Mišljenje 14/2021 o nacrtu provedbene odluke Europske komisije na temelju Uredbe (EU) 2016/679 o primjerenosti zaštite osobnih podataka u Ujedinjenoj Kraljevini

Doneseno 13. travnja 2021.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

SADRŽAJ

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (s) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „Opća uredba o zaštiti podataka"),

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru (dalje u tekstu „EGP") te posebno njegov Prilog XI. i Protokol 37. kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 12. i 22. svojeg Poslovnika,

DONIO JE SLJEDEĆE MIŠLJENJE:

1. SAŽETAK

1. Europska komisija potvrdila je 19. veljače 2021.[2] svoj nacrt provedbene odluke (dalje u tekstu „nacrt odluke") o primjerenosti zaštite osobnih podataka u Ujedinjenoj Kraljevini na temelju Opće uredbe o zaštiti podataka. Nakon toga Europska komisija pokrenula je postupak za njezino službeno donošenje.

2. Istog je dana Europska komisija zatražila mišljenje Europskog odbora za zaštitu podataka (dalje u tekstu „EOZP")[3]. EOZP je svoju procjenu primjerenosti razine zaštite osigurane u Ujedinjenoj Kraljevini proveo na temelju ispitivanja samog nacrta odluke te na temelju analize dokumentacije koju je Europska komisija stavila na raspolaganje.

3. EOZP se usredotočio na procjenu općih aspekata nacrta odluke povezanih s Općom uredbom o zaštiti podataka i na pristup javnih tijela osobnim podacima prenesenima iz EGP-a za potrebe izvršavanja zakonodavstva i nacionalne sigurnosti, uključujući pravne lijekove dostupne pojedincima u EGP-u. EOZP je procjenjivao i jesu li zaštitne mjere predviđene pravnim okvirom Ujedinjene Kraljevine uspostavljene i djelotvorne.

4. EOZP je u tom radu kao glavni referentni dokument upotrijebio svoj Referentni dokument o primjerenosti u skladu s Općom uredbom o zaštiti podataka[4], donesen u veljači 2018., i Preporuke EOZP-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora[5].

[1] Upućivanja na „države članice" u ovom Mišljenju treba tumačiti kao upućivanja na „države članice EGP-a".
[2] Vidjeti priopćenje za medije Europske komisije, Zaštita podataka: Europska komisija pokreće postupak u vezi s prijenosom osobnih podataka Ujedinjenoj Kraljevini, 19. veljače 2021., https://ec.europa.eu/commission/presscorner/detail/hr/ip_21_661.
[3] Idem.
[4] Vidjeti Referentni dokument o primjerenosti Radne skupine iz članka 29., donesen 6. veljače 2018., WP 254 rev.01 (potvrdio EOZP, vidjeti https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (dalje u tekstu „Referentni dokument o primjerenosti").
[5] Vidjeti Preporuke EOZP-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora, donesene 10. studenoga 2020., https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_hr.

1.1. Područja konvergencije

5. Ključni je cilj EOZP-a dati mišljenje Europskoj komisiji o primjerenosti razine zaštite osigurane pojedincima u Ujedinjenoj Kraljevini. Važno je uzeti u obzir da EOZP ne očekuje da pravni okvir Ujedinjene Kraljevine bude preslika europskog prava o zaštiti podataka.

6. Međutim, EOZP podsjeća na to da se člankom 45. Opće uredbe o zaštiti podataka i sudskom praksom Suda Europske unije (dalje u tekstu „Sud EU-a") zahtijeva da se zakonodavstvom treće zemlje poštuje bit temeljnih načela sadržanih u Općoj uredbi o zaštiti podataka kako bi se moglo smatrati da je osigurana primjerena razina zaštite. Okvir Ujedinjene Kraljevine za zaštitu podataka uvelike se temelji na okviru EU-a za zaštitu podataka (posebno na Općoj uredbi o zaštiti podataka i Direktivi (EU) 2016/680 Europskog parlamenta i Vijeća, dalje u tekstu „Direktiva EU-a o zaštiti podataka pri izvršavanju zakonodavstva"), što proizlazi iz činjenice da je Ujedinjena Kraljevina bila država članica EU-a sve do 31. siječnja 2020. Osim toga, Zakonom Ujedinjene Kraljevine o zaštiti podataka iz 2018., koji je stupio na snagu 23. svibnja 2018. i kojim je izvan snage stavljen Zakon Ujedinjene Kraljevine o zaštiti podataka iz 1998., dodatno se, uz prenošenje Direktive EU-a o zaštiti podataka pri izvršavanju zakonodavstva, utvrđuje primjena Opće uredbe o zaštiti podataka u pravu Ujedinjene Kraljevine te se dodjeljuju ovlasti i uvode obveze za nacionalno nadzorno tijelo za zaštitu podataka, odnosno Ured povjerenika Ujedinjene Kraljevine za informiranje. Stoga EOZP potvrđuje da okvir Ujedinjene Kraljevine za zaštitu podataka najvećim dijelom odražava Opću uredbu o zaštiti podataka.

7. **Iz analize prava i prakse treće zemlje koja je donedavno bila država članica EU-a jasno je da je EOZP utvrdio da su mnogi aspekti u načelu istovjetni.**

8. Kad je riječ o području zaštite podataka, EOZP navodi da su okvir Opće uredbe o zaštiti podataka i pravni okvir Ujedinjene Kraljevine u velikoj mjeri usklađeni u pogledu određenih ključnih odredbi kao što su pojmovi (npr. „osobni podaci", „obrada osobnih podataka", „voditelj obrade podataka"), osnove za zakonitu i pravednu obradu u zakonite svrhe, ograničenje svrhe, kvaliteta podataka i razmjernost, zadržavanje, sigurnost i povjerljivost podataka, transparentnost, posebne kategorije podataka, izravni marketing, automatizirano donošenje odluka i izrada profila.

1.2. Otvorena pitanja

9. Ujedinjena Kraljevina donedavno je bila država članica EU-a te je stoga EOZP pri analizi njezina prava i prakse utvrdio da su mnogi aspekti u načelu istovjetni. S obzirom na svoju ulogu u postupku donošenja nalaza o primjerenosti, ali i vremenska ograničenja, EOZP se odlučio usredotočiti na one aspekte za koje smatra da ih je potrebno pobliže razmotriti i detaljnije pregledati.

10. Međutim, neka pitanja ostaju otvorena i EOZP smatra da bi stavke navedene u nastavku trebalo dodatno procijeniti kako bi se osigurala u načelu istovjetna razina zaštite i da bi Europska komisija trebala pomno pratiti te aspekte u Ujedinjenoj Kraljevini.

1.2.1. Općenito

11. Prvi je otvoreno pitanje općenito, a odnosi se na praćenje razvoja pravnog sustava Ujedinjene Kraljevine za zaštitu podataka u cjelini. Vlada Ujedinjene Kraljevine doista je izrazila namjeru da razvije zasebne i neovisne politike u području zaštite podataka s mogućnošću odstupanja od zakonodavstva EU-a o zaštiti podataka. Te političke izjave još se nisu konkretizirale u pravnom okviru Ujedinjene Kraljevine. Međutim, to moguće buduće **odstupanje moglo bi ugroziti razinu zaštite osobnih podataka koji se prenose iz EU-a**. **Stoga se Europska komisija poziva da pomno prati takve**

promjene od stupanja na snagu njezine odluke o primjerenosti i poduzme potrebne mjere, uključujući izmjenu i/ili suspenziju odluke, prema potrebi.

1.2.2. Opći aspekti zaštite podataka

12. Prvo, takozvano „**izuzeće o useljavanju**", utvrđeno u **dijelu 1.** stavku 4. **Priloga 2. Zakonu o zaštiti podataka iz 2018. „široko" je formulirano.** Točnije, primjenjuje se i u slučaju kad voditelj obrade ne prikuplja osobne podatke u svrhu kontrole useljavanja, ali ih stavlja na raspolaganje drugom voditelju obrade koji te osobne podatke obrađuje u svrhu kontrole useljavanja.

13. EOZP poziva Europsku komisiju da provjeri trenutačno stanje postupka u predmetu Open Rights Group & Anor, R (na zahtjev) protiv Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) i, s obzirom na to da ta presuda nije konačna (*res judicata*), da provjeri je li potvrđena ili revidirana presudom u žalbenom postupku, uzme u obzir eventualne izmjene u tom pogledu i navede ih u odluci. **EOZP poziva Europsku komisiju i da u odluci o primjerenosti navede dodatne informacije o izuzeću o useljavanju[6], posebno s obzirom na nužnost i razmjernost takvog širokog izuzeća u pravu Ujedinjene Kraljevine te na široko područje primjene *ratione personae*.** EOZP osim toga poziva Europsku komisiju da dodatno istraži postoje li odnosno bi li se mogle predvidjeti dodatne zaštitne mjere u pravnom okviru Ujedinjene Kraljevine, na primjer s pomoću pravno obvezujućih instrumenata kojima bi se izuzeće o useljavanju dopunilo povećanjem njegove predvidljivosti i zaštitnih mjera za ispitanike te omogućili bolja i brža procjena i praćenje zahtjeva u pogledu nužnosti i razmjernosti.

14. Drugo, iako EOZP uviđa da je Ujedinjena Kraljevina najvećim dijelom preslikala poglavlje V. Opće uredbe o zaštiti podataka u svoj okvir za zaštitu podataka, utvrdio je određene aspekte pravnog okvira Ujedinjene Kraljevine **u pogledu daljnjih prijenosa** koji bi mogli ugroziti razinu zaštite osobnih podataka koji se prenose iz EGP-a.

15. Naime, člankom 44. Opće uredbe o zaštiti podataka[7] propisano je da se prijenosi i daljnji prijenosi osobnih podataka odvijaju jedino ako nije ugrožena razina zaštite pojedinaca zajamčena tom uredbom. **To znači ne samo da zakonodavstvo Ujedinjene Kraljevine mora biti „u načelu istovjetno" zakonodavstvu EU-a u pogledu obrade osobnih podataka koji se prenose u Ujedinjenu Kraljevinu na temelju buduće odluke o primjerenosti, već i da se pravilima koja se u Ujedinjenoj Kraljevini primjenjuju na daljnji prijenos tih podataka u treće zemlje mora osigurati zadržavanje u načelu istovjetne razine zaštite.**

16. Iako EOZP uzima u obzir mogućnost da Ujedinjena Kraljevina na temelju svojeg pravnog okvira smatra da neka područja pružaju primjerenu razinu zaštite podataka s obzirom na okvir Ujedinjene Kraljevine za zaštitu podataka, želi istaknuti da ta područja zasad možda neće imati pozitivnu odluku

[6] Među ostalim i kao ishod trenutačnog preispitivanja primjene izuzeća o useljavanju spomenutog na str. 5. Okvira vlade Ujedinjene Kraljevine za obrazloženje rasprava o primjerenosti, odjeljak E3: Prilog 2. Ograničenja, 13. ožujka 2020., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

[7] „Svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju odvija se jedino ako, u skladu s drugim odredbama ove Uredbe, voditelj obrade i izvršitelj obrade djeluju u skladu s uvjetima iz ovog poglavlja koji vrijede i za daljnje prijenose osobnih podataka iz treće zemlje ili međunarodne organizacije u još jednu treću zemlju ili međunarodnu organizaciju. Sve odredbe iz ovog poglavlja primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca zajamčena ovom Uredbom."

Europske komisije o primjerenosti u svoju korist niti će moći osigurati razinu zaštite koja je „u načelu istovjetna" razini zajamčenoj u EU-u. To bi moglo dovesti do rizika u pogledu zaštite osobnih podataka koji se prenose iz EGP-a, posebno ako se u budućnosti okvir Ujedinjene Kraljevine bude razlikovao od pravne stečevine EU-a. Osim toga, Ujedinjena Kraljevina već je kao primjerene priznala treće zemlje za koje je Europska komisija donijela nalaz o primjerenosti u skladu s Direktivom 95/46/EZ[8], no Europska komisija uskoro će preispitati te nalaze, a zaključci tog preispitivanja još nisu poznati.

17. **U prethodno navedenim situacijama Europska komisija trebala bi izvršiti svoju funkciju praćenja i, ako se ne zadrži u načelu istovjetna razina zaštite osobnih podataka prenesenih iz EGP-a, razmotriti izmjenu odluke o primjerenosti radi uvođenja posebnih zaštitnih mjera za podatke prenesene iz EGP-a i/ili suspendirati odluku o primjerenosti.**

18. **Kad je riječ o međunarodnim sporazumima koje su sklopile Ujedinjena Kraljevina i treće zemlje,** Europska komisija poziva se da ispita povezanost okvira Ujedinjene Kraljevine za zaštitu podataka i njezinih međunarodnih obveza, i izvan okvira Sporazuma o pristupu elektroničkim podacima za potrebe suzbijanja teških kaznenih djela koji su sklopili Ujedinjena Kraljevina i Sjedinjene Američke Države (dalje u tekstu „SAD")[9] (dalje u tekstu „Sporazum UK-a i SAD-a o zakonu CLOUD"), posebno kako bi se osigurala neprekinuta razina zaštite osobnih podataka koji se prenose iz EU-a u Ujedinjenu Kraljevinu na temelju odluke o primjerenosti za Ujedinjenu Kraljevinu i koji se zatim dalje prenose u druge treće zemlje, te da neprekidno prati situaciju i prema potrebi poduzme mjere u slučaju da sklapanje međunarodnih sporazuma između Ujedinjene Kraljevine i trećih zemalja ugrozi razinu zaštite osobnih podataka predviđenu u EU-u.

