Mnenje 14/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu posameznikov pri obdelavi osebnih podatkov v Združenem kraljestvu

Sprejeto 13. aprila 2021

VSEBINA

Evropski odbor za varstvo podatkov je –

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

ob upoštevanju Sporazuma o Evropskem gospodarskem prostoru (v nadaljevanju: EGP) ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE MNENJE:

1. POVZETEK

1. Evropska komisija je 19. februarja 2021 potrdila svoj osnutek izvedbenega sklepa (v nadaljevanju: osnutek sklepa) o ustreznem varstvu osebnih podatkov v Združenem kraljestvu v skladu s Splošno uredbo o varstvu podatkov [2]. Po tem je začela postopek za njegovo uradno sprejetje.

2. Istega dne je Evropska komisija zaprosila za mnenje Evropskega odbora za varstvo podatkov (v nadaljevanju: EOVP)[3]. Ocena EOVP o ustreznosti ravni varstva, ki se zagotavlja v Združenem kraljestvu, je bila opravljena na podlagi proučitve osnutka sklepa in analize dokumentacije, ki jo je zagotovila Evropska komisija.

3. EOVP se je osredinil na oceno splošnih vidikov Splošne uredbe o varstvu podatkov v osnutku sklepa ter na dostop javnih organov do osebnih podatkov, prenesenih iz EGP za namene kazenskega pregona in državne varnosti, vključno s pravnimi sredstvi, ki so na voljo posameznikom v EGP. EOVP je ocenil tudi, ali so zaščitni ukrepi, navedeni v pravnem okviru Združenega kraljestva, vzpostavljeni in učinkoviti.

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

1.1 Področja zbliževanja

[1] Sklicevanja na „države članice“ v tem mnenju je treba razumeti kot sklicevanja na „države članice EGP“.
[2] Glej sporočilo Evropske komisije za medije, Varstvo podatkov: Evropska komisija začenja postopek glede pretoka osebnih podatkov v Združeno kraljestvo, 19. februar 2021, https://ec.europa.eu/commission/presscorner/detail/sl/ip_21_661.
[3] Glej prejšnjo opombo.
[4] Glej referenčni dokument o ustreznosti, ki ga je pripravila Delovna skupina iz člena 29 in je bil sprejet 28. novembra 2017, kot je bil nazadnje revidiran in sprejet 6. februarja 2018, WP254 rev.01 (ki ga je potrdil EOVP, glej https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines), (v nadaljevanju: referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov).
[5] Glej Priporočila EOVP 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_sl.

5. Ključni cilj EOVP je podati mnenje Evropski komisiji glede ustreznosti ravni varstva, ki se posameznikom zagotavlja v Združenem kraljestvu. Treba je priznati, da EOVP od Združenega kraljestva ne pričakuje, da bo v svojem pravnem okviru posnemalo evropsko zakonodajo o varstvu podatkov.

6. EOVP kljub temu opozarja, da člen 45 Splošne uredbe o varstvu podatkov in sodna praksa Sodišča Evropske unije za zagotovitev ustrezne ravni varstva zahtevata usklajenost zakonodaje tretje države z bistvom temeljnih načel, določenih v Splošni uredbi o varstvu podatkov. Okvir Združenega kraljestva za varstvo podatkov večinoma temelji na okviru EU za varstvo podatkov (zlasti na Splošni uredbi o varstvu podatkov in Direktivi (EU) 2016/680 Evropskega parlamenta in Sveta – v nadaljevanju: direktiva o kazenskem pregonu), kar izhaja iz dejstva, da je bilo Združeno kraljestvo do 31. januarja 2020 država članica EU. Poleg tega Zakon Združenega kraljestva o varstvu podatkov iz leta 2018, ki je začel veljati 23. maja 2018 in s katerim je bil razveljavljen Zakon Združenega kraljestva o varstvu podatkov iz leta 1998, podrobneje določa uporabo Splošne uredbe o varstvu podatkov v pravu Združenega kraljestva, poleg prenosa direktive EU o kazenskem pregonu, ter podeljuje pooblastila in nalaga dolžnosti nacionalnemu nadzornemu organu za varstvo podatkov, uradu informacijskega pooblaščenca Združenega kraljestva. Zato EOVP potrjuje, da je Združeno kraljestvo večino Splošne uredbe o varstvu podatkov preneslo v svoj okvir za varstvo podatkov.

7. **Pri analizi zakonodaje in prakse tretje države, ki je bila do nedavnega država članica EU, je očitno, da je EOVP za številne vidike ugotovil, da so v osnovi enakovredni.**

8. EOVP ugotavlja, da sta okvir Splošne uredbe o varstvu podatkov in pravni okvir Združenega kraljestva na področju varstva podatkov močno usklajena v nekaterih temeljnih določbah, kot so na primer pojmi (denimo „osebni podatki“, „obdelava osebnih podatkov“, „upravljavec podatkov“); razlogi za zakonito in pošteno obdelavo za zakonite namene, omejitev namena, kakovost in sorazmernost podatkov, hramba, varnost in zaupnost podatkov, preglednost, posebne kategorije podatkov, neposredno trženje ter avtomatizirano odločanje in oblikovanje profilov.

1.2 Izzivi

9. Združeno kraljestvo je bilo do nedavnega država članica EU, zato je EOVP pri analizi njene zakonodaje in prakse za številne vidike ugotovil, da so v osnovi enakovredni. Hkrati se je glede na svojo vlogo pri ugotavljanju ustreznosti in zaradi časovne omejitve odločil, da se bo osredinil na tiste vidike, za katere meni, da jih je treba podrobneje proučiti in natančneje pregledati.

10. Kljub temu izzivi ostajajo in EOVP meni, da bi bilo treba naslednje točke dodatno proučiti, da bi se zagotovilo, da se doseže v osnovi enakovredna raven varstva, Evropska komisija pa bi morala to v Združenem kraljestvu pozorno spremljati.

1.2.1 Splošno

11. Prvi, splošni izziv se nanaša na spremljanje razvoja pravnega sistema Združenega kraljestva o varstvu podatkov kot celote. Vlada Združenega kraljestva je dejansko navedla, da namerava pripraviti ločene in neodvisne politike na področju varstva podatkov, pri čemer je možno, da bodo te odstopale od zakonodaje EU o varstvu podatkov. Take politične izjave se v pravnem okviru Združenega kraljestva še niso uresničile. Vendar lahko morebitno prihodnje **odstopanje ustvari tveganja za ohranjanje ravni varstva, zagotovljene za osebne podatke, ki se prenašajo iz EU**. **Zato je Evropska komisija pozvana, naj pozorno spremlja tak razvoj od začetka veljavnosti svojega sklepa o ustreznosti in sprejme potrebne ukrepe, po potrebi tudi s spremembo in/ali odlogom veljavnosti takega sklepa.**

1.2.2 Splošni vidiki varstva podatkov

12. Prvič, tako imenovana **izjema glede priseljevanja** iz odstavka 4 **dela 1 dodatka 2 k Zakonu o varstvu podatkov iz leta 2018, je široko opredeljena**. Natančneje, uporablja se tudi, kadar upravljavec osebnih podatkov ne zbira za namene nadzora nad priseljevanjem, ampak jih da na voljo drugemu upravljavcu, ki take osebne podatke obdela za namene nadzora nad priseljevanjem.

13. EOVP Evropsko komisijo poziva, naj preveri trenutno stanje postopka v zadevi Open Rights Group & Anor, R (On the Application Of) proti Secretary of State for the Home Department & Anor (2019) EWHC 2562 (Admin), in naj, ker ta sodba ni pravnomočna (*res judicata*), preveri, ali je potrjena ali revidirana s sodbo, izdano v pritožbenem postopku, pri čemer se upoštevajo morebitne posodobitve glede tega in se opredelijo v sklepu o ustreznosti. **EOVP Evropsko komisijo poziva še, naj v sklepu o ustreznosti zagotovi dodatne informacije o izjemi glede priseljevanja[6], zlasti glede potrebnosti in sorazmernosti tako široke izjeme v zakonodaji Združenega kraljestva, še posebno ob upoštevanju širokega osebnega področja uporabe.** Hkrati Evropsko komisijo poziva, naj dodatno prouči, ali v pravnem okviru Združenega kraljestva obstajajo dodatni zaščitni ukrepi ali pa bi jih bilo mogoče predvideti, na primer s pravno zavezujočimi instrumenti, ki bi dopolnjevali izjemo glede priseljevanja s povečanjem njene predvidljivosti in zaščitne ukrepe za posameznike, na katere se nanašajo osebni podatki, kar bi omogočalo tudi boljšo in takojšnjo oceno ter spremljanje zahtev glede potrebnosti in sorazmernosti.

14. Drugič, čeprav EOVP potrjuje, da je Združeno kraljestvo večino poglavja V Splošne uredbe o varstvu podatkov preneslo v svoj okvir za varstvo podatkov, je ugotovil, da bi lahko nekateri vidiki pravnega okvira Združenega kraljestva **glede nadaljnjih prenosov podatkov** ogrozili raven varstva osebnih podatkov, ki se prenašajo iz EGP.

15. Dejansko člen 44 Splošne uredbe o varstvu podatkov [7] določa, da se prenosi in nadaljnji prenosi osebnih podatkov izvedejo le, če ni ogrožena raven varstva posameznikov, ki jo zagotavlja Splošna uredba o varstvu podatkov. **To pomeni, da je zakonodaja Združenega kraljestva v osnovi enakovredna zakonodaji EU, kar zadeva obdelavo osebnih podatkov, prenesenih v Združeno kraljestvo na podlagi prihodnjega sklepa o ustreznosti, ter da pravila, ki veljajo v Združenem kraljestvu glede nadaljnjih prenosov takih podatkov v tretje države, zagotavljajo, da se bo še naprej zagotavljala v osnovi enakovredna raven varstva.**

16. Čeprav EOVP ugotavlja, da je Združeno kraljestvo v skladu s svojim pravnim okvirom zmožno za ozemlja priznati, da glede na okvir Združenega kraljestva za varstvo podatkov zagotavljajo ustrezno raven varstva, želi poudariti, da ta ozemlja do danes morda ne bi imela koristi od sklepa o ustreznosti, ki ga je izdala Evropska komisija, in ne bi zagotavljala ravni varstva, ki je v osnovi enakovredna ravni, ki je zagotovljena v EGP. To bi lahko povzročilo morebitna tveganja pri varstvu osebnih podatkov, prenesenih iz EGP, zlasti če bo v prihodnosti okvir Združenega kraljestva za varstvo podatkov odstopal od pravnega reda EU. Poleg tega je Združeno kraljestvo že potrdilo kot ustrezne tretje

[6] Tudi kot rezultat tekočega pregleda uporabe izjeme glede priseljevanja, navedene na strani 5 obrazložitvenega okvira Združenega kraljestva za razprave o ustreznosti, oddelek E3: omejitve iz dodatka 2, 13. marec 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] „Vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, se ob upoštevanju drugih določb te uredbe izvede le, če upravljavec in obdelovalec ravnata v skladu s pogoji iz tega poglavja, kar velja tudi za nadaljnje prenose osebnih podatkov iz tretje države ali mednarodne organizacije v drugo tretjo državo ali drugo mednarodno organizacijo. Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba.“

države, za katere je Evropska komisija v skladu z Direktivo 95/46/ES[8] ugotovila ustreznost, Evropska komisija pa bo te ugotovitve pregledala kmalu in sklepi tega pregleda še niso znani.

17. **Evropska komisija bi morala v zgoraj navedenih primerih izvajati svojo vlogo spremljanja ter če v osnovi enakovredna raven varstva osebnih podatkov, prenesenih iz EGP, ni ohranjena, premisliti o spremembi sklepa o ustreznosti ter uvesti posebne zaščitne ukrepe za podatke, prenesene iz EGP, in/ali zadržati izvajanje sklepa o ustreznosti.**

18. Evropska komisija je **glede mednarodnih sporazumov, sklenjenih med Združenim kraljestvom in tretjimi državami**, pozvana, naj prouči medsebojni vpliv med okvirom Združenega kraljestva za varstvo podatkov in njegovimi mednarodnimi zavezami, ki presega sporazum med Združenim kraljestvom in Združenimi državami Amerike o dostopu do elektronskih podatkov za namene boja proti hudim kaznivim dejanjem[9] (v nadaljevanju: Sporazum Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov), zlasti za zagotovitev neprekinjenosti ravni varstva, kadar se osebni podatki prenesejo iz EU v Združeno kraljestvo na podlagi sklepa o ustreznosti Združenega kraljestva in nato nadalje prenesejo v druge tretje države, ter nenehno spremlja in po potrebi ukrepa, če bi sklepanje mednarodnih sporazumov med Združenim kraljestvom in tretjimi državami lahko ogrozilo raven varstva osebnih podatkov, ki ga zagotavlja EU.

19. Poleg tega je Evropska komisija pozvana, naj spremlja, ali Sporazum Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov zagotavlja ustrezne dodatne zaščitne ukrepe, pri čemer naj upošteva raven občutljivosti zadevnih vrst podatkov in zahteve, da elektronske dokaze prenašajo neposredno ponudniki storitev, ne da se prenašajo med organi, poleg tega naj ugotovi, v katerih okoliščinah bi se lahko zaščitni ukrepi zagotovili z ustreznim izvajanjem prilagojenega krovnega sporazuma med ZDA in EU[10].

20. Poleg tega EOVP ugotavlja, da lahko nadaljnji prenosi potekajo tudi iz Združenega kraljestva v drugo tretjo državo na podlagi **orodij za prenos v skladu z veljavno zakonodajo Združenega kraljestva o varstvu podatkov[11]**. Na podlagi sodbe v zadevi Schrems II[12] Evropsko komisijo poziva, naj v sklepu o ustreznosti poskrbi za zagotovilo, da bodo potrebni zaščitni ukrepi dejansko vzpostavljeni, ob upoštevanju zakonodaje tretje države prejemnice.

21. EOVP glede neobstoja **varstva, ki je zagotovljeno v skladu s členom 48 Splošne uredbe o varstvu podatkov**, v zakonodaji Združenega kraljestva, Evropsko komisijo poziva, naj poskrbi za dodatna zagotovila in specifične sklice na zakonodajo Združenega kraljestva, ki zagotavljajo, da je raven varstva v pravnem okviru Združenega kraljestva v osnovi enakovredna ravni varstva, zagotovljeni v EGP.

22. Glede **postopkovnih mehanizmov in mehanizmov izvrševanja** EOVP ugotavlja, da so obstoj in učinkovito delovanje neodvisnega nadzornega organa, obstoj sistema, ki zagotavlja visoko raven

[8] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23. 11. 1995, str. 31).
[9] Glej Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, ZDA, 3. oktober 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[10] Glej Sporazum med Združenimi državami Amerike in Evropsko unijo o varstvu osebnih podatkov pri preprečevanju, preiskovanju, odkrivanju in pregonu kaznivih dejanj, december 2016 (v nadaljevanju: krovni sporazum med ZDA in EU), https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=LEGISSUM%3A3104_8.
[11] Glej člena 46 in 47 Splošne uredbe Združenega kraljestva o varstvu podatkov.
[12] Glej sodbo v zadevi Schrems II.

skladnosti, in sistem dostopa do ustreznih mehanizmov pravnega varstva, ki posameznikom v EGP zagotavlja sredstvo za uveljavljanje njihovih pravic in pravnega varstva, ne da bi se pri tem srečevali z zapletenimi ovirami za upravno in sodno varstvo, ključni elementi, ki jih mora imeti okvir za varstvo podatkov, ki je skladen z evropskim.

23. EOVP potrjuje, da je Združeno kraljestvo ustrezne določbe Splošne uredbe o varstvu podatkov večinoma preneslo v Splošno uredbo Združenega kraljestva o varstvu podatkov in v Zakon o varstvu podatkov iz leta 2018, kljub temu pa je Evropska komisija pozvana, naj stalno spremlja vse spremembe pravnega okvira Združenega kraljestva in prakse, ki bi lahko privedle do škodljivih vplivov na zadevnih področjih.

1.2.3 O dostopu javnih organov do podatkov, ki se prenašajo v Združeno kraljestvo

24. EOVP opaža precejšnje spremembe v pravnem okviru Združenega kraljestva, ki se uporablja za varnostne in obveščevalne agencije, zlasti glede prestrezanja in pridobivanja komunikacijskih podatkov. Razume, da so te spremembe med drugim odziv na postopke, začete pred Sodiščem EU in Evropskim sodiščem za človekove pravice, ter njune nedavne sodbe v zvezi s tem.

25. EOVP pozdravlja zlasti, da je Združeno kraljestvo ustanovilo sodišče, ki obravnava preiskovalna pooblastila (*Investigatory Powers Tribunal*). To sodišče ni pristojno le za obravnavo zadev o uporabi preiskovalnih pooblastil organov kazenskega pregona, ampak tudi obveščevalnih služb. EOVP zato razume, da sodišče, ki obravnava preiskovalna pooblastila, deluje kot pristojno sodišče v smislu člena 47 Listine Evropske unije o temeljnih pravicah.

26. Poleg tega EOVP z zadovoljstvom ugotavlja, da vključitev pravosodnih pooblaščencev v Zakon o preiskovalnih pooblastilih iz leta 2016 pomeni pomembno izboljšavo. Razume, da je pomembna funkcija pravosodnih pooblaščencev, da v posameznih primerih predhodno odobrijo različne nadzorne ukrepe, vključno s ciljno usmerjenim prestrezanjem in množičnim pridobivanjem komunikacijskih podatkov (tako imenovani postopek z dvojnim varovalom).

27. Vendar meni, da je treba za oceno učinkovitosti te dodatne ravni nadzora dodatno pojasniti scenarije, za katere je mogoče zakonito prestrezanje brez odobritve pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil ali pravosodnih pooblaščencev, ter Evropsko komisijo poziva, naj dodatno oceni in dokaže, da pravni okvir Združenega kraljestva tudi, kadar se ne uporablja postopek z dvojnim varovalom, zagotavlja ustrezne zaščitne ukrepe, tudi z učinkovitim naknadnim nadzorom in možnostmi pravnega varstva, ki so na voljo posameznikom, ter tako zagotavlja raven varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU.

28. Poleg tega EOVP Evropsko komisijo poziva, naj dodatno oceni pogoje, pod katerimi se je mogoče sklicevati na nujnost, in predloži pojasnila o možnostih uveljavljanja pravic za zadevne posameznike, na katere se nanašajo osebni podatki, in možnostih pravnega varstva, ki so jim na voljo v okviru postopkov poseganja v opremo, zlasti v primeru odstopanja od postopka z dvojnim varovalom.

29. EOVP meni še, da je treba dodatno pojasniti in oceniti množično prestrezanje, zlasti glede izbire in uporabe izbirnikov za razjasnitev obsega, v katerem dostop do osebnih podatkov izpolnjuje pragove, ki jih je določilo Sodišče EU, in kateri zaščitni ukrepi so vzpostavljeni za zaščito temeljnih pravic posameznikov, katerih podatki se prestrezajo v tem okviru, tudi v zvezi z obdobji hrambe podatkov. Še posebej koristna bi bila neodvisna ocena, ki bi jo pripravili pristojni nadzorni organi Združenega kraljestva. EOVP poudarja tudi, da se zdi še toliko bolj kritično, da komunikacije, povezane s tujino, ki spadajo v obseg praks množičnega prestrezanja, očitno pomenijo, da bi lahko Združeno kraljestvo neposredno prestrezalo in množično zbiralo podatke v EU, vključno s podatki, ki so v tranzitu med

EU in Združenim kraljestvom, ki bi spadali na področje uporabe osnutka sklepa. Glede na pomen tega vidika EOVP Evropsko komisijo poziva, naj pozorno spremlja razvoj takih dogodkov.

30. EOVP glede množičnega prestrezanja poudarja tudi usklajeno oceno, ki jo pripravita Evropsko sodišče za človekove pravice in Sodišče EU, ter opozarja na pomisleke, izražene v zvezi s sekundarnimi podatki, za katere bi se morali zaradi njihove občutljivosti uporabljati posebni zaščitni ukrepi. EOVP zato Evropsko komisijo poziva, naj natančno oceni, ali zaščitni ukrepi, določeni v zakonodaji Združenega kraljestva za tako vrsto osebnih podatkov, zagotavljajo v osnovi enakovredno raven varstva, kot je zagotovljena v EGP.

31. V tem okviru se EOVP zaveda, da se javno poročilo parlamentarnega odbora za obveščevalno in varnostno dejavnost iz leta 2016 o uporabi pooblastil v večjem obsegu[13] nanaša na prakse iz prejšnjega pravnega okvira, ki je bil pozneje nadomeščen z Zakonom o preiskovalnih pooblastilih iz leta 2016. Vendar meni, da sta potrebna nadaljnja neodvisna ocena in nadzor, kako orodja za avtomatizirano obdelavo podatkov uporabljajo pristojni nadzorni organi Združenega kraljestva, ter Evropsko komisijo poziva, naj dodatno oceni to vprašanje in zaščitne ukrepe, ki se bodo in/ali bi se lahko zagotovili posameznikom v EGP, na katere se nanašajo osebni podatki, v tem okviru.

32. EOVP se strinja z mnenjem pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, da sta potrebna nadaljnji pregled in spremljanje za zagotovitev, da se zaščitni ukrepi, ki jih pristojni organi uporabljajo v praksi na področju državne varnosti in obveščevalne dejavnosti za odpravo neskladnosti z uporabo ustrezne zakonodaje, ohranjajo in se bodo še naprej izboljševali. EOVP pozdravlja tudi, da je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil leta 2019 posledično izvedel pregled svojega pristopa k preiskovanju množičnega prestrezanja, „ki je vključeval natančen pregled tehnično zapletenih načinov, na katere se množično prestrezanje dejansko izvaja“, in se zavezal, da bo v preiskave množičnega prestrezanja od leta 2020 vključil „podrobno preiskavo izbirnikov in iskalnih kriterijev, ki jih je zgoraj navedlo ESČP“. Glede na pomen tega vidika je EOVP zaskrbljen, ker pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil še ni podrobno proučil izbirnikov in iskalnih kriterijev, ter Evropsko komisijo poziva, naj pozorno spremlja razvoj dogodkov v zvezi s tem, zlasti ker je treba konkretno obliko takega nadzora še razjasniti.

33. EOVP poudarja, da glede razkritij v tujini uporaba izjeme zaradi državne varnosti, določene v zakonodaji Združenega kraljestva, lahko privede do neobstoja zaščitnih ukrepov, ki bi zagotavljali, da se bodo spoštovala tudi načela omejitve namena, potrebnosti in sorazmernosti, ter predvidevali, da bodo zadostne pravice posameznikov, nadzor in pravno varstvo zagotovljeni ali se bodo spoštovali tudi v namembni tretji državi. EOVP zato Evropski komisiji priporoča, naj dodatno proučí splošne zaščitne ukrepe, določene v zakonodaji Združenega kraljestva, kar zadeva razkritje v tujini, zlasti glede na uporabo izjem zaradi državne varnosti.

34. Nazadnje, EOVP je zaskrbljen zaradi drugih oblik izmenjave informacij in razkritij, na podlagi drugih instrumentov, zlasti različnih mednarodnih sporazumov, ki jih je Združeno kraljestvo sklenilo z drugimi tretjimi državami, zlasti kadar ti instrumenti ostajajo nedostopni javnosti, kot je sporazum o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA. Učinek takega sporazuma bi lahko privedel do izogibanja zaščitnim ukrepom, opredeljenim v zvezi z dostopom do osebnih podatkov in njihovo uporabo za namene državne varnosti. EOVP meni, da lahko sklenitev dvostranskih in večstranskih sporazumov s tretjimi državami za namene

[13] Glej poročilo o pregledu pooblastil v večjem obsegu, ki ga je pripravil neodvisni pregledovalec zakonodaje o terorizmu, avgust 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

sodelovanja med obveščevalnimi službami, ki bi zagotavljali pravno podlago za neposredno prestrezanje in pridobivanje osebnih podatkov ali prenos osebnih podatkov v te države, pomembno vpliva tudi na pogoje za nadaljnjo uporabo zbranih informacij, ker bodo taki sporazumi verjetno vplivali na pravni okvir Združenega kraljestva za varstvo podatkov, kot je bil ocenjen.

1.3 Sklep

35. EOVP meni, da je ocena ustreznosti Združenega kraljestva edinstvena zaradi prejšnjega statusa Združenega kraljestva kot države članice EU. Poleg tega bi bil to prvi sklep o ustreznosti, ki bi vključeval samoderogacijsko klavzulo.

36. V skladu s tem EOVP potrjuje številna področja zbliževanja med okviroma Združenega kraljestva in EU za varstvo podatkov. Sočasno in po natančni presoji osnutka sklepa Evropske komisije in zakonodaje Združenega kraljestva o varstvu podatkov pa je opredelil številne izzive, ki so temeljito proučeni v tem mnenju. V tem okviru EOVP poudarja poglavitno vlogo Evropske komisije pri spremljanju vseh ustreznih razvojnih dogodkov v Združenem kraljestvu.

