lahko določbe mednarodnih sporazumov vplivajo na zagotovljeno raven varstva osebnih podatkov, prenesenih iz EGP v Republiko Korejo na podlagi zakonodajnega okvira in praks v zvezi z razkritji v tujini za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in državne varnosti.

4.7. Nadzor

176. EOVP ugotavlja, da nadzor nad organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter za državno varnost zagotavlja kombinacija različnih notranjih in zunanjih organov.

[91] Glej sodbo v zadevi *Schrems II*, točki 175 in 180.

177. Glede tega je treba opozoriti, da je Sodišče Evropske unije večkrat poudarilo potrebo po neodvisnem nadzoru kot bistvenem elementu varstva fizičnih oseb v zvezi z obdelavo njihovih osebnih podatkov. Pojem neodvisnosti zajema področja institucionalne avtonomije, svobode od navodil in materialne neodvisnosti. Da bi zagotovili dosledno spremljanje in izvajanje zakonodaje o varstvu podatkov, morajo imeti nadzorni organi učinkovita pooblastila, vključno s pooblastili za korektivne ukrepe in za odpravo nepravilnosti.

178. EOVP se strinja z ugotovitvijo Evropske komisije, da se v splošni oceni lahko šteje, da ima Republika Koreja neodvisen in učinkovit nadzorni sistem, čeprav številni organi nadzornega sistema ne izpolnjujejo zgoraj navedenih zahtev. Večina jih na primer nima izvršilnih pooblastil, ampak je omejena zgolj na priporočila, na primer nacionalna komisija za človekove pravice ali svet za revizijo in pregled. Poleg tega večina zadevnih javnih organov niso izključno institucije za varstvo podatkov, ampak so jim običajno zaupane druge naloge na področju varstva temeljnih pravic.

179. V skladu s pojasnili Evropske komisije pa EOVP ugotavlja, da je nadzor organov kazenskega pregona celovito in brez izjeme zagotovljen z zakonom o varstvu osebnih podatkov. Zato ima odbor za varstvo osebnih podatkov preiskovalna pooblastila za odpravo kršitev in izvršilna pooblastila v skladu z zakonom o varstvu osebnih podatkov ter drugimi zakoni o varstvu podatkov (na primer zakon o varstvu zasebnosti v komunikacijah), ki veljajo za celotno področje dostopa organov kazenskega pregona in organov za državno varnost do osebnih podatkov.

180. Glede tega želi EOVP znova poudariti, da morajo imeti nadzorni organi za izvajanje svojih nalog in pooblastil zadostne človeške, tehnične in finančne vire. Glede tega žal ni nobenih informacij o imenovanih nadzornih organih, zlasti o odboru za varstvo osebnih podatkov. Zato EOVP Evropsko komisijo znova poziva, naj o tem zagotovi dodatne informacije.

181. Na splošno želi EOVP opozoriti, da v osnutku sklepa ni skoraj nobenih navedb, primerov ali številk v zvezi z nadzornimi dejavnostmi ter pravnim izvajanjem zakonodaje o varstvu podatkov s strani nadzornih organov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter državne varnosti. Ti podatki bi bili koristni pri proučevanju učinkovitosti nadzornih organov.

1.8. Sodno varstvo in pravna sredstva

182. EOVP opozarja, da je za ustrezno raven varstva podatkov ključno, da so posameznikom, na katere se nanašajo osebni podatki, zagotovljeni celoviti sodno varstvo in pravna sredstva v primeru nepooblaščenega dostopa do podatkov ali njihove obdelave. Ta pravna sredstva morajo biti zadostna, da posamezniku, na katerega se nanašajo osebni podatki, omogočijo dostop do podatkov, shranjenih o njem, in zahtevajo njihov popravek ali izbris.

183. Glede na sodbi Sodišča Evropske unije v zadevah *Schrems I* in *Schrems II* je jasno, da je za domnevo o ustreznosti prava tretje države poleg pravice, da se obrnejo na pristojne organe, poglavitno tudi učinkovito sodno varstvo v smislu člena 47(1) Listine Evropske unije o temeljnih pravicah.

184. EOVP potrjuje, da je Republika Koreja vzpostavila različne možnosti za zagotavljanje pravic posameznikov do dostopa, hrambe, izbrisa in začasnega preklica na podlagi zakona o varstvu osebnih podatkov. Te pravice se lahko uresničujejo pri upravljavcu ali s pritožbo, vloženo pri odboru za varstvo osebnih podatkov ali drugih nadzornih organih, na primer pri nacionalni komisiji za človekove pravice. Poleg tega je EOVP seznanjen z možnostjo izpodbijanja odločitve upravljavcev ali javnih organov v odgovor na njihovo zahtevo na podlagi zakona o upravnem sporu.