19. Nadalje, Europska komisija poziva se da prati jamče li se Sporazumom UK-a i SAD-a o zakonu CLOUD odgovarajuće dodatne zaštitne mjere s obzirom na razinu osjetljivosti predmetnih kategorija podataka i isključive zahtjeve u pogledu izravnog prijenosa elektroničkih dokaza s pružatelja usluga, a ne između tijela, procjenjujući i okolnosti u kojima se zaštitne mjere mogu predvidjeti odgovarajućom prilagodbom Krovnog sporazuma EU-a i SAD-a[10].

20. Osim toga, EOZP navodi da se daljnji prijenosi mogu odvijati i iz Ujedinjene Kraljevine u treću zemlju na temelju **alata za prijenos podataka u skladu s primjenjivim zakonodavstvom Ujedinjene Kraljevine o zaštiti podataka[11]**. Na temelju presude u predmetu Schrems II[12] EOZP poziva Europsku komisiju da odlukom o primjerenosti zajamči djelotvornu uspostavu zaštitnih mjera uzimajući u obzir i zakonodavstvo treće zemlje primateljice.

21. Kad je riječ o nepostojanju **zaštitnih mjera propisanih na temelju članka 48. Opće uredbe o zaštiti podataka** u zakonodavstvu Ujedinjene Kraljevine, EOZP poziva Europsku komisiju da iznese dodatna jamstva i konkretna upućivanja na zakonodavstvo Ujedinjene Kraljevine kojima se osigurava da je

[8] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL L 281, 23.11.1995., str. 31.).

[9] Vidjeti Sporazum između Vlade Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske i Vlade Sjedinjenih Američkih Država o pristupu elektroničkim podacima za potrebe suzbijanja teških kaznenih djela, Washington DC, SAD, 3. listopada 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] Vidjeti Sporazum između Sjedinjenih Američkih Država i Europske unije o zaštiti osobnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i progonom kaznenih djela, prosinac 2016. (dalje u tekstu „Krovni sporazum EU-a i SAD-a"), https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=LEGISSUM%3A3104_8.

[11] Vidjeti članke 46. i 47. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka.

[12] Vidjeti presudu u predmetu Schrems II.

razina zaštite na temelju pravnog okvira Ujedinjene Kraljevine u načelu istovjetna razini zaštite zajamčenoj u EGP-u.

22. Kad je riječ o **postupovnim i provedbenim mehanizmima**, EOZP navodi da su postojanje i djelotvorno funkcioniranje neovisnog nadzornog tijela, postojanje sustava kojim se osigurava dobra razina usklađenosti te sustav pristupa odgovarajućim mehanizmima pravne zaštite zahvaljujući kojima pojedinci u EGP-u mogu ostvariti svoja prava i zatražiti pravnu zaštitu bez opterećujućih prepreka administrativnoj i sudskoj zaštiti ključne značajke koje okvir za zaštitu podataka usklađen s europskim okvirom mora imati.
23. EOZP prima na znanje da je Ujedinjena Kraljevina najvećim dijelom preslikala odgovarajuće odredbe Opće uredbe o zaštiti podataka u svojoj Općoj uredbi o zaštiti podataka i Zakonu o zaštiti podataka iz 2018. Ipak, Europska komisija poziva se da kontinuirano prate sve promjene u pravnom okviru i praksi Ujedinjene Kraljevine koje bi mogle štetno utjecati na ta područja.

1.2.3. Pristup javnih tijela podacima prenesenima u Ujedinjenu Kraljevinu

24. EOZP prima na znanje znatne promjene pravnog okvira Ujedinjene Kraljevine koje se odnose na sigurnosne i obavještajne agencije, a posebno na presretanje i pribavljanje komunikacijskih podataka. EOZP razumije da su te promjene, među ostalim, posljedica postupaka pokrenutih u tom kontekstu pred Sudom EU-a i Europskim sudom za ljudska prava (dalje u tekstu „ESLJP”) te presuda donesenih u tim postupcima.

25. EOZP posebno pozdravlja činjenicu da je Ujedinjena Kraljevina osnovala Sud za istražne ovlasti. Sud za istražne ovlasti nadležan je za predmete koji proističu iz toga kako se tijela za izvršavanje zakonodavstva, ali i obavještajne službe, koriste svojim istražnim ovlastima. EOZP stoga smatra da Sud za istražne ovlasti ima funkciju valjanog suda u smislu članka 47. Povelje Europske unije o temeljnim pravima (dalje u tekstu „Povelja EU-a”).

26. Osim toga, EOZP smatra da je uvođenje „pravosudnih povjerenika” u Zakonu o istražnim ovlastima iz 2016. pozitivan i velik napredak. Razumije da je važna funkcija pravosudnih povjerenika *ex ante* odobravati mjere nadzora u pojedinačnim slučajevima, uključujući ciljano presretanje i masovno pribavljanje komunikacijskih podataka (takozvani postupak „dvostruke zaštite”).

27. Međutim, EOZP smatra da je za procjenu djelotvornosti te dodatne razine nadzora potrebno detaljnije pojasniti scenarije u kojima je moguće zakonito presretanje bez odobrenja povjerenika za istražne ovlasti ili pravosudnih povjerenika te poziva Europsku komisiju da provede dodatnu procjenu i dokaže da su, čak i u slučajevima u kojima se ne primjenjuje postupak dvostruke zaštite, pravnim okvirom Ujedinjene Kraljevine predviđene odgovarajuće zaštitne mjere, uključujući djelotvoran *ex post* nadzor i mogućnosti pravne zaštite za pojedince, čime se osigurava razina zaštite koja je u načelu istovjetna razini osiguranoj u EU-u.

28. Nadalje, EOZP poziva Europsku komisiju da dodatno procijeni uvjete pod kojima se može pozvati na hitnost te da razjasni moguće načine ostvarivanja prava dotičnih ispitanika i moguće oblike pravne zaštite koji su im dostupni u kontekstu operacija ometanja opreme, posebno u slučaju odstupanja od postupka dvostruke zaštite.

29. EOZP smatra i da postoji potreba za dodatnim pojašnjenjem i procjenom masovnih presretanja, posebno s obzirom na odabir i primjenu čimbenika za odabir, kako bi se razjasnilo u kojoj mjeri pristup osobnim podacima zadovoljava prag koji je utvrdio Sud EU-a i koje su zaštitne mjere uspostavljene radi zaštite temeljnih prava pojedinaca čiji se osobni podaci presreću u tom kontekstu, uključujući one koje se odnose na razdoblja zadržavanja podataka. Posebno bi korisna bila neovisna

procjena nadležnih nadzornih tijela Ujedinjene Kraljevine. EOZP ističe i da se još važnijim čini da „komunikacija povezana s inozemstvom" u okviru postupaka masovnog presretanja naizgled upućuje na to da bi Ujedinjena Kraljevina mogla izravno presretati i masovno prikupljati podatke u EU-u, uključujući podatke u tranzitu između EU-a i Ujedinjene Kraljevine koji bi bili obuhvaćeni područjem primjene nacrta odluke. S obzirom na važnost tog aspekta EOZP poziva Europsku komisiju da pomno prati razvoj događaja u tom pogledu.

30. U pogledu masovnog presretanja EOZP ističe i dosljednu procjenu ESLJP-a i Suda EU-a te podsjeća na iskazane sumnje u pogledu sekundarnih podataka, na koje bi se zbog njihove osjetljivosti trebale primjenjivati posebne zaštitne mjere. EOZP stoga poziva Europsku komisiju da pažljivo procijeni jamči li se zaštitnim mjerama predviđenima pravom Ujedinjene Kraljevine za tu kategoriju osobnih podataka razina zaštite koja je u načelu istovjetna razini zajamčenoj u EGP-u.

31. U tom je kontekstu EOZP svjestan činjenice da se javno izvješće Odbora za obavještajne poslove i sigurnost o izvršavanju masovnih ovlasti iz 2016.[13] odnosi na postupke u skladu s prethodnim pravnim okvirom, koji je 2016. zamijenjen Zakonom o istražnim ovlastima. Ipak, vidljiva je potreba za daljnjom neovisnom procjenom i nadzorom alata za automatiziranu obradu kojima se služe nadležna nadzorna tijela Ujedinjene Kraljevine pa EOZP poziva Europsku komisiju da dodatno procijeni to pitanje i zaštitne mjere koje bi se u tom kontekstu osigurale i/ili mogle osigurati ispitanicima iz EGP-a.

32. EOZP dijeli stajalište povjerenika za istražne ovlasti da je potrebno daljnje preispitivanje i praćenje kako bi se osiguralo da se zadrže zaštitne mjere koje nadležna tijela u području nacionalne sigurnosti i obavještajnih poslova primjenjuju u praksi radi ispravljanja neusklađenosti s primjenom mjerodavnog zakonodavstva i da se nastave poboljšavati. EOZP pozdravlja i činjenicu da je zbog navedenog povjerenik za istražne ovlasti proveo preispitivanje svojeg pristupa ispitivanju masovnog presretanja 2019., „koje je uključivalo pažljivo preispitivanje tehnički složenih načina na koje se masovno presretanje zapravo provodi" te se obvezao uključiti „detaljan pregled čimbenika za odabir i kriterija pretraživanja na koje je prethodno uputio ESLJP" u ispitivanje masovnog presretanja od 2020. nadalje. S obzirom na važnost tog aspekta EOZP je zabrinut jer povjerenik za istražne ovlasti još nije proveo detaljno ispitivanje čimbenika za odabir i kriterija pretraživanja te poziva Europsku komisiju da pomno prati razvoj događaja u tom pogledu, posebno jer konkretan oblik tog nadzora tek treba razjasniti.

33. Kad je riječ o otkrivanju podataka povezanom s inozemstvom, EOZP ističe da primjena izuzeća za nacionalnu sigurnost predviđenog pravom Ujedinjene Kraljevine može dovesti do izostanka zaštitnih mjera kojima se osigurava poštovanje načela ograničenja svrhe, nužnosti i razmjernosti ili kojima se predviđa da će se u trećoj zemlji odredišta u dostatnoj mjeri osigurati ili poštovati prava pojedinaca, nadzor i pravna zaštita. EOZP stoga preporučuje Europskoj komisiji da dodatno ispita opće zaštitne mjere predviđene pravom Ujedinjene Kraljevine za otkrivanje podataka povezano s inozemstvom, posebno s obzirom na primjenu izuzeća za nacionalnu sigurnost.

34. Naposljetku, EOZP ima dvojbe u pogledu ostalih oblika razmjene i otkrivanja informacija na temelju drugih instrumenata, a posebno raznih međunarodnih sporazuma koje je Ujedinjena Kraljevina sklopila s drugim trećim zemljama, osobito ako ti instrumenti nisu dostupni javnosti, primjerice

[13] Vidjeti *Report of the bulk powers review* (Izvješće o preispitivanju masovnih ovlasti), koje je sastavio neovisni revizor zakonodavstva o terorizmu, kolovoz 2016., https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

Sporazum UK-a i SAD-a o komunikacijskoj obavještajnoj djelatnosti. Takav bi sporazum mogao dovesti do zaobilaženja zaštitnih mjera utvrđenih za pristup osobnim podacima i njihovu upotrebu za potrebe nacionalne sigurnosti. EOZP smatra da sklapanje bilateralnih ili multilateralnih sporazuma s trećim zemljama u svrhu obavještajne suradnje, koji čine pravnu osnovu za izravno presretanje i pribavljanje osobnih podataka ili prijenos osobnih podataka u te zemlje, može znatno utjecati i na uvjete za daljnju upotrebu prikupljenih informacija jer će takvi sporazumi vjerojatno utjecati na procijenjeni pravni okvir Ujedinjene Kraljevine za zaštitu podataka.

1.3. Zaključak

35. EOZP smatra da je procjena primjerenosti za Ujedinjenu Kraljevinu jedinstvena zbog prethodnog statusa Ujedinjene Kraljevine kao države članice EU-a. Osim toga, bila bi to prva odluka o primjerenosti koja uključuje klauzulu o vremenskom ograničenju valjanosti.

36. U skladu s tim EOZP uviđa da postoje brojna područja konvergencije između okvira za zaštitu podataka Ujedinjene Kraljevine i EU-a. Ipak, nakon pažljive analize nacrta odluke Europske komisije i zakonodavstva Ujedinjene Kraljevine o zaštiti podataka EOZP je utvrdio niz otvorenih pitanja koja se opširno ispituju u ovom mišljenju. U tom kontekstu EOZP želi naglasiti ključnu ulogu Europske komisije u praćenju svih relevantnih promjena u Ujedinjenoj Kraljevini.

37. S obzirom na navedeno EOZP preporučuje Europskoj komisiji da radi na rješavanju otvorenih pitanja navedenih u ovom mišljenju. Osim toga, EOZP poziva Europsku komisiju da pomno prati sve relevantne promjene u Ujedinjenoj Kraljevini koje mogu utjecati na bitnu ekvivalentnost osobnih podataka te da prema potrebi brzo poduzme odgovarajuće mjere.

2. UVOD

2.1. Okvir Ujedinjene Kraljevine za zaštitu podataka

38. Okvir Ujedinjene Kraljevine za zaštitu podataka uvelike se temelji na okviru EU-a za zaštitu podataka (posebno na Općoj uredbi o zaštiti podataka i Direktivi o izvršavanju zakonodavstva), što proizlazi iz činjenice da je Ujedinjena Kraljevina bila država članica EU-a sve do 31. siječnja 2020. Osim toga, Zakonom Ujedinjene Kraljevine o zaštiti podataka iz 2018., koji je stupio na snagu 23. svibnja 2018. i kojim je izvan snage stavljen Zakon o zaštiti podataka iz 1998., dodatno se, uz prenošenje Direktive EU-a o zaštiti podataka pri izvršavanju zakonodavstva, utvrđuje primjena Opće uredbe o zaštiti podataka u pravu Ujedinjene Kraljevine te se dodjeljuju ovlasti i uvode obveze za nacionalno nadzorno tijelo za zaštitu podataka, odnosno Ured povjerenika za informiranje.