37. Glede na zgoraj navedeno Evropski komisiji priporoča, naj obravnava izzive, poudarjene v tem mnenju. EOVP Evropsko komisijo poziva še, naj pozorno spremlja vse ustrezne razvojne dogodke v Združenem kraljestvu, ki bi lahko vplivali na v osnovi enakovredno raven varstva osebnih podatkov, in po potrebi hitro sprejme ustrezne ukrepe.

2. UVOD

2.1 Okvir Združenega kraljestva za varstvo podatkov

38. Okvir Združenega kraljestva za varstvo podatkov pretežno temelji na okviru EU za varstvo podatkov (zlasti na Splošni uredbi o varstvu podatkov in direktivi o kazenskem pregonu), kar izhaja iz dejstva, da je bilo Združeno kraljestvo do 31. januarja 2020 država članica EU. Poleg tega Zakon Združenega kraljestva o varstvu podatkov iz leta 2018, ki je začel veljati 23. maja 2018 in s katerim je bil razveljavljen Zakon Združenega kraljestva o varstvu podatkov iz leta 1998, podrobneje določa uporabo Splošne uredbe o varstvu podatkov v zakonodaji Združenega kraljestva, poleg prenosa direktive EU o kazenskem pregonu, ter podeljuje pooblastila in nalaga dolžnosti nacionalnemu nadzornemu organu za varstvo podatkov, uradu informacijskega pooblaščenca Združenega kraljestva.

39. Kot je navedeno v uvodni izjavi 12 osnutka sklepa Evropske komisije, je vlada Združenega kraljestva leta 2018 sprejela Zakon o izstopu iz Evropske unije, ki v zakonodajo Združenega kraljestva vključuje zakonodajo EU, ki se uporablja neposredno. Ministri Združenega kraljestva so na podlagi tega zakona pooblaščeni, da z akti z zakonsko močjo sprejmejo sekundarno zakonodajo, s katero se ohranjeno pravo EU po izstopu Združenega kraljestva iz EU po potrebi prilagodi nacionalnemu okviru.

40. Zato zadevni pravni okvir, ki se v Združenem kraljestvu uporablja po koncu prehodnega obdobja[14], vključuje:

— Splošno uredbo Združenega kraljestva o varstvu podatkov, kakor je bila vključena v zakonodajo Združenega kraljestva na podlagi Zakona o izstopu iz Evropske unije iz leta 2018, kakor je bil

[14] Prehodno obdobje traja do 31. decembra 2020, po tem datumu pa se zakonodaja EU v Združenem kraljestvu ne uporablja več. „Premostitveno obdobje“ bo trajalo najpozneje do 30. junija 2021 in pomeni dodatno obdobje, v katerem se prenos osebnih podatkov iz EGP v Združeno kraljestvo ne šteje za prenos.

spremenjen z Uredbo o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd.) (izstop iz EU) iz leta 2019;

— Zakon o varstvu podatkov iz leta 2018, kakor je bil spremenjen z Uredbo o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd.) (izstop iz EU) iz leta 2019 in Uredbo o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd.) (izstop iz EU) iz leta 2020, ter

— Zakon o preiskovalnih pooblastilih iz leta 2016

(skupaj v nadaljevanju: okvir Združenega kraljestva za varstvo podatkov).

2.2 Obseg ocene EOVP

41. Osnutek sklepa Evropske komisije je rezultat ocene okvira Združenega kraljestva za varstvo podatkov, ki so ji sledile razprave z vlado Združenega kraljestva. EOVP naj bi v skladu s členom 70(1)(s) Splošne uredbe o varstvu podatkov podal neodvisno mnenje o ugotovitvah Evropske komisije, opredelil morebitne pomanjkljivosti glede ustreznosti in si prizadeval navesti predloge za njihovo odpravo.

42. Kot je navedeno v referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, „bi morale biti informacije, ki jih predloži Evropska komisija, izčrpne, pri čemer Evropskemu odboru za varstvo podatkov omogočijo, da oceni analizo Komisije v zvezi z ravnjo varstva podatkov v tretji državi“[15].

43. Glede tega je treba opozoriti, da je EOVP le delno prejel dokumente, ki so pomembni za pravočasno proučitev pravnega okvira Združenega kraljestva. EOVP je večino zakonodaje Združenega kraljestva, ki je navedena v osnutku sklepa, prejel prek povezav, navedenih v njem. Evropska komisija EOVP ni mogla zagotoviti pisnih pojasnil in zavez Združenega kraljestva o izmenjavah med organi Združenega kraljestva in Evropsko komisijo, pomembnih za to oceno[16].

44. EOVP se je ob upoštevanju zgoraj navedenega in zaradi omejenega časovnega okvira (dva meseca), ki ga ima za sprejetje tega mnenja, odločil osrediniti na nekatere posebne točke, predstavljene v osnutku sklepa, ter glede njih podati svojo analizo in mnenje.

[15] Glej WP254 rev.01, str. 3.

[16] V zvezi s: členom 48 Splošne uredbe o varstvu podatkov (sprotna opomba 78 osnutka sklepa); okrepljenimi zaščitnimi in varnostnimi ukrepi, ki jih upravljavci uporabljajo pri obdelavi v okviru zagotavljanja državne varnosti (sprotna opomba 64 osnutka sklepa); zahtevo, da upravljavec prouči, ali je treba uveljavljati izjemo zaradi državne varnosti za vsak primer posebej, tudi če je bilo izdano potrdilo glede državne varnosti (uvodna izjava 126 in sprotna opomba 172 osnutka sklepa); dejstvom, da se bo zaščita na podlagi krovnega sporazuma med ZDA in EU uporabljala za vse osebne podatke, ki se predložijo ali zavarujejo na podlagi sporazuma Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov, ne glede na naravo ali vrsto organa, ki predloži zahtevo, v zvezi s podrobnostmi konkretnega izvajanja zaščitnih ukrepov za varstvo podatkov, o katerih še potekajo pogovori med Združenim kraljestvom in ZDA, potrditvijo, da bodo organi Združenega kraljestva omogočili začetek veljavnosti sporazuma šele, ko bodo prepričani, da je njegovo izvrševanje skladno s pravnimi obveznostmi v njem, vključno z jasnostjo glede zagotavljanja skladnosti s standardi varstva podatkov glede katerih koli podatkov, ki se zahtevajo na podlagi sporazuma (uvodna izjava 153 osnutka sklepa); primeri, ko se podatki prenašajo iz EU v Združeno kraljestvo v okviru področja uporabe tega osnutka sklepa, in dejstvom, da vedno obstaja „povezava z Britanskim otočjem“, zaradi česar je treba za vsak poseg v opremo, ki se nanaša na take podatke, pridobiti obvezno odredbo v skladu s členom 13(1) Zakona o preiskovalnih pooblastilih iz leta 2016 (uvodna izjava 206 osnutka sklepa), ter primeri navedenih operativnih namenov (uvodna izjava 216 in sprotna opomba 369 osnutka sklepa).

45. Pri analizi zakonodaje in prakse tretje države, ki je bila do nedavnega država članica EU, je očitno, da je EOVP za številne vidike ugotovil, da so v osnovi enakovredni. EOVP se je glede na svojo vlogo pri ugotavljanju ustreznosti ter obsega zakonodaje in prakse, ki ju je treba analizirati, odločil, da se bo osredinil na tiste vidike, za katere je presodil, da jih je treba natančneje pregledati. Poleg tega v skladu s sodno prakso Sodišča EU zelo pomemben del analize zajema pravno ureditev dostopa za potrebe državne varnosti do osebnih podatkov, ki se prenašajo v Združeno kraljestvo, in prakso aparata državne varnosti v Združenem kraljestvu. Vendar je treba upoštevati, da je državna varnost očitno področje prava in prakse, na katerem zakonodaja držav članic ni usklajena na ravni EU in se zato lahko razlikuje.

46. EOVP je upošteval veljavni evropski okvir za varstvo podatkov, vključno s členi 7, 8 in 47 Listine EU o temeljnih pravicah o varstvu pravice do zasebnega in družinskega življenja, pravice do varstva osebnih podatkov in pravice do učinkovitega pravnega sredstva in nepristranskega sodišča ter členom 8 Evropske konvencije o človekovih pravicah o varstvu pravice do zasebnega in družinskega življenja. EOVP je poleg zgoraj navedenega upošteval tudi zahteve Splošne uredbe o varstvu podatkov in ustrezno sodno prakso.

47. Cilj tega pregleda je Evropski komisiji podati mnenje o oceni ustreznosti ravni varstva v Združenem kraljestvu. Pojem „ustrezna raven varstva“, ki je obstajal že v okviru Direktive 95/46/ES, je Sodišče EU nadalje razvilo. Pomembno je opozoriti na standard, ki ga je Sodišče EU določilo v zadevi Schrems I, in sicer da – čeprav mora biti raven varstva v tretji državi v osnovi enakovredna ravni, zagotovljeni v EU – „so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Unije“[17]. Cilj torej ni v celoti prenesti vseh točk evropske zakonodaje, ampak določiti bistvene in temeljne zahteve zakonodaje, ki se pregleduje. Ustreznost se lahko doseže s kombinacijo pravic za posameznike, na katere se nanašajo osebni podatki, in obveznosti za tiste, ki obdelujejo osebne podatke ali izvajajo nadzor nad tako obdelavo, ter nadzora, ki ga izvajajo neodvisni organi. Vendar so predpisi o varstvu podatkov učinkoviti samo, če so izvršljivi in se izvajajo v praksi. Torej ni dovolj obravnavati samo vsebine predpisov, ki se uporabljajo za osebne podatke, prenesene v tretjo državo ali mednarodno organizacijo, ampak je treba proučiti tudi sistem, vzpostavljen za zagotavljanje učinkovitosti takih predpisov. Učinkoviti mehanizmi izvrševanja so zelo pomembni za učinkovitost predpisov o varstvu podatkov[18].

2.3 Splošne pripombe in pomisleki

2.3.1 Mednarodne zaveze, ki jih je sprejelo Združeno kraljestvo

48. Evropska komisija pri ocenjevanju ustreznosti ravni varstva v tretji državi v skladu s členom 45(2)(c) Splošne uredbe o varstvu podatkov in referenčnim dokumentom o ustreznosti v skladu s Splošno uredbo o varstvu podatkov [19] 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, pa tudi izvajanje takih obveznosti. Poleg tega bi bilo treba upoštevati tudi pristop tretje države h Konvenciji Sveta Evrope z dne 28. januarja 1981 o varstvu

[17] Glej zadevo C-362/14, Maximillian Schrems proti Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650 (v nadaljnjem besedilu: Schrems I), točki 73 in 74.
[18] Glej WP254 rev.01, str. 2.
[19] Glej WP254 rev.01, str. 2.

posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljevanju: Konvencija št. 108)[20] in Dodatnemu protokolu h Konvenciji[21].

49. **EOVP glede tega pozdravlja, da je Združeno kraljestvo pristopilo k Evropski konvenciji o človekovih pravicah in je pod pristojnostjo Evropskega sodišča za človekove pravice. Združeno kraljestvo je pristopilo tudi h Konvenciji št. 108 in Dodatnemu protokolu k tej konvenciji, leta 2018 podpisalo Konvencijo št. 108+[22] in trenutno vodi postopek za njeno ratifikacijo.**

2.3.2 Mogoča prihodnja odstopanja okvira Združenega kraljestva za varstvo podatkov

50. Kot je navedeno v uvodni izjavi 281 osnutka sklepa, mora Evropska komisija upoštevati, da bo Združeno kraljestvo ob izteku prehodnega obdobja, določenega v sporazumu o izstopu[23], in takoj po prenehanju uporabe premostitvene določbe iz člena FINPROV.10A sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom[24] uveljavilo, uporabljalo in izvajalo svojo ureditev varstva podatkov, kar lahko vključuje zlasti dopolnitve ali spremembe okvira za varstvo podatkov, ki se ocenjuje v osnutku sklepa, ter drug ustrezen razvoj.

51. Evropska komisija se je zato odločila, da bo v svoj osnutek sklepa vključila samoderogacijsko klavzulo[25], ki določa datum prenehanja veljavnosti štiri leta po začetku njegove veljavnosti.

52. Opozoriti je treba, da bo lahko sekundarna zakonodaja, ki jo bodo lahko pristojni minister Združenega kraljestva in preostali ministri sprejeli po koncu premostitvenega obdobja, v prihodnosti privedla do bistvenega odstopanja okvira Združenega kraljestva za varstvo podatkov od okvira EU za varstvo podatkov.

53. Vlada Združenega kraljestva je dejansko navedla, da namerava razviti ločene in neodvisne politike na področju varstva podatkov z možnostjo odstopanja od zakonodaje EU o varstvu podatkov[26]. Ta

[20] Glej Konvencijo o varstvu posameznikov glede na obdelavo osebnih podatkov, Konvencija št. 108, 28. januar 1981.
[21] Glej Dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki se nanaša na nadzorne organe in čezmejni prenos podatkov, na voljo za podpis 8. novembra 2001.
[22] Glej Protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (v nadaljevanju: Konvencija št. 108+), 18. maj 2018.
[23] Glej Sporazum o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo (UL L 29, 31. 1. 2020, str. 7).
[24] Glej Sporazum o trgovini in sodelovanju med Evropsko unijo in Evropsko skupnostjo za atomsko energijo na eni strani ter Združenim kraljestvom Velika Britanija in Severna Irska na drugi strani (UL L 444, 31. 12. 2020, str. 14).
[25] Glej člen 4 osnutka sklepa. Glej tudi uvodno izjavo 282 osnutka sklepa.
[26] Nacionalna strategija Združenega kraljestva za podatke (nazadnje posodobljena 9. decembra 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) kot eno od svojih poslanstev vključuje naslednje: „Zavzemanje za mednarodni pretok podatkov. Čezmejni pretok informacij spodbuja globalne poslovne dejavnosti, dobavne verige in trgovino ter s tem krepi rast po vsem svetu. Ima tudi širšo družbeno vlogo. Prenos osebnih podatkov zagotavlja izplačevanje plač ljudem in jim pomaga, da se od daleč povežejo z ljubljenimi osebami. In, kot je pokazala pandemija covid-19, lahko izmenjava zdravstvenih podatkov pomaga pri pomembnih znanstvenih raziskavah bolezni ter hkrati združuje države pri njihovem odzivanju na globalne izredne zdravstvene razmere. **Po izstopu iz Evropske unije si bo Združeno kraljestvo prizadevalo za koristi, ki jih lahko zagotovijo podatki.** Spodbujali bomo domače dobre prakse in sodelovali z mednarodnimi partnerji, **da bi zagotovili, da podatki niso neustrezno omejeni zaradi nacionalnih meja in razdrobljenih regulativnih ureditev**, tako da se lahko v celoti izkoristijo“ (poudarek dodan).

namera zajema vključitev vidikov osebnih podatkov v trgovinske sporazume[27], tj. prakso, ki pomeni tveganje znižanja ravni varstva osebnih podatkov, ki jo zagotavlja Združeno kraljestvo[28].

54. Nazadnje, ne le, da Združenega kraljestva od konca prehodnega obdobja ne zavezuje več sodna praksa Sodišča EU, temveč bo to morda veljalo tudi za že sprejete sodbe Sodišča EU, ki se štejejo za ohranjeno sodno prakso v pravnem okviru Združenega kraljestva, to pa zlasti zato, ker ima Združeno kraljestvo možnost, da po koncu premostitvenega obdobja spremeni ohranjeno pravo EU, njegovega vrhovnega sodišča pa sodna praksa EU ne zavezuje[29].

55. **EOVP glede na tveganja, povezana z morebitnim odstopanjem okvira Združenega kraljestva za varstvo podatkov od pravnega reda EU po koncu premostitvenega obdobja, pozdravlja odločitev Evropske komisije, da bo v osnutek sklepa vključila samoderogacijsko klavzulo štirih let. Vendar EOVP na tej točki želi poudariti pomen vloge spremljanja, ki jo ima Evropska komisija[30]. Evropska komisija bi namreč morala spremljati ustrezen razvoj dogodkov v Združenem kraljestvu, ki bi lahko vplival na v osnovi enakovredno raven varstva osebnih podatkov, prenesenih na podlagi sklepa o ustreznosti Združenega kraljestva, redno in stalno od začetka njegove veljavnosti. Poleg tega bi morala Evropska komisija ustrezno ukrepati, tako da glede na zadevne okoliščine začasno zadrži, spremeni ali razveljavi sklep o ustreznosti, če ima Evropska komisija po sprejetju sklepa o ustreznosti znake, da ustrezna raven varstva v Združenem kraljestvu ni več zagotovljena.**

56. EOVP si bo po najboljših močeh prizadeval Evropsko komisijo obveščati o vseh pomembnih ukrepih nadzornih organov za varstvo podatkov držav članic, v gospodarstvu ali javnem sektorju, zlasti glede pritožb posameznikov iz EGP, na katere se nanašajo osebni podatki, v zvezi s prenosom osebnih podatkov iz EGP v Združeno kraljestvo.

3. SPLOŠNI VIDIKI VARSTVA PODATKOV

3.1 Vsebinska načela

57. 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 se njegova raven varstva podatkov šteje za v osnovi enakovredno ravni, zagotovljeni v EU. EOVP priznava, da Združeno kraljestvo nima kodificirane ustave, ker ni enotnega dokumenta, ki bi določal njena veljavna temeljna

[27] Prav tam: „Olajševanje čezmejnega pretoka podatkov: **Na globalni ravni si bomo prizadevali za odpravo nepotrebnih ovir za mednarodni pretok podatkov. V naših trgovinskih pogajanjih se bomo dogovorili o ambicioznih določbah o podatkih** in izkoristili naš novi neodvisni sedež v Svetovni trgovinski organizaciji za vplivanje na trgovinske predpise za podatke z namenom njihovega izboljšanja. **Odpravili bomo ovire za mednarodne prenose podatkov**, ki podpirajo rast in inovacije, tudi z razvojem nove zmogljivosti Združenega kraljestva, ki zagotavlja nove in inovativne mehanizme za mednarodne prenose podatkov. Poleg tega bomo sodelovali s partnerji v skupini G20, da bi vzpostavili interoperabilnost med nacionalnimi ureditvami podatkov za zmanjšanje neskladnosti pri prenašanju podatkov med različnimi državami“ (poudarek dodan).

[28] Glej resolucijo Evropskega parlamenta z dne 12. decembra 2017 z naslovom Digitalni trgovinski strategiji naproti (2017/2065(INI)), oddelek V, v kateri je poudarjeno, da „varstvo osebnih podatkov ne sme biti del pogajanj o trgovinskih sporazumih [EU], na voljo na: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf. Glej tudi resolucijo Evropskega parlamenta z dne 25. marca 2021 o poročilu Komisije o oceni izvajanja Splošne uredbe o varstvu podatkov dve leti po začetku uporabe, odstavek 28, v katerem je navedeno: „podpira prakso Komisije, da varstvo podatkov in pretok osebnih podatkov obravnava ločeno od trgovinskih sporazumov“, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_SL.html.

[29] Glej člen 6(3) do (6) Zakona o izstopu iz Evropske unije iz leta 2018.

[30] Glej člen 45(4) Splošne uredbe o varstvu podatkov.

pravila. Vendar sta pravica do spoštovanja zasebnega in družinskega življenja (ter pravica do varstva podatkov kot del te pravice) in pravica do poštenega sojenja[31] vključeni v Zakon o človekovih pravicah iz leta 1998, sodišča Združenega kraljestva pa so priznala ustavno vrednost tega zakona. Dejansko Zakon o človekovih pravicah iz leta 1998 vključuje pravice, vsebovane v Evropski konvenciji o človekovih pravicah [32]. Poleg tega je v Zakonu o človekovih pravicah iz leta 1998 kot zelo pomembno navedeno, da morajo biti vsi ukrepi javnih organov skladni z Evropsko konvencijo o človekovih pravicah [33].

58. Poleg strukturnih in formalističnih razlik med zakonodajo Združenega kraljestva in zakonodajo EU EOVP ugotavlja, da je, kot je mogoče pričakovati, pristop Združenega kraljestva k varstvu podatkov podoben pristopu v EU, kar izhaja iz dejstva, da je bilo Združeno kraljestvo do 31. januarja 2020 država članica EU. Zato so številna vsebinska načela usklajena z načeli Splošne uredbe o varstvu podatkov, tako da zagotavljajo raven varstva, ki je v osnovi enakovredna ravni, ki jo zagotavlja EU. EOVP se je odločil, da ne bo dodatno razvil analize tistih vsebinskih načel, ki so usklajena z zakonodajo EU, in je zadovoljen z analizo, ki jo je izvedla Evropska komisija v svojem osnutku sklepa. Taka vsebinska načela so na primer: pojmi (na primer „osebni podatki“, „obdelava osebnih podatkov“, „upravljavec podatkov“), razlogi za zakonito in pošteno obdelavo za zakonite namene, omejitev namena, kakovost in sorazmernost podatkov, hramba, varnost in zaupnost podatkov, preglednost, posebne kategorije podatkov, neposredno trženje ter avtomatizirano odločanje in oblikovanje profilov. EOVP ugotavlja še, da Splošna uredba Združenega kraljestva o varstvu podatkov in Zakon o varstvu podatkov iz leta 2018 vključujeta vsebinska načela, ki presegajo tisto, kar zahteva referenčni dokument o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, ter odražata načela, vključena v Splošno uredbo o varstvu podatkov, s čimer zvišujeta raven varstva, zagotovljeno v Združenem kraljestvu. Taka vsebinska načela so na primer načela, povezana z obvestili o kršitvi varstva osebnih podatkov, pooblaščeno osebo za varstvo podatkov, ocenami učinka v zvezi z varstvom podatkov ter vgrajenim in privzetim varstvom podatkov.

59. Vendar, kot je navedeno v uvodu, želi EOVP v tem mnenju posebej obravnavati nekatere točke, glede katerih ima pomisleke, in Evropska komisijo prositi za pojasnila.

3.1.1 Pravica do dostopa, popravka, izbrisa in ugovora

60. Tako imenovana „izjema glede priseljevanja“, določena v odstavku 4 **dela 1 dodatka 2 k Zakonu o varstvu podatkov iz leta 2018**, upravljavcem, vključenim v „nadzor priseljevanja“, omogoča, da ne upoštevajo nekaterih pravic posameznikov, na katere se nanašajo osebni podatki, zagotovljenih z Zakonom o varstvu podatkov iz leta 2018, če bi to lahko vplivalo na „vzdrževanje učinkovitega nadzora nad priseljevanjem“ ali na „preiskovanje oziroma odkrivanje dejavnosti, ki lahko ovirajo vzdrževanje učinkovitega nadzora nad priseljevanjem“.

61. Kot je priznala Evropska komisija v osnutku svojega sklepa[34] in kot je navedeno v mnenju Odbora LIBE Evropskega parlamenta o sklenitvi, v imenu EU, Sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom[35], je ta izjema **široko opredeljena**. Nanaša se na naslednje pravice: pravico

[31] Glej člena 6 in 8 Evropske konvencije o človekovih pravicah (dodatek 1 k Zakonu o človekovih pravicah iz leta 1998).
[32] Za več informacij glej uvodne izjave 8 do 10 osnutka sklepa.
[33] Glej člen 6 Zakona o človekovih pravicah iz leta 1998.
[34] Glej uvodne izjave 62 do 65 osnutka sklepa.
[35] O tem za **široko opredelitev** izjeme glede priseljevanja glej mnenje Odbora za državljanske svoboščine, pravosodje in notranje zadeve o sklenitvi, v imenu Unije, Sporazuma o trgovini in sodelovanju med Evropsko unijo in Evropsko skupnostjo za atomsko energijo na eni strani ter Združenim kraljestvom Velika Britanija in

do obveščenosti, pravico do dostopa, pravico do izbrisa, pravico do omejitve obdelave in pravico do ugovora.

62. Poleg tega je treba opozoriti, da se ta izjema uporablja tudi, kadar upravljavec (upravljavec 1) ne zbira osebnih podatkov za namene nadzora nad priseljevanjem, ampak jih da na voljo drugemu upravljavcu (upravljavec 2), ki take osebne podatke obdela za namene nadzora nad priseljevanjem (na primer ministrstvo za notranje zadeve Združenega kraljestva)[36].

63. V zadevi Open Rights Group & Anor, R (On the Application Of) proti Secretary of State for the Home Department & Anor (2019) EWHC 2562 (Admin) (3. oktober 2019) so pritožniki izpodbijali zakonitost izjeme glede priseljevanja z utemeljitvijo, da je v nasprotju s členom 23 Splošne uredbe o varstvu podatkov in ni skladna s pravicami, zagotovljenimi na podlagi členov 7 in 8 Listine EU o temeljnih pravicah v zvezi z zasebnostjo in varstvom osebnih podatkov. Višje sodišče Anglije in Walesa (v nadaljevanju: višje sodišče) je proučilo, ali je izjema glede priseljevanja iz odstavka 4 dela 1 dodatka 2 k Zakonu o varstvu podatkov iz leta 2018 zakonita, in sklenilo, da je izjema zakonita.