185. Poleg tega EOVP iz pojasnil Evropske komisije razume, da lahko posamezniki na podlagi zakona o upravnem sporu in zakona o ustavnem sodišču izpodbijajo ukrepe organov kazenskega pregona in

državne varnosti pred pristojnimi sodišči ter imajo možnost, da pridobijo odškodnino za škodo na podlagi zakona o državni odškodnini[92].

186. V tem okviru pa je EOVP zaskrbljen glede učinkovitega pravnega varstva posameznikov iz Evropske unije v zadevah državne varnosti, v katere ni vpleten južnokorejski državljan. Kot je navedeno v točki 33 in naslednjih, organom za državno varnost ni treba obveščati posameznikov, na katere se nanašajo osebni podatki, o zbiranju in obdelavi njihovih osebnih podatkov. Ker je v teh primerih precej težje doseči učinkovito pravno varstvo, želi EOVP poudariti, da so v tem primeru potrebni nekateri pravni zaščitni ukrepi, če gre za podatke, prenesene iz EGP. Ti zaščitni ukrepi morajo posameznikom, na katere se nanašajo osebni podatki, omogočiti učinkovito ukrepanje proti nezakoniti obdelavi podatkov na pravno varen način, ne da bi jih pri tem ovirale preozke postopkovne zahteve, na primer naložitev dokaznega bremena, ki ga ne morejo izpolniti, če ne vedo za obdelavo. Poleg tega morajo imeti posamezniki, na katere se nanašajo osebni podatki, možnost, da se obrnejo na pristojni organ, ki izpolnjuje zahteve iz člena 47 Listine Evropske unije o temeljnih pravicah, tj. ki je pristojen za ugotavljanje, ali se podatki obdelujejo, za preverjanje zakonitosti obdelave in ima izvršljiva pooblastila za odpravo nepravilnosti, če je obdelava podatkov nezakonita. Glede na to zgolj pravica do pritožbe na primer pri nacionalni komisiji za človekove pravice ne bi zadostovala. EOVP zato Komisijo poziva, naj podrobneje pojasni, kako se te zahteve izvajajo v postopkovnem in vsebinskem smislu, na primer ali se lahko posamezniki, na katere se nanašajo osebni podatki, obrnejo tako na odbor za varstvo osebnih podatkov kot tudi na sodišče, ne da bi jim bilo treba dokazati zadevno obdelavo podatkov.

187. Poleg tega EOVP ugotavlja, da osnutek sklepa predvideva mehanizem za posredovanje pritožb, tj. da lahko posamezniki iz EU vložijo pritožbo pri odboru za varstvo osebnih podatkov prek svojega nacionalnega organa za varstvo podatkov ali EOVP. Odbor za varstvo osebnih podatkov bo nato po isti poti obvestil posameznika, ko bo preiskava končana[93]. EOVP odobrava prizadevanja za lažji dostop do pravnih sredstev zoper južnokorejske organe državne varnosti. Hkrati se zavzema za to, da bi bil tak mehanizem napotitve posredovan prek evropskih nacionalnih organov za varstvo podatkov, ne prek EOVP, saj so ti pristojni in lažje obravnavajo posamezne pritožbe.

188. Poleg tega EOVP ugotavlja morebitno protislovje v zvezi s prostovoljnimi razkritji. Po eni strani osnutek sklepa navaja, da lahko posamezniki v primeru nezakonitega razkritja svojih podatkov na podlagi zahteve za prostovoljno razkritje pridobijo odškodnino, tudi zoper organ kazenskega pregona, ki je izdal zahtevo[94]. Po drugi strani pa se osnutek sklepa sklicuje na zahtevo po neposrednem vplivu glede pravice posameznika, da izpodbija ukrepe javnih organov, pri čemer kot primer, v katerem naj bi upravni ukrep neposredno vplival na pravico do zasebnosti, navaja (samo) zahteve za zavezujoče razkritje[95]. EOVP iz pojasnil Evropske komisije razume, da dejansko ni nobene omejitve možnosti pravnega varstva zoper zahteve za prostovoljno razkritje, zato Evropsko komisijo poziva, naj to v sklepu dodatno pojasni, na področju tako preprečevanja, odkrivanja in preiskovanja kaznivih dejanj kot državne varnosti (v nasprotju z oddelkom o preprečevanju, odkrivanju in preiskovanju kaznivih dejanj oddelek o prostovoljnem razkritju za namene državne varnosti ne vsebuje izrecne izjave o pravnem varstvu v tem kontekstu).

[92] Glej oddelek 3.2.4 Priloge II v povezavi z oddelkom 2.4.3.
[93] Glej uvodno izjavo 205 in Prilogo I, str. 19 osnutka sklepa.
[94] Glej uvodno izjavo 166 osnutka sklepa.
[95] Glej uvodno izjavo 181 (kazenski pregon) ter uvodni izjavi 208 in 181 (državna varnost) osnutka sklepa.