39. Kako je navedeno u uvodnoj izjavi 12. nacrta odluke Europske komisije, vlada Ujedinjene Kraljevine donijela je Zakon o povlačenju iz Europske unije iz 2018., kojim se izravno primjenjivo zakonodavstvo EU-a uključuje u pravo Ujedinjene Kraljevine. Na temelju tog zakona ministri Ujedinjene Kraljevine ovlašteni su za uvođenje sekundarnog zakonodavstva zakonskim instrumentima kako bi se zadržano pravo EU-a prilagodilo kontekstu te zemlje nakon njezina povlačenja iz EU-a.

40. U skladu s tim mjerodavni pravni okvir koji se primjenjuje u Ujedinjenoj Kraljevini nakon isteka prijelaznog razdoblja[14] čine sljedeći propisi:

[14] Prijelazno razdoblje traje do 31. prosinca 2020., nakon čega se pravo EU-a više ne primjenjuje u Ujedinjenoj Kraljevini. Razdoblje prilagodbe traje najkasnije do 30. lipnja 2021. i podrazumijeva dodatno razdoblje u kojem se prosljeđivanje osobnih podataka iz EGP-a u Ujedinjenu Kraljevinu ne smatra prijenosom.

- Opća uredba Ujedinjene Kraljevine o zaštiti podataka, kako je ugrađena u pravo Ujedinjene Kraljevine na temelju Zakona o povlačenju iz Europske unije iz 2018. i izmijenjena uredbama DPPEC (o zaštiti podataka, privatnosti i elektroničkim komunikacijama) (izmjena itd.) (izlazak iz EU-a) iz 2019.
- Zakon o zaštiti podataka iz 2018., kako je izmijenjen uredbama DPPEC iz 2019, i uredbe o zaštiti podataka, privatnosti i elektroničkim komunikacijama (izmjene itd.) (izlazak iz EU-a) iz 2020. i
- Zakon o istražnim ovlastima iz 2016.

(zajedno „okvir Ujedinjene Kraljevine za zaštitu podataka").

2.2. Opseg procjene EOZP-a

41. Nacrt odluke Europske komisije rezultat je procjene okvira Ujedinjene Kraljevine za zaštitu podataka i razgovora s vladom Ujedinjene Kraljevine. U skladu s člankom 70. stavkom 1. točkom (s) Opće uredbe o zaštiti podataka od EOZP-a se očekuje da daje neovisno mišljenje o nalazima Europske komisije, utvrđuje nedostatke okvira za primjerenost ako postoje i nastoji donijeti prijedloge za njihovo uklanjanje.

42. Kao što je navedeno u Referentnom dokumentu o primjerenosti: „Informacije koje dostavlja Europska komisija trebale bi u svakom slučaju biti iscrpne i EOZP bi trebao zahvaljujući njima biti u mogućnosti provesti vlastitu procjenu razine zaštite podataka u trećoj zemlji"[15].

43. U tom pogledu treba napomenuti da je EOZP primio samo dio relevantnih dokumenata za pravodobno ispitivanje pravnog okvira Ujedinjene Kraljevine. Veći dio zakonodavstva Ujedinjene Kraljevine na koje se upućuje u nacrtu odluke EOZP je primio putem poveznica navedenih u tom nacrtu. Europska komisija nije bila u mogućnosti dostaviti EOZP-u pisana objašnjenja i obveze Ujedinjene Kraljevine povezane s razmjenom informacija relevantnih za taj postupak između tijela Ujedinjene Kraljevine i Europske komisije[16].

44. Uzimajući u obzir prethodno navedeno i ograničeni rok (dva mjeseca) koji je EOZP dobio za donošenje ovog Mišljenja, EOZP se odlučio usredotočiti na određene točke predstavljene u nacrtu odluke te iznijeti svoju analizu i mišljenje u tom pogledu.

[15] Vidjeti WP 254 rev.01, str. 3.

[16] U vezi sa sljedećim: člankom 48. Opće uredbe o zaštiti podataka (bilješka 78. u nacrtu odluke); povećanim zaštitnim i sigurnosnim mjerama koje voditelji obrade primjenjuju pri obradi u kontekstu nacionalne sigurnosti (bilješka 64. nacrta odluke); zahtjevom da voditelj obrade razmotri postoji li potreba za oslanjanjem na izuzeće na temelju pojedinog slučaja čak i ako je izdana potvrda o nacionalnoj sigurnosti (uvodna izjava 126. i bilješka 172. nacrta odluke); činjenicom da će se zaštitni mehanizmi iz Krovnog sporazuma EU-a i SAD-a primjenjivati na sve osobne podatke koji se proizvode ili čuvaju u skladu sa Sporazumom UK-a i SAD-a o zakonu CLOUD, neovisno o prirodi ili vrsti tijela koje podnosi zahtjev, uzimajući u obzir pojedinosti o konkretnoj provedbi mjera za zaštitu podataka koje su i dalje predmet rasprava između Ujedinjene Kraljevine i SAD-a; potvrdom tijela Ujedinjene Kraljevine da će dopustiti stupanje na snagu tog sporazuma tek kad se uvjere da je njegova provedba u skladu s pravnim obvezama koje su u njemu utvrđene, uključujući jasnoću u pogledu ispunjavanja standarda zaštite podataka za sve podatke koji se zatraže na temelju tog sporazuma (uvodna izjava 153. nacrta odluke); situacijama u kojima se podaci prenose iz EU-a u Ujedinjenu Kraljevinu u okviru područja primjene tog nacrta odluke i činjenicom da će uvijek postojati „poveznica s britanskim otocima" te bi svako ometanje opreme koje obuhvaća takve podatke podlijegalo obveznom izdavanju naloga iz članka 13. stavka 1. Zakona o istražnim ovlastima iz 2016. (uvodna izjava 206. nacrta odluke) i navedenim primjerima operativnih svrha (uvodna izjava 216. i bilješka 369. nacrta odluke).

45. Iz analize prava i prakse treće zemlje koja je donedavno bila država članica EU-a jasno je da je EOZP utvrdio da su mnogi aspekti u načelu istovjetni. S obzirom na svoju ulogu u postupku donošenja nalaza o primjerenosti te opseg prava i prakse koje treba analizirati EOZP je odlučio svoju pažnju usmjeriti na aspekte u kojima je uvidio najveću potrebu za detaljnijom analizom. Osim toga, u skladu sa sudskom praksom Suda EU-a vrlo važan dio analize obuhvaća pravni sustav za pristup tijela nacionalne sigurnosti osobnim podacima prenesenima u Ujedinjenu Kraljevinu i praksu sustava nacionalne sigurnosti u Ujedinjenoj Kraljevini. Međutim, treba imati na umu da je nacionalna sigurnost očito područje prava i prakse u kojem zakonodavstvo država članica nije usklađeno na razini EU-a i stoga se može razlikovati.

46. EOZP je uzeo u obzir primjenjivi europski okvir za zaštitu podataka, uključujući članke 7., 8. i 47. Povelje EU-a, kojima se štite pravo na privatni i obiteljski život, pravo na zaštitu osobnih podataka te pravo na djelotvoran pravni lijek i na pošteno suđenje, i članak 8. Europske konvencije o ljudskim pravima (dalje u tekstu „EKLJP"), kojim se štiti pravo na privatni i obiteljski život. Usto, EOZP je razmotrio zahtjeve Opće uredbe o zaštiti podataka i relevantnu sudsku praksu.

47. Cilj je tog postupka Europskoj komisiji dati mišljenje o procjeni primjerenosti razine zaštite u Ujedinjenoj Kraljevini. Pojam „primjerene razine zaštite", koji je već postojao u Direktivi 95/46/EZ, dodatno je razradio Sud EU-a. Važno je prisjetiti se standarda koji je Sud EU-a utvrdio u predmetu Schrems I, odnosno da se, iako „razina zaštite" u trećoj zemlji mora biti „u načelu istovjetna" onoj koja je zajamčena u EU-u, „u tom pogledu pravna sredstva kojima se koristi treća zemlja za osiguranje takve razine zaštite mogu razlikovati od onih koja se provode u [EU-u]"[17]. Cilj stoga nije preslikati europsko zakonodavstvo točku po točku, već uspostaviti bitne i temeljne zahtjeve zakonodavstva koje se ispituje. Primjerenost se može ostvariti kombinacijom prava ispitanika i obveza onih koji obrađuju podatke ili onih koji izvršavaju kontrolu nad obradom te nadzora koji provode neovisna tijela. Međutim, pravila o zaštiti podataka djelotvorna su samo ako su provediva i ako se poštuju u praksi. Stoga je potrebno razmotriti sadržaj pravila primjenjivih na osobne podatke koji se prenose u treću zemlju ili međunarodnu organizaciju, ali i sustav koji je uspostavljen radi osiguravanja djelotvornosti tih pravila. Učinkoviti mehanizmi provedbe iznimno su važni za djelotvornost pravila o zaštiti podataka[18].

2.3. Opće napomene i dvojbe

2.3.1. Međunarodne obveze koje je preuzela Ujedinjena Kraljevina

48. U skladu s člankom 45. stavkom 2. točkom (c) Opće uredbe o zaštiti podataka i Referentnim dokumentom o primjerenosti[19] Europska komisija pri procjeni primjerenosti stupnja zaštite treće zemlje među ostalim uzima u obzir međunarodne obveze koje je treća zemlja preuzela ili druge obveze koje proizlaze iz sudjelovanja treće zemlje u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka, te provedbu tih obveza. Osim toga, trebalo bi uzeti u obzir pristupanje treće zemlje Konvenciji Vijeća Europe od 28. siječnja 1981. za zaštitu osoba glede

[17] Vidjeti presudu Suda EU-a u predmetu C-362/14, Maximilian Schrems protiv Data Protection Commissioner, 6. listopada 2015., ECLI:EU:C:2015:650 (dalje u tekstu „Schrems I"), točke od 73. do 74.
[18] Vidjeti WP 254 rev.01, str. 2.
[19] Vidjeti WP 254 rev.01, str. 2.

automatizirane obrade osobnih podataka (dalje u tekstu „Konvencija br. 108")[20] i njezinu Dodatnom protokolu[21].

49. **U tom pogledu EOZP pozdravlja činjenicu da je Ujedinjena Kraljevina pristupila EKLJP-u te da je pod nadležnošću ESLJP-a. Osim toga, Ujedinjena Kraljevina pristupila je i Konvenciji br. 108 i njezinu Dodatnom protokolu te je 2018. potpisala Konvenciju br. 108+[22] i trenutačno radi na njezinoj ratifikaciji.**

2.3.2. Moguće buduće razlike u okviru Ujedinjene Kraljevine za zaštitu podataka

50. Kako je navedeno u uvodnoj izjavi 281. nacrta odluke, Europska komisija mora uzeti u obzir da nakon završetka prijelaznog razdoblja predviđenog Sporazumom o povlačenju[23] Ujedinjena Kraljevina upravlja vlastitim režimom zaštite podataka, primjenjuje ga i provodi što bi, čim se privremena odredba iz članka FINPROV.10A Sporazuma o trgovini i suradnji između EU-a i UK-a[24] prestane primjenjivati, moglo posebno podrazumijevati dopune ili izmjene okvira za zaštitu podataka koji se procjenjuje u nacrtu odluke te druge relevantne promjene.

51. Europska komisija stoga je odlučila u svoj nacrt odluke uključiti klauzulu o vremenskom ograničenju valjanosti[25], u kojoj se utvrđuje rok valjanosti od četiri godine nakon njezina stupanja na snagu.

52. Važno je napomenuti da bi mogućnost da ministri Ujedinjene Kraljevine i ministar unutarnjih poslova uvedu sekundarno zakonodavstvo nakon završetka razdoblja za prilagodbu mogla u budućnosti dovesti do znatnog odstupanja okvira Ujedinjene Kraljevine za zaštitu podataka od okvira EU-a.

53. Vlada Ujedinjene Kraljevine doista je izrazila namjeru da razvije zasebne i neovisne politike u području zaštite podataka koje bi mogle dovesti do odstupanja od zakonodavstva EU-a o zaštiti podataka[26]. Ta namjera obuhvaća uključivanje aspekata osobnih podataka u trgovinske sporazume[27],

---

[20] Vidjeti Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka, Konvencija br. 108, 28. siječnja 1981.

[21] Vidjeti Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi s nadzornim tijelima i prekograničnim protokom podataka, otvoren za potpisivanje 8. studenoga 2001.

[22] Vidjeti Protokol o izmjeni Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka („Konvencija br. 108+"), 18. svibnja 2018.

[23] Vidjeti Sporazum o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju (SL L 029, 31.1.2020., str. 7.).

[24] Vidjeti Sporazum o trgovini i suradnji između Europske unije i Europske zajednice za atomsku energiju, s jedne strane, i Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske, s druge strane (SL L 444, 31.12.2020., str. 14.).

[25] Vidjeti članak 4. nacrta odluke. Vidjeti i uvodnu izjavu 282. nacrta odluke.

[26] Jedna od misija Nacionalne podatkovne strategije Ujedinjene Kraljevine (zadnji put ažurirana 9. prosinca 2020., https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) uključuje sljedeće: „Zalaganje za međunarodni protok podataka. Prekogranični protok informacija potiče globalne poslovne aktivnosti, lance opskrbe i trgovinu te jača rast u cijelom svijetu. On ima i širu društvenu ulogu. Prijenosom osobnih podataka ljudima se osigurava isplata plaća i pomaže im se u tome da i na daljinu ostanu povezani sa svojim najmilijima. Osim toga, kako je dokazala pandemija bolesti COVID-19, razmjena zdravstvenih podataka može pomoći u ključnim znanstvenim istraživanjima bolesti, ali i ujediniti zemlje u njihovu odgovoru na globalne zdravstvene krize. **Nakon napuštanja Europske unije Ujedinjena Kraljevina promicat će prednosti koje podaci mogu donijeti.** Promicat ćemo najbolju domaću praksu i surađivati s međunarodnim partnerima **kako bismo osigurali da podaci ne budu neprimjereno ograničeni državnim granicama i rascjepkanim regulatornim režimima** te da se njihov potencijal može u potpunosti iskoristiti." (naknadno istaknuto).