64. Višje sodišče je zlasti menilo, da:

— „[…] se izjema glede priseljevanja očitno nanaša na ‚pomemben javni interes' in ‚uresničuje legitimni cilj' […]", točka 30;

— „izjema glede priseljevanja izpolnjuje zahtevo, da mora biti ukrep ‚skladen z zakonodajo'. […]", točka 38;

— „Pomembno je, da se je na izjemo glede priseljevanja mogoče sklicevati le, če in kolikor bi upoštevanje ‚zadevnih določb Splošne uredbe o varstvu podatkov' **verjetno posegalo** v

---

Severna Irska na drugi strani ter Sporazum med Evropsko unijo in Združenim kraljestvom Velika Britanija in Severna Irska v zvezi z varnostnimi postopki za izmenjavo in varovanje tajnih podatkov (2020/0382(NLE)), 5. februar 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, odstavek 10: „v zvezi s tem opozarja na resoluciji Parlamenta iz februarja in junija 2020, pri čemer poudarja **splošno in široko izjemo**, ki velja za obdelavo osebnih podatkov za namene priseljevanja, iz zakona Združenega kraljestva o varstvu podatkov", in odstavek 11: „meni, da je treba **splošno in široko** izjemo, ki velja za obdelavo osebnih podatkov za namene priseljevanja, iz zakona Združenega kraljestva o varstvu podatkov [...], spremeniti, preden se lahko dodeli veljaven sklep o ustreznosti;" (poudarek dodan).

[36] Glej primer v „Vodniku za Splošno uredbo o varstvu podatkov (SUVP)" (Guide to the General Data Protection Regulation (GDPR)) urada informacijskega pooblaščenca z dne 1. januarja 2021, str. 307 (poudarek dodan). „Zasebna organizacija (upravljavec 1) opozori ministrstvo za notranje zadeve (upravljavec 2) na zaposlenega, ki naj bi domnevno predložil lažne listine kot dokazilo svoje identitete in kvalifikacij za pridobitev zaposlitve. Delodajalec predloži ministrstvu za notranje zadeve ustrezne informacije. Pravica posameznika do obveščenosti o tem, da so se njegovi osebni podatki posredovali ministrstvu za notranje zadeve, je omejena, če bi njena uveljavitev verjetno vplivala na preiskavo.

Delodajalec zato ni dolžan obvestiti posameznika, da so se njegovi podatki posredovali ministrstvu za notranje zadeve, **ministrstvo za notranje zadeve** pa posledično ni dolžno posamezniku poslati obvestila o zasebnosti, s katerim bi ga obvestilo, da zdaj obdeluje njegove podatke. Izjema v enakem obsegu velja tudi za upravljavce.

Vendar zaposleni od ministrstva za notranje zadeve zahteva kopijo svojih osebnih podatkov, ki jih ministrstvo zdaj preiskuje. **Ministrstvo za notranje zadeve lahko uveljavlja izjemo** za zadržanje dela njegovih podatkov, če bi lahko razkritje vplivalo na preiskavo. Če zaposleni podobno zahteva od **svojega delodajalca, lahko ta** v enakem obsegu **uveljavlja izjemo**."

Z drugimi besedami, kot je pojasnjeno na strani 300: „V večini primerov je ministrstvo za notranje zadeve, ali eden od njegovih agencij in izvajalcev, upravljavec, ki uveljavlja to izjemo. Vendar je treba opozoriti, da uporaba te izjeme ni omejena samo na ministrstvo za notranje zadeve. Lahko je pomembna tudi za druge upravljavce, kot so delodajalci, univerze in policija, ki sodelujejo z ministrstvom za notranje zadeve pri zadevah, povezanih s priseljevanjem."

vzdrževanje učinkovitega nadzora nad priseljevanjem ali v preiskovanje oziroma odkrivanje dejavnosti, ki lahko ovirajo vzdrževanje učinkovitega nadzora nad priseljevanjem. Besedilo ‚bi verjetno posegalo' se je v okviru Zakona o varstvu podatkov iz leta 1998 (ki ga je nasledil Zakon o varstvu podatkov iz leta 2018) razlagalo kot ‚znatna in pomembna verjetnost poseganja v opredeljene javne interese'. Stopnja tveganja mora biti tolikšna, da je ‚precejšnja verjetnost' poseganja v navedene interese, tudi če tveganje še zdaleč ne dosega standarda, da je poseganje bolj verjetno kot ne […]", točka 39 (poudarek dodan).

65. Opozoriti je treba, da ta sodba, kot je znano EOVP, ni pravnomočna in da je bila zoper njo vložena pritožba.

66. Kot je navedeno v Smernicah EOVP o omejitvah na podlagi člena 23 Splošne uredbe o varstvu podatkov („člen 23 Smernic na podlagi SUVP)"[37] „[…] se, v okviru SUVP, omejitve **določene v zakonodajnem ukrepu**, nanašajo na **omejeno število pravic posameznikov, na katere se nanašajo osebni podatki, in/ali obveznosti upravljavcev**, navedene v členu 23 SUVP, **spoštujejo bistvo** zadevnih temeljnih pravic in svoboščin, so **potreben in sorazmeren ukrep** v demokratični družbi ter ščitijo enega od razlogov iz člena 23(1) SUVP […]"[38].

67. EOVP opozarja tudi, da je v uvodni izjavi 41 Splošne uredbe o varstvu podatkov navedeno, da „[k]adar je v tej uredbi sklicevanje na **pravno podlago ali zakonodajni ukrep**, v ta namen ni nujno potreben zakonodajni akt, ki bi ga sprejel parlament, brez poseganja v zahteve v skladu z ustavnim redom zadevne države članice. Vendar bi morala biti takšna pravna podlaga ali zakonodajni ukrep **jasna in natančna, njena oziroma njegova uporaba pa predvidljiva za osebe, na katere se nanašata**, v skladu s sodno prakso Sodišča Evropske unije […] in Evropskega sodišča za človekove pravice" (poudarek dodan).

68. Čeprav je Evropsko sodišče za človekove pravice navedlo, da „[n]adalje, kar zadeva besedilo ‚določeno z zakonom' in ‚ki jih določa zakon' navedeno v členih 8 do 11 Konvencije, [Evropsko sodišče za človekove pravice] ugotavlja, da izraz ‚zakon' že od nekdaj razume v njegovem ‚vsebinskem' in ne ‚formalnem smislu'; hkrati zajema zapisano pravo', ki vključuje tako besedila nižjega ranga od zakonskih aktov kot tudi predpise, ki jih sprejme strokovno združenje na podlagi pooblastila zakonodajalca v okviru svojega avtonomnega pooblastila za normativno urejanje, ter ‚nezapisano pravo'. ‚Zakon' je treba razumeti tako, da vključuje zapisano besedilo **in ‚pravo, ki ga izoblikujejo' sodišča**"[39], člen 23 Smernic na podlagi Splošne uredbe o varstvu podatkov opozarja, da „[mora] [v]sak **zakonodajni ukrep**, sprejet na podlagi člena 23(1) SUVP, zlasti **izpolnjevati posebne zahteve, določene v členu 23(2) SUVP**. V členu 23(2) SUVP je navedeno, da zakonodajni ukrep, ki nalaga omejitev pravic posameznikov, na katere se nanašajo osebni podatki, in obveznosti upravljavcev, vsebuje, kjer je ustrezno, **posebne določbe o več merilih, opisanih v nadaljevanju**. Praviloma **bi morale biti** vse zahteve, ki so podrobneje opredeljene v nadaljevanju, **vključene v zakonodajni ukrep**, ki nalaga omejitve na podlagi člena 23 SUVP"[40].

---

[37] Glej Smernice EOVP 10/2020 o omejitvah na podlagi člena 23 Splošne uredbe o varstvu podatkov, različica 1.0, sprejete 15. decembra 2020, ki so po javnem posvetovanju trenutno v fazi finalizacije, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-102020-restrictions-under-article-23_sl.

[38] Glej člen 23 Smernic na podlagi Splošne uredbe o varstvu podatkov, odstavek 9, str. 5.

[39] Glej sodbo Evropskega sodišča za človekove pravice z dne 14. septembra 2010 v zadevi Sanoma Uitgevers B.V. proti The Netherlands, EC:ECHR:2010:0914JUD003822403, točka 83 (poudarek dodan).

[40] Glej člen 23 Smernic na podlagi Splošne uredbe o varstvu podatkov, odstavka 45 in 46, str. 11. V členu 52(3) Listine EU o temeljnih pravicah je navedeno, da „[k]olikor ta listina vsebuje pravice, ki ustrezajo pravicam,

69. Glede tega je mogoče ugotoviti, da sama **izjema glede priseljevanja ne določa naslednjih elementov iz člena 23(2) Splošne uredbe o varstvu podatkov**:

— „zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa“ (d);

— „upravljavca ali vrst upravljavcev“ (e)[41];

— „tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki“ (g);

— „pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve“ (h).

70. „Vodnik za Splošno uredbo o varstvu podatkov (SUVP)“ (*Guide to the General Data Protection Regulation (GDPR)*) urada informacijskega pooblaščenca[42], vključno s poglavjem o „izjemi glede priseljevanja“, vsebuje pojasnila o izjemi glede priseljevanja, vendar **ne more** sam po sebi določati zavezujočih pravil, ki bi jo dopolnjevala. Poleg tega je vprašanje „kakovosti zakona“ zlasti pomembno ob upoštevanju pomena omejenih pravic in razširitve izjeme[43].

---

zagotovljenim z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, sta vsebina in obseg teh pravic enaka kot vsebina in obseg pravic, ki ju določa navedena konvencija. Ta določba ne preprečuje širšega varstva po pravu Unije.“ Glede pojma „**predpisano z zakonom**“ iz člena 52(1) Listine EU o temeljnih pravicah bi se morala uporabljati merila, ki jih je oblikovalo Evropsko sodišče za človekove pravice, kot je predlagano v več mnenjih generalnega pravobranilca Sodišča EU, glej na primer mnenja v združenih zadevah C-203/15 in C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, točke 137–154, ter zadevi C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, točke 88–114. Tako se je mogoče sklicevati, med drugim, na sodbo Evropskega sodišča za človekove pravice v zadevi *Weber in Saravia proti Nemčiji*, točka 84: „Sodišče ponavlja, da izraz ‚**določeno z zakonom**‘ v smislu člena 8(2) [Evropske konvencije o človekovih pravicah] zahteva, prvič, da ima sporni ukrep podlago v **nacionalnem pravu**; nanaša se tudi na **kakovost** zadevnega **zakona**, ki mora tako biti dostopen zadevnim osebam, ki morajo biti tudi sposobne predvideti, kakšne bodo njegove posledice zanje, in združljiv s pravno državo“ (poudarek dodan).
Glej tudi uvodno izjavo 41 Splošne uredbe o varstvu podatkov: „[T]akšna pravna podlaga ali zakonodajni ukrep [bi morala biti] jasna in natančna, njena oziroma njegova uporaba pa **predvidljiva za osebe**, na katere se nanašata, v skladu s sodno prakso Sodišča Evropske unije [...] in Evropskega sodišča za človekove pravice.“ (poudarek dodan).

[41] Glej zgoraj navedeno zadevo višjega sodišča, točka 54: „Menim, da pri tem, da je izjema glede priseljevanja na voljo **vsem upravljavcem podatkov**, ki obdelujejo podatke za določen namen, ni nič nezakonitega. Kot poudarjajo obdolženci, bi bila brez odstavkov 4(3)–(4) izjema glede priseljevanja neučinkovita v primerih, ko so podatki pridobljeni od tretjih oseb (kot je lokalni organ ali davčna in carinska uprava) za namene ohranjanja učinkovitega nadzora nad priseljevanjem“ (poudarek dodan), ki tako potrjuje splošno uporabo omejitev.

[42] „Vodnik za Splošno uredbo o varstvu podatkov (SUVP)“ (*Guide to the General Data Protection Regulation (GDPR)*) urada informacijskega pooblaščenca z dne 1. januarja 2021, str. 299–307.

[43] Glej točko 57 zgoraj navedene zadeve višjega sodišča: „G. Knight me je obvestil, da pooblaščenec končuje pripravo smernic o izjemi, vendar da bodo imele smernice ‚zakonski‘ status le v smislu, da so bile izdane v skladu s pooblastili pooblaščenca iz člena 57(1) SUVP. Ne bodo pa imele pravnega statusa v skladu z zakonom o varstvu podatkov iz leta 2018.“
Razlog za uvedbo pravno zavezujočih smernic, ki jih podpira urad informacijskega pooblaščenca, je naveden zlasti v točkah 56–60 sodbe:
„56. Nazadnje, ponavljam trditev pooblaščenca, da brez spremljevalnih zakonsko predpisanih smernic za zagotovitev zaščitnih ukrepov, kar zadeva pomen in uporabo izjeme glede priseljevanja, izjema ne bi pomenila sorazmernega izvajanja člena 23(1) Splošne uredbe o varstvu podatkov. G. Knight meni, da je določba, dopolnjena s takimi smernicami, sorazmerna.
57. G. Knight me je obvestil, da pooblaščenec končuje pripravo smernic, vendar da bodo imele smernice ‚zakonski‘ status le v smislu, da so bile izdane v skladu s pooblastili pooblaščenca iz člena 57(1) Splošne uredbe o varstvu podatkov. Ne bodo pa imele pravnega statusa v skladu z zakonom o varstvu podatkov iz leta 2018. Vem tudi, da je ministrstvo za notranje zadeve pripravilo osnutek smernic za notranje osebje o izjemi glede

71. *A fortiori* „**preskus poseganja**“ ne določa, da zaščitni ukrepi preprečujejo zlorabo ali nezakoniti dostopa ali prenos ali da jih na primer izvaja ministrstvo za notranje zadeve.

72. Glede na vse zgoraj navedeno EOVP pripominja, da so potrebna dodatna pojasnila o uporabi izjeme glede priseljevanja.

73. Poleg tega pripominja, da ne obstaja pravno zavezujoč instrument, ki bi pojasnil izjemo glede priseljevanja z vidika proučitve, ali je v osnovi enakovredna členu 23 Splošne uredbe o varstvu podatkov ter členoma 7 in 8 Listine EU o temeljnih pravicah. Hkrati meni, da mora Evropska komisija dodatno dokazati potrebnost in sorazmernost širokega osebnega področja uporabe izjeme glede priseljevanja s predložitvijo dokazov.

74. **Na koncu EOVP Evropsko komisijo poziva, naj preveri trenutno stanje postopka v zgoraj navedeni zadevi Open Rights Group & Anor, R (On the Application Of) proti Secretary of State for the Home Department & Anor (2019) EWHC 2562 (Admin) in naj, ker ta sodba ni pravnomočna (*res iudicata*), preveri, ali je potrjena ali revidirana s sodbo, izdano v pritožbenem postopku, pri čemer se upoštevajo morebitne posodobitve glede tega in se opredelijo v sklepu o ustreznosti. EOVP tudi Evropsko komisijo poziva, naj predloži dodatne informacije o potrebnosti in sorazmernosti izjeme glede priseljevanja, zlasti ob upoštevanju širokega osebnega področja uporabe.**

---

priseljevanja (glej [22] zgoraj). V praksi imajo smernice, ki jih izda pooblaščenec, vpliv ne glede na njihovo pravno podlago. Vendar pooblaščenec nima pooblastila za izdajo takih ‚zavezujočih' smernic, kot jih je imelo v mislih vrhovno sodišče v zadevi Christian Institute (v točkah [101] in [107]). Zdi se, da bi bila potrebna primarna zakonodaja, če bi se štelo, da morajo obstajati smernice o izjemi glede priseljevanja z enakim statusom, kot ga imajo kodeksi ravnanja, ki so trenutno določeni v členih 121–124 Zakona o varstvu podatkov iz leta 2018.

58. G. Knight v svoji utemeljitvi za zakonsko predpisane smernice trdi, da je okvir, v katerem se bo uporabljala izjema glede priseljevanja, nujno povezan s pomisleki glede potrebnosti in sorazmernosti njenega obstoja in uporabe. Opozarja na dve vprašanji, zlasti v pravnem okviru. Prvič, osebni podatki, za katere se uporablja izjema glede priseljevanja, bodo verjetno sami po sebi vključevali posebno vrsto podatkov v smislu člena 9(1) Splošne uredbe o varstvu podatkov (tj. podatke, „ki razkrivajo rasno ali etnično poreklo“). Taki podatki so opredeljeni v Splošni uredbi o varstvu podatkov, ker zahtevajo višji varstveni ukrep (Mnenje 1/15 [2019] 3 C.M.L.R. 25, točka [141]). Drugič, osnovna predpostavka zakonodaje o varstvu podatkov je, da je pravica posameznikov do dostopa zelo pomembna kot steber omogočanja uveljavljanja drugih pravic, zagotovljenih posameznikom, na katere se nanašajo osebni podatki (glej YS proti Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18, točka [44]).

59. G. Knight je opredelil štiri praktične točke. Prvič, če upravljavci ne pojasnijo posameznikom, na katere se nanašajo osebni podatki, da so uporabili zakonsko določeno izjemo, niti ne predložijo obširnega povzetka razlogov za to, posameznik, na katerega se nanašajo osebni podatki, ne bo vedel, da je bila izjema uporabljena, in je posledično ne bo mogel učinkovito izpodbijati. Drugič, posamezniki, na katere se nanašajo osebni podatki, se bodo zlasti zanašali na to, da upravljavci uporabljajo izjemo preudarno in samo, če je potrebno. Čeprav imajo vsi posamezniki, na katere se nanašajo osebni podatki, pravico, da se pri pooblaščencu pritožijo glede uporabe izjeme ali začnejo postopek pred sodiščem, je verjetno, da ne bodo seznanjeni s svojimi pravicami in ne bodo imeli sredstev za sprejetje pravnih ukrepov, v okoliščinah, v katerih je potrebna takojšnja in natančna uskladitev s pravicami varstva podatkov. Tretjič, posameznik, na katerega se nanašajo osebni podatki, bo kot priseljenec verjetno v ranljivem položaju. Četrtič, to ni abstraktno vprašanje glede na dokaze obdolžencev v zvezi z uporabo izjeme glede priseljevanja (glej [4] zgoraj).

60. G. Knight trdi, da obstaja velika podobnost med sedanjim izzivom za izjemo glede priseljevanja in utemeljitvijo Sodišča v zadevi Christian Institute [2016] UKSC 51. Tako kot v zadevi Christian Institute navaja, da je izjema glede priseljevanja široka, da so v njej uporabljeni neopredeljeni izrazi in nizek prag, da je predmet nadzora, ki ni naveden v določbi, ter da se uporablja za zelo širok nabor okoliščin in pravic. Vendar v nasprotju z zadevo Christian Institute ni javno dostopnih smernic, še manj pa zakonskega statusa, ki bi ga bilo treba upoštevati, o izjemi glede smernic.“

75. **Hkrati Evropsko komisijo poziva, naj dodatno prouči, ali v pravnem okviru Združenega kraljestva obstajajo dodatni zaščitni ukrepi ali pa bi jih bilo mogoče predvideti, na primer s pravno zavezujočimi instrumenti, ki bi dopolnjevali izjemo glede priseljevanja s povečanjem njene predvidljivosti in zaščitne ukrepe za posameznike, na katere se nanašajo osebni podatki, kar bi omogočalo tudi boljšo in takojšnjo oceno ter spremljanje zahtev glede potrebnosti in sorazmernosti.**

3.1.2 Omejitve nadaljnjih prenosov

76. Člen 44 Splošne uredbe o varstvu podatkov določa, da se prenosi in nadaljnji prenosi osebnih podatkov izvedejo le, če ni ogrožena raven varstva posameznikov, ki jo zagotavlja Splošna uredba o varstvu podatkov. Zato je za osebne podatke, ki se prenašajo iz EGP v Združeno kraljestvo na podlagi sklepa o ustreznosti, zagotovljena raven varstva, ki je v osnovi enakovredna ravni, določeni v okviru EU za varstvo podatkov. **To pomeni, da je zakonodaja Združenega kraljestva v osnovi enakovredna zakonodaji EU glede obdelave osebnih podatkov, ki se prenašajo v Združeno kraljestvo na podlagi osnutka sklepa, pa tudi, da pravila, ki veljajo v Združenem kraljestvu glede nadaljnjega prenosa takih podatkov v tretje države, zagotavljajo, da se v osnovi enakovredna raven varstva zagotavlja še naprej.**

77. Zato je pomembno, da je vsak nadaljnji prenos osebnih podatkov iz EGP iz Združenega kraljestva v drugo tretjo državo ustrezno zavarovan z zaščitnimi ukrepi ali se izvede v skladu s pravili o odstopanjih[44], da se zagotovi neprekinjeno varstvo, ki ga zagotavlja zakonodaja EU. **Če takega varstva ni mogoče zagotoviti, se nadaljnji prenosi osebnih podatkov iz EGP ne bi smeli izvajati.**

78. EOVP potrjuje, da je Združeno kraljestvo večino poglavja V Splošne uredbe o varstvu podatkov preneslo v Splošno uredbo Združenega kraljestva o varstvu podatkov (členi 44–49) in Zakon o varstvu podatkov iz leta 2018[45]. **Vendar je opredelil nekatere vidike zakonodajnega okvira Združenega kraljestva glede nadaljnjih prenosov, ki bi lahko ogrozili raven varstva osebnih podatkov, ki se prenašajo iz EGP.**

79. **Prvi izziv**, ki ga je opredelil EOVP, se nanaša na priznanje tretjih držav, mednarodnih organizacij ali ozemelj[46] kot ustreznih prejemnikov s strani Združenega kraljestva v skladu s postopkom, kot je opredeljen v Zakonu o varstvu podatkov iz leta 2018. Dejansko lahko nadaljnji prenosi osebnih podatkov iz EGP potekajo iz Združenega kraljestva v druge tretje države na podlagi prihodnje morebitne uredbe Združenega kraljestva o ustreznosti[47].

80. Natančneje, kot je pojasnjeno v uvodni izjavi 77 osnutka sklepa, lahko pristojni minister Združenega kraljestva po posvetovanju z uradom informacijskega pooblaščenca določi, da tretja država (ali ozemlje oziroma sektor znotraj tretje države), mednarodna organizacija ali opis take države, ozemlja, sektorja ali organizacije zagotavlja ustrezno raven varstva osebnih podatkov[48]. Pri presoji ustreznosti ravni varstva mora pristojni minister Združenega kraljestva upoštevati enake elemente, kot jih mora Evropska komisija proučiti na podlagi člena 45(2)(a) do (c) Splošne uredbe o varstvu podatkov, ki se

[44] Glej člen 49 Splošne uredbe Združenega kraljestva o varstvu podatkov.
[45] Glej člene 17A, 17B, 17C in 18 Zakona o varstvu podatkov iz leta 2018.
[46] Glej člen 17A Zakona o varstvu podatkov iz leta 2018.
[47] Ekvivalent Združenega kraljestva sklepa o ustreznosti na podlagi Splošne uredbe o varstvu podatkov.
[48] Glej člen 182(2) Zakona o varstvu podatkov iz leta 2018. Glej tudi memorandum o soglasju o vlogi urada informacijskega pooblaščenca pri novih ocenah ustreznosti Združenega kraljestva, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

razlaga v povezavi z njeno uvodno izjavo 104 in ohranjeno sodno prakso EU. To pomeni, da je pri presoji ustrezne ravni varstva v tretji državi zadevni standard ta, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, ki se zagotavlja v Združenem kraljestvu. Čeprav EOVP ugotavlja, da je Združeno kraljestvo v skladu s Splošno uredbo Združenega kraljestva o varstvu podatkov zmožno za ozemlja priznati, da glede na okvir Združenega kraljestva za varstvo podatkov zagotavljajo ustrezno raven varstva, želi poudariti, da zadnje navedena ozemlja do danes morda ne bi imela koristi od sklepa o ustreznosti, ki ga je izdala Evropska komisija in ki priznava raven varstva, ki je v osnovi enakovredna ravni, ki jo zagotavlja EU. To bi lahko povzročilo morebitna tveganja pri varstvu osebnih podatkov, prenesenih iz EGP, zlasti če bo v prihodnosti okvir Združenega kraljestva za varstvo podatkov odstopal od pravnega reda EU. Opozoriti je treba, da je julija 2020 Sodišče EU v prelomni zadevi Schrems II[49] odločilo, da sklep o zasebnostnem ščitu ni veljaven, saj po mnenju Sodišča EU za pravni okvir ZDA ni mogoče šteti, da zagotavlja raven varstva, ki je v osnovi enakovredna ravni varstva, ki se zagotavlja v EU. Vendar pa za Združeno kraljestvo že sprejete sodbe Sodišča EU, ki veljajo za ohranjeno sodno prakso v pravnem okviru Združenega kraljestva, morda ne bodo več zavezujoče, to pa zlasti zato, ker ima Združeno kraljestvo možnost, da po koncu premostitvenega obdobja spreminja ohranjeno pravo EU, njegovega vrhovnega sodišča pa ohranjena sodna praksa EU ne zavezuje[50].

81. **EOVP Evropsko komisijo poziva, naj pozorno spremlja postopek ocenjevanja ustreznosti in merila organov Združenega kraljestva glede drugih tretjih držav, zlasti glede tretjih držav, ki jih EU v skladu s Splošno uredbo o varstvu podatkov ne priznava kot ustrezne. Če Evropska komisija ugotovi, da tretja država, ki jo je Združeno kraljestvo prepoznalo kot ustrezno, ne zagotavlja ravni varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU, EOVP pozove Evropsko komisijo, naj sprejme kakršne koli in vse potrebne korake, kot je na primer sprememba sklepa o ustreznosti Združenega kraljestva za uvedbo posebnih zaščitnih ukrepov za osebne podatke, ki izvirajo iz EGP, in/ali razmislek o začasnem zadržanju izvajanja sklepa o ustreznosti Združenega kraljestva, kadar se osebni podatki, preneseni iz EGP v Združeno kraljestvo, nadalje prenašajo v zadevno tretjo državo na podlagi uredbe o ustreznosti Združenega kraljestva.**

82. **Drugi izziv** se nanaša na prihodnji pregled že obstoječih sklepov o ustreznosti, ki jih je Evropska komisija izdala v skladu z Direktivo 95/46/ES. Po tem pregledu lahko Evropska komisija odloči, da nekatere države, ki so imele do zdaj koristi od sklepa o ustreznosti, ne zagotavljajo več v osnovi enakovredne ravni varstva ob upoštevanju veljavne zakonodaje EU in nedavne sodne prakse. Vendar, kot je določeno v četrtem odstavku dodatka 21 k Zakonu o varstvu podatkov iz leta 2018, je Združeno kraljestvo že priznalo zadevne države kot države, ki zagotavljajo ustrezno raven varstva. Čeprav mora pristojni minister Združenega kraljestva v štirih letih izvesti pregled teh ugotovitev o ustreznosti, Evropska komisija v svojem osnutku sklepa ugotavlja, da te ugotovitve o ustreznosti ne bodo samodejno prenehale obstajati, če pristojni minister Združenega kraljestva ne bo izvedel zahtevanega pregleda v določenem štiriletnem obdobju[51].

83. **EOVP Evropsko komisijo poziva, naj po končanem pregledu že obstoječih sklepov o ustreznosti, izvedenem v EU, spremlja, ali Združeno kraljestvo državo, za katero se šteje, da ne zagotavlja več ustrezne ravni varstva, še vedno obravnava kot tako. Če je tako, EOVP Evropsko komisijo poziva, naj na podlagi uvodnih izjav 277–280 osnutka sklepa sprejme ustrezne ukrepe za izboljšanje razmer, na primer s spremembo sklepa o ustreznosti, da se dodajo posebne zahteve za osebne**

[49] Glej sodbo v zadevi Schrems II.
[50] Glej člen 6(3) do (6) Zakona o izstopu iz Evropske unije iz leta 2018.
[51] Glej uvodno izjavo 82 osnutka sklepa.

podatke, ki izvirajo iz EGP, in/ali zadržanjem sklepa o ustreznosti, če so osebni podatki, ki se prenašajo iz EGP v Združeno kraljestvo, predmet nadaljnjih prenosov v zadevne tretje države. EOVP Evropsko komisijo poziva, naj še naprej izvaja spremljanje ves čas trajanja sklepa Združenega kraljestva o ustreznosti.

84. **Tretji izziv** se nanaša na nadaljnji prenos osebnih podatkov iz EGP v neustrezne države na podlagi orodij za prenos, določenih v členih 46 in 47 Splošne uredbe Združenega kraljestva o varstvu podatkov. Čeprav Splošna uredba Združenega kraljestva o varstvu podatkov določa enaka orodja za prenos, kot so določena v Splošni uredbi o varstvu podatkov, EOVP poudarja, da je treba zagotoviti, da zaščitni ukrepi, ki jih vključujejo, zagotavljajo učinkovito varstvo v tretji državi, zlasti ob upoštevanju sodbe v zadevi Schrems II.

85. EOVP je v skladu s sodbo v zadevi Schrems II, v kateri je Sodišče EU opozorilo, da se mora za osebne podatke, ne glede na to, kam se prenesejo, zagotoviti enakovredno varstvo, že sprejel prvotna priporočila o dopolnilnih ukrepih[52], da bi pomagal izvoznikom, kjer je to potrebno, pri zagotavljanju, da je posameznikom, na katere se nanašajo osebni podatki, zagotovljena raven varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU.

86. Po mnenju Sodišča EU so izvozniki podatkov odgovorni za preverjanje, za vsak primer posebej in, kjer je to ustrezno, v sodelovanju z uvoznikom podatkov v tretji državi, ali zakonodaja ali praksa tretje države vpliva na učinkovitost ustreznih zaščitnih ukrepov, vsebovanih v orodjih za prenos iz člena 46 Splošne uredbe o varstvu podatkov [53]. Če vpliva, bi morali izvozniki podatkov izvesti dopolnilne ukrepe za zapolnitev teh vrzeli v varstvu in varstvo povzdigniti na raven, ki jo zahteva zakonodaja EU.

87. **EOVP Evropsko komisijo poziva, naj za zagotovitev neprekinjenega varstva v osnutek sklepa vključi zagotovila, da če izvozniki podatkov v Združenem kraljestvu za nadaljnje prenose podatkov, prenesenih iz EGP, v druge tretje države uporabljajo orodja za prenos iz členov 46 in 47 Splošne uredbe o varstvu podatkov Združenega kraljestva, ti izvozniki podatkov za vsak primer posebej ocenijo okvir zadevne tretje države za varstvo podatkov in po potrebi sprejmejo ustrezne ukrepe za zagotovitev učinkovitega spoštovanja zaščitnih ukrepov, vsebovanih v izbranem orodju za prenos, da zagotovijo raven varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU. EOVP poudarja, da brez teh zagotovil obstaja tveganje, da bo raven varstva, ki je v osnovi enakovredna ravni, zagotovljeni v EU, ogrožena zaradi nadaljnjih prenosov iz Združenega kraljestva.**

88. **Četrti izziv** glede nadaljnjih prenosov se nanaša na mednarodne sporazume, ki jih je Združeno kraljestvo sklenilo ali jih bo sklenilo v prihodnosti, in morebitni neposredni dostop organov tretjih držav, ki so pogodbenice takih sporazumov, do osebnih podatkov iz EGP. Dejansko ima EOVP velike pomisleke glede že sklenjenega sporazuma Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov, pri čemer Evropska komisija priznava ta izziv in poudarja, da bi „morebiten začetek veljavnosti sporazuma lahko vplival na raven varstva, ki se ocenjuje s tem sklepom“[54]. Dejansko bi na podlagi tega sporazuma po začetku njegove veljavnosti za osebne podatke, ki se prenašajo iz EGP v Združeno kraljestvo v skladu z osnutkom sklepa, veljale določbe

[52] Glej Priporočila 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos, za zagotovitev skladnosti z ravnjo varstva osebnih podatkov na ravni EU, sprejeta 10. novembra 2020, ki so po javnem posvetovanju trenutno v fazi finalizacije, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_sl.pdf.

[53] Glej sodbo v zadevi Schrems II, točka 134.

[54] Glej uvodno izjavo 153 osnutka sklepa.

tega sporazuma, ki določajo pogoje za neposredni dostop organov ZDA in vplivajo na okvir Združenega kraljestva za varstvo podatkov, vključno z določbami o nadaljnjem prenosu. Posledično bi lahko določbe sporazuma, sklenjenega z ZDA, znatno vplivale na raven varstva, zagotovljeno za podatke, prenesene iz EGP, ki bi lahko vplivala na raven varstva takih podatkov. EOVP glede tega ugotavlja, da se Evropska komisija sklicuje na pojasnila organov Združenega kraljestva iz uvodne izjave 153 svojega osnutka sklepa, ne da bi navedla ali predložila kakršno koli konkretno zagotovilo ali zavezo in ne da bi opozorila na posebne pravne določbe zakonodaje Združenega kraljestva za priznanje takih pojasnil.

89. EOVP je predhodno izrazil te pomisleke v dopisu, naslovljenem na Evropski parlament, z dne 15. junija 2020[55]. EOVP je poudaril, da ima na podlagi „pravnega reda EU na področju varstva podatkov ter zlasti SUVP in direktive o kazenskem pregonu“ pomisleke glede tega, ali bi se zaščitni ukrepi iz sporazuma o dostopu do osebnih podatkov v Združenem kraljestvu uporabljali v nekaterih okoliščinah, ki zahtevajo obveznosti razkritja za ZDA, in glede tega, ali so ti zaščitni ukrepi glede na standarde EU zadostni, da raven varstva osebnih podatkov, zagotovljena v EU, ni ogrožena.

90. Poleg tega lahko določbe Sporazuma Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov znatno vplivajo na vsebinske in postopkovne pogoje, pod katerimi lahko organi ZDA neposredno dostopajo do osebnih podatkov, ki jih hranijo upravljavci ali obdelovalci v Združenem kraljestvu, kar vpliva na raven varstva, ki jo zagotavlja zakonodaja Združenega kraljestva. Za zagotovitev ravni varstva, ki je v osnovi enakovredna ravni, zagotovljeni na podlagi zakonodaje EU, je na primer „bistveno, da zaščitni ukrepi v skladu s takim sporazumom vključujejo obvezno predhodno sodno odobritev kot temeljno jamstvo za dostop do metapodatkov in podatkov o vsebini. EOVP na podlagi svoje predhodne ocene, kljub ugotovitvi, da se sporazum nanaša na uporabo nacionalne zakonodaje, v sporazumu, sklenjenim med Združenim kraljestvom in ZDA, ni našel tako jasne določbe“[56].

91. Čeprav Evropska komisija poudarja, da bi bili podatki, pridobljeni na podlagi tega sporazuma, zaščiteni enako kot na podlagi posebnih zaščitnih ukrepov iz tako imenovanega „krovnega sporazuma med ZDA in EU“, ima EOVP pomisleke glede tega, ali bi vključitev teh zaščitnih ukrepov v sporazum Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov zgolj s sklicevanjem na smiselno uporabo izpolnila merila glede jasnih, natančnih in dostopnih pravil o dostopu do osebnih podatkov, in ali bi sporazum v zadostni meri vključeval take zaščitne ukrepe, da bi bili učinkoviti in izvedljivi v skladu z zakonodajo Združenega kraljestva.

92. **EOVP zato predlaga, naj Evropska komisija pojasni, kako in na podlagi katerega pravnega instrumenta bi se varstvo, ki bi bilo enakovredno varstvu na podlagi posebnih zaščitnih ukrepov iz krovnega sporazuma med ZDA in EU, lahko uveljavilo in postalo zavezujoče na podlagi prava Združenega kraljestva.**

93. EOVP ugotavlja še, da določbe sporazuma Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov v povezavi z oddelkom 3 Zakona ZDA o pojasnitvi zakonite čezmejne uporabe podatkov[57] odpirajo vprašanja glede dejanske uporabe zaščitnih ukrepov, ki jih

[55] Glej odgovor EOVP poslancema Evropskega parlamenta Sophie in’t Veld in Moritzu Körnerju o sporazumu med ZDA in Združenim kraljestvom na podlagi zakona ZDA o pojasnitvi zakonite čezmejne uporabe podatkov, sprejetega 15. junija 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

[56] Glej zgoraj navedeni dopis EOVP.

[57] Glej Zakon ZDA o pojasnitvi zakonite čezmejne uporabe podatkov, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

sporazum zagotavlja za dostop organov ZDA za kazenski pregon do osebnih podatkov v Združenem kraljestvu, ki jih obdelujejo ponudniki elektronskih komunikacijskih storitev ali storitev oddaljenega računalništva (v nadaljevanju: ponudniki komunikacijskih storitev), ki spadajo v pristojnost ZDA. Dejansko bi bilo treba, če bi za ponudnike komunikacijskih storitev iz Združenega kraljestva veljala zakonodaja ZDA (na primer ker gre za odvisno podjetje ameriške družbe), preveriti, ali bi se morali organi ZDA za pridobitev podatkov zanašati na sporazum Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov. Glede na to, da Evropska komisija poudarja, da „bo posebna pozornost namenjena uporabi in prilagoditvi varstva na podlagi krovnega sporazuma posebnih vrst prenosov, ki so zajeti v sporazumu med Združenim kraljestvom in ZDA“, EOVP poudarja, da na podlagi njegove predhodne ocene ni jasno, ali bi se zaščitni ukrepi iz sporazuma Združenega kraljestva in ZDA o zakonu o pojasnitvi zakonite čezmejne uporabe podatkov, in s tem zaščitni ukrepi, določeni v krovnem sporazumu med ZDA in EU, uporabljali za vse, če sploh, zahteve organov ZDA za dostop do podatkov v Združenem kraljestvu na podlagi Zakona ZDA o pojasnitvi zakonite čezmejne uporabe podatkov.

94. Združeno kraljestvo bo v prihodnosti morda sklenilo tudi druge mednarodne sporazume ali zaveze s tretjimi državami, ki se bodo uporabljali za osebne podatke, ki se prenašajo iz EGP v Združeno kraljestvo na podlagi osnutka sklepa[58]. Ti mednarodni sporazumi lahko, odvisno od njihovih določb in uporabe posebnih zaščitnih klavzul, z vplivanjem na okvir Združenega kraljestva za varstvo podatkov tudi znatno vplivajo na vsebinske in postopkovne pogoje za dostop organov tretjih držav do osebnih podatkov v Združenem kraljestvu. To zlasti velja za osnutek drugega dodatnega protokola h Konvenciji Sveta Evrope o kibernetski kriminaliteti (v nadaljevanju: Budimpeška konvencija), o katerem se trenutno pogajajo pogodbenice te konvencije, med katerimi je več tretjih držav. Dejansko osnutek protokola vsebuje klavzule, ki jih lahko pogodbenice samovoljno uveljavljajo, na primer glede pooblastila, da odobrijo dostop do podatkov o vsebini ali ne. Medtem ko bi vse države članice uveljavljale klavzule v skladu s pravili EU o varstvu podatkov, ni bilo zagotovljenega nobenega jamstva v zvezi z Združenim kraljestvom, ki bi lahko močno odstopalo od ravni varstva, ki bi bila nato zagotovljena v EU. Drug primer zgoraj predstavljenih vprašanj je sporazum med Združenim kraljestvom in Japonsko o celovitem gospodarskem partnerstvu[59] (v nadaljevanju: CEPA), tj. prvi trgovinski sporazum Združenega kraljestva po brexitu, ki je začel veljati 1. januarja 2021[60] in vključuje določbe o osebnih podatkih[61]. EOVP nadalje ugotavlja, da je Združeno kraljestvo 1. februarja 2021 tudi uradno najavilo svojo zahtevo po pridružitvi Celostnemu in naprednemu sporazumu za čezpacifiško partnerstvo, ki vključuje Sporazum za čezpacifiško partnerstvo[62].

[58] Glej oddelek 2.3.3 zgoraj.

[59] Glej Sporazum med Združenim kraljestvom in Japonsko o celovitem gospodarskem partnerstvu [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Glej smernice vlade Združenega kraljestva o trgovinskih sporazumih Združenega kraljestva s tretjimi državami, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] V skladu s petim odstavkom člena 8.80 sporazuma CEPA se pogodbenice zavezujejo, da bodo spodbujale razvoj mehanizmov za spodbujanje združljivosti različnih pravnih pristopov do varstva (osebnih) podatkov. V skladu s členom 8.84 se pogodbenice zavezujejo, da ne bodo prepovedale ali omejile čezmejnega prenosa informacij z elektronskimi sredstvi, vključno z osebnimi informacijami, če je ta dejavnost namenjena opravljanju poslov zajete osebe v smislu sporazuma CEPA.

[62] V skladu z drugim odstavkom člena 14.11 Sporazuma za čezpacifiško partnerstvo vsaka pogodbenica omogoči čezmejni prenos informacij z elektronskimi sredstvi, vključno z osebnimi informacijami, če je dejavnost namenjena opravljanju poslov zajete osebe.

95. EOVP ugotavlja, da razen sporazuma Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov zgoraj navedeni mednarodni sporazumi niso obravnavani v osnutku sklepa.

96. **EOVP Evropsko komisijo poziva, naj:**

- **prouči medsebojni vpliv med okvirom Združenega kraljestva za varstvo podatkov in njegovimi mednarodnimi zavezami, ki presega Sporazum Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov, zlasti za zagotovitev neprekinjenosti ravni varstva v primeru nadaljnjih prenosov osebnih podatkov iz EGP v Združeno kraljestvo na podlagi sklepa Združenega kraljestva o ustreznosti, ter nenehno spremlja in po potrebi ukrepa glede sklepanja drugih mednarodnih sporazumov med Združenim kraljestvom in tretjimi državami, ki bi lahko ogrozili raven varstva osebnih podatkov, ki ga zagotavlja EU;**

- **mu zagotovi pisne zaveze organov Združenega kraljestva in opredeli posebne določbe zakonodaje Združenega kraljestva glede pojasnila, ki se nanaša na možno uporabo in izvajanje Sporazuma Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov, iz uvodne izjave 153 osnutka sklepa;**

- **glede tega spremlja, ali Sporazum Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov poleg zaščitnih ukrepov, ki bi se lahko zagotovili z ustreznim izvajanjem prilagojenega krovnega sporazuma med ZDA in EU, zagotavlja tudi ustrezne dodatne zaščitne ukrepe za upoštevanje ravni občutljivosti vrst zadevnih podatkov in edinstvenih zahtev, da se elektronski dokazi prenašajo neposredno s strani ponudnikov komunikacijskih storitev in ne med organi;**

- **oceni vpliv in morebitna tveganja določb o osebnih podatkih, vsebovanih v mednarodnih sporazumih, ki jih je nedavno sklenilo Združeno kraljestvo, kot je sporazum SEPA.**

97. **Peti izziv**, ki je opredeljen, se nanaša na uporabo odstopanj za prenose osebnih podatkov v tretje države. Čeprav so razpoložljiva odstopanja na podlagi Splošne uredbe Združenega kraljestva o varstvu podatkov enaka tistim, ki so zagotovljena na podlagi Splošne uredbe o varstvu podatkov, je pomembno, da urad informacijskega pooblaščenca uporablja in bo še naprej uporabljal razlago glede uporabe teh odstopanj, ki je usklajena z razlago EOVP. V nasprotnem primeru ali če bo Združeno kraljestvo v prihodnosti odstopalo od te razlage, bi bila raven varstva podatkov, ki se prenašajo iz EGP v tretje države prek Združenega kraljestva, lahko ogrožena.

98. **EOVP Evropsko komisijo poziva, naj v okviru svoje naloge spremljanja posebej preveri, ali je razlaga Združenega kraljestva glede uporabe odstopanj še vedno usklajena z razlago EU. Če pa Združeno kraljestvo uporablja drugačno razlago uporabe odstopanj, ki ogroža raven varstva, je bistveno, da Evropska komisija sprejme potrebne ukrepe s spremembo sklepa o ustreznosti, da zagotovi, da raven varstva, zagotovljena za osebne podatke, ki se prenašajo iz EGP v Združeno kraljestvo, ne bo ogrožena, kadar se bodo ti podatki nadalje prenašali iz Združenega kraljestva v tretje države na podlagi drugačne razlage odstopanj.**

99. **Šesti izziv**, ki je zadnji v tem oddelku, se nanaša na neobstoj varstva, ki je zagotovljeno v skladu s členom 48 Splošne uredbe o varstvu podatkov, v okviru Združenega kraljestva za varstvo podatkov.

100. Evropska komisija v svojem osnutku sklepa dejansko pojasnjuje, da lahko prenos zaradi neobstoja predpisov o ustreznosti ali ustreznih zaščitnih ukrepov poteka le na podlagi odstopanj, opredeljenih v členu 49 Splošne uredbe Združenega kraljestva o varstvu podatkov, „z izjemo člena 48 Uredbe (EU) 2016/679, ki ga Združeno kraljestvo ni vključilo v splošno uredbo o varstvu podatkov Združenega

kraljestva“[63]. Neobstoj določbe, ki bi bila v osnovi enakovredna členu 48 Splošne uredbe o varstvu podatkov, vključenem v okvir Združenega kraljestva za varstvo podatkov, glede prenosov ali razkritji, na podlagi sodbe sodišča ali odločbe upravnega organa druge tretje države, bi lahko povzročila pravno negotovost glede znatnega vpliva na raven varstva osebnih podatkov, ki se prenašajo iz EGP v Združeno kraljestvo na podlagi osnutka odločbe.

101. EOVP v svojem referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov poudarja, da, kar zadeva nadaljnje prenose, „bi morali biti nadaljnji prenosi osebnih podatkov s strani prvotnega prejemnika prvotnega prenosa podatkov dovoljeni le, kadar tudi za nadaljnjega prejemnika veljajo pravila, ki zagotavljajo ustrezno raven varstva in nadaljnji prejemnik upošteva ustrezna navodila pri obdelavi podatkov v imenu upravljavca podatkov“[64]. Poleg tega EOVP poudarja, da „mora prvotni prejemnik podatkov, prenesenih iz EU, zagotoviti, da so za nadaljnje prenose podatkov zaradi neobstoja sklepa o ustreznosti zagotovljeni ustrezni zaščitni ukrepi. Taki nadaljnji prenosi podatkov bi se morali izvajati le za omejene in točno določene namene ter dokler za takšno obdelavo obstaja pravna podlaga“[65]. V okviru poglavja V Splošne uredbe o varstvu podatkov je treba pri ocenjevanju, ali pravni okvir združenega kraljestva glede tega zagotavlja v osnovi enakovredno raven varstva, v celoti upoštevati člen 48[66].

102. EOVP glede tega poudarja sodno prakso Sodišča EU v zvezi s tveganjem zlorabe ali nezakonitega dostopa do podatkov in njihove nezakonite uporabe, pri čemer zlasti navaja, da „[k]ar zadeva raven varstva temeljnih svoboščin in pravic, zagotovljenega v Uniji, mora predpis Unije, ki pomeni poseg v temeljne pravice, zagotovljene v členih 7 in 8 Listine EU o temeljnih pravicah, v skladu z ustaljeno sodno prakso Sodišča EU določati jasna in natančna pravila, ki urejajo obseg in uporabo ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih podatkov. Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov“[67].

103. EOVP glede tega ugotavlja, da na podlagi informacij, ki so na voljo v osnutku sklepa, v okviru Združenega kraljestva za varstvo podatkov ni jasno določeno, da se katera koli sodba sodišča in odločba upravnega organa tretje države, ki od upravljavca ali obdelovalca zahteva prenos ali razkritje osebnih podatkov, lahko prizna ali izvrši na kateri koli način le, če temelji na veljavnem mednarodnem sporazumu, sklenjenem med tretjo državo prosilko in Združenim kraljestvom. Člen 48 Splošne uredbe o varstvu podatkov je temeljna določba poglavja V Splošne uredbe o varstvu podatkov, saj določa, da se lahko prenos ali razkritje osebnih podatkov na podlagi sodbe ali odločbe sodišča oziroma upravnega organa tretje države prizna ali izvrši le, če temelji na mednarodnem sporazumu, sklenjenem med tretjo državo prosilko in Unijo ali državo članico, brez poseganja v druge razloge za prenos na podlagi tega navedenega poglavja. EOVP dejansko opozarja, da „zahteva tujega organa sama po sebi ni pravna podlaga za prenos. Odredba se lahko prizna le, če temelji na mednarodnem sporazumu, kot je pogodba o medsebojni pravni pomoči, sklenjenem med tretjo državo prosilko in

[63] Glej sprotno opombo 78 osnutka sklepa.
[64] Glej WP254 rev.01, str. 6.
[65] Glej WP254 rev.01, str. 6.
[66] Glej zlasti zadnjo poved člena 44 Splošne uredbe o varstvu podatkov: „Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba.“
[67] Glej sodbo v zadevi Schrems I, točka 91.

Unijo ali državo članico“[68]. Zato je ključno, da se lahko v zakonodaji Združenega kraljestva opredelijo v osnovi enakovredne določbe.

104. Evropska komisija v osnutku sklepa navaja pojasnila organov Združenega kraljestva, v skladu s katerimi na podlagi občega prava ali zakona tuja sodna odločba, s katero se zahtevajo podatki, ni izvršljiva v Združenem kraljestvu brez mednarodnega sporazuma, za vsak prenos podatkov na podlagi zahteve tujega sodišča ali upravnega organa pa je potrebno orodje za prenos, kot so uredba o ustreznosti ali ustrezni zaščitni ukrepi, razen če se uporablja odstopanje iz člena 49 Splošne uredbe Združenega kraljestva o varstvu podatkov. Vendar EOVP niso bile predložene izmenjave med Evropsko komisijo in organi Združenega kraljestva[69] glede tega, zato ne more analizirati in neodvisno oceniti, ali so jamstva, ki so jih zagotovili organi Združenega kraljestva, zadostna za zagotovitev v osnovi enakovredne ravni varstva glede na zaščitne ukrepe iz člena 48 Splošne uredbe o varstvu podatkov.