[27] Ibid: „Omogućavanje lakšeg prekograničnog protoka podataka: **Djelovat ćemo globalno kako bi se uklonile nepotrebne prepreke međunarodnom protoku podataka. U trgovinskim pregovorima dogovorit ćemo**

što je praksa koja podrazumijeva rizik od snižavanja razine zaštite osobnih podataka zajamčene u Ujedinjenoj Kraljevini[28].

54. Konačno, od završetka prijelaznog razdoblja Ujedinjena Kraljevina ne samo da više nije obvezana sudskom praksom Suda EU-a, već možda više nije obvezana ni već donesenim presudama Suda EU-a, koje se smatraju zadržanom sudskom praksom u pravnom okviru Ujedinjene Kraljevine, posebno zato što Ujedinjena Kraljevina ima mogućnost izmijeniti zadržano pravo EU-a nakon završetka razdoblja prilagodbe, a njezin Vrhovni sud nije obvezan nikakvom zadržanom sudskom praksom EU-a[29].

55. **S obzirom na rizike povezane s mogućim odstupanjem okvira Ujedinjene Kraljevine za zaštitu podataka od pravne stečevine EU-a nakon razdoblja prilagodbe EOZP je zadovoljan odlukom Europske komisije da u nacrt odluke uključi četverogodišnju klauzulu o vremenskom ograničenju valjanosti. Ipak, EOZP želi istaknuti važnost praćenja koje provodi Europska komisija[30]. Naime, Europska komisija trebala bi neprekidno i trajno pratiti sve relevantne promjene u Ujedinjenoj Kraljevini koje mogu utjecati na bitnu ekvivalentnost razine zaštite osobnih podataka koji se prenose u skladu s odlukom o primjerenosti za Ujedinjenu Kraljevinu od njezina stupanja na snagu. Osim toga, Europska komisija trebala bi poduzeti odgovarajuće mjere suspendiranjem, izmjenom ili stavljanjem izvan snage odluke o primjerenosti na temelju postojećih okolnosti ako nakon donošenja odluke o primjerenosti bude imala naznake za to da u Ujedinjenoj Kraljevini više nije osigurana primjerena razina zaštite.**

56. EOZP će dati sve od sebe kako bi Europsku komisiju obavijestio o svim relevantnim mjerama koje su poduzela nadzorna tijela države članice za zaštitu podataka u komercijalnom ili javnom sektoru, a posebno o pritužbama ispitanika u EGP-u koje se odnose na prijenos osobnih podataka iz EGP-a u Ujedinjenu Kraljevinu.

3. OPĆI ASPEKTI ZAŠTITE PODATAKA

3.1. Sadržajna načela

57. Poglavlje 3. Referentnog dokumenta o primjerenosti posvećeno je „sadržajnim načelima". Sustav treće zemlje mora sadržavati ta načela kako bi se njezina razina zaštite podataka smatrala u načelu istovjetnom razini zajamčenoj u EU-u. EOZP prepoznaje činjenicu da Ujedinjena Kraljevina nema

---

ambiciozne odredbe o podacima i iskoristiti svoju neovisnu ulogu u Svjetskoj trgovinskoj organizaciji kako bismo pozitivno utjecali na donošenje trgovinskih pravila za podatke. **Uklonit ćemo prepreke međunarodnim prijenosima podataka** kojima se podupiru rast i inovacije, među ostalim razvojem novih kapaciteta Ujedinjene Kraljevine za uspostavu novih i inovativnih mehanizama za međunarodne prijenose podataka. Surađivat ćemo i s partnerima u skupini G20 kako bismo uspostavili interoperabilnost među nacionalnim podatkovnim sustavima radi smanjenja poteškoća pri prijenosu podataka među različitim zemljama". (naknadno istaknuto).

[28] Vidjeti Rezoluciju Europskog parlamenta od 12. prosinca 2017. „Ususret strategiji digitalne trgovine „(2017/2065(INI)), uvodnu izjavu V., u kojoj se ističe da „zaštita osobnih podataka nije pitanje o kojem se pregovara u okviru trgovinskih sporazuma [EU-a]", dostupnu na: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_HR.pdf. Vidjeti i Rezoluciju Europskog parlamenta od 25. ožujka 2021. o evaluacijskom izvješću Komisije o provedbi Opće uredbe o zaštiti podataka dvije godine nakon njezina stupanja na snagu, stavak 28., u kojem se navodi: „podržava praksu Komisije da zaštitu podataka i prijenos osobnih podataka rješava odvojeno od trgovinskih sporazuma", https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_HR.html.

[29] Vidjeti članak 6. stavke od 3. do 6. Zakona o povlačenju iz EU-a iz 2018.

[30] Vidjeti članak 45. stavak 4. Opće uredbe o zaštiti podataka.

kodificirani ustav jer ne postoji jedinstveni dokument u kojem su utvrđena njezina temeljna pravila. Ipak, pravo na poštovanje privatnog i obiteljskog života (i pravo na zaštitu podataka u okviru tog prava) te pravo na pošteno suđenje[31] uključeni su u Zakon o ljudskim pravima iz 1998., a sudovi Ujedinjene Kraljevine priznali su ustavnu vrijednost tog zakona. U Zakon o ljudskim pravima iz 1998. uključena su prava iz EKLJP-a[32]. Osim toga, u Zakonu o ljudskim pravima iz 1998. navodi se da je vrlo važno da svako djelovanje javnih tijela bude u skladu s EKLJP-om[33].

58. Osim strukturnih i formalističkih razlika između zakonodavstva Ujedinjene Kraljevine i EU-a EOZP navodi da je, očekivano, pristup Ujedinjene Kraljevine zaštiti podataka sličan pristupu EU-a, što proizlazi iz činjenice da je Ujedinjena Kraljevina bila država članica EU-a do 31. siječnja 2020. Zbog toga su mnoga sadržajna načela usklađena s Općom uredbom o zaštiti podataka, čime se osigurava razina zaštite koja je u načelu istovjetna onoj koju osigurava EU. EOZP je odlučio da neće dodatno analizirati sadržajna načela koja su usklađena sa zakonodavstvom EU-a te je zadovoljan analizom koju je Europska komisija iznijela u svojem nacrtu odluke. Ta su sadržajna načela na primjer sljedeća: pojmovi (npr. „osobni podaci", „obrada osobnih podataka", „voditelj obrade podataka"), osnove za zakonitu i pravednu obradu u zakonite svrhe, ograničenje svrhe, kvaliteta podataka i razmjernost, zadržavanje, sigurnost i povjerljivost podataka, transparentnost, posebne kategorije podataka, izravni marketing, automatizirano donošenje odluka i izrada profila. EOZP dalje navodi da Opća uredba Ujedinjene Kraljevine o zaštiti podataka i Zakon o zaštiti podataka iz 2018. sadržavaju sadržajna načela koja premašuju ono što se zahtijeva Referentnim dokumentom o primjerenosti i odražavaju načela iz Opće uredbe o zaštiti podataka, čime se povećava razina zaštite osigurana u Ujedinjenoj Kraljevini. Ta sadržajna načela odnose se, na primjer, na izvješćivanje o povredi osobnih podataka, službenika za zaštitu podataka, procjene učinka na zaštitu podataka te tehničku i integriranu zaštitu podataka.

59. Međutim, kako je navedeno u uvodu, EOZP u ovom Mišljenju želi posebno razmotriti određene stavke o kojima ima dvojbe i traži pojašnjenja od Europske komisije.

3.1.1. Prava na pristup, ispravak, brisanje i prigovor

60. Takozvanim „izuzećem o useljavanju" utvrđenim u **dijelu 1. stavku 4. Priloga 2. Zakonu o zaštiti podataka iz 2018.** dopušta se voditeljima obrade koji su uključeni u „kontrolu useljavanja" da ne primjenjuju određena prava ispitanika predviđena Zakonom o zaštiti podataka iz 2018. ako bi se time vjerojatno „doveli u pitanje održavanje učinkovite kontrole useljavanja" odnosno „istraga ili otkrivanje aktivnosti kojima bi se ugrozilo održavanje učinkovite kontrole useljavanja".

61. Kao što je Europska komisija potvrdila u svojem nacrtu odluke[34] i kako je navedeno u Mišljenju odbora LIBE Europskog parlamenta o sklapanju, u ime EU-a, Sporazuma o trgovini i suradnji između EU-a i Ujedinjene Kraljevine[35], to je izuzeće **„široko" formulirano**. Primjenjuje se na sljedeća prava:

[31] Vidjeti članke 6. i 8. EKLJP-a (Prilog 1. Zakonu o ljudskim pravima iz 1998.).
[32] Za više informacija vidjeti uvodne izjave od 8. do 10. nacrta odluke.
[33] Vidjeti članak 6. Zakona o ljudskim pravima iz 1998.
[34] Vidjeti uvodne izjave od 62. do 65. nacrta odluke.
[35] U pogledu **široke formulacije** izuzeća o useljavanju vidjeti Mišljenje Odbora za građanske slobode, pravosuđe i unutarnje poslove o sklapanju, u ime Unije, Sporazuma o trgovini i suradnji između Europske unije i Europske zajednice za atomsku energiju, s jedne strane, i Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske, s druge strane, te Sporazuma između Europske unije i Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske o sigurnosnim postupcima za razmjenu i zaštitu klasificiranih podataka (2020/0382(NLE)), 5. veljače 2021., https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_HR.pdf, stavak 10.: „u tom pogledu

pravo na informacije, pravo na pristup, pravo na brisanje, pravo na ograničenje obrade i pravo na prigovor.

62. Osim toga, važno je napomenuti da se to izuzeće primjenjuje i u slučaju da voditelj obrade („voditelj obrade br. 1") ne prikuplja osobne podatke za potrebe kontrole useljavanja, ali ih stavlja na raspolaganje drugom voditelju obrade („voditelj obrade br. 2") koji obrađuje takve osobne podatke za potrebe kontrole useljavanja (npr. Ministarstvo unutarnjih poslova Ujedinjene Kraljevine)[36].

63. U predmetu Open Rights Group & Anor, R (na zahtjev) protiv Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3. listopada 2019.) tužitelji su osporili zakonitost izuzeća o useljavanju na osnovi njegove suprotnosti s člankom 23. Opće uredbe o zaštiti podataka i nespojivosti s pravima zajamčenima člancima 7. i 8. Povelje EU-a, koji se odnose na privatnost i zaštitu osobnih podataka. Visoki sud Engleske i Walesa, dalje u tekstu „Visoki sud", razmatrao je zakonitost izuzeća o useljavanju iz dijela 1. stavka 4. Priloga 2. Zakonu o zaštiti podataka iz 2018. te zaključio da je ono zakonito.

64. Visoki sud osobito je smatrao sljedeće:

- „[...] izuzeće o useljavanju samo je pitanje ‚važnog javnog interesa' i ima zakonit cilj [...]", točka 30.,
- „izuzeće o useljavanju ispunjava uvjete za mjere koje su ‚usklađene sa zakonom'. [...]", točka 38.,
- „Na izuzeće o useljavanju može se pozvati samo ako i u mjeri u kojoj bi se poštovanjem ‚navedenih odredbi Opće uredbe o zaštiti podataka' **vjerojatno doveli u pitanje** održavanje učinkovite kontrole useljavanja ili istraga odnosno otkrivanje aktivnosti kojima bi se ugrozilo održavanje učinkovite kontrole useljavanja. Riječi ‚vjerojatno doveli u pitanje' u kontekstu Zakona o zaštiti podataka iz 1998. (koji je prethodio Zakonu o zaštiti podataka iz 2018.)

---

podsjeća na rezolucije Parlamenta iz veljače i lipnja 2020., u kojima se ističe **opće i široko izuzeće** za obradu osobnih podataka u imigracijske svrhe iz Zakona Ujedinjene Kraljevine o zaštiti podataka", i stavak 11.: „smatra da je potrebno izmijeniti **opće i široko** izuzeće za obradu osobnih podataka u imigracijske svrhe iz Zakona o zaštiti podataka Ujedinjene Kraljevine [...] prije nego što se može donijeti valjana odluka o primjerenosti;" (naknadno istaknuto).

[36] Vidjeti primjer u Vodiču za Opću uredbu o zaštiti podataka Ureda povjerenika za informiranje, verzija od 1. siječnja 2021., str. 307. (naknadno istaknuto): „Privatna organizacija (voditelj obrade br. 1) upozorava Ministarstvo unutarnjih poslova (voditelj obrade br. 2) o zaposleniku za kojeg se vjeruje da je dostavio krivotvorene isprave o svojem identitetu i kvalifikacijama za dobivanje posla. Poslodavac dostavlja Ministarstvu unutarnjih poslova relevantne informacije. Pravo pojedinca na informaciju o tome da su njegovi osobni podaci proslijeđeni Ministarstvu unutarnjih poslova ograničeno je jer bi ostvarenje tog prava vjerojatno dovelo istragu u pitanje.

Poslodavac stoga nema obvezu obavijestiti pojedinca o tome da su njegovi podaci proslijeđeni Ministarstvu unutarnjih poslova, a s druge strane **Ministarstvo unutarnjih poslova** nema obvezu poslati pojedincu obavijest o tome da sada obrađuje njegove osobne podatke. Izuzeće se u jednakoj mjeri primjenjuje na oba voditelja obrade.

Međutim, zaposlenik traži kopiju svojih osobnih podataka od Ministarstva unutarnjih poslova, koje trenutačno o njemu vodi istragu. **Ministarstvo unutarnjih poslova može se pozvati na izuzeće** te uskratiti dio podataka ako bi njihovo otkrivanje moglo dovesti istragu u pitanje. Ako zaposlenik podnese sličan zahtjev **svojem poslodavcu, i on bi mogao primijeniti izuzeće** u jednakoj mjeri."

Drugim riječima, kako je pojašnjeno na str. 300.: „U većini slučajeva Ministarstvo unutarnjih poslova ili jedna od njegovih agencija odnosno jedan od izvođača bit će voditelj obrade koji primjenjuje to izuzeće. No važno je napomenuti da primjena tog izuzeća nije ograničena samo na Ministarstvo unutarnjih poslova. Ono može biti relevantno i za druge voditelje obrade, kao što su poslodavci, sveučilišta i policija, koji surađuju s Ministarstvom unutarnjih poslova na imigracijskim pitanjima."

protumačene su kao ‚znatna i vrlo velika mogućnost dovođenja u pitanje određenog javnog interesa. Razina rizika mora biti takva da bi se ti interesi ‚vrlo vjerojatno mogli' dovesti u pitanje, čak i ako je daleko manje vjerojatno da će se taj rizik ostvariti [...]", točka 39. (naknadno istaknuto).

65. Treba napomenuti da, prema saznanjima EOZP-a, ta presuda nije konačna i protiv nje je podnesena žalba.

66. Kao što je navedeno u Smjernicama EOZP-a o ograničenjima na temelju članka 23. Opće uredbe o zaštiti podataka („Smjernice o članku 23. Opće uredbe o zaštiti podataka")[37], „[...] u kontekstu Opće uredbe o zaštiti podataka ograničenja se **predviđaju zakonodavnom mjerom**, obuhvaćaju **ograničen broj prava ispitanika i/ili obveza voditelja obrade** navedenih u članku 23. Opće uredbe o zaštiti podataka, **poštuju bit** predmetnih temeljnih prava i sloboda, **nužna su i razmjerna mjera** u demokratskom društvu i štite jedan od elemenata iz članka 23. stavka 1. Opće uredbe o zaštiti podataka [...]"[38].

67. EOZP podsjeća i na to da je u uvodnoj izjavi 41. Opće uredbe o zaštiti podataka navedeno da „[a]ko se ovom Uredbom upućuje na **pravnu osnovu ili zakonodavnu mjeru**, to ne znači nužno da parlament mora donijeti zakonodavni akt, ne dovodeći u pitanje zahtjeve u skladu s ustavnim poretkom dotične države članice. Međutim, takva pravna osnova ili zakonodavna mjera trebala bi biti **jasna i precizna, a njezina primjena trebala bi biti predvidljiva osobama na koje se primjenjuje** sukladno sudskoj praksi Suda Europske unije [...] i Europskog suda za ljudska prava" (naknadno istaknuto).

68. Iako je ESLJP utvrdio da „nadalje, kad je riječ o formulacijama ‚u skladu sa zakonom' i ‚propisan zakonom' u člancima od 8. do 11. Konvencije, [ESLJP] napominje da je riječ ‚zakon' uvijek tumačio u ‚materijalnom' smislu, a ne u ‚formalnom'; ona uključuje i ‚pisano pravo', koje obuhvaća propise nižeg stupnja i regulatorne mjere koje donose stručna regulatorna tijela na temelju neovisnih ovlasti donošenja propisa koje im je dodijelio parlament, i ‚nepisano pravo'. ‚Zakon' se mora shvatiti tako da obuhvaća i propise **i ‚pravo' koje stvaraju sudovi**"[39], u Smjernicama o članku 23. Opće uredbe o zaštiti podataka podsjeća se da „[u] skladu sa sudskom praksom Suda EU-a svaka **zakonodavna mjera** donesena na temelju članka 23. stavka 1. Opće uredbe o zaštiti podataka mora osobito **biti usklađena s posebnim zahtjevima utvrđenima u članku 23. stavku 2. Opće uredbe o zaštiti podataka**. U članku 23. stavku 2. Opće uredbe o zaštiti podataka navodi se da zakonodavne mjere kojima se ograničavaju prava ispitanika i obveze voditelja obrade sadržavaju, prema potrebi, **posebne odredbe o nekoliko kriterija navedenih u nastavku**. U pravilu bi sve zahtjeve navedene u nastavku **trebalo uključiti u zakonodavnu mjeru** kojom se uvode ograničenja na temelju članka 23. Opće uredbe o zaštiti podataka."[40]

---

[37] Vidjeti Smjernice EOZP-a 10/2020 o ograničenjima na temelju članka 23. Opće uredbe o zaštiti podataka, verziju 1.0, donesenu 15. prosinca 2020., koje se trenutačno finaliziraju nakon javnog savjetovanja, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

[38] Vidjeti Smjernice o članku 23. Opće uredbe o zaštiti podataka, točku 9., str. 5.

[39] Vidjeti presudu ESLJP-a u predmetu Sanoma Uitgevers B.V. protiv Nizozemske, 14. rujna 2010., EC:ECHR:2010:0914JUD003822403, t. 83. (naknadno istaknuto).

[40] Vidjeti Smjernice o članku 23. Opće uredbe o zaštiti podataka, točke 45. i 46., str. 11. U skladu s člankom 52. stavkom 3. Povelje EU-a, „[u] onoj mjeri u kojoj ova Povelja sadrži prava koja odgovaraju pravima zajamčenima Konvencijom za zaštitu ljudskih prava i temeljnih sloboda, značenje i opseg primjene tih prava jednaki su onima iz spomenute Konvencije. Ova odredba ne sprječava pravo Unije da pruži širu zaštitu". Kad je riječ o pojmu

69. U tom se pogledu može primijetiti da u samom **izuzeću o useljavanju nisu navedeni sljedeći elementi iz članka 23. stavka 2. Opće uredbe o zaštiti podataka**:

- zaštitne mjere za sprečavanje zlouporabe ili nezakonitog pristupa ili prijenosa iz točke (d)
- voditelj obrade ili kategorije voditelja obrade iz točke (e)[41],
- rizici za prava i slobode ispitanika iz točke (g)
- pravo ispitanika da budu obaviješteni o ograničenju, osim ako može biti štetno za svrhu tog ograničenja iz točke (h).

70. U Vodiču za Opću uredbu o zaštiti podataka[42] Ureda povjerenika za informiranje, koji sadržava poglavlje o „izuzeću o useljavanju", navode se pojašnjenja za izuzeće o useljavanju, no on **ne može** sam po sebi sadržavati obvezujuća pravila koja ga dopunjuju. Osim toga, pitanje „kvalitete zakona" osobito je relevantno s obzirom na važnost ograničenih prava i proširenja izuzeća[43].

„**predviđeno zakonom**" iz članka 52. stavka 1. Povelje EU-a, kriteriji koje je razvio ESLJP trebali bi se upotrebljavati na način predložen u nekoliko mišljenja nezavisnih odvjetnika Suda EU-a, vidjeti na primjer mišljenja u spojenim predmetima C-203/15 i C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, t. od 137. do 154., i u predmetu C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, t. od 88. do 114. Stoga se, među ostalim, može uputiti na presudu ESLJP-a u predmetu Weber i Saravia protiv Njemačke, t. 84.: „Sud ponavlja da izraz ‚**u skladu sa zakonom**' u smislu članka 8. stavka 2. [EKLJP-a] zahtijeva, prvo, da sporna mjera ima osnovu u **nacionalnom pravu**; upućuje i na **kvalitetu** predmetnog **zakona**, zahtijevajući da on bude dostupan zainteresiranoj osobi koja, osim toga, mora moći predvidjeti njegove posljedice za sebe, i da bude u skladu s vladavinom prava." (naknadno istaknuto).
Vidjeti i uvodnu izjavu 41. Opće uredbe o zaštiti podataka: „takva pravna osnova ili zakonodavna mjera trebala bi biti **jasna** i **precizna**, a njezina primjena trebala bi biti **predvidljiva osobama na koje se primjenjuje** sukladno sudskoj praksi Suda Europske unije [...] i Europskog suda za ljudska prava" (naknadno istaknuto).

[41] Vidjeti prethodno spomenuti predmet Visokog suda, t. 54.: „Smatram da nema ničeg nezakonitog u pogledu činjenice da je izuzeće o useljavanju dostupno **svim voditeljima obrade podataka** koji obrađuju podatke u navedene svrhe. Kao što ističu tuženici, bez točke 4. podtočaka od 3. do 4. izuzeće o useljavanju izgubilo bi učinak u predmetima u kojima su podaci dobiveni od trećih osoba (kao što su lokalno tijelo ili Porezna i carinska uprava Ujedinjene Kraljevine) za potrebe održavanja učinkovite kontrole useljavanja." (naknadno istaknuto), što potvrđuje **općenitu** primjenu ograničenja.

[42] Vodič za Opću uredbu o zaštiti podatak Ureda povjerenika za informiranje, verzija od 1. siječnja 2021., str. 299.–307.

[43] Vidjeti točku 57. prethodno spomenutog predmeta Visokog suda: „G. Knight obavještava me da povjerenik dovršava smjernice o izuzeću, no da će imati ‚zakonski' status samo u smislu da se izdaju na temelju ovlasti povjerenika iz članka 57. stavka 1. Opće uredbe o zaštiti podataka. Neće imati pravni status na temelju Zakona o zaštiti podataka iz 2018."
Razlozi za uvođenje pravno obvezujućih smjernica uz potporu Ureda povjerenika za informiranje posebno su navedeni u točkama od 56. do 60. presude:
„56. Naposljetku razmatram argument povjerenika da bez pratećih zakonskih smjernica kojima se osiguravaju zaštitne mjere u odnosu na značenje i primjenu izuzeća o useljavanju izuzeće ne bi činilo razmjernu provedbu članka 23. stavka 1. Opće uredbe o zaštiti podataka. G. Knight kaže da je ta odredba razmjerna kad se dopuni tim smjernicama.
57. G. Knight obavještava me da povjerenik dovršava smjernice o izuzeću, no da će imati ‚zakonski' status samo u smislu da se izdaju na temelju ovlasti povjerenika iz članka 57. stavka 1. Opće uredbe o zaštiti podataka. Neće imati pravni status na temelju Zakona o zaštiti podataka iz 2018. Shvaćam i da je Ministarstvo unutarnjih poslova izradilo nacrt internih smjernica za osoblje o izuzeću o useljavanju (vidjeti prethodnu točku 22.). U praksi su smjernice koje je izdao povjerenik učinkovite neovisno o pravnoj osnovi. Međutim, povjerenik nema ovlasti za izdavanje onakvih ‚obvezujućih' smjernica na koje je Vrhovni sud mislio u predmetu *Christian Institute* (t. 101. i 107.). Čini se da bi primarno zakonodavstvo bilo potrebno kad bi se smatralo nužnim da smjernice o

71. *A fortiori*, „testom dovođenja u pitanje" ne utvrđuju se zaštitne mjere za sprečavanje zlouporabe ili nezakonitog pristupa odnosno prijenosa, koje bi, na primjer, provodilo Ministarstvo unutarnjih poslova.

72. S obzirom na sve navedeno EOZP napominje da su potrebna dodatna pojašnjenja primjene izuzeća o useljavanju.

73. Osim toga, EOZP navodi da ne postoji pravno obvezujući instrument kojim bi se pojasnilo izuzeće o useljavanju i utvrdilo je li ono u načelu istovjetno članku 23. Opće uredbe o zaštiti podataka te člancima 7. i 8. Povelje EU-a. Nadalje, EOZP smatra da Europska komisija treba dodatno pokazati i potkrijepiti dokazima nužnost i razmjernost širokog područja primjene *ratione personae* izuzeća o useljavanju.

74. **Kao zaključak, EOZP poziva Europsku komisiju da provjeri trenutačno stanje prethodno navedenog postupka u predmetu Open Rights Group & Anor, R (na zahtjev) protiv Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) i, s obzirom na to da ta presuda nije konačna (*res judicata*), da provjeri je li potvrđena ili preispitana presudom u žalbenom postupku, uzme u obzir eventualne izmjene u tom pogledu i navede ih u odluci o primjerenosti. EOZP poziva Europsku komisiju da dostavi dodatne informacije o nužnosti i razmjernosti izuzeća o useljavanju, posebno s obzirom na široko područje primjene *ratione personae*.**

75. **EOZP osim toga poziva Europsku komisiju da dodatno istraži postoje li odnosno bi li se mogle predvidjeti dodatne zaštitne mjere u pravnom okviru Ujedinjene Kraljevine, na primjer s pomoću pravno obvezujućih instrumenata kojima bi se izuzeće o useljavanju dopunilo povećanjem njegove predvidljivosti i zaštitnih mjera za ispitanike te omogućili bolja i brža procjena i praćenje zahtjeva u pogledu nužnosti i razmjernosti.**

---

izuzeću o useljavanju imaju jednak status kao kodeksi prakse koji su trenutačno predviđeni člancima od 121. do 124. Zakona o zaštiti podataka iz 2018.

58. U svojem argumentu u korist zakonskih smjernica g. Knight tvrdi da kontekst u kojem će doći do primjene izuzeća o useljavanju nužno donosi dvojbe u pogledu nužnosti i razmjernosti njegova postojanja i primjene. Upućuje na dva problema koja se posebno odnose na pravni kontekst. Prvo, osobni podaci na koje se primjenjuje izuzeće o useljavanju vjerojatno uključuju posebne kategorije podataka u smislu članka 9. stavka 1. Opće uredbe o zaštiti podataka (tj. podatke 'koji otkrivaju rasno ili etničko podrijetlo'). Ti su podaci definirani u Općoj uredbi o zaštiti podataka jer zahtijevaju višu razinu zaštite (Mišljenje 1/15 [2019.] 3 C.M.L.R. *25*, t. 141.). Drugo, temeljno je načelo prava o zaštiti podataka da je pravo ispitanika na pristup vrlo važno jer omogućuje ostvarivanje ostalih prava osiguranih ispitanicima (vidjeti *YS protiv Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015.] 1 C.M.L.R. 18*, t. 44.).