105. **EOVP Evropsko komisijo poziva, naj predloži dodatna zagotovila in specifične sklice na zakonodajo Združenega kraljestva, ki zagotavljajo, da je raven varstva v pravnem okviru Združenega kraljestva v osnovi enakovredna ravni varstva, zagotovljeni v EGP. Zato Evropsko komisijo poziva, naj predloži pisna pojasnila in zaveze organov Združenega kraljestva glede izvajanja varstva, ki je v osnovi enakovredno varstvu, zagotovljenemu s členom 48 Splošne uredbe o varstvu podatkov.**

106. **EOVP meni, da je opredelitev določb zakonodaje Združenega kraljestva, ki bi zagotavljale v osnovi enakovredno raven varstva glede na zaščitne ukrepe iz člena 48 Splošne uredbe o varstvu podatkov, še toliko pomembnejša ob upoštevanju predhodno izraženih pomislekov glede zahtev organov ZDA ali drugih tretjih držav za dostop do podatkov v Združenem kraljestvu in ob upoštevanju, da se v skladu s sklepom o ustreznosti osebni podatki lahko prenesejo iz EGP v Združeno kraljestvo brez kakršnih koli dodatnih jamstev ali zavezujoče zaveze prejemnika v zvezi z zahtevami organov drugih tretjih držav za dostop do podatkov.**

3.2 Postopkovni mehanizmi in mehanizmi izvrševanja

107. EOVP je na podlagi meril, določenih v referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov, proučil naslednje vidike okvira Združenega kraljestva za varstvo podatkov, kot so zajeti v osnutku sklepa: obstoj in učinkovito delovanje neodvisnega nadzornega organa; obstoj sistema, ki zagotavlja visoko raven skladnosti; in sistem dostopa do ustreznih mehanizmov pravnega varstva, ki posameznikom v EGP zagotavlja sredstvo za uveljavljanje njihovih pravic in pravnega varstva, ne da bi se pri tem srečevali z zapletenimi ovirami za upravno in sodno varstvo.

3.2.1 Pristojni neodvisni nadzorni organ

108. EOVP pozdravlja prizadevanja Evropske komisije za celovito proučitev vzpostavitve, delovanja in pooblastil nadzornega organa Združenega kraljestva iz poglavja 2.6 osnutka sklepa. V Združenem kraljestvu je informacijski pooblaščenec zadolžen za nadzor in uveljavljanje skladnosti s Splošno uredbo Združenega kraljestva o varstvu podatkov in Zakonom o varstvu podatkov iz leta 2018. V skladu z dodatkom 12 k Zakonu o varstvu podatkov iz leta 2018 je informacijski pooblaščenec

[68] Glej prilogo k skupnemu odgovoru EOVP in ENVP za odbor LIBE o vplivu zakona ZDA o pojasnitvi zakonite čezmejne uporabe podatkov na evropski pravni okvir za varstvo osebnih podatkov, sprejet 10. julija 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[69] Glej sprotno opombo 78 osnutka sklepa.

Corporation Sole, tj. ločen enoosebni pravni subjekt, ki ga podpira urad, tj. urad informacijskega pooblaščenca.

109. Glede neodvisnosti informacijskega pooblaščenca EOVP poudarja, da člen 51 Splošne uredbe Združenega kraljestva o varstvu podatkov ne vsebuje izrecnega pojasnila, da je informacijski pooblaščenec javni organ, kot je navedeno v členu 51 Splošne uredbe o varstvu podatkov v zvezi z nadzornimi organi. EOVP kljub temu potrjuje, da Splošna uredba Združenega kraljestva o varstvu podatkov v členu 52 na podoben način odraža ustrezna pravila v zvezi z neodvisnostjo, kot so določena v členu 52(1) do (3) Splošne uredbe o varstvu podatkov.

110. Poleg tega poudarja, da člen 52 Splošne uredbe Združenega kraljestva o varstvu podatkov ne vsebuje obveznosti, ki bi ustrezale členu 52(4) do (6) Splošne uredbe o varstvu podatkov, ki izrecno zagotavlja, da so ustreznemu nadzornemu organu zagotovljena sredstva, potrebna za učinkovito opravljanje njegovih nalog in izvrševanje njegovih pooblastil. Vendar EOVP potrjuje, da Zakon o varstvu podatkov iz leta 2018 vsebuje določbe, ki so namenjene zagotovitvi ustreznega financiranja urada informacijskega pooblaščenca[70], in okoliščino, da je urad informacijskega pooblaščenca trenutno eden največjih nadzornih organov v primerjavi z nadzornimi organi v EU/EGP. Ker je tekoče dodeljevanje ustreznih sredstev, zlasti glede osebja in proračuna[71], nujno za zagotovitev ustreznega delovanja nadzornega organa, da lahko opravlja vse naloge, ki so mu dodeljene, in ga je tudi Evropski parlament nedavno označil za zelo pomembnega[72], EOVP meni, da je treba posebno pozornost nameniti prihodnjim spremembam na tem področju.

111. **Zato EOVP Evropsko komisijo poziva, naj spremlja morebitne spremembe glede dodeljevanja sredstev uradu informacijskega pooblaščenca, ki bi lahko škodile ustreznemu izpolnjevanju nalog urada.**

3.2.2 Obstoj sistema varstva podatkov, ki zagotavlja visoko raven skladnosti

112. V osnutku sklepa je izveden celovit pregled pooblastil, ki jih ima urad informacijskega pooblaščenca na podlagi člena 58 Splošne uredbe Združenega kraljestva varstvu podatkov in Zakona o varstvu podatkov iz leta 2018 za zagotavljanje spremljanja in izvrševanja zakonodaje. EOVP potrjuje, da člen 58 Splošne uredbe Združenega kraljestva o varstvu podatkov natančno odraža ustrezna pravila glede pooblastil nadzornih organov, kot so določena v členu 58 Splošne uredbe o varstvu podatkov. Glede pooblastila za nalaganje upravnih glob glede na okoliščine vsakega posameznega primera člen 83 Splošne uredbe Združenega kraljestva o varstvu podatkov vsebuje podobne določbe in najvišje zneske, kot so določeni v členu 83 Splošne uredbe o varstvu podatkov. Zato EOVP meni, da je pravni okvir Združenega kraljestva na tem področju trenutno skladen s standardi, kot so določeni v ustrezni zakonodaji EU. Kljub temu pa glede tega poudarja, da ima obstoj *učinkovitih* sankcij pomembno vlogo pri zagotavljanju spoštovanja pravil[73].

113. **Glede na zgoraj navedeno EOVP Evropsko komisijo poziva, naj spremlja učinkovitost sankcij in ustreznih pravnih sredstev v okviru Združenega kraljestva za varstvo podatkov.**

[70] Glej člene 137, 138 in 182 ter deveti odstavek dodatka 12 k Zakonu o varstvu podatkov iz leta 2018.
[71] Glej WP254 rev.01, str. 7.
[72] Resolucija Evropskega parlamenta z dne 25. marca 2021 o poročilu Komisije o oceni izvajanja Splošne uredbe o varstvu podatkov dve leti po začetku uporabe, odstavek 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_SL.html.
[73] Glej WP254 rev.01, str. 7.

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

114. Učinkovit mehanizem pravnega varstva, ki omogoča neodvisno preiskavo pritožb za ugotavljanje in kaznovanje kršitev pravic posameznikov, na katere se nanašajo osebni podatki, ter učinkovito upravno in sodno varstvo (vključno z nadomestilom škode zaradi nezakonite obdelave osebnih podatkov posameznika, na katerega se nanašajo osebni podatki) so ključni elementi za oceno, ali sistem varstva podatkov zagotavlja ustrezno raven varstva.

115. EOVP pozdravlja, da urad informacijskega pooblaščenca na svojem spletnem mestu zagotavlja celovite informacije in smernice, ki so namenjene ozaveščanju upravljavcev in obdelovalcev glede njihovih obveznosti in nalog ter podpiranju posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o svojih pravicah s področja varstva osebnih podatkov, in uveljavljanju njihovih pravic na podlagi Splošne uredbe Združenega kraljestva o varstvu podatkov in Zakona o varstvu podatkov iz leta 2018.

116. **Ne glede na trenutno stanje EOVP Evropsko komisijo poziva, naj redno spremlja raven podpore, ki jo urad informacijskega pooblaščenca zagotavlja posebej posameznikom, katerih osebni podatki so bili preneseni v Združeno kraljestvo na podlagi sklepa o ustreznosti, da bi jim pomagal uveljavljati njihove pravice v skladu z ureditvijo varstva podatkov v Združenem kraljestvu.**

4. DOSTOP DO OSEBNIH PODATKOV, PRENESENIH IZ EU, S STRANI JAVNIH ORGANOV V ZDRUŽENEM KRALJESTVU, IN NJIHOVA UPORABA

4.1 Dostop in uporaba s strani javnih organov Združenega kraljestva za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

4.1.1 Pravna podlaga in omejitve/zaščitni ukrepi, ki se uporabljajo

117. Evropska komisija glede ocene, ki jo je izvedla in ki je dokumentirana v uvodni izjavi 132, ter na podlagi osnutka sklepa o **dostopu za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj**, zagotavlja raznolike in podrobne informacije ter načeloma sprejema razumljive sklepe. Zato EOVP v tem mnenju ne povzema dejanske ugotovitve in ocen. Vendar pa v nekaterih primerih opis dejstev ali pojasnilo ugotovitev ne zadošča, da bi ga EOVP sprejel.

4.1.1.1 Uporaba privolitve

118. EOVP ugotavlja, da Evropska komisija v sprotni opombi 184 osnutka sklepa[74] navaja, da **uporaba privolitve** glede ustreznosti ni pomembna, saj v primerih prenosa organ Združenega kraljestva za kazenski pregon podatkov ne zbira neposredno od posameznika, na katerega se nanašajo osebni podatki, na podlagi privolitve. Zato Evropska komisija ne ocenjuje uporabe privolitve kot pravne podlage na področju policijske dejavnosti.

119. EOVP glede tega opozarja, da člen 45(2)(a) ZOVP zahteva ocenjevanje širokega nabora elementov, ki niso omejeni na prenos, kar vključuje „načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno splošno in področno zakonodajo, tudi […] kazensk[o] prav[o]“.

[74] Glej točko 37 osnutka sklepa.

120. Tudi na podlagi informacij, ki jih je Evropska komisija zagotovila v uvodni izjavi 38 svojega osnutka izvedbenega sklepa v skladu z Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta o ustreznem varstvu posameznikov pri obdelavi osebnih podatkov v Združenem kraljestvu (v nadaljevanju: osnutek sklepa o ustreznosti v skladu z direktivo o kazenskem pregonu), ugotavlja, da bo morala uporaba privolitve, kot je oblikovana v ureditvi Združenega kraljestva, v okviru kazenskega pregona vedno temeljiti na pravni podlagi. To pomeni, da tudi če ima policija za namen preiskave zakonska pooblastila za obdelavo podatkov, lahko v nekaterih posebnih okoliščinah (na primer za odvzem vzorca DNK) meni, da je primerno zaprositi za privolitev posameznika, na katerega se nanašajo osebni podatki.

121. **EOVP Evropsko komisijo poziva, naj v sklep o ustreznosti vključi svojo analizo možne uporabe privolitve v okviru kazenskega pregona, določeno v osnutku sklepa o ustreznosti v skladu z direktivo o kazenskem pregonu.**

4.1.1.2 Odredbe o preiskavi in o predložitvi dokazov

122. Čeprav EOVP na splošno nima pripomb glede policijskega pridobivanja dokazov z odredbami o preiskavi in o predložitvi dokazov, iz uvodne izjave 136 osnutka sklepa izhaja, da je Evropska komisija svoje premisleke glede dostopa za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj osredinila na policijo in da je bila obdelava osebnih podatkov s strani drugih organov kazenskega pregona manj proučena.

123. Na primer, v obrazložitvenem okviru Združenega kraljestva za razprave o ustreznosti, oddelek F: kazenski pregon[75], je na strani 11 zapisano, da bi lahko bila **nacionalna agencija za boj proti kriminalu** služba kazenskega pregona posebnega pomena, ki ima med drugim tudi širšo funkcijo kriminalističnega obveščanja. Nacionalna agencija za boj proti kriminalu opisuje svoje poslanstvo kot združevanje obveščevalnih podatkov iz različnih virov, da bi se čim bolj povečale priložnosti za analizo, ocenjevanje in taktične poteze, vključno s podatki iz tehničnega prestrezanja komunikacij, od partnerskih organov kazenskega pregona v Združenem kraljestvu in v tujini ter varnostnih in obveščevalnih agencij[76]. Nacionalna agencija za boj proti kriminalu je tudi ena glavnih sogovornic mednarodnih partnerskih organov kazenskega pregona in ima ključno vlogo pri izmenjavi kriminalistično obveščevalnih podatkov[77].

---

[75] Glej obrazložitveni okvir Združenega kraljestva za razprave o ustreznosti, oddelek F: kazenski pregon, 13. marec 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Glej spletno mesto nacionalne agencije za boj proti kriminalu (National Crime Agency), Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Čeprav niso vsi obveščevalni podatki, ki jih obdeluje nacionalna agencija za boj proti kriminalu, osebni podatki, so lahko precejšen del osebne informacije, tukaj opisane dejavnosti pa se razlikujejo od klasičnega nadzora, tako da ocena dostopa organov kazenskega pregona v Združenem kraljestvu do osebnih podatkov ne bi bila popolna brez temeljite ocene dejavnosti nacionalne agencije za boj proti kriminalu. Zdi se smiselno, da se v vseh zadevnih organih kazenskega pregona zagotovi enak pomen načel varstva podatkov, s čimer se torej izpostavi agencija, ki še posebej temelji na podatkih, kot je nacionalna agencija za boj proti kriminalu. Poleg tega je na spletni strani pod naslovom „Looking to the future“ (Pogled v prihodnost) nadalje pojasnjeno: „Nenehno iščemo nove priložnosti za zbiranje, razvoj in izboljšanje tradicionalnih zmogljivosti za povečanje količine in kakovosti obveščevalnih podatkov, ki so na voljo za uporabo v Združenem kraljestvu in v tujini.“ „V okviru tega na podlagi pooblastil, ki jih agenciji podeljuje Zakon o kriminalu in sodiščih, razvijamo novo nacionalno zmogljivost za uporabo podatkov za povezovanje, dostop in uporabo podatkov, ki jih hrani državna

124. EOVP nadalje upošteva dejstvo, da vladna obveščevalna služba, katere dejavnosti običajno spadajo na področje uporabe dela 4 Zakona o varstvu podatkov iz leta 2018, tj. državna varnost, v tesnem sodelovanju z notranjim ministrstvom, nacionalno agencijo za boj proti kriminalu, davčno in carinsko upravo ter drugimi vladnimi službami prevzema tudi aktivno vlogo pri zmanjševanju družbene in finančne škode, ki jo v Združenem kraljestvu povzročajo huda kazniva dejanja in organizirana kriminaliteta[78]. Njene dejavnosti zajemajo boj proti spolni zlorabi otrok; goljufijam; drugim oblikam gospodarske kriminalitete, vključno s pranjem denarja; kaznivi uporabi tehnologije; kibernetski kriminaliteti; organizirani kriminaliteti na področju nezakonitega priseljevanja, vključno s trgovino z ljudmi, drogami in strelnim orožjem ter drugimi dejavnostmi tihotapljenja.

125. **EOVP Evropsko komisijo poziva, naj svojo analizo dopolni z analizo agencij, dejavnih na področju kazenskega pregona, za katere se zdi, da so se pri svojih vsakodnevnih dejavnostih osredinile predvsem na zbiranje in analiziranje podatkov, vključno z osebnimi podatki, zlasti nacionalne agencije za boj proti kriminalu. Poleg tega EOVP Komisijo poziva, naj podrobneje prouči agencije, kot je vladna obveščevalna služba, katerih dejavnosti spadajo na področje kazenskega pregona in državne varnosti, ter pravni okvir, ki zanje velja pri obdelavi osebnih podatkov.**

4.1.1.3 Preiskovalna pooblastila za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

126. V poglavju 4 referenčnega dokumenta o ustreznosti v skladu s Splošno uredbo o varstvu podatkov „Temeljna jamstva v tretjih **državah za dostop za namene kazenskega pregona** in nacionalne varnosti za omejitev poseganja v temeljne pravice“ EOVP opozarja, da je „v tem okviru sodišče kritično ugotovilo tudi, da prejšnja odločba o varnem pristanu ni vsebovala nobene ugotovitve v zvezi z obstojem, v ZDA, pravil, ki bi jih država sprejela za omejitev poseganja v temeljne pravice oseb, katerih podatki se prenašajo iz Evropske unije v ZDA, **tj. poseganja, v katero bi se državni subjekti zadevne države lahko vmešali za uresničitev legitimnega cilja**, kot je državna varnost‘“[79]. V tem referenčnem dokumentu EOVP navaja, da je **treba za dostop vseh tretjih držav do podatkov**, bodisi za namene državne varnosti bodisi za **namene kazenskega pregona**, **spoštovati štiri evropska temeljna jamstva**[80], **da se šteje za ustreznega**, pri čemer je **treba dokazati** zlasti **potrebnost in sorazmernost glede postavljenih legitimnih ciljev**.

127. V tem oddelku osnutka sklepa je Evropska komisija sklenila (uvodna izjava 139), da „ker so ta preiskovalna pooblastila, določena v Zakonu o preiskovalnih pooblastilih iz leta 2016, enaka tistim, ki so na voljo agencijam za državno varnost, so pogoji, omejitve in zaščitni ukrepi, ki se uporabljajo pri takih pooblastilih, podrobneje obravnavani v oddelku o dostopu do osebnih podatkov in njihovi uporabi s strani javnih organov Združenega kraljestva za namene državne varnosti“. Vendar iz sodne prakse Sodišča EU izhaja, da so pri uporabi preskusa potrebnosti in sorazmernosti za zakonodajo držav članic, ki omogoča hrambo in dostop do osebnih podatkov s strani javnih organov, legitimni cilji, kot je državna varnost ali boj proti hudim kaznivim dejanjem, različni, zaradi česar bi nekdo lahko upravičil posamezno vrsto poseganja, nekdo drug pa je ne bi mogel[81].

---

uprava.“ „S tem se bomo hitreje in prožneje odzivali na nove grožnje, zaradi česar bomo bolj proaktivno zbirali in analizirali informacije in obveščevalne podatke o nastajajočih grožnjah, da bomo lahko ukrepali, preden se grožnje uresničijo.“

[78] Glej spletišče vladne obveščevalne službe, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

[79] Glej WP254 rev.01, str. 9.

[80] Glej Priporočila EOVP 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe.

[81] Glej sodbo Sodišča EU z dne 6. oktobra 2020 v združenih zadevah C-511/18, C-512/18 in C-520/18, La Quadrature du Net in drugi, ECLI:EU:C:2020:791.

128. **EOVP bi zato v okviru sklepa pozdravil posebno oceno potrebnosti in sorazmernosti pogojev, omejitev in zaščitnih ukrepov, opisanih v uvodni izjavi 174 in naslednjih – ki je oddelek, namenjen ukrepom za uresničitev ciljev državne varnosti –, kar zadeva uporabo teh pogojev, omejitev in zaščitnih ukrepov v okviru ukrepa za uresničitev cilja kazenskega pregona. Zato Evropsko komisijo poziva, naj podrobneje pojasni, ali sta opisana hramba osebnih podatkov in dostop do njih za namene kazenskega pregona dovolj omejena, da je zagotovljena raven varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU.**

4.1.2 Nadaljnja uporaba informacij, zbranih za namene kazenskega pregona (uvodne izjave 140–154)

129. EOVP ugotavlja, da okvir Združenega kraljestva za varstvo podatkov glede nadaljnje uporabe informacij, zbranih za namene kazenskega pregona, zagotavlja podobne zaščitne ukrepe in omejitve, kot so določeni v zakonodaji EU.

4.1.2.1 Nadaljnja uporaba za druge namene kazenskega pregona

130. Zakon o varstvu podatkov iz leta 2018 dejansko določa, da se lahko osebni podatki (s strani prvotnega ali drugega upravljavca), ki jih pristojni organ zbere za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, nadalje obdelajo za kateri koli drug namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni drug namen ter če je obdelava potrebna in sorazmerna glede na navedeni namen. Evropska komisija ugotavlja, da se vsi zaščitni ukrepi, navedeni v delu 3 Zakona o varstvu podatkov iz leta 2018, uporabljajo za obdelavo, ki jo izvaja organ prejemnik. Vendar EOVP poudarja, da členi 44(4), 45(4), 48(3) in 68(7) v delu 3 Zakona o varstvu podatkov iz leta 2018 predvidevajo možnost omejitve pravic posameznika, na katerega se nanašajo osebni podatki, člen 79 pa možnost izdaje potrdil, ki potrjujejo, da je omejitev potreben in sorazmeren ukrep za zaščito državne varnosti. **EOVP zato priporoča, naj Evropska komisija dodatno oceni morebitni vpliv takih omejitev na raven varstva osebnih podatkov glede nadaljnje uporabe zbranih informacij. Podobno bi bilo treba zagotoviti dodatna pojasnila glede pravnega okvira Združenega kraljestva, ki omogoča tako nadaljnjo izmenjavo, zlasti Zakona o digitalnem gospodarstvu iz leta 2017 ter Zakona o kriminalu in sodiščih iz leta 2013, ki omogoča izmenjavo informacij z nacionalnim pristojnim organom.**

4.1.2.2 Nadaljnja uporaba za namene, ki niso nameni preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, v Združenem kraljestvu

131. Zakon o varstvu podatkov iz leta 2018 določa še, da se lahko osebni podatki, zbrani za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelujejo za namene, ki ne spadajo na področje preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če tako obdelavo omogoča zakon. V tem primeru je pravna podlaga, ki dovoljuje tako izmenjavo, člen 19 Zakona o boju proti terorizmu iz leta 2008. EOVP glede tega ugotavlja, da Evropska komisija v svoji oceni ni v celoti obravnavala področja uporabe in določb člena 19 Zakona o boju proti terorizmu, ki bi lahko pomenili širšo uporabo, zlasti glede člena 19(2), ki določa, da lahko „informacije, ki jih pridobi katera koli obveščevalna služba v zvezi z izvajanjem katere koli svoje funkcije, […] ta služba uporablja v zvezi z izvajanjem katere koli svoje druge funkcije“.

132. EOVP ugotavlja tudi, da bi bilo sklicevanje Evropske komisije na dejstvo, da so pristojni organi javni organi, ki morajo ravnati v skladu z Evropsko konvencijo o človekovih pravicah, vključno z njenim členom 8, s čimer zagotavljajo, da so vse izmenjave podatkov med organi kazenskega pregona in obveščevalnimi službami skladne z zakonodajo o varstvu podatkov in Evropsko konvencijo o

človekovih pravicah, mogoče dodatno utemeljiti z opredelitvijo ustreznih aktov in zakonov v pravnem redu Združenega kraljestva, v katerih so take omejitve jasno in natančno določene.

4.1.2.3 Nadaljnja uporaba v okviru nadaljnjih prenosov zunaj Združenega kraljestva

133. Evropska komisija se je sklicevala na dejstvo, da bi lahko Sporazum Združenega kraljestva in ZDA o Zakonu o pojasnitvi zakonite čezmejne uporabe podatkov vplival na nadaljnje prenose od ponudnikov komunikacijskih storitev v Združenem kraljestvu v ZDA, EOVP pa poudarja še, da bi lahko začetek veljavnosti tega sporazuma vplival tudi na nadaljnjo uporabo informacij, zbranih z nadaljnjimi prenosi s strani organov kazenskega pregona v Združenem kraljestvu, zlasti glede izdajanja in posredovanja nalogov po členu 5 tega sporazuma.

134. V širšem smislu EOVP meni, da lahko sklenitev prihodnjih dvostranskih sporazumov s tretjimi državami za namene sodelovanja na področju kazenskega pregona, ki bi zagotavljali pravno podlago za prenos osebnih podatkov v te države, znatno vpliva na pogoje za nadaljnjo uporabo zbranih informacij, saj lahko taki sporazumi vplivajo na okvir Združenega kraljestva za varstvo podatkov, kot je bil ocenjen. EOVP torej priporoča, naj Evropska komisija podrobneje oceni to točko, z opredelitvijo obstoja mednarodnih sporazumov, in pojasni, ali bi določbe teh sporazumov lahko vplivale na uporabo zakonodaje Združenega kraljestva o varstvu podatkov, in določi nadaljnje omejitve ali izjeme glede nadaljnje uporabe in razkritja informacij, zbranih za namene kazenskega pregona, v tujini. EOVP meni, da so take informacije in ocene ključne, da se omogoči celovita ocena ravni varstva, ki jo zagotavljajo zakonodajni okvir in prakse Združenega kraljestva v zvezi z razkritjem in nadaljnjo uporabo v tujini.