59. G. Knight navodi četiri praktična aspekta. Prvo, kad voditelji obrade ispitanicima ne objasne da su se pozvali na zakonsko izuzeće niti to sažeto obrazlože, ispitanik neće znati da je izuzeće primijenjeno i stoga ga neće moći učinkovito osporiti. Drugo, ispitanici će posebno ovisiti o tome da voditelji obrade primjenjuju izuzeće pažljivo i samo u mjeri u kojoj je to nužno. Iako svaki ispitanik ima pravo na primjenu izuzeća uložiti prigovor povjereniku ili pokrenuti sudski postupak pred sudovima, vjerojatno je da ispitanik neće biti upoznat sa svojim pravima i da neće imati sredstava za poduzimanje pravnih koraka u okolnostima u kojima postoji potreba za brzim i točnim poštovanjem prava na zaštitu podataka. Treće, kao imigrant, ispitanik će vjerojatno će biti u ranjivom položaju. Četvrto, to nije apstraktno pitanje s obzirom na dokaze koje je tuženik iznio u pogledu primjene izuzeća o useljavanju (vidjeti prethodnu točku 4.).

60. G. Knight navodi da su predmetno osporavanje izuzeća o useljavanju i obrazloženja Suda u predmetu *Christian Institute [2016.] UKSC 51* blisko povezani. Tvrdi da je, kao i u predmetu *Christian Institute*, izuzeće o useljavanju široko, sadržava nedefinirane pojmove, ima nizak prag za primjenu, podliježe kontrolama koje ne proizlaze jasno iz odredbe i primjenjuje se na vrlo širok raspon konteksta i prava. Za razliku od predmeta *Christian Institute*, o izuzeću o useljavanju nema javno dostupnih smjernica, kao ni zakonskog statusa koji bi trebalo uzeti u obzir."

3.1.2. Ograničenja daljnjeg prijenosa

76. Člankom 44. Opće uredbe o zaštiti podataka propisano je da se prijenosi i daljnji prijenosi osobnih podataka odvijaju jedino ako nije ugrožena razina zaštite pojedinaca zajamčena tom uredbom. Stoga se za osobne podatke koji se prenose iz EGP-a u Ujedinjenu Kraljevinu na temelju odluke o primjerenosti osigurava u načelu istovjetna razina zaštite onoj razini koja se pruža na temelju okvira EU-a za zaštitu podataka. **To znači ne samo da zakonodavstvo Ujedinjene Kraljevine mora biti „u načelu istovjetno" zakonodavstvu EU-a u pogledu obrade osobnih podataka koji se prenose u Ujedinjenu Kraljevinu na temelju nacrta odluke, već i da se pravilima koja se u Ujedinjenoj Kraljevini primjenjuju na daljnji prijenos tih podataka u treće zemlje mora osigurati zadržavanje u načelu istovjetne razine zaštite.**

77. Stoga je važno da je svaki daljnji prijenos osobnih podataka koji potječu iz EGP-a iz Ujedinjene Kraljevine u drugu treću zemlju primjereno zaštićen zaštitnim mjerama ili da se provodi u skladu s pravilima o odstupanjima[44] kako bi se osigurao kontinuitet zaštite osigurane zakonodavstvom EU-a. **Ako se takva zaštita ne može osigurati, ne bi smjelo doći do daljnjih prijenosa osobnih podataka iz EGP-a.**

78. EOZP uviđa da je Ujedinjena Kraljevina najvećim dijelom preslikala poglavlje V. Opće uredbe o zaštiti podataka u Uredbi Ujedinjene Kraljevine o zaštiti podataka (članci od 44. do 49.) i u Zakonu o zaštiti podataka iz 2018.[45] **Ipak, EOZP je utvrdio određene aspekte zakonodavnog okvira Ujedinjene Kraljevine povezane s daljnjim prijenosima koji bi mogli ugroziti razinu zaštite osobnih podataka koji se prenose iz EGP-a.**

79. **Prvi problem** koji je EOZP utvrdio odnosi se na treće zemlje, međunarodne organizacije ili područja[46] koje Ujedinjena Kraljevina priznaje kao primjerene primatelje na temelju postupka opisanog u Zakonu o zaštiti podataka iz 2018. Ujedinjena Kraljevina može dalje prenositi osobne podatke iz EGP-a u druge treće zemlje na temelju eventualnog budućeg propisa o primjerenosti Ujedinjene Kraljevine[47].

80. Točnije, kako je objašnjeno u uvodnoj izjavi 77. nacrta odluke, ministar unutarnjih poslova Ujedinjene Kraljevine ovlašten je nakon savjetovanja s Uredom povjerenika za informiranje[48] priznati da treća zemlja (ili područje ili sektor u trećoj zemlji), međunarodna organizacija ili opis te zemlje, područja, sektora ili organizacije osigurava primjerenu razinu zaštite osobnih podataka. Pri ocjeni primjerenosti razine zaštite ministar unutarnjih poslova Ujedinjene Kraljevine mora uzeti u obzir iste one elemente koje Europska komisija mora ocijeniti u skladu s člankom 45. stavkom 2. točkama od (a) do (c) Opće uredbe o zaštiti podataka, tumačenim u vezi s uvodnom izjavom 104. Opće uredbe o zaštiti podataka i zadržanom sudskom praksom EU-a. To znači da će pri procjeni primjerene razine zaštite u trećoj zemlji biti relevantno osigurava li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" razini zajamčenoj u Ujedinjenoj Kraljevini. Iako EOZP uzima u obzir mogućnost da Ujedinjena Kraljevina na temelju Opće uredbe Ujedinjene Kraljevine o zaštiti podataka smatra da neka područja

[44] Vidjeti članak 49. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka.
[45] Vidjeti članke 17.A, 17.B, 17.C i 18 Zakona o zaštiti podataka iz 2018.
[46] Vidjeti članak 17.A Zakona o zaštiti podataka iz 2018.
[47] Instrument Ujedinjene Kraljevine istovjetan odluci o primjerenosti na temelju Opće uredbe o zaštiti podataka.
[48] Vidjeti članak 182. stavak 2. Zakona o zaštiti podataka iz 2018. Vidjeti i Memorandum o razumijevanju o ulozi Ureda povjerenika za informiranje u pogledu novih procjena primjerenosti za Ujedinjenu Kraljevinu, 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/.

osiguravaju primjerenu razinu zaštite u skladu s okvirom Ujedinjene Kraljevine za zaštitu podataka, želi istaknuti da ta područja zasad možda neće imati pozitivnu odluku Europske komisije o primjerenosti u kojoj se njihova razina zaštite smatra „u načelu istovjetnom" razini zajamčenoj u EU-u. To bi moglo dovesti do mogućih rizika u pogledu zaštite osobnih podataka koji se prenose iz EGP-a, posebno ako se u budućnosti okvir Ujedinjene Kraljevine za zaštitu podataka bude razlikovao od pravne stečevine EU-a. Treba napomenuti da je u srpnju 2020. povijesnom presudom Suda EU-a u predmetu Schrems II[49] poništena Odluka o europsko-američkom sustavu zaštite privatnosti jer je Sud EU-a smatrao da pravni okvir SAD-a ne osigurava u načelu istovjetnu razinu zaštite u odnosu na razinu u EU-u. No već donesene presude Suda EU-a, koje se smatraju zadržanom sudskom praksom u pravnom okviru Ujedinjene Kraljevine, možda više neće obvezivati Ujedinjenu Kraljevinu, posebno zato što Ujedinjena Kraljevina može izmijeniti zadržano pravo EU-a nakon završetka razdoblja prilagodbe, a njezin Vrhovni sud nije obvezan nikakvom zadržanom sudskom praksom EU-a[50].

81. **EOZP poziva Komisiju da pomno prati postupak i kriterije procjene primjerenosti koju tijela Ujedinjene Kraljevine provode u pogledu drugih trećih zemalja, posebno s obzirom na treće zemlje koje EU ne priznaje kao primjerene na temelju Opće uredbe o zaštiti podataka. Ako Europska komisija utvrdi da treća zemlja koju Ujedinjena Kraljevina smatra primjerenom ne osigurava razinu zaštite koja je u načelu istovjetna razini zajamčenoj u EU-u, EOZP poziva Europsku komisiju da poduzme sve potrebne mjere, kao što su izmjene odluke o primjerenosti za Ujedinjenu Kraljevinu kako bi se uvele posebne zaštitne mjere za osobne podatke koji potječu iz EGP-a, i/ili da razmotri suspenziju odluke o primjerenosti za Ujedinjenu Kraljevinu ako osobni podaci preneseni iz EGP-a u Ujedinjenu Kraljevinu podliježu daljnjim prijenosima u predmetnu treću zemlju na temelju propisa o primjerenosti Ujedinjene Kraljevine.**

82. **Drugi problem** odnosi se na predstojeće preispitivanje postojećih odluka o primjerenosti koje je Europska komisija donijela na temelju Direktive 95/46/EZ. Na temelju tog preispitivanja Europska komisija mogla bi odlučiti da određene zemlje na koje se dosad primjenjivala odluka o primjerenosti više ne osiguravaju u načelu istovjetnu razinu zaštite s obzirom na postojeće zakonodavstvo EU-a i nedavnu sudsku praksu. Međutim, kako je predviđeno u točki 4. Priloga 21. Zakonu o zaštiti podataka iz 2018., Ujedinjena Kraljevina već je priznala da te zemlje osiguravaju primjerenu razinu zaštite. Iako ministar unutarnjih poslova Ujedinjene Kraljevine mora preispitati te nalaze o primjerenosti u roku od četiri godine, Europska komisija u svojem nacrtu odluke navodi da ti nalazi o primjerenosti neće automatski prestati postojati ako ministar Ujedinjene Kraljevine ne provede potrebno preispitivanje u propisanom roku od četiri godine[51].

83. **EOZP poziva Europsku komisiju da prati smatra li Ujedinjena Kraljevina da neka zemlja i dalje osigurava primjerenu razinu zaštite čak i ako se za nju, nakon što EU dovrši preispitivanje postojećih odluka o primjerenosti, zaključi da više ne osigurava primjerenu razinu zaštite. U tom slučaju EOZP na temelju uvodnih izjava od 277. do 280. nacrta odluke poziva Europsku komisiju da poduzme sve odgovarajuće mjere za ispravljanje situacije, na primjer izmjenom odluke o primjerenosti kako bi se dodali posebni zahtjevi za osobne podatke koji potječu iz EGP-a i/ili suspenzijom odluke o primjerenosti ako osobni podaci preneseni iz EGP-a u Ujedinjenu Kraljevinu podliježu daljnjim prijenosima u predmetnu treću zemlju. EOZP poziva Europsku komisiju da nastavi s tim praćenjem sve dok traje odluka o primjerenosti Ujedinjene Kraljevine.**

[49] Vidjeti presudu u predmetu Schrems II.
[50] Vidjeti članak 6. stavke od 3. do 6. Zakona o povlačenju iz EU-a iz 2018.
[51] Vidjeti uvodnu izjavu 82nacrta odluke.

84. **Treći problem** odnosi se na daljnji prijenos osobnih podataka iz EGP-a u neprimjerene zemlje na temelju alata za prijenos podataka predviđenih člancima 46. i 47. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka. Iako su Općom uredbom Ujedinjene Kraljevine o zaštiti podataka predviđeni alati za prijenos podataka jednaki onima iz Opće uredbe o zaštiti podataka, EOZP ističe da je potrebno osigurati da se zaštitnim mjerama koje oni sadržavaju osigura učinkovita zaštita u trećoj zemlji, posebno s obzirom na presudu u predmetu Schrems II.

85. Nakon presude u predmetu Schrems II, u kojoj Sud EU-a podsjeća na to da zaštita osigurana za osobne podatke u EU-u mora te podatke pratiti i drugdje, EOZP je već donio početne preporuke o dopunskim mjerama[52] za pomoć izvoznicima kako bi, prema potrebi, ispitanicima osigurali razinu zaštite koja je u načelu istovjetna razini zajamčenoj u EU-u.

86. Sud EU-a smatra da su izvoznici podataka odgovorni za to da u svakom slučaju zasebno i, ako je potrebno, u suradnji s uvoznikom podataka u trećoj zemlji provjere dovodi li se pravom ili praksom treće zemlje u pitanje učinkovitost primjerenih zaštitnih mjera sadržanih u alatima za prijenos podataka iz članka 46. Opće uredbe o zaštiti podataka[53]. U tom bi slučaju izvoznici podataka trebali provesti dopunske mjere da bi se ti nedostaci u zaštiti uklonili i da bi se ona uskladila s razinom potrebnom na temelju prava EU-a.

87. **EOZP poziva Europsku komisiju da, kako bi se osigurao kontinuitet zaštite, u nacrt odluke uključi jamstva da će izvoznici podataka u Ujedinjenoj Kraljevini provesti procjenu okvira treće zemlje za zaštitu podataka u svakom pojedinom slučaju kad budu upotrebljavali alate za prijenos podataka iz članaka 46. i 47. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka za daljnje prijenose podataka prenesenih iz EGP-a u treće zemlje. Nadalje, ako je potrebno, poziva Europsku komisiju da provede primjerene mjere kako bi se osiguralo stvarno poštovanje zaštitnih mjera sadržanih u odabranom alatu za prijenos podataka radi postizanja razine zaštite koja je u načelu istovjetna razini zajamčenoj u EU-u. EOZP ističe da bez tih jamstava postoji rizik da će se razina zaštite koja je u načelu istovjetna razini zajamčenoj u EU-u smanjiti kroz daljnje prijenose iz Ujedinjene Kraljevine.**

88. **Četvrti problem** povezan s daljnjim prijenosima odnosi se na međunarodne sporazume koje je Ujedinjena Kraljevina sklopila ili će ih sklopiti u budućnosti i na mogući izravan pristup tijela iz trećih zemalja koja su stranke u takvim sporazumima osobnim podacima iz EGP-a. EOZP ima velike dvojbe u pogledu već sklopljenog Sporazuma UK-a i SAD-a o zakonu CLOUD, a Europska komisija prepoznaje taj izazov i ističe da bi „moguće stupanje Sporazuma na snagu moglo utjecati na razinu zaštite koja se procjenjuje u ovoj Odluci”[54]. Nakon što taj sporazum stupi na snagu, na temelju njega bi osobni podaci preneseni iz EGP-a u Ujedinjenu Kraljevinu u skladu s nacrtom odluke podlijegali odredbama Sporazuma u kojima se utvrđuju uvjeti za izravan pristup tijela SAD-a, što bi utjecalo na okvir Ujedinjene Kraljevine za zaštitu podataka, uključujući odredbe o daljnjim prijenosima. Zbog toga bi odredbe sporazuma sklopljenog sa SAD-om mogle znatno utjecati na razinu zaštite podataka prenesenih iz EGP-a. EOZP u tom kontekstu navodi da Europska komisija u uvodnoj izjavi 153. svojeg nacrta odluke upućuje na objašnjenja koja su dala tijela Ujedinjene Kraljevine, bez

[52] Vidjeti Preporuke EOZP-a 01/2020 o mjerama kojima se dopunjuju alati za prijenos podataka kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u, donesene 10. studenoga 2020., koje se trenutačno finaliziraju nakon javnog savjetovanja, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_hr.pdf.

[53] Vidjeti presudu u predmetu Schrems II, t. 134.

[54] Vidjeti uvodnu izjavu 153nacrta odluke.

citiranja ili navođenja konkretnih pisanih jamstava ili obveza i isticanja konkretnih pravnih odredbi na temelju prava Ujedinjene Kraljevine kojima bi se takva objašnjenja potkrijepila.

89. EOZP je prethodno izrazio te dvojbe u dopisu upućenom Europskom parlamentu 15. lipnja 2020[55]. EOZP je istaknuo da na temelju „pravne stečevine EU-a u području zaštite podataka, a posebno Opće uredbe o zaštiti podataka i Direktive o izvršavanju zakonodavstva" ima zadrške o tome bi li se zaštitne mjere u Sporazumu za potrebe pristupa osobnim podacima u Ujedinjenoj Kraljevini primjenjivale na SAD u određenim okolnostima koje zahtijevaju obvezu otkrivanja te jesu li te mjere dovoljne s obzirom na standarde EU-a kako se ne bi ugrozila razina zaštite osigurana u EU-u.

90. Nadalje, odredbe Sporazuma UK-a i SAD-a o zakonu CLOUD mogu znatno utjecati na materijalne i postupovne uvjete pod kojima tijela SAD-a mogu izravno pristupiti osobnim podacima koje posjeduju voditelji obrade ili izvršitelji obrade u Ujedinjenoj Kraljevini, a time i na razinu zaštite zajamčenu pravom Ujedinjene Kraljevine. Da bi se osigurala razina zaštite koja je u načelu istovjetna razini zajamčenoj pravom EU-a, nužno je, na primjer, „da zaštitne mjere u okviru takvog sporazuma uključuju obvezno prethodno sudsko odobrenje kao temeljno jamstvo za pristup metapodacima i podacima o sadržaju. Na temelju svoje preliminarne procjene EOZP nije mogao utvrditi takvu jasnu odredbu u sporazumu koji su sklopili Ujedinjena Kraljevina i SAD iako napominje da se u sporazumu upućuje na primjenu nacionalnog prava"[56].

91. Europska komisija ističe da bi podaci dobiveni na temelju tog sporazuma imali razinu zaštite koja je ekvivalentna posebnim zaštitnim mjerama osiguranima takozvanim „Krovnim sporazumom EU-a i SAD-a", ali EOZP ima dvojbe o tome bi li uključivanje tih zaštitnih mjera u Sporazum UK-a i SAD-a o zakonu CLOUD jednostavnim upućivanjem koje se primjenjuje *mutatis mutandis* ispunjavalo kriterije jasnih, preciznih i dostupnih pravila za pristup osobnim podacima odnosno bi li u dovoljnoj mjeri uključivalo djelotvorne zaštitne mjere koje su djelotvorne i sudski provedive u skladu s pravom Ujedinjene Kraljevine.

92. **EOZP stoga preporučuje da Europska komisija pojasni kako bi se i na temelju kojeg pravnog instrumenta osigurala razina zaštite ekvivalentna posebnim zaštitnim mjerama predviđenima Krovnim sporazumom EU-a i SAD-a te kako bi ona postala obvezujuća na temelju prava Ujedinjene Kraljevine.**

93. EOZP navodi i da iz odredbi Sporazuma UK-a i SAD-a o zakonu CLOUD, tumačenih u vezi s člankom 3. zakona CLOUD SAD-a[57], proizlaze pitanja o stvarnoj primjeni zaštitnih mjera predviđenih u Sporazumu za pristup tijela za izvršavanje zakonodavstva u SAD-u osobnim podacima u Ujedinjenoj Kraljevini koje obrađuju pružatelji usluga elektroničke komunikacije ili pružatelji računalnih usluga na daljinu (dalje u tekstu „pružatelji usluga u oblaku") koji su pod jurisdikcijom SAD-a. Ako se na pružatelja usluga u oblaku koji se nalazi u Ujedinjenoj Kraljevini primjenjuje pravo SAD-a (npr. jer je riječ o društvu kćeri trgovačkog društva iz SAD-a), potrebno je utvrditi bi li se tijela SAD-a pri prikupljanju tih podataka morala osloniti na Sporazum UK-a i SAD-a o zakonu CLOUD. Dok Europska komisija ističe da će se „[p]osebna pozornost posvetiti primjeni zaštitnih mjera iz Krovnog sporazuma i njihovoj prilagodbi posebnoj vrsti prijenosa obuhvaćenoj Sporazumom UK-a i SAD-a", EOZP naglašava da na temelju njegove preliminarne procjene nije jasno bi li se zaštitne mjere iz Sporazuma UK-a i SAD-a o zakonu CLOUD, a time i one predviđene Krovnim sporazumom EU-a i SAD-a,

[55] Vidjeti odgovor EOZP-a zastupnicima u Europskom parlamentu Sophie in't Veld i Moritzu Körneru o sporazumu SAD-a i UK-a, donesen 15. lipnja 2020., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.
[56] Vidjeti prethodno navedeni dopis EOZP-a.
[57] Vidjeti zakon CLOUD SAD-a, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

primjenjivale na sve zahtjeve tijela SAD-a za pristup podacima u Ujedinjenoj Kraljevini na temelju zakona CLOUD SAD-a, ako bi se uopće primjenjivale.

94. Ujedinjena Kraljevina mogla bi ubuduće sklopiti i druge međunarodne sporazume ili preuzeti zajedničke obveze s trećim zemljama koje bi se primjenjivale na osobne podatke koji se prenose iz EGP-a u Ujedinjenu Kraljevinu na temelju nacrta odluke[58]. Ovisno o odredbama tih sporazuma i primjeni posebnih zaštitnih klauzula ti međunarodni sporazumi svojim utjecajem na okvir Ujedinjene Kraljevine za zaštitu podataka mogu znatno utjecati i na materijalne i postupovne uvjete za pristup tijela trećih zemalja osobnim podacima u Ujedinjenoj Kraljevini. To posebno vrijedi za nacrt drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu (dalje u tekstu „Konvencija iz Budimpešte"), o kojem trenutačno pregovaraju stranke te Konvencije, među njima i nekoliko zemalja koje nisu članice EU-a. Nacrt protokola sadržava klauzule koje stranke mogu slobodno aktivirati, na primjer kad je riječ o odobrenju pristupa podacima o sadržaju. Iako bi sve države članice EU-a aktivirale klauzule u skladu s pravilima EU-a o zaštiti podataka, nema jamstva da bi to učinila i Ujedinjena Kraljevina, pa bi moglo doći do znatnog odstupanja od razine zaštite koja bi se pružala u EU-u. Drugi je primjer prethodno navedenih problema Sporazum između Ujedinjene Kraljevine i Japana o sveobuhvatnom gospodarskom partnerstvu[59] („CEPA"), prvi trgovinski sporazum Ujedinjene Kraljevine nakon Brexita, koji je stupio na snagu 1. siječnja 2021.[60] i sadržava odredbe o osobnim podacima[61]. EOZP nadalje navodi da je Ujedinjena Kraljevina 1. veljače 2021. službeno objavila i svoj zahtjev za pristupanje Sveobuhvatnom i progresivnom transpacifičkom partnerstvu („CPTPP"), koje uključuje Sporazum o transpacifičkom partnerstvu („TPP")[62].

95. EOZP napominje da se, osim Sporazuma UK-a i SAD-a o zakonu CLOUD, navedeni međunarodni sporazumi ne spominju u nacrtu odluke.

96. **EOZP stoga poziva Europsku komisiju:**

- **da ispita međudjelovanje okvira Ujedinjene Kraljevine za zaštitu podataka i njezinih međunarodnih obveza, osim Sporazuma UK-a i SAD-a o zakonu CLOUD, posebno kako bi se osigurao kontinuitet razine zaštite u slučaju daljnjih prijenosa osobnih podataka prenesenih iz EGP-a u Ujedinjenu Kraljevinu u druge treće zemlje na temelju odluke o primjerenosti Ujedinjene Kraljevine te da neprekidno prati situaciju i prema potrebi poduzme mjere u pogledu sklapanja drugih međunarodnih sporazuma između Ujedinjene Kraljevine i trećih zemalja koji bi mogli ugroziti razinu zaštite osobnih podataka predviđenu u EU-u**

[58] Vidjeti prethodni odjeljak 2.3.3.

[59] Vidjeti Sporazum između Ujedinjene Kraljevine i Japana o sveobuhvatnom gospodarskom partnerstvu [CS Japan br. 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Vidjeti Smjernice Vlade Ujedinjene Kraljevine o trgovinskim sporazumima Ujedinjene Kraljevine sa zemljama koje nisu članice EU-a, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] U skladu s člankom 8.80 stavkom 5. CEPA-e stranke se obvezuju poticati razvoj mehanizama za promicanje usklađenosti svojih različitih pravnih pristupa zaštiti (osobnih) podataka. U skladu s člankom 8.84 stranke se obvezuju da neće zabraniti ili ograničiti prekogranični prijenos informacija elektroničkim putem, uključujući osobne informacije, ako se on izvršava za poslovne potrebe obuhvaćene osobe u smislu CEPA-e.

[62] U skladu s člankom 14.11 stavkom 2. TPP-a svaka stranka dopušta prekogranični prijenos informacija elektroničkim putem, uključujući osobne informacije, ako se on izvršava za poslovne potrebe obuhvaćene osobe.

- **da EOZP-u dostavi pisane obveze tijela Ujedinjene Kraljevine i utvrdi posebne odredbe u pravu Ujedinjene Kraljevine u kojima se objašnjavaju moguća primjena i provedba Sporazuma UK-a i SAD-a o zakonu CLOUD, kako je navedeno u uvodnoj izjavi 153. nacrta odluke**

- **da u tom kontekstu prati jamče li se Sporazumom UK-a i SAD-a o zakonu CLOUD, uz zaštitne mjere koje bi se mogle osigurati odgovarajućom prilagodbom Krovnog sporazuma EU-a i SAD-a, odgovarajuće dodatne zaštitne mjere kako bi se u obzir uzeli razina osjetljivosti predmetnih kategorija podataka i jedinstveni zahtjevi u pogledu izravnog prijenosa elektroničkih dokaza s pružatelja usluga u oblaku umjesto između tijela;**
- **da ocijeni učinak i potencijalne rizike odredbi o osobnim podacima sadržanih u međunarodnim sporazumima koje je Ujedinjena Kraljevina nedavno potpisala, kao što je CEPA.**

97. **Peti problem** odnosi se na primjenu odstupanja za prijenose osobnih podataka u treću zemlju. Iako su dostupna odstupanja na temelju Opće uredbe Ujedinjene Kraljevine o zaštiti podataka jednaka odstupanjima utvrđenima u Općoj uredbi o zaštiti podataka, važno je da Ured povjerenika za informiranje tumači i da nastavi tumačiti okolnosti za primjenu tih odstupanja onako kako ih tumači EOZP. U suprotnom, ili ako Ujedinjena Kraljevina odstupi od tog tumačenja u budućnosti, postojao bi rizik od ugrožavanja razine zaštite podataka koji se prenose iz EGP-a u treće zemlje preko Ujedinjene Kraljevine.

98. **EOZP poziva Europsku komisiju da u okviru svojeg praćenja posebno provjeri tumači li Ujedinjena Kraljevina okolnosti za primjenu odstupanja i dalje na isti način kao EU. Međutim, kad bi Ujedinjena Kraljevina tumačila primjenu odstupanja na drukčiji način kojim se ugrožava razina zaštite, bilo bi ključno da Europska komisija poduzme potrebne korake izmjenom odluke o primjerenosti kako bi osigurala da se razina zaštite osobnih podataka iz EGP-a koji se prenose u Ujedinjenu Kraljevinu neće ugroziti kad se ti podaci budu dalje prenosili iz Ujedinjene Kraljevine u treće zemlje na temelju različitog tumačenja odstupanja.**

99. **Šesti problem**, zadnji u ovom odjeljku, odnosi se na izostanak zaštitnih mjera propisanih člankom 48. Opće uredbe o zaštiti podataka u okviru Ujedinjene Kraljevine za zaštitu podataka.