4.1.3 Nadzor

135. EOVP ugotavlja, da nadzor nad organi kazenskega pregona poleg urada informacijskega pooblaščenca zagotavljajo tudi različni pooblaščenci. V osnutku ugotovitev o ustreznosti so navedeni pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil, pooblaščenec za hrambo in uporabo biometričnih podatkov ter pooblaščenec za uporabo nadzornih kamer. Glede tega je treba opozoriti, da je Sodišče EU že večkrat poudarilo potrebo po neodvisnem nadzoru. Pri vprašanjih dostopa do osebnih podatkov, prenesenih v Združeno kraljestvo, je še posebno pomemben pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil. EOVP razume, da je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil tako imenovani „pravosodni pooblaščenec“ v smislu drugih pravosodnih pooblaščencev, ki bodo navedeni v okviru poglavja o državni varnosti, in da ti pravosodni pooblaščenci uživajo neodvisnost sodnikov tudi pri opravljanju funkcije pooblaščencev. Evropska komisija v uvodni izjavi 245 osnutka sklepa glede urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil pojasnjuje, da ta deluje neodvisno kot samostojni organ, hkrati pa ga financira ministrstvo za notranje zadeve.

136. EOVP v osnutku sklepa ni našel nadaljnjih navedb, na podlagi katerih bi lahko ocenil neodvisnost pooblaščenca za hrambo in uporabo biometričnih podatkov ter pooblaščenca za uporabo nadzornih kamer.

137. **Evropska komisija je pozvana, naj dodatno oceni neodvisnost pravosodnih pooblaščencev, tudi kadar pooblaščenec ne opravlja (več) funkcije sodnika, ter neodvisnost pooblaščenca za hrambo in uporabo biometričnih podatkov in pooblaščenca za uporabo nadzornih kamer.**

4.2 Splošni pravni okvir za varstvo podatkov na področju državne varnosti

4.2.1 Potrdila državne varnosti

138. V skladu s členom 111 Zakona o varstvu podatkov iz leta 2018 lahko upravljavci zaprosijo za potrdila državne varnosti, ki jih izdajo minister, član kabineta, generalni državni tožilec ali generalni pravobranilec za Škotsko in ki potrjujejo, da so izjeme od obveznosti in pravic, določenih v delih 4 do 6 Zakona o varstvu podatkov iz leta 2018, potreben in sorazmeren ukrep za zaščito državne varnosti. Ta potrdila naj bi upravljavcem zagotavljala večjo pravno varnost in bodo ponujala trden dokaz dejstva, da se pri obdelavi osebnih podatkov uporablja državna varnost. Vendar je treba navesti, da ta potrdila niso potrebna za uporabo izjeme zaradi državne varnosti, ampak so ukrep preglednosti[82].

139. EOVP iz členov 17 in 18 dodatka 20 k Zakonu o varstvu podatkov iz leta 2018 razume, da je bil učinek potrdila državne varnosti, izdanega v skladu z Zakonom o varstvu podatkov iz leta 1998 (v nadaljevanju: staro potrdilo), za obdelavo osebnih podatkov podaljšan v skladu z Zakonom o varstvu podatkov iz leta 2018 do 25. maja 2019. Do tega datuma so se stara potrdila, razen če so bila nadomeščena ali preklicana, obravnavala, kot da so bila izdana v skladu z Zakonom o varstvu podatkov iz leta 2018.

140. Kadar pa potrdilo državne varnosti, izdano v skladu z Zakonom o varstvu podatkov iz leta 1998, nima izrecnega roka veljavnosti, EOVP razume, da bo takšno potrdilo še naprej veljalo glede obdelave na podlagi Zakona o varstvu podatkov iz leta 1998, razen če se potrdilo ne prekliče ali razveljavi[83]. Čeprav je varnost, ki jo zagotavljajo ta stara potrdila, omejena na obdelavo osebnih podatkov na podlagi Zakona o varstvu podatkov iz leta 1998, EOVP ugotavlja, da se lahko v skladu z Zakonom o varstvu podatkov iz leta 1998 izdajo nova potrdila državne varnosti za osebne podatke, ki so bili obdelani v skladu z Zakonom o varstvu podatkov iz leta 1998[84].

141. **Zaradi izčrpnosti EOVP Evropsko komisijo poziva, naj v svojem osnutku sklepa pojasni, da se potrdila državne varnosti še vedno lahko izdajajo po Zakonu o varstvu podatkov iz leta 1998. EOVP Evropsko komisijo poziva še, naj v svojem osnutku sklepa opiše mehanizme pravnega varstva in nadzora nad potrdili, izdanimi po Zakonu o varstvu podatkov iz leta 1998. Nazadnje EOVP Evropsko komisijo poziva, naj v svoj osnutek sklepa vključi število obstoječih potrdil, izdanih v skladu z Zakonom o varstvu podatkov iz leta 1998, in ta vidik pozorno spremlja.**

4.2.2 Pravica do popravka in izbrisa

142. Glede pravice do popravka in izbrisa EOVP ugotavlja, da se lahko posamezniki, na katere se nanašajo osebni podatki, v skladu s členoma 100 in 149 Zakona o varstvu podatkov iz leta 2018 obrnejo na sodišče High Court (ali sodišče Court of Session na Škotskem), da upravljavcu odredi, naj njihove podatke nemudoma popravi ali jih izbriše.

143. **EOVP poudarja, da je treba učinkovito zagotavljati uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki; zato Evropsko komisijo poziva, naj v svojem osnutku sklepa opiše, kako**

[82] Glej UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, avgust 2020, odstavek 4, str. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

[83] Glej Home Office, The Data Protection Act 2018, National Security Certificates Guidance, avgust 2020, str. 5.

[84] Glej Home Office, The Data Protection Act 2018, National Security Certificates Guidance, avgust 2020, odstavek 8, str. 5.

člen 100 Zakona o varstvu podatkov iz leta 2018 deluje v praksi, in naj pozorno spremlja uporabo tega člena.

4.2.3 Izjeme zaradi državne varnosti

144. EOVP želi opozoriti na člen 110 Zakona o varstvu podatkov iz leta 2018 in zlasti na dodatek 11, v katerem so opredeljeni posebni nameni, zaradi katerih lahko obveščevalne službe odstopajo od nekaterih načel varstva podatkov, tudi glede pravic posameznikov, na katere se nanašajo osebni podatki, in jim ni treba sporočati kršitev varstva osebnih podatkov uradu informacijskega pooblaščenca[85].

145. **EOVP Evropsko komisijo poziva, naj dodatno pojasni področje uporabe izjem, saj se sprašuje, ali so vse izjeme iz dodatka 11 Zakona o varstvu podatkov iz leta 2018 pomembne za delo obveščevalnih služb in ali zagotavljajo enakovrednost z načelom potrebnosti in sorazmernosti.** Natančneje, **EOVP Evropsko komisijo poziva, naj zagotovi več pojasnil glede tega, v katerih okoliščinah bi se lahko obveščevalna služba sklicevala na člen 10 dodatka 11 k Zakonu o varstvu podatkov iz leta 2018, v katerem je navedeno, da „se navedene določbe ne uporabljajo za osebne podatke, ki vsebujejo zapise o namenih upravljavca v zvezi z morebitnimi pogajanji s posameznikom, na katerega se nanašajo osebni podatki, če bi uporaba teh določb verjetno posegala v pogajanja“.**

4.3 Dostop in uporaba s strani javnih organov Združenega kraljestva za namene državne varnosti

146. EOVP na splošno priznava, da imajo države na voljo široko polje proste presoje pri vprašanjih državne varnosti, kar priznava tudi Evropsko sodišče za človekove pravice. EOVP tudi opozarja, da, kot je poudarjeno v njegovih posodobljenih priporočilih o temeljnih evropskih jamstvih za nadzorne ukrepe[86], člen 6(3) Pogodbe o Evropski uniji določa, da so temeljne pravice iz Evropske konvencije o človekovih pravicah splošna načela prava EU. Vendar, kot Sodišče EU opozarja v svoji sodni praksi, Evropska konvencija o človekovih pravicah, dokler EU ne bo pristopila k njej, ne predstavlja pravnega instrumenta, ki je formalno vključen v pravo EU[87]. Zato je treba raven varstva temeljnih pravic, ki jo zahteva člen 45 Splošne uredbe o varstvu podatkov, določiti na podlagi določb navedene uredbe, brati pa jo ob upoštevanju temeljnih pravic iz Listine EU o temeljnih pravicah. Glede na to morajo imeti v skladu s členom 52(3) Listine EU o temeljnih pravicah pravice, vsebovane v njej, ki ustrezajo pravicam, ki jih zagotavlja Evropska konvencija o človekovih pravicah, enak pomen in področje uporabe kot tiste, ki so določene v Evropski konvenciji o človekovih pravicah. Zato je treba, kot je opozorilo Sodišče EU, upoštevati sodno prakso Evropskega sodišča za človekove pravice glede pravic, ki so predvidene tudi v Listini EU o temeljnih pravicah, kot minimalni prag varstva za razlago ustreznih pravic iz Listine EU o temeljnih pravicah[88]. Vendar v skladu z zadnjo povedjo člena 52(3) Listine EU o temeljnih pravicah „[t]a določba ne preprečuje širšega varstva po pravu Unije“.

---

[85] Ti nameni so preprečevanje in odkrivanje „kaznivih dejanj“, „informacije, ki jih je treba razkriti v skladu z zakonom itd. ali v povezavi s pravnimi postopki“, „parlamentarni privilegiji“, „sodni postopki“, „državna čast in dostojanstvo“, „oborožene sile“, „gospodarska blaginja“, „varovanje zaupnosti sporazumevanja med odvetnikom in stranko“, „pogajanja“, „zaupne informacije upravljavca“, „izpitne pole in ocene“, „raziskave in statistični podatki“ ter „arhiviranje v javnem interesu“.

[86] Glej Priporočila EOVP 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe.

[87] Glej sodbo v zadevi Schrems II, točka 98.

[88] Glej sodbo Sodišča EU z dne 6. oktobra 2020 v združenih zadevah C-511/18, C-512/18 in C-520/18, La Quadrature du Net in drugi, ECLI:EU:C:2020:791, točka 124.

147. Zato je EOVP pri naslednji oceni upošteval sodno prakso Evropskega sodišča za človekove pravice, kolikor Listina EU o temeljnih pravicah, kot jo razlaga Sodišče EU, ne določa višje ravni varstva, ki predpisuje druge zahteve kot sodna praksa Evropskega sodišča za človekove pravice.

4.3.1 Pravna podlaga, omejitve in zaščitni ukrepi – preiskovalna pooblastila, ki se izvršujejo v okviru državne varnosti

4.3.1.1 Splošne pripombe

148. EOVP opozarja, da je Zakon o preiskovalnih pooblastilih iz leta 2016 nedavno sprejeti zakon, ki spreminja več določb Zakona o obveščevalnih službah iz leta 1994. V njem je opredeljen obseg, v katerem se preiskovalna pooblastila lahko uporabljajo za poseganje v zasebnost[89]. Kljub dvema poročiloma pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, ki zagotavljata koristne informacije glede uporabe tega novega pravnega okvira, še vedno ni bil opravljen pregled nekaterih vidikov, zlasti v zvezi z izbirniki in iskalnimi kriteriji, ki se uporabljajo.

149. Na splošno EOVP glede Zakona o preiskovalnih pooblastilih iz leta 2016 in njegovega področja uporabe poudarja tudi naslednje štiri točke, ki jim je treba nameniti pozornost:

150. Glede **prve točke, ki ji je treba nameniti pozornost,** nanaša pa se na značilnosti zakona, želi EOVP poudariti dva vidika:

151. Prvič, EOVP ugotavlja, da se zakonodaja nanaša na široke namene uporabe postopkov, določenih v Zakonu o preiskovalnih pooblastilih iz leta 2016, in ne na kategorije posameznikov, ki bi jih lahko zadevalo zbiranje podatkov na podlagi delov 2 do 7 Zakona o preiskovalnih pooblastilih iz leta 2016. Glede tega EOVP opozarja, da bi morala obstajati povezava med kategorijami posameznikov, ki bi bili lahko predmet nadzornih ukrepov, in nameni, ki jim sledi zakonodaja, za opredelitev osebnega področja uporabe zakona.

152. Poleg tega EOVP poudarja, da je tudi opredelitev pojmov „telekomunikacijski operaterji“, „telekomunikacijska storitev“ in „telekomunikacijski sistem“, ki opredeljuje področje uporabe zakona, zelo široka in deloma nejasna. Dejansko EOVP poudarja, da je treba te pojme na področju Zakona o preiskovalnih pooblastilih iz leta 2016 razumeti veliko širše kot v okviru drugih zakonodaj na področju telekomunikacij, kot je na primer opredeljeno v Evropskem zakoniku o elektronskih komunikacijah[90]. Ugotavlja tudi, da naj bi bila opredelitev pojmov „telekomunikacijska storitev“ in „telekomunikacijski sistem“ v zakonu namenoma široka, da bosta pojma ostala relevantna za nove tehnologije. Podobno je široka tudi opredelitev telekomunikacijskega operaterja, ki bi lahko vključevala na primer spletne videoigre z vključeno funkcijo klepeta ali druga spletna mesta, ki bi vključevala samo taka okna za klepet[91].

---

[89] Glej člen 1 Zakona o preiskovalnih pooblastilih iz leta 2016.

[90] Glej člen 2(5) Evropskega zakonika o elektronskih komunikacijah, v katerem je na primer „medosebna komunikacijska storitev“ opredeljena kot „storitev, ki se navadno opravlja za plačilo in omogoča neposredno medosebno in interaktivno izmenjavo informacij prek elektronskih komunikacijskih omrežij med omejenim številom oseb, pri čemer osebe, ki začnejo ali sodelujejo v komunikaciji, določajo prejemnike, in ne vključuje storitev, katerih medosebna in interaktivna komunikacija je zgolj manjši pomožni del storitve, ki je dejansko povezan z drugo storitvijo“.

[91] Glej Home Office, Code of practice on the interception of communications, marec 2018, odstavek 2.5 in naslednji, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

153. Poleg tega, čeprav so načeloma določeni postopki in nadzor glede ocene potrebnosti in sorazmernosti zbiranja podatkov in dostopa do njih, merila za začetek take ocene v zakonu niso opredeljena. Dodatne elemente je mogoče najti v drugih dokumentih, kot so kodeksi ravnanja.

154. Vendar, kot je opozoril EOVP v Priporočilih EOVP 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, je Sodišče EU navedlo, da „zahteva, da mora biti vsaka omejitev uveljavljanja temeljnih pravic določena z zakonom, pomeni, da mora biti v sami pravni podlagi, ki dovoljuje poseganje v take pravice, opredeljeno področje uporab omejitve uveljavljanja zadevne pravice“[92]. Natančneje, Sodišče EU je pojasnilo, da „[mora ureditev] [z]a izpolnitev zahteve po sorazmernosti ureditev določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe. Ta ureditev mora biti zakonsko zavezujoča v nacionalnem pravu, v njej pa mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno“[93].

155. Evropsko sodišče za človekove pravice poudarja tudi pomen jasnosti zakona, da lahko posamezniki „v zadostni meri razberejo, v katerih okoliščinah in pod katerimi pogoji so javni organi pooblaščeni za uporabo kakršnih koli takih ukrepov“[94].

156. **EOVP zato Evropsko komisijo poziva, naj dodatno oceni te vidike, kar zadeva natančnost, jasnost in izčrpnost zadevnega zakona, in zagotovi dodatne elemente, da dokaže, da se zagotavlja raven varstva, ki je v osnovi enakovredna ravni varstva, ki je zagotovljena v EU, kar zadeva značilnosti zakona. EOVP poudarja še, da bi bilo treba široke opredelitve oceniti tudi glede na sorazmernost ukrepov prestrezanja.**

157. Poleg tega, čeprav so v več notranjih kodeksih pristojnih organov obveščevalne skupnosti ti elementi delno razviti, na primer glede ocene potrebnosti in sorazmernosti zbiranja podatkov, EOVP poudarja, da zahteve Sodišča EU v zvezi z naravo zakona pomenijo, da morajo biti temeljni elementi, tudi za to, da se lahko posamezniki opirajo nanje v okviru pravnega varstva, določeni v zakonodaji, ki zagotavlja pravice, na podlagi katerih je mogoče ukrepati[95]. Dejansko je v odstavku 6 dodatka 7 k Zakonu o preiskovalnih pooblastilih iz leta 2016 navedeno, da sodišča (in nadzorni organi) „upoštevajo neupoštevanje kodeksa s strani osebe pri določanju vprašanja v vsakem takem postopku“, ne da bi pojasnili, ali se lahko posamezniki sklicujejo na kršitev kodeksov pred sodišči (ali nadzornimi organi). Poleg tega se elementi, ki so za zdaj navedeni v osnutku sklepa, bodisi nanašajo na priznanje predvidljivosti pravil, določenih[96] v zadevnih kodeksih, in ne na njihovo „možnost uveljavljanja“ na

[92] Glej sodbo v zadevi Schrems II, točka 175, in navedeno sodno prakso ter sodbo Sodišča EU z dne 6. Oktobra 2020 v zadevi C-623/17, Privacy International proti Secretary of State for Foreign and Commonwealth Affairs in drugim, ECLI:EU:C:2020:790 (v nadaljevanju: Privacy International), točka 65.

[93] Glej sodbo v zadevi Privacy International, točka 68.

[94] Glej sodbo z dne 4. decembra 2015 v zadevi Zakharov proti Rusiji, CE:ECHR:2015:1204JUD004714306, točka 229.

[95] Glede tega je Sodišče EU na primer menilo, da predsedniška politična direktiva št. 28 (PPD-28) v ZDA ni izpolnjevala pogojev, čeprav je določala tudi nekatere omejitve glede množičnega zbiranja, glej sodbo v zadevi Schrems II, točka 181.

[96] Glej sodbo Evropskega sodišča za človekove pravice z dne 13. septembra 2018 v zadevi *Big Brother Watch in drugi proti Združenemu kraljestvu*, ECLI:CE:ECHR:2018:0913JUD005817013 (v nadaljevanju: Big Brother Watch), točka 325: „ker je kodeks o prestrezanju komunikacij javni dokument, ki ga potrdita oba domova parlamenta in ki ga morajo upoštevati tisti, ki izvršujejo naloge prestrezanja, ter sodišča, je sodišče izrecno sprejelo, da je njegove določbe mogoče upoštevati pri presoji predvidljivosti ureditve na podlagi zakona o urejanju preiskovalnih pooblastil“.

sodišču, kot je zahtevalo Sodišče EU, bodisi na dejstvo, da so se sodišča Združenega kraljestva v nekaterih primerih sklicevala na kodekse, nobeden od navedenih primerov pa ne ponazarja možnosti, da posamezniki uveljavljajo pravice, ki izhajajo iz kodeksov. **Če se ugotovi, da pravo Združenega kraljestva ne navaja v zadostni meri okoliščin in pogojev, pod katerimi se lahko sprejme ukrep, in da so ti elementi dejansko določeni z notranjimi kodeksi organov obveščevalne skupnosti, bo EOVP Evropsko komisijo pozval, naj dodatno oceni, ali lahko posamezniki uveljavljajo in izvršujejo omejitve in zaščitne ukrepe, določene v različnih mednarodnih kodeksih organov obveščevalne skupnosti, na sodišču.**

158. **Druga točka, ki ji je treba nameniti pozornost**, zadeva dejstvo, da se določbe, ki se nanašajo, na eni strani, na ciljno pridobivanje in hrambo komunikacijskih podatkov in, na drugi strani, na množično zbiranje, bodisi v Zakonu o preiskovalnih pooblastilih iz leta 2016 bodisi v drugih zakonih, kot sta Zakon o obveščevalnih službah iz leta 1994 ali Zakon o urejanju preiskovalnih pooblastil iz leta 2000, uporabljajo tudi za podatke, ki se prenašajo iz EU v Združeno kraljestvo. Glede množičnega zbiranja EOVP poudarja, da ustrezne določbe prava Združenega kraljestva omogočajo zbiranje podatkov zunaj Združenega kraljestva: to bi lahko na primer vključevalo podatke v tranzitu, ki se prenašajo iz EGP v Združeno kraljestvo na podlagi sklepa o ustreznosti[97]. Poleg tega EOVP opozarja, da je Evropska komisija navedla, da „je treba poudariti, da se hramba in pridobivanje komunikacijskih podatkov običajno ne nanašata na osebne podatke posameznikov iz EU, na katere se nanašajo osebni podatki, ki se prenašajo v Združeno kraljestvo na podlagi tega sklepa. Obveznost hrambe ali razkritja komunikacijskih podatkov na podlagi dela 3 in 4 Zakona o preiskovalnih pooblastilih iz leta 2016 se nanaša na podatke, ki jih zbirajo telekomunikacijski operaterji v Združenem kraljestvu neposredno od uporabnikov telekomunikacijskih storitev[98]. Vendar pa EOVP opozarja na pomanjkanje jasnosti glede dejstva, da lahko zahtevke pristojnih organov Združenega kraljestva prejmejo samo tiste enote teh operaterjev, ki so v Združenem kraljestvu, saj opredelitev telekomunikacijskega operaterja iz člena 261(10) Zakona o preiskovalnih pooblastilih iz leta 2016 določa, da „je telekomunikacijski operater oseba, ki ponuja ali zagotavlja telekomunikacijske storitve osebam v Združenem kraljestvu ali ki nadzoruje oziroma zagotavlja telekomunikacijski sistem, ki je (v celoti ali delno) v Združenem kraljestvu ali se nadzoruje iz Združenega kraljestva“. Zato bi bili lahko zajeti tudi osebni podatki posameznikov, na katere se nanašajo osebni podatki, iz EGP, na primer v primeru podatkov, ki jih zbere ali ustvari enota telekomunikacijskega operaterja iz Združenega kraljestva, ki je v EGP, in se prenesejo enoti istega operaterja, ki je v Združenem kraljestvu, na podlagi sklepa o ustreznosti (za komercialne namene) ter jih nato, v Združenem kraljestvu, zbirajo pristojni javni organi.

159. **EOVP zato meni, da je ocena teh določb pomembna tudi za oceno ravni ustreznosti pravnega okvira Združenega kraljestva, ter Evropsko komisijo poziva, naj pojasni ta vidik in podrobneje oceni, v kolikšni meri to drži. Natančneje, EOVP Evropsko komisijo poziva, naj pojasni svoje razumevanje področja uporabe te zakonodaje, vključno s tem, kaj pojem „uporabniki telekomunikacijskih storitev“ zajema in ali je mogoče zahtevati podatke od enote telekomunikacijskih operaterjev zunaj Združenega kraljestva, če gre za podatke posameznikov, na katere se nanašajo osebni podatki, iz EGP, glede na zelo široko opredelitev telekomunikacijskih operaterjev.**

160. **Tretja točka, ki ji je treba nameniti pozornost**, se nanaša na postopek z dvojnim varovalom. EOVP ugotavlja, da je bil v Zakon o preiskovalnih pooblastilih iz leta 2016 vključen nov postopek z dvojnim varovalom. Vendar tudi razume, da čeprav lahko zbiranje podatkov ali dostop do njih za namene

[97] Glej točko 183 in naslednje v sodbi v zadevi Schrems II o oceni zakonodaje, ki zagotavlja dostop do podatkov v tranzitu med EU in tretjo državo v okviru sklepa o ustreznosti.
[98] Glej uvodno izjavo 196 osnutka sklepa.

državne varnosti ali obveščevalne namene načeloma poteka le na podlagi odredbe, ki jo odobri pravosodni pooblaščenec, Zakon o preiskovalnih pooblastilih iz leta 2016 določa, da „je v nekaterih omejenih primerih mogoče tudi zakonito prestrezanje brez odredbe in da se zahteva le predhodna odobritev samih pristojnih organov informacijskega pooblaščenca [glej oddelek o nadzoru], tudi za prestrezanja v skladu z zahtevami iz tujine (člen 52 Zakona o preiskovalnih pooblastilih iz leta 2016)“. Kot je poudarjeno v nadaljevanju, je to skladno s pomisleki EOVP, zlasti glede razkritij v tujini. Poleg tega EOVP ugotavlja tudi, da je za poseganje v opremo, ciljno ali množično, mogoče tudi odstopanje od postopka z dvojnim varovalom in da lahko pravosodni pooblaščenec odobri podaljšanje veljavnosti odredb o ukrepih v večjem obsegu šele po začetnem obdobju, ki ne sme biti daljše od šest mesecev. **EOVP Evropsko komisijo poziva, naj dodatno oceni in dokaže, da tudi v primerih, kadar se postopek z dvojnim varovalom ne uporablja, pravni okvir Združenega kraljestva zagotavlja ustrezne zaščitne ukrepe, tudi z učinkovitim naknadnim nadzorom in možnostmi pravnega varstva, ki so na voljo posameznikom, ter tako zagotavlja raven varstva, ki je v osnovi enakovredna ravni varstva, zagotovljeni v EU (glej tudi oddelek 4.3.3 o nadzoru).**

161. Poleg tega ima EOVP, čeprav je bil z Zakonom o preiskovalnih pooblastilih iz leta 2016 dejansko uveden postopek z dvojnim varovalom, še vedno pomisleke glede nekaterih značilnosti nove zakonodaje. Po predstavitvi ustreznih oddelkov osnutka sklepa je EOVP proučil naslednje vrste zbiranja podatkov in dostopa do njih v enakem vrstnem redu, kot jih je predstavila Evropska komisija. Vrstni red elementov, proučenih v nadaljevanju, zato ne izraža hierarhije v smislu stopnje zaskrbljenosti EOVP.

4.3.1.2 Ciljno pridobivanje in hramba komunikacijskih podatkov

162. EOVP ugotavlja, da obstajata dve uradni osebi, ki lahko izdata dovoljenja za ciljno pridobivanje komunikacijskih podatkov: odredbodajalec v uradu za izdajo dovoljenj za ciljno pridobivanje komunikacijskih podatkov (v nadaljevanju: pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil), tj. pooblaščeni višji uslužbenec (oseba, ki ima v ustreznem javnem organu predpisano funkcijo ali položaj), in, v nekaterih primerih, pravosodni pooblaščenec. Vendar EOVP na podlagi zakona in zadevnega kodeksa še vedno ni jasno, kateri natančno so ti uradni organi, za katero vrsto ciljnega pridobivanja komunikacijskih podatkov gre in v kakšnem obsegu bi bila imenovana uradna oseba dovolj neodvisna[99].

163. **EOVP zato Evropsko komisijo poziva, naj podrobneje oceni ta vidik in predloži jasnejša pojasnila o teh elementih.**

164. Glede obvestila, ki zahteva hrambo komunikacijskih podatkov, EOVP tudi ugotavlja, da so taka obvestila lahko namenjena tudi „opisu operaterjev“. Zdi se, da ta pojem pomeni, da se lahko od več operaterjev hkrati zahteva, da vsi hranijo podatke. Dejansko se ciljna narava pridobivanja ne nanaša na število operaterjev, ampak na ime ali opis oseb, organizacij, lokacije ali skupine oseb, ki pomenijo tarčo, opis narave preiskave ter opis dejavnosti, za katere se oprema uporablja. EOVP zato poudarja, da je lahko obvestilo, glede na število operaterjev, na katere se nanaša tak „opis operaterjev“, širše od tistega, kar se zdi, da pomeni postopek za ciljno hrambo. **EOVP Evropsko komisijo poziva, naj dodatno oceni ta vidik in predloži dodatna zagotovila, da so obvestila tudi, če so naslovljena na več operaterjev, še vedno omejena na tisto, kar je nujno potrebno in sorazmerno.**

[99] Glej tudi oddelek v zvezi z oceno postopka z dvojnim varovalom in neodvisnostjo pravosodnega pooblaščenca.

4.3.1.3 Poseganje v opremo

165. EOVP opozarja, da lahko „poseganje v opremo“ v nujnih primerih odstopa od postopka z dvojnim varovalom[100]. Zato je zaskrbljen, da so nameni, za katere se tako poseganje v opremo lahko zahteva, široki in da merila za nujne primere (v katerih pravosodnemu pooblaščencu ni treba predložiti predhodnega dovoljenja na podlagi ocene potrebnosti in sorazmernosti poseganja v opremo) ostajajo nejasna. Ker v slednjem primeru „odredba ne učinkuje več in njene veljavnosti ni mogoče podaljšati“, če pravosodni pooblaščenec ne odobri poseganja v opremo naknadno, EOVP razume, da medtem zbrani podatki ostanejo zakonito zbrani. Za izbris teh podatkov lahko pravosodni pooblaščenec izda posebno odredbo[101].

166. **EOVP Evropsko komisijo poziva, naj dodatno oceni pogoje, pod katerimi se je mogoče sklicevati na nujnost, in predloži pojasnila o možnostih uveljavljanja pravic za zadevne posameznike, na katere se nanašajo osebni podatki, in možnostih pravnega varstva, ki so jim na voljo v okviru postopkov poseganja v opremo, zlasti kadar se izvajajo v okviru nujnosti, ki vodi do odstopanja od postopka dvojnega varovala.**

4.3.1.4 Množično prestrezanje podatkov nosilcev

167. Kot je opisano v poročilu o pregledu pooblastil v večjem obsegu[102], „množično prestrezanje običajno vključuje zbiranje komunikacij med prehajanjem prek določenih nosilcev (komunikacijskih povezav)“. V uradnem informativnem listu Zakona o preiskovalnih pooblastilih iz leta 2016 je „množično prestrezanje“ opisano kot „postopek zbiranja komunikacij v večjem obsegu, ki mu sledi izbira določenih komunikacij za branje, ogled ali poslušanje, če je to potrebno in sorazmerno“. EOVP ugotavlja, da množično prestrezanje podatkov dejansko pomeni zbiranje podatkov še pred kakršnim koli filtriranjem po izbirnikih (preprostim v okviru spremljanja posameznikov, za katere je že znano, da pomenijo grožnjo, ali zapletenim v okviru opredelitve novih groženj in prej neznanih oseb, ki bi jih podatki lahko zanimali).

168. Množično pridobivanje komunikacijskih podatkov je bilo tudi eno od vprašanj, ki ga je Sodišče EU proučilo v zadevi Privacy International, v kateri je veliki senat izdal sodbo 6. oktobra 2020 (poleg vprašanja, ali je tako zbiranje podatkov potekalo v okviru prava EU, tudi za namene državne varnosti). Zakon o preiskovalnih pooblastilih iz leta 2016 je nadomestil zakonodajo, ki je bila predmet te sodbe.

169. EOVP ugotavlja, da se z uvedbo Zakona o preiskovalnih pooblastilih iz leta 2016 v pravo Združenega kraljestva odredba zdaj zahteva tudi za množično prestrezanje podatkov. Postopek za izdajo te odredbe temelji na določitvi „operativnih namenov“. Seznam teh operativnih namenov pripravijo vodje obveščevalnih služb, nato pa ga odobri pristojni minister. Ta sklep je odobril neodvisni pravosodni pooblaščenec, ki mora preveriti, ali je odredba potrebna in sorazmerna za operativne namene. EOVP razume, da pravosodni pooblaščenec nima pooblastil za ocenjevanje samih operativnih namenov, ampak za oceno, ali je odredba potrebna in sorazmerna za operativne namene, navedene v odredbi. Parlamentarnemu odboru za obveščevalno in varnostno dejavnost se vsake tri mesece predloži kopija seznama, predsednik vlade pa vsaj enkrat letno pregleda seznam teh operativnih namenov.

170. Vendar se na podlagi elementov, ki jih je Evropska komisija navedla v osnutku sklepa, zdi, da je težko oceniti obseg teh operativnih namenov, navedenih na seznamu, in ali zbiranje podatkov, ki ga

[100] Glej člen 109 Zakona o preiskovalnih pooblastilih iz leta 2016.
[101] Glej točko (b) pododdelka 3 člena 110 Zakona o preiskovalnih pooblastilih iz leta 2016.
[102] Glej poročilo o pregledu pooblastil v večjem obsegu, ki ga je pripravil neodvisni pregledovalec zakonodaje o terorizmu, avgust 2016.

omogočajo, dosega prag, ki ga je določilo Sodišče EU (na primer omejitev zbiranja podatkov na geografsko območje lahko zajema le nekaj ulic ali pa zbiranje podatkov iz EGP kot celote).

171. Poleg tega EOVP poudarja, da se podatki, ki se zbirajo množično, lahko hranijo daljša obdobja (da so na voljo za nadaljnji dostop za pregled). Dejansko EOVP ugotavlja, da odstavka 5 in 6 člena 150 Zakona o preiskovalnih pooblastilih iz leta 2016 določata samo uničenje kopij zbranih podatkov in le v primeru, če njihova hramba ni potrebna ali verjetno ne bo potrebna, ni v interesu državne varnosti ali iz katerega koli drugega razloga iz člena 138(2) Zakona o preiskovalnih pooblastilih iz leta 2016 ali če hramba ni potrebna za več drugih namenov[103]. EOVP poudarja, da se zdijo ti razlogi zelo široki in da so v vsakem primeru navedene samo kopije pridobljenih podatkov.

172. Poleg tega ugotavlja, da Zakon o preiskovalnih pooblastilih iz leta 2016 omogoča tudi spremembo odredb brez prehodne odobritve pravosodnega pooblaščenca in da v primeru, če pravosodni pooblaščenec, s katerim je v treh delovnih dneh po spremembi opravljeno naknadno posvetovanje, ne odobri spremembe, odredba velja, kot da sprememba ne bi bila izvedena, zbrani podatki pa ostanejo zakonito zbrani[104]. Za izbris teh podatkov lahko pravosodni pooblaščenec izda posebno odredbo[105].

173. **EOVP zato Evropsko komisijo poziva, naj dodatno pojasni in oceni množično prestrezanje, zlasti glede izbire in uporabe izbirnikov v okviru teh postopkov množičnega prestrezanja za razjasnitev obsega, v katerem dostop do osebnih podatkov izpolnjuje pragove, ki jih je določilo Sodišče EU (glej tudi oddelek 4.3.1.7 v nadaljevanju, zlasti o nadzoru nad izbirniki), in kateri zaščitni ukrepi so vzpostavljeni za zaščito temeljnih pravic posameznikov, katerih podatki se prestrezajo v tem okviru, tudi glede obdobij hrambe podatkov. Še posebej koristna bi bila neodvisna ocena pristojnih nadzornih organov Združenega kraljestva.**

174. **EOVP poudarja še, da se zdi še toliko bolj kritično, da „komunikacija, povezana s tujino“, ki spada v obseg praks množičnega prestrezanja, očitno pomeni, da bi lahko Združeno kraljestvo neposredno prestrezalo in množično zbiralo podatke v EGP, vključno s podatki, ki se prenašajo med EGP in Združenim kraljestvom in ki bi spadali na področje uporabe osnutka sklepa (glej oddelek 4.3.2 v nadaljevanju o nadaljnji uporabi informacij, zbranih za namene državne varnosti in razkritja v tujini).**

4.3.1.5 Varstvo in zaščitni ukrepi za sekundarne podatke

175. EOVP je zaskrbljen tudi glede tega, da ustrezna zakonodaja Združenega kraljestva, ki se nanaša na množično prestrezanje, ne zagotavlja enake ravni varstva za vse komunikacijske podatke. „Sekundarni podatki, ki se lahko pridobijo z odredbo o ukrepih v večjem obsegu, so, v skladu s členom 137 Zakona o preiskovalnih pooblastilih iz leta 2016, tako „podatki o sistemih“, „ki so del komunikacije, vključeni vanjo, priloženi komunikaciji ali z njo logično povezani (prek pošiljatelja ali kako drugače)“, kot tudi „identifikacijski podatki“, „ki so del komunikacije, vključeni vanjo, priloženi komunikaciji ali z njo logično povezani (prek pošiljatelja ali kako drugače), jih je mogoče logično ločiti od preostale komunikacije in se ob taki ločitvi z njimi ne bi razkrilo nič, kar bi se razumno lahko štelo za (kateri koli) pomen komunikacije, ne glede na kateri koli pomen, ki izhaja iz dejstva komunikacije ali iz katerih koli podatkov, ki se nanašajo na prenos komunikacije“[106].

[103] Glej pododdelka 3 in 6 člena 150 Zakona o preiskovalnih pooblastilih iz leta 2016.
[104] Glej člen 147 Zakona o preiskovalnih pooblastilih iz leta 2016 (poglavje I dela 6).
[105] Glej točko (b) pododdelka 3 člena 181 Zakona o preiskovalnih pooblastilih iz leta 2016.
[106] „Sistemski podatki“ in „identifikacijski podatki“ so opredeljeni v členu 263 Zakona o preiskovalnih pooblastilih iz leta 2016.

176. EOVP ugotavlja, da se zdi, da ti „sekundarni podatki“, znani tudi kot „metapodatki“[107], ki se zbirajo množično, ne uživajo enakih zaščitnih ukrepov kot podatki, ki se zbirajo na podlagi ciljne odredbe, in podatki o vsebini, ki se zbirajo množično. EOVP dejansko ugotavlja, da ima izbira katere koli prestrežene vsebine koristi od več zaščitnih ukrepov[108] kot izbira sekundarnih podatkov[109].

177. Poleg tega EOVP poudarja, da sta Evropsko sodišče za človekove pravice[110] in Sodišče EU[111] podvomila o tem, da so taki podatki manj občutljivi kot drugi podatki in zlasti podatki o vsebini. Dejansko so v kodeksu ravnanja glede prestrezanj predstavljeni primeri sekundarnih podatkov (podatki o sistemih, kot so nastavitve usmerjevalnika, e-naslovi ali uporabniška identifikacijska koda ter alternativni identifikatorji računov, in identifikacijski podatki, kot so lokacija sestanka v koledarskem terminu, informacije o fotografiji, kot so ura, datum in lokacija posnete fotografije). **EOVP tako poudarja usklajeno oceno Evropskega sodišča za človekove pravice in Sodišča EU ter opozarja na pomisleke, izražene glede sekundarnih podatkov, za katere bi morali biti zaradi njihove občutljivosti koriščeni zaščitni ukrepi. Zato Evropsko komisijo poziva, naj natančno oceni, ali zaščitni ukrepi, določeni v zakonodaji Združenega kraljestva za tako kategorijo osebnih podatkov, zagotavljajo v osnovi enakovredno raven varstva, kot je zagotovljena v EU.**

4.3.1.6 Avtomatizirana obdelava komunikacijskih podatkov

178. EOVP ugotavlja, da organi obveščevalne skupnosti ne uporabljajo samo enostavnih ali zapletenih izbirnikov za filtriranje podatkov, pridobljenih v večjem obsegu, ampak da lahko uporabljajo tudi druga orodja za avtomatizirano obdelavo podatkov za analizo „velikih količin informacij, ki agencijam omogočajo, da poiščejo povezave, vzorce, asociacije ali vedenja, ki lahko kažejo na resno grožnjo, ki zahteva preiskavo“, kot je navedeno v poročilu odbora za obveščevalno in varnostno dejavnost iz leta 2015[112]. **EOVP se zaveda, da se to javno poročilo nanaša na prakse iz prejšnjega pravnega okvira, ki ga je pozneje nadomestil Zakon o preiskovalnih pooblastilih iz leta 2016. Vendar meni, da sta**

---

[107] Glej poročilo o pregledu pooblastil v večjem obsegu, ki ga je pripravil neodvisni pregledovalec zakonodaje o terorizmu, avgust 2016.

[108] Glej točko (c) pododdelka 1 ter pododdelek 3 in naslednje člena 152 Zakona o preiskovalnih pooblastilih iz leta 2016.

[109] Glej točki (a) in (b) pododdelka 1 člena 152 Zakona o preiskovalnih pooblastilih iz leta 2016.

[110] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, točka 357, pod sklicevanjem na veliki senat: „Čeprav Sodišče ne dvomi, da so povezani komunikacijski podatki bistveno orodje za obveščevalne storitve v boju proti terorizmu in hudim kaznivim dejanjem, meni, da organi niso vzpostavili pravičnega ravnovesja med konkurenčnimi javnimi in zasebnimi interesi s tem, ko so jih v celoti izvzeli iz zaščitnih ukrepov, ki se uporabljajo za iskanje in preiskovanje vsebine. Čeprav Sodišče ne meni, da bi morali biti povezani komunikacijski podatki dostopni samo za namene ugotavljanja, ali je posameznik na Britanskem otočju ali ne, saj bi to pomenilo, da se za povezane komunikacije podatke zahteva uporaba strožjih standardov, kot se uporabljajo za vsebino, pa bi morali biti vzpostavljeni zadostni zaščitni ukrepi, ki bi zagotavljali, da je izvzetje povezanih komunikacijskih podatkov iz zahtev člena 16 Zakona o urejanju preiskovalnih pooblastil omejeno na obseg, ki je potreben za ugotovitev, ali je posameznik trenutno na Britanskem otočju.“

[111] Glej sodbo Sodišča EU v zadevi Privacy International, 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, 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).“

[112] Glej Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, odstavek 18, str. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

potrebna nadaljnja neodvisna ocena in nadzor, kako nadzorni organi Združenega kraljestva uporabljajo orodja za avtomatizirano obdelavo podatkov, ter Evropsko komisijo poziva, naj dodatno oceni to vprašanje in zaščitne ukrepe, ki bi se lahko zagotovili posameznikom v EGP, na katere se nanašajo osebni podatki, v tem okviru.

4.3.1.7 Tveganja glede skladnosti in neskladne prakse pristojnih organov obveščevalne skupnosti

179. EOVP ugotavlja, da so na voljo podrobna poročila o nadzoru. Ta poročila zagotavljajo dragocene elemente, kar zadeva tisto, kar ocenjujejo kot pozitivne prakse zagotavljanja skladnosti, ter tveganja glede skladnosti in opredeljene neskladne prakse.

180. Glede tega po navedbah pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil v njegovem poročilu za leto 2019 več elementov, ki se nanašajo na uporabo pravnega okvira s strani različnih pristojnih organov, razkriva nekatera (tveganja) neskladnosti s strani pristojnih organov.

181. Prvič, EOVP je ugotovil, da se zdi, da merila za opredelitev nabora podatkov kot nabora osebnih podatkov v večjem obsegu ali kot ciljno usmerjenih podatkov niso vedno jasna za varnostni službi MI5 in SIS, zlasti za MI5, kar lahko privede do neobstoja ustreznih zaščitnih ukrepov, ki bi se uporabljali za podatke[113]. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil je v svojem poročilu za leto 2019 predlagal, naj „se to vprašanje prednostno reši“[114]. V zvezi z nabori osebnih podatkov v večjem obsegu EOVP ugotavlja še, da čeprav se zdi opredelitev naborov osebnih podatkov v večjem obsegu zadovoljiva (vendar jo mora pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil še pregledati), je marca 2019 notranji pregled skladnosti odredb, ki ga je izvedla namenska skupina, pri vladni obveščevalni službi zbudil resne pomisleke, saj 50 % utemeljitev odredb o množičnem pridobivanju podatkov, ki jih je pregledala skupina vladne obveščevalne službe za skladnost, ni izpolnjevalo zahtevanega standarda. Po navedbah pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil je skupina za skladnost začela delo za proučitev težave in ponovno usposabljanje osebja za izboljšanje tega standarda. Z osvežitvenim usposabljanjem o določbah zakona o preiskovalnih pooblastilih iz leta 2016 in dodatnim usposabljanjem, ki so ga izvedle mreže za politiko in skladnost, se je izboljšala skladnost vladne obveščevalne službe na tem področju. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil ne pričakuje poslabšanja tega standarda pri prihodnjih pregledih, vendar bo še naprej pozorno spremljal to področje[115]. **EOVP se zato strinja, da mora Evropska komisija nadalje pregledati in spremljati navedene elemente v**

[113] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), 15. december 2020, točka 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: „Opazili smo pozitiven razvoj [odbora za nadzor nad nabori osebnih podatkov v večjem obsegu (*Bulk Oversight Panel* – BOP)] in smo seznanjeni z njegovim vplivom pri upravljanju notranje skladnosti. Še naprej si bomo prizadevali za večjo jasnost v zvezi s postopkom, ki ga MI5 uporablja za izvajanje začetnega pregleda novih naborov podatkov za boljše razumevanje odločitev o opredelitvi nabora podatkov kot nabora osebnih podatkov v večjem obsegu ali, na primer, kot ciljno usmerjenih podatkov. Bili smo zaskrbljeni zaradi nerešenega ukrepa iz zapisnika odbora za nadzor nad nabori osebnih podatkov v večjem obsegu v zvezi z odpravo neskladnosti med dodelitvami nabora osebnih podatkov v večjem obsegu med MI5 in SIS. Zaradi različnih uporab podatkov in različnih omejitev podatkov, ki se hranijo, je mogoče, da bi obe varnostni službi hranili isti nabor podatkov, ali njegove različice, ki bi ga lahko ena zakonito opredelila kot nabor podatkov v večjem obsegu, druga pa kot ciljno usmerjene podatke. Obstaja tveganje, da bi se, če bi ena od varnostnih služb napačno opredelila nosilca podatkov kot ciljno usmerjenega, podatki nato hranili brez ustrezne odredbe in se zanje morda ne bi uporabljali ustrezni zaščitni ukrepi.“

[114] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 8.39.

[115] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.48.

okviru ocene ravni varstva, da bi se zagotovilo izboljšanje tega standarda, kot je poudarjeno v poročilu pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, ter opozarja, da se pri ocenjevanju v osnovi enakovredne ravni varstva tretje države, upoštevata tudi izvajanje in konkretna uporaba pravnega okvira, kot je določeno v členu 45 Splošne uredbe o varstvu podatkov.

182. V širšem smislu EOVP poudarja točke, ki jim je treba nameniti pozornost in jih je navedel pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil v zvezi z „iskanji, ki temeljijo na nalogah“, ki jih vodijo pripadniki MI5 – kar preiskovalcu omogoča, da izvede več kot eno iskanje osebnih podatkov v večjem obsegu, ki so mu na voljo, in „resnimi tveganji glede skladnosti, povezanimi z nekaterimi tehnološkimi okolji, ki jih uporablja MI5“, glede tega, kje so se podatki hranili, kdo je imel dostop do njih, obsega, v katerem so se kopirali ali izmenjevali, postopki brisanja, ki so se uporabljali zanje, in glede obdobij hrambe. Čeprav je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil navedel, da so bili sprejeti ukrepi in uvedeni zaščitni ukrepi, pri čemer so se nekateri še vedno izvajali ročno in se upravljajo na individualni, človeški osnovi, poudarja, da je ključno, da „MI5 še naprej ohranja te nove postopke in zagotavlja zadostna sredstva za njihovo učinkovito delovanje. Če MI5 ugotovi porast neskladnega ravnanja“[116]. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil pričakuje, da bo čim prej seznanjen z njim. **EOVP zato Evropsko komisijo poziva, naj v prihodnosti pozorno spremlja te vidike**.

183. V zvezi z vladno obveščevalno službo EOVP glede na poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil razume, da je bila pri operacijah, ki so se izvajale na podlagi odredb o ukrepih v večjem obsegu, „kakovost zahtevkov za notranjo odobritev različna in da smo ugotovili, da obstajajo možnosti za izboljšave načina opredelitve takih zahtevkov“[117], ter da so bila za ciljno poseganje v opremo pojasnila za uporabo splošnih deskriptorjev včasih preveč splošna in nenatančna[118]. EOVP je tudi ugotovil, da pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil glede množičnega poseganja v opremo priporoča, „naj se v zahtevkih dosledno in izrecno navaja povezava med ciljem in namenom, opredeljenim z zakonom, ter obveščevalnimi zahtevami“[119] in „naj se v zahtevkih pri ocenjevanju sorazmernosti jasno obravnavajo možnost postranskih posegov in ukrepi za blažitev“[120], ter da je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil poudaril, da kljub napredku „še vedno obstajajo možnosti za izboljšave“[121] in da bo tudi v prihodnosti potrebna nadaljnja pozornost.

184. Glede ureditve množičnega prestrezanja v skladu z Zakonom o urejanju preiskovalnih pooblastil iz leta 2000, ki je bil pozneje nadomeščen z določbami v Zakonu o preiskovalnih pooblastilih iz leta 2016, EOVP opozarja, da je bil nezadosten nadzor nad izbiro nosilcev interneta za prestrezanje ter filtriranjem, iskanjem in izbiro prestreženih komunikacij za pregled eden od ključnih vidikov, ki ga je Evropsko sodišče za človekove pravice v zadevi Big Brother Watch, ki je zdaj predložena velikemu

[116] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 8.52.
[117] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.2.
[118] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točki 10.16 in 10.17.
[119] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.23.
[120] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.23.
[121] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.23.

senatu, štel za neskladnega s členom 8 Evropske konvencije o človekovih pravicah v zvezi s prejšnjo zakonodajo o preiskovalnih pooblastilih organov Združenega kraljestva v okviru državne varnosti. **EOVP Evropsko komisijo poziva, naj preveri trenutno stanje postopka v zadevi, da bi upoštevala te elemente, in jih navede v sklepu o ustreznosti, če ga bo Evropska komisija sprejela.**

185. V tej zadevi Evropsko sodišče za človekove pravice: „ni bilo prepričano, da so zaščitni ukrepi, ki urejajo izbiro nosilcev za prestrezanje in izbiro prestreženega gradiva za pregled dovolj strogi, da zagotavljajo ustrezna jamstva za preprečevanje zlorab. Vendar pa skrb najbolj vzbuja neobstoj zanesljivega neodvisnega nadzora nad izbirniki in iskalnimi kriteriji, ki se uporabljajo za filtriranje prestreženih komunikacij“[122]. Kot je poudaril pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil, „je ta ugotovitev izražala podobno priporočilo v poročilu Intelligence and Security Committee's Privacy and Security: A modern and transparent legal framework iz marca 2015 (Zasebnost in varnost odbora za obveščevalne in varnostne zadeve: sodoben in pregleden pravni okvir)“[123]. **EOVP pozdravlja dejstvo, da je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil leta 2019 posledično izvedel pregled svojega pristopa k preiskovanju množičnega prestrezanja, „ki je vključeval natančen pregled tehnično zapletenih načinov, na katere se množično prestrezanje dejansko izvaja“[124], in se zavezal, da bo v preiskave množičnega prestrezanja od leta 2020 naprej vključil „podrobno preiskavo izbirnikov in iskalnih kriterijev, ki jih je zgoraj navedlo ESČP“[125]. Glede na pomen tega vidika je EOVP zaskrbljen, ker pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil še ni podrobno proučil izbirnikov in iskalnih kriterijev, ter Evropsko komisijo poziva, naj glede tega pozorno spremlja razvoj dogodkov, zlasti ker je treba konkretno obliko takega nadzora še razjasniti[126].**

4.3.2 Nadaljnja uporaba informacij, zbranih za namene državne varnosti in razkritje v tujini

186. Glede nadaljnje uporabe informacij, zbranih za namene državne varnosti, se Evropska komisija v svoji oceni sklicuje na člen 87(1) Zakona o varstvu podatkov iz leta 2018, ki dejansko določa, da „tako zbranih podatkov ni dovoljeno obdelati na način, ki ni skladen z namenom, za katerega so bili zbrani“. Vendar EOVP poudarja, da lahko za to določbo veljajo izjeme zaradi državne varnosti v skladu s členom 110 Zakona o varstvu podatkov iz leta 2018. Poleg tega ugotavlja, da zakonodaja zagotavlja možnost „razkritja v tujini“ za ciljno usmerjeno prestrezanje in pregledovanje, za ciljno pridobivanje in hrambo komunikacijskih podatkov, za ciljno poseganje v opremo ali za množično prestrezanje in množično poseganje v opremo.

4.3.2.1 Nadaljnja uporaba, razkritje v tujini in veljavni pravni okvir v Združenem kraljestvu

187. Evropska komisija je del 4 Zakona o varstvu podatkov iz leta 2018 in zlasti njegov člen 109 opredelila kot pomembne določbe, ki določajo zahteve za nadaljnjo uporabo zbranih informacij in zlasti mednarodni prenos osebnih podatkov s strani obveščevalnih služb v tretje države ali mednarodne organizacije. Vendar EOVP ugotavlja, da je v členu 110 Zakona o varstvu podatkov iz leta 2018

[122] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, točka 347.
[123] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.28.
[124] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.28.
[125] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.28.
[126] Glej Annual Report of the Investigatory Powers Commissioner 2019 (Letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019), točka 10.28: „o natančni obliki takega pregleda se je treba še dogovoriti“.

določena izjema zaradi državne varnosti in navedeno, da se nekatere določbe Zakona o varstvu podatkov iz leta 2018 ne uporabljajo, če je izjema od teh določb potrebna za zaščito državne varnosti. Zadevne določbe, ki se morda ne uporabljajo, vključujejo poglavje 2 dela 4 Zakona o varstvu podatkov iz leta 2018 glede načel varstva podatkov, vključno z omejitvijo namena, in poglavje 3 dela 4 Zakona o varstvu podatkov iz leta 2018 glede pravic posameznikov, na katere se nanašajo osebni podatki. Člen 109 Zakona o varstvu podatkov iz leta 2018 v povezavi s členom 110 Zakona o varstvu podatkov iz leta 2018 in pogoji, pod katerimi se uporablja, lahko privede do primerov, v katerih mednarodni prenos osebnih podatkov, ki ga izvedejo obveščevalne službe, v tretje države poteka brez uporabe določb v zvezi z načeli varstva podatkov in pravicami posameznikov, na katere se nanašajo osebni podatki.

188. Kot je opredelila Evropska komisija, je treba tako izjemo oceniti za vsak primer posebej in se je nanjo mogoče sklicevati le, če bi uporaba posamezne določbe imela negativne posledice za državno varnost. Dejansko je izdaja potrdila glede državne varnosti za obveščevalne službe Združenega kraljestva namenjena potrditvi, da je izjema potrebna glede navedenih osebnih podatkov, ki se obdelujejo za zaščito državne varnosti. Vendar EOVP ugotavlja, da ministrstvo za notranje zadeve Združenega kraljestva v svojih smernicah o potrdilih glede državne varnosti na podlagi Zakona o varstvu podatkov iz leta 2018 pojasnjuje, da „je pomembno že na začetku opozoriti, da se potrdilo ne zahteva za uporabo izjeme zaradi državne varnosti; dejansko upravljavci v večini primerov sami določijo, ali se uporablja izjema zaradi državne varnosti.“ [127] Poleg tega je v smernicah ministrstva za notranje zadeve Združenega kraljestva navedeno, da „se potrdila glede državne varnosti lahko uporabljajo za osebne podatke, ki jih je mogoče izrecno opredeliti ali ki zajemajo širšo kategorijo osebnih podatkov. Lahko se izdajo vnaprej ali za nazaj.“ [128] Izjema zaradi državne varnosti se zato lahko uporablja glede mednarodnega prenosa osebnih podatkov s strani obveščevalnih služb v tretje države brez potrdila glede državne varnosti.

189. EOVP nadalje ugotavlja, da na primer potrdilo glede državne varnosti DPA/S27/Security Service[129] določa, da so do 24. julija 2024 osebni podatki, ki se obdelujejo „za varnostno službo, v njenem imenu, na njeno zahtevo ali z njeno pomočjo ali podporo“, in „če je taka obdelava potrebna za olajšanje ustreznega opravljanja nalog varnostne službe, opisanih v členu 1 Zakona o varnostnih službah iz leta 1989“, izvzeti iz določb zakonodaje Združenega kraljestva, ki ustrezajo poglavju V Splošne uredbe o varstvu podatkov glede prenosov osebnih podatkov v tretje države ali mednarodne organizacije. Ker druga potrdila glede državne varnosti, ki so javno dostopna, ne določajo izvzetja iz določb člena 109 Zakona o varstvu podatkov iz leta 2018, je treba opozoriti, da se del besedila ali celotno besedilo potrdila glede državne varnosti lahko zadrži, če bi bila njegova objava v nasprotju z interesi državne varnosti, v nasprotju z javnim interesom ali bi lahko ogrozila varnost katero koli osebe.

190. Na splošno EOVP pri ocenjevanju osnutka sklepa glede teh določb ugotavlja, da zaščitni ukrepi za ta razkritja vključujejo zgolj zahtevo, da prejemnik podatkov spoštuje zahteve glede varnosti podatkov, obsega razkritja, ki je omejen na tisto, kar je potrebno, hrambe podatkov in omejitve dostopa do podatkov na omejeno število oseb. Zato **EOVP poudarja, da glede razkritij v tujini uporaba izjeme**

[127] Glej Home Office, The Data Protection Act 2018, National Security Certificates Guidance, avgust 2020, odstavek 3, str. 3.
[128] Glej Home Office, The Data Protection Act 2018, National Security Certificates Guidance, avgust 2020, odstavek 5, str. 4.
[129] Glej DPA/S27/Security Service, člen 27 Zakona o varstvu podatkov iz leta 2018, Certificate of the Secretary of State, 24. julij 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

zaradi državne varnosti, določene v zakonodaji Združenega kraljestva, lahko privede do primerov, v katerih zaščitni ukrepi, ki zagotavljajo spoštovanje načel omejitve namena, potrebnosti in sorazmernosti ter pravice posameznikov, nadzor in pravno varstvo, v namembni tretji državi niso zagotovljeni ali se ne spoštujejo. EOVP zato Evropski komisiji priporoča, naj dodatno prouči splošne zaščitne ukrepe, določene v zakonodaji Združenega kraljestva glede razkritja v tujini, zlasti glede na uporabo izjem zaradi državne varnosti.

4.3.2.2 Razkritje v tujini in izmenjava obveščevalnih podatkov v okviru mednarodnega sodelovanja

191. EOVP ugotavlja še, da Evropska komisija v okviru svoje ocene ustreznosti ni proučila veljavnih mednarodnih sporazumov, sklenjenih med Združenim kraljestvom in tretjimi državami ali mednarodnimi organizacijami, ki morda vsebujejo posebne določbe za mednarodni prenos osebnih podatkov s strani obveščevalnih služb v tretje države.

192. EOVP poudarja še, da ocena Evropske komisije večinoma temelji na oceni dela 4 Zakona o varstvu podatkov iz leta 2018 in je zlasti zaskrbljen, ker se Zakon o preiskovalnih pooblastilih iz leta 2016 osredinja na zahteve po izmenjavi obveščevalnih podatkov s tujimi partnerji, ne obravnava pa drugih oblik izmenjave obveščevalnih podatkov. EOVP glede tega ugotavlja, da osnutek sklepa Evropske komisije ne vključuje ali ocenjuje povezave med zakonodajnim okvirom Združenega kraljestva in „sporazum o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA“. V nedavni izjavi ob proslavitvi 75. obletnice tega sporazuma je Agencija ZDA za državno varnost navedla, da to partnerstvo omogoča „izmenjavo informacij med obema agencijama v največji možni meri, s čim manjšimi omejitvami“ ter da „so bili s tem prelomnim dokumentom vzpostavljeni politike in postopki za izmenjavo komunikacij, prevodov, analiz in informacij za dešifriranje med strokovnjaki Združenega kraljestva in ZDA za obveščevalno dejavnost“[130]. Ta sporazum je postal temelj tudi za druga partnerstva na področju obveščevalne dejavnosti z Avstralijo, Kanado in Novo Zelandijo.

193. Tajnost tega sporazuma in njegove posebne določbe so resen izziv v smislu jasnosti in predvidljivosti prava glede nadaljnje uporabe informacij, ki jih organi Združenega kraljestva zbirajo za namene državne varnosti, in njihovim razkritjem v tujini. V tem okviru EOVP opozarja, da je Sodišče EU, kar zadeva raven varstva, zagotovljenega v EU, poudarilo, da mora zakonodaja, ki vključuje poseganje v temeljno pravico do varstva osebnih podatkov, „določati jasna in natančna pravila, ki urejajo obseg in uporabo ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih podatkov. Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov. Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov“[131]. EOVP zato meni, da bi morala Evropska komisija v svoji oceni ustreznosti proučiti vpliv sporazuma o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA.

194. Evropsko sodišče za človekove pravice je v prvem delu svoje sodbe z dne 13. septembra 2018 v zadevi *Big Brother Watch* ocenilo ureditev izmenjave obveščevalnih podatkov v Združenem kraljestvu in zlasti sporazum o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA. Evropsko sodišče za človekove pravice je dejansko navedlo, da „zakonski okvir,

[130] Glej sporočilo Agencije ZDA za državno varnost za medije, GCHQ and NSA Celebrate 75 Years of Partnership, 5. februar 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

[131] Glej sodbo v zadevi Schrems I, točka 91.

ki obveščevalnim službam Združenega kraljestva dovoljuje, da od tujih obveščevalnih agencij zahtevajo prestreženo gradivo, ni vključen v Zakon o urejanju preiskovalnih pooblastil. Sporazum o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA z dne 5. marca 1946 izrecno dovoljuje izmenjavo gradiva med ZDA in Združenim kraljestvom“[132]. Evropsko sodišče za človekove pravice je menilo, da obstaja „pravna podlaga za zahtevanje obveščevalnih podatkov od tujih obveščevalnih agencij in da je pravo dovolj dostopno“[133]. Čeprav je Evropsko sodišče za človekove pravice sklenilo, da ni bil kršen člen 8[134] Evropske konvencije o človekovih pravicah, EOVP glede ureditve izmenjave obveščevalnih podatkov ugotavlja, da je bila ta sodba predložena velikemu senatu, ki še ni sprejel odločitve. EOVP ugotavlja še, da je sodnica Koskelo, ki se ji je pridružila sodnica Turković, v delno pritrdilnem in delno odklonilnem mnenju o tej sodbi[135] sklenila, da je bil kršen člen 8 Evropske konvencije o človekovih pravicah v zvezi z ureditvijo izmenjave obveščevalnih podatkov, pri čemer je navedla, da „se ni težko strinjati z načelom, da noben dogovor, v skladu s katerim se obveščevalni podatki iz prestreženih komunikacij pridobivajo prek tujih obveščevalnih služb, bodisi na podlagi zahtevkov za izvedbo takega prestrezanja ali za razkritje njegovih rezultatov, ne bi smel pomeniti izogibanja zaščitnim ukrepom, ki morajo biti vzpostavljeni za kakršen koli nadzor, ki ga izvajajo nacionalni organi (glej točke 216, 423 in 447). Dejansko kateri koli drug pristop ne bi bil verjeten“.

195. Kot je poudarjeno v več poročilih medijev in nevladnih organizacij[136, 137], zadnja objavljena različica sporazuma o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA sega v leto 1956, od takrat pa sta se komunikacijska tehnologija in narava obveščevalnih dejavnosti SIGINT močno spremenila. Poročila medijev so na primer razkrila, da podatke, ki prek podmorskih kablov prehajajo v Združeno kraljestvo, prestreza vladna obveščevalna služba in jih daje na voljo Agenciji za državno varnost[138].

196. Za EOVP je ključno vprašanje glede izmenjave obveščevalnih podatkov, ali bodo člen 109 Zakona o varstvu podatkov iz leta 2018 in določbe Zakona o preiskovalnih pooblastilih iz leta 2016 še naprej veljali, ko bodo obveščevalne službe Združenega kraljestva delovale v skladu s sporazumom o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA. Drug ključni element, ki ga je treba oceniti, je, ali določbe ali učinkovita uporaba tega sporazuma vplivajo na raven varstva osebnih podatkov, ki so v tranzitu med EGP in Združenim kraljestvom, ali omogočajo neposreden dostop do osebnih podatkov in njihovo pridobivanje s strani obveščevalnih služb tretjih držav.

197. Zato je **EOVP**, poleg zadržkov, izraženih glede „razkritij v tujini“ na podlagi dela 4 Zakona o varstvu podatkov iz leta 2018 in z njim povezane izjeme glede državne varnosti, ter zahtev v okviru Zakona o preiskovalnih pooblastilih iz leta 2016, **zaskrbljen zaradi drugih oblik izmenjave informacij in razkritij, na podlagi drugih instrumentov, zlasti različnih mednarodnih sporazumov, sklenjenih med**

---

[132] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, točka 425.
[133] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, točka 427.
[134] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, točka 448.
[135] Glej sodbo Evropskega sodišča za človekove pravice v zadevi *Big Brother Watch*, delno pritrdilno in delno odklonilno mnenje sodnice Koskelo, ki se ji je pridružila sodnica Turković.
[136] Glej BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5. marec 2021, https://www.bbc.com/news/uk-56284453.
[137] Glej Privacy International, Policy Briefing – UK Intelligence Sharing Arrangements, april 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Glej The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21. junij 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Združenim kraljestvom in tretjimi državami, zlasti ti instrumenti ostajajo nedostopni za javnost, kot je sporazum o pridobivanju obveščevalnih podatkov s prestrezanjem komunikacij med Združenim kraljestvom in ZDA. Učinek takega sporazuma bi lahko privedel do izogibanja zaščitnim ukrepom, opredeljenim v zvezi z dostopom do osebnih podatkov in njihovo uporabo za namene državne varnosti.

198. EOVP se dejansko strinja z mnenjem posebnega poročevalca Združenih narodov Joeja Cannataccija, da „izmenjava obveščevalnih podatkov ne sme voditi do prikritega pridobivanja obveščevalnih podatkov ali olajševanja drugim, da pridobijo obveščevalne podatke brez nacionalnih zaščitnih ukrepov, niti ustvarjati vrzeli, ki bi tujim vladam z nižjimi standardi na področju varstva zasebnosti (ali drugih človekovih pravic) omogočila pridobivanje obveščevalnih podatkov od obveščevalnih služb Združenega kraljestva in bi lahko povzročila kršitve človekovih pravic“[139].

199. Poleg tega **EOVP meni, da lahko sklenitev dvostranskih in večstranskih sporazumov s tretjimi državami za namene sodelovanja na področju obveščevalne dejavnosti, ki bi zagotavljali pravno podlago za neposredno prestrezanje in pridobivanje osebnih podatkov ali prenos osebnih podatkov v te države, znatno vpliva tudi na pogoje za nadaljnjo uporabo zbranih informacij, saj bodo taki sporazumi verjetno vplivali na pravni okvir Združenega kraljestva za varstvo podatkov, kot je bil ocenjen.**

4.3.3 Nadzor

200. EOVP poudarja pomen celovitega nadzora s strani neodvisnih nadzornih organov za ustrezno raven varstva podatkov. Jamstvo neodvisnosti nadzornih organov v smislu člena 8(3) Listine EU o temeljnih pravicah je namenjeno zagotovitvi učinkovitega in zanesljivega spremljanja skladnosti s pravili o varstvu posameznikov pri obdelavi osebnih podatkov.

201. Če se do osebnih podatkov dostopa ali se ti uporabljajo za namene državne varnosti, funkcijo nadzora večinoma opravljata pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil in pravosodni pooblaščenci (v nadaljevanju: pravosodni pooblaščenci).

202. **EOVP na splošno priznava vključitev pravosodnih pooblaščencev v Zakon o preiskovalnih pooblastilih iz leta 2016 kot znatno izboljšavo.** V skladu z zgoraj navedeno zahtevo je Evropska komisija pozvana, naj **podrobneje** oceni neodvisnost **pravosodnih pooblaščencev in zlasti, v kakšnem obsegu je neodvisnost pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil in urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil zakonsko zaščitena, saj to v Zakonu o preiskovalnih pooblastilih iz leta 2016 ni navedeno.** To je še toliko pomembneje, ker pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil odloča o pritožbah vlade, če pravosodni pooblaščenec zavrne zahtevek za nadzorni **ukrep**.

203. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil opravlja funkciji predhodnega in naknadnega nadzora. Glede predhodnega nadzora EOVP razume, da so pravosodni pooblaščenci zadolženi za odobritev, v posameznem primeru, različnih nadzornih ukrepov, vključno s ciljno usmerjenim prestrezanjem in množičnim pridobivanjem komunikacijskih podatkov. EOVP nadalje

[139] Glej zaključek izjave o opravljeni misiji posebnega poročevalca za pravico do zasebnosti ob zaključku njegove misije v Združenem kraljestvu Velika Britanija in Severna Irska, London, 29. junij 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

ugotavlja, da predhodne odobritve nadzornih ukrepov ni mogoče izpeljati iz sodne prakse Sodišča EU kot absolutne zahteve za sorazmernost nadzornih ukrepov[140].

204. Vendar EOVP meni, da je treba za oceno učinkovitosti te ravni nadzora podrobneje pojasniti scenarije, za katere je mogoče zakonito prestrezanje brez prehodne odobritve pravosodnih pooblaščencev.

205. Evropska komisija v sprotnih opombah 201 in 266 osnutka sklepa navaja „nekatere omejene primere“, ki so določeni v členih 44 do 52 Zakona o preiskovalnih pooblastilih iz leta 2016 glede ciljno usmerjenega prestrezanja. EOVP ugotavlja, da so členi 45 do 51 Zakona o preiskovalnih pooblastilih iz leta 2016 izjeme, za katere se šteje, da jih obveščevalne službe ne uporabljajo redno. Poleg tega **EOVP razume**, da se v **primerih, v katerih se uporabljajo izjeme** (na primer ponudniki telekomunikacijskih in poštnih storitev), predhodna odobritev pravosodnih pooblaščencev izvede, če organi kazenskega pregona ali obveščevalne službe **zahtevajo** dostop do teh podatkov, **in Evropsko komisijo poziva, naj v svojem sklepu potrdi, da to drži.**

206. EOVP priznava, da člen 44(2) Zakona o preiskovalnih pooblastilih iz leta 2016 dovoljuje prestrezanje komunikacij, če z njo soglaša ena od strani (pošiljatelj ali prejemnik) in obstaja dovoljenje v skladu z Zakonom o urejanju preiskovalnih pooblastil iz leta 2000 ali Zakonom o urejanju preiskovalnih pooblastil iz leta 2000, ki se uporablja na Škotskem (škotski uradni list (*Acts of the Scottish Parliament*) 2000, št. 11). EOVP Evropsko komisijo **poziva**, naj pojasni, ali to pomeni, da se v primerih, v katerih je soglasje enostransko, predhodna odobritev sploh ne uporablja.

207. Pri naknadnem nadzoru je pomembno preveriti tudi, ali se učinkovit neodvisni nadzor zagotavlja brez vrzeli, zlasti če ni predviden naknadni nadzor.

208. EOVP ugotavlja, da pravosodni pooblaščenci v skladu s členi 48–52 Zakona o preiskovalnih pooblastilih iz leta 2016 izvajajo naknadni pregled, in **Evropsko komisijo poziva, naj pojasni, v skladu s katerimi zahtevami in na čigavo pobudo se izvede tak naknadni pregled**.

209. V skladu s členom 229(4) Zakona o preiskovalnih pooblastilih iz leta 2016 pregled izvajanja nekaterih funkcij ni potreben. V zvezi s tem EOVP Evropsko komisijo poziva, naj pojasni določbe člena 229(4)(d) in (e) Zakona o preiskovalnih pooblastilih iz leta 2016 glede njegovega praktičnega vpliva na pristojnost pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za pregled. **EOVP razume, da je urad informacijskega pooblaščenca pristojen nadzorni organ v primeru uporabe izjem iz člena 229(4) Zakona o preiskovalnih pooblastilih iz leta 2016, in Evropsko komisijo poziva, naj v svojem sklepu potrdi, da to drži.**

210. **Zdi se, da je pri izvajanju** naknadnega nadzora vloga **pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil omejena** na dajanje priporočil v primerih neskladnosti in obveščanje o tem posameznika, na katerega se nanašajo osebni podatki, če gre za hudo napako in je obveščanje osebe v javnem interesu. **EOVP Evropsko komisijo poziva, naj pojasni, kako lahko urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil učinkovito zagotavlja spoštovanje zakonodaje.**

211. **Nazadnje, EOVP razume, da se prizadeti posamezniki ne morejo obrniti neposredno na urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, ampak morajo vložiti pritožbo pri uradu informacijskega pooblaščenca, ki pa ima omejene pristojnosti na področju državne varnosti. Zato EOVP Evropsko komisijo poziva, naj dodatno pojasni, kako je pravno zagotovljeno, da urad**

[140] Vendar ugotavlja tudi, da je bilo Sodišče EU, ko je razveljavilo zasebnostni ščit v zadevi Schrems II, seznanjeno, da pravo ZDA, tako imenovano sodišče FISA, „ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe (kot sta programa PRISM in UPSTREAM) na podlagi letnih potrdil“ (točka 179).

pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil v teh primerih obravnava pritožbe.

4.3.4 Pravno varstvo

212. Ob upoštevanju sodb Sodišča EU v zadevah Schrems I in Schrems II je jasno, da je učinkovito sodno varstvo v smislu člena 47 Listine EU o temeljnih pravicah temeljnega pomena za predpostavko o ustreznosti prava tretje države. Sodbi sta tudi pokazali, da je treba posebno pozornost glede tega nameniti učinkovitemu sodnemu varstvu na področju dostopa do osebnih podatkov za potrebe državne varnosti.

213. **EOVP priznava, da je Združeno kraljestvo vzpostavilo sodišče, ki obravnava preiskovalna pooblastila. To sodišče ni pristojno le za obravnavo zadev o uporabi preiskovalnih pooblastil organov kazenskega pregona, ampak tudi obveščevalnih služb. EOVP razume, da sodišče, ki obravnava preiskovalna pooblastila, deluje kot ustrezno sodišče v smislu člena 47 Listine o temeljnih pravicah. Kar zadeva njegova pooblastila, je Evropska komisija pozvana, naj potrdi, da ima vsa pooblastila, navedena v uvodni izjavi 262 osnutka sklepa, ne glede na pravno podlago, na kateri temelji pritožba.**

214. Prikriti nadzor, ki ga izvajajo obveščevalne agencije, pogosto pomeni, da objekt nadzora, tj. posameznik, na katerega se nanašajo osebni podatki, ni in ne bo seznanjen z nadzorom. V tem okviru je EOVP, ko je moral proučiti pravo ZDA, večkrat izrazil pomisleke glede zahteve za „procesno upravičenje“, kot jo razlaga pravo ZDA, v primerih nadzora. Glede na to EOVP ugotavlja, da je za pritožbo pri sodišču, ki obravnava preiskovalna pooblastila, potreben samo preskus razumne domneve, v skladu s katerim mora pritožnik dokazati, da je v morebitni nevarnosti za izpostavljenost ukrepu.

215. EOVP pri proučevanju sodišča, ki obravnava preiskovalna pooblastila, posebno pozornost namenja dejstvu, da je bilo večkrat ugotovljeno, da je njegovo delovanje skladno z Evropsko konvencijo o človekovih pravicah, kot jo razlaga Evropsko sodišče za človekove pravice.