100. Europska komisija u svojem nacrtu odluke pojašnjava da se u nedostatku propisa o primjerenosti ili odgovarajućih zaštitnih mjera prijenos može izvršiti samo na temelju odstupanja utvrđenih u članku 49. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka, „uz iznimku članka 48. Uredbe (EU) 2016/679, za koji je Ujedinjena Kraljevina odlučila da ga neće uključiti u Opći uredbu Ujedinjene Kraljevine o zaštiti podataka”.[63] Nepostojanje odredbe o prijenosima ili otkrivanju podataka na temelju presude suda ili odluke upravnog tijela treće zemlje koja je u načelu istovjetna članku 48. Opće uredbe o zaštiti podataka u okviru Ujedinjene Kraljevine za zaštitu podataka može dovesti do pravne nesigurnosti u pogledu materijalnog utjecaja na razinu zaštite osobnih podataka koji se prenose iz EGP-a u Ujedinjenu Kraljevinu na temelju nacrta odluke.

101. U svojem Referentnom dokumentu o primjerenosti EOZP u pogledu daljnjih prijenosa ističe da bi „daljnji prijenosi osobnih podataka koje izvršava prvotni primatelj izvornog prijenosa podataka trebali biti dopušteni samo ako i daljnji primatelj podliježe pravilima kojima se osigurava odgovarajuća razina zaštite i ako slijedi odgovarajuće upute pri obradi podataka uime voditelja obrade podataka”[64]. Nadalje, EOZP ističe da „prvotni primatelj podataka prenesenih iz EU-a mora osigurati odgovarajuće zaštitne mjere za daljnje prijenose podataka ako ne postoji odluka o primjerenosti. Takvi daljnji prijenosi podataka trebali bi se odvijati samo u ograničene i točno

[63] Vidjeti bilješku 78. nacrta odluke.
[64] Vidjeti WP 254 rev.01, str. 6.

određene svrhe i ako postoji pravna osnova za takvu obradu"[65]. Kao dio poglavlja V. Opće uredbe o zaštiti podataka, članak 48. u potpunosti se mora uzeti u obzir kad se procjenjuje osigurava li se pravnim okvirom Ujedinjene Kraljevine u načelu istovjetna razina zaštite u tom pogledu[66].

102. EOZP u tom kontekstu ističe sudsku praksu Suda EU-a povezanu s rizikom od zlouporabe ili nezakonitog pristupa podacima i njihove nezakonite upotrebe te posebno navodi da „[k]ad je riječ o razini zaštite temeljnih sloboda i prava zajamčenih u Uniji, propis Unije koji se miješa u temeljna prava zajamčena u člancima 7. i 8. Povelje mora prema ustaljenoj sudskoj praksi Suda predvidjeti jasna i precizna pravila koja uređuju doseg i primjenu mjere te propisati minimalne uvjete na način da osobe čiji se osobni podaci obrađuju raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih podataka od rizika zloporabe kao i od svih nezakonitih pristupa i uporabe tih podataka. Nužnost raspolaganja takvim jamstvima još je i značajnija kada su osobni podaci podvrgnuti automatskoj obradi te postoji značajan rizik od nezakonitog pristupa tim podacima"[67].

103. EOZP u tom pogledu na temelju informacija dostupnih u nacrtu odluke napominje da u okviru Ujedinjene Kraljevine za zaštitu podataka nije jasno utvrđeno da se svaka presuda suda i odluka upravnog tijela treće zemlje kojom se od voditelja obrade ili izvršitelja obrade zahtijeva prijenos ili otkrivanje osobnih podataka može priznati ili izvršiti na bilo koji način samo ako se temelji na važećem međunarodnom sporazumu između treće zemlje koja podnosi zahtjev i Ujedinjene Kraljevine. Članak 48. Opće uredbe o zaštiti podataka ključna je odredba iz poglavlja V. te uredbe jer se njime zahtijeva da se prijenos ili otkrivanje osobnih podataka na temelju presude ili odluke suda ili upravnog tijela treće zemlje mogu priznati ili izvršiti samo ako se temelje na međunarodnom sporazumu koji je na snazi između treće zemlje koja je podnijela zahtjev i Unije ili države članice, ne dovodeći u pitanje druge razloge za prijenos u skladu s poglavljem V. Opće uredbe o zaštiti podataka. EOZP podsjeća na to da „zahtjev inozemnog tijela sam po sebi nije pravna osnova za prijenos. Nalog se može priznati samo ako se temelji na međunarodnom sporazumu kao što je ugovor o uzajamnoj pravnoj pomoći koji je na snazi između treće zemlje koja podnosi zahtjev i Unije ili države članice"[68]. Stoga je ključno da se u pravu Ujedinjene Kraljevine mogu utvrditi u načelu istovjetne odredbe.

104. U nacrtu odluke Europska komisija navodi objašnjenja tijela Ujedinjene Kraljevine prema kojima je, u skladu sa sudskom praksom ili propisima, inozemna presuda kojom se zahtijevaju podaci neizvršiva u Ujedinjenoj Kraljevini bez međunarodnog sporazuma i svaki prijenos podataka na zahtjev inozemnog suda ili upravnog tijela zahtijeva alat za prijenos podataka kao što su propis o primjerenosti ili primjerene zaštitne mjere, osim ako se primjenjuje odstupanje u skladu s člankom 49. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka. Međutim, EOZP-u nije dostavljena korespondencija između Europske komisije i tijela Ujedinjene Kraljevine[69] u tom pogledu, zbog čega on ne može analizirati i neovisno procijeniti jesu li jamstva tijela Ujedinjene Kraljevine dovoljna za osiguravanje u načelu istovjetne razine zaštite u odnosu na zaštitne mjere iz članka 48. Opće uredbe o zaštiti podataka.

[65] Vidjeti WP 254 rev.01, str. 6.
[66] Vidjeti članak 44. Opće uredbe o zaštiti podataka, posebno zadnju rečenicu: „Sve odredbe iz ovog poglavlja primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca zajamčena ovom Uredbom."
[67] Vidjeti presudu u predmetu Schrems II, t. 91.
[68] Vidjeti prilog Zajedničkom odgovoru EOZP-a i EDPS-a odboru LIBE o učinku zakona CLOUD SAD-a na europski pravni okvir za zaštitu osobnih podataka, donesen 10. srpnja 2019., https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[69] Vidjeti bilješku 78. nacrta odluke.

105. **EOZP poziva Europsku komisiju da iznese dodatna jamstva i konkretna upućivanja na zakonodavstvo Ujedinjene Kraljevine kojima se osigurava da je razina zaštite na temelju pravnog okvira Ujedinjene Kraljevine u načelu istovjetna razini zaštite zajamčenoj u EGP-u. Stoga EOZP poziva Europsku komisiju da dostavi pisana objašnjenja i obveze tijela Ujedinjene Kraljevine o provedbi zaštitnih mjera koje su u načelu istovjetne mjerama utvrđenima člankom 48. Opće uredbe o zaštiti podataka.**

106. **EOZP smatra da je utvrđivanje odredbi iz prava Ujedinjene Kraljevine kojima se osigurava razina zaštite koja je u načelu istovjetna zaštitnim mjerama iz članka 48. Opće uredbe o zaštiti podataka još važnije s obzirom na prethodno izražene dvojbe u pogledu zahtjeva tijela SAD-a ili ostalih trećih zemalja za pristup podacima u Ujedinjenoj Kraljevini te s obzirom na to da bi se, u skladu s odlukom o primjerenosti, osobni podaci mogli prenijeti iz EGP-a u Ujedinjenu Kraljevinu bez daljnjeg jamstva ili obveze primatelja u pogledu zahtjeva tijela drugih trećih zemalja za pristup podacima.**

3.2. Postupovni i provedbeni mehanizmi

107. Na temelju kriterija utvrđenih u Referentnom dokumentu o primjerenosti EOZP je analizirao sljedeće aspekte okvira Ujedinjene Kraljevine za zaštitu podataka obuhvaćene nacrtom odluke: postojanje i učinkovito funkcioniranje neovisnog nadzornog tijela, postojanje sustava kojim se osigurava dobra razina usklađenosti i sustav pristupa odgovarajućim mehanizmima pravne zaštite zahvaljujući kojima pojedinci u EU-u mogu ostvariti svoja prava i zatražiti pravnu zaštitu bez opterećujućih prepreka administrativnoj i sudskoj zaštiti.

3.2.1. Nadležno neovisno nadzorno tijelo

108. EOZP pozdravlja rad Europske komisije na sveobuhvatnom ispitivanju uspostave, funkcioniranja i ovlasti nadzornog tijela Ujedinjene Kraljevine u poglavlju 2.6. nacrta odluke. Povjerenik za informiranje Ujedinjene Kraljevine zadužen je za nadzor usklađenosti i usklađivanje s Općom uredbom Ujedinjene Kraljevine o zaštiti podataka i Zakonom o zaštiti podataka iz 2018. U skladu s Prilogom 12. Zakonu o zaštiti podataka iz 2018. povjerenik za informiranje takozvani je *Corporation Sole*, odnosno zasebni pravni subjekt koji čini jedna osoba uz potporu Ureda povjerenika za informiranje.

109. S obzirom na neovisnost povjerenika za informiranje EOZP ističe da članak 51. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka ne sadržava izričito pojašnjenje da je povjerenik za informiranje neovisno tijelo javne vlasti, kao što je u članku 51. Opće uredbe o zaštiti podataka navedeno za nadzorna tijela. EOZP ipak uviđa da se u članku 52. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka na sličan način navode odgovarajuća pravila u pogledu neovisnosti kao što su ona utvrđena u članku 52. stavcima od 1. do 3. Opće uredbe o zaštiti podataka.

110. Nadalje, EOZP ističe da članak 52. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka ne sadržava obveze u skladu s člankom 52. stavcima od 4. do 6. Opće uredbe o zaštiti podataka kojima se odgovarajućem nadzornom tijelu izričito osiguravaju resursi potrebni za učinkovito izvršavanje njegovih zadaća i ovlasti. Ipak, EOZP uviđa činjenicu da Zakon o zaštiti podataka iz 2018. sadržava odredbe čiji je cilj osigurati odgovarajuće financiranje Ureda povjerenika za informiranje[70], ali i okolnost da je Ured povjerenika za informiranje trenutačno jedno od najvećih nadzornih tijela u usporedbi s nadzornim tijelima u EU-u/EGP-u. Budući da je trajno dodjeljivanje odgovarajućih resursa, posebno u pogledu osoblja i proračuna[71], ključno da bi se osiguralo pravilno funkcioniranje

[70] Vidjeti članke 137., 138. i 182. te točku 9. Priloga 12. Zakonu o zaštiti podataka iz 2018.
[71] Vidjeti WP 254 rev.01, str. 7.

nadzornog tijela kako bi ono ispunilo sve zadaće koje su mu dodijeljene i da je i Europski parlament nedavno istaknuo veliku važnost dodjele resursa[72], EOZP smatra ključnim posebno pomno pratiti buduće promjene u tom području.

111. **Stoga EOZP poziva Europsku komisiju da prati promjene u pogledu dodjele resursa Uredu povjerenika za informiranje, koja bi bila ključna za pravilno ispunjavanje zadaća tog tijela.**

3.2.2. Postojanje sustava zaštite podataka kojim se osigurava dobra razina usklađenosti

112. U nacrtu odluke sveobuhvatno se ispituju ovlasti Ureda povjerenika za informiranje na temelju članka 58. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka i Zakona o zaštiti podataka iz 2018. kako bi se osigurali praćenje i izvršavanje zakonodavstva. EOZP uviđa da se u članku 58. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka uvelike odražavaju ovlasti nadzornih tijela utvrđene u članku 58. Opće uredbe o zaštiti podataka. Kad je riječ o ovlasti za određivanje administrativnih novčanih kazni ovisno o okolnostima svakog pojedinog predmeta, članak 83. Uredbe Ujedinjene Kraljevine o zaštiti podataka sadržava odredbe i najviše iznose slične onima iz članka 83. Opće uredbe o zaštiti podataka. Stoga EOZP smatra da je pravni okvir Ujedinjene Kraljevine u tom području trenutačno usklađen sa standardima utvrđenima u mjerodavnom pravu EU-a. Ipak, EOZP u tom pogledu ističe da je postojanje *učinkovitih* sankcija važno da bi se osiguralo poštovanje pravila[73].

113. **S obzirom na navedeno EOZP poziva Europsku komisiju da prati učinkovitost sankcija i odgovarajućih pravnih lijekova u okviru Ujedinjene Kraljevine za zaštitu podataka.**

3.2.3. Sustavom zaštite podataka moraju se pružiti potpora i pomoć ispitanicima u ostvarivanju njihovih prava i odgovarajućih mehanizama sudske pomoći

114. Učinkovit mehanizam nadzora, koji omogućuje neovisnu istragu pritužbi radi utvrđivanja i kažnjavanja povreda prava ispitanika u praksi, te učinkovita administrativna i sudska zaštita (uključujući naknadu štete proizišle iz nezakonite obrade ispitanikovih osobnih podataka) ključni su elementi za procjenu toga osigurava li neki sustav za zaštitu podataka primjerenu razinu zaštite.

115. EOZP pozdravlja činjenicu da Ured povjerenika za informiranje na svojim internetskim stranicama objavljuje sveobuhvatne informacije i smjernice namijenjene informiranju voditelja obrade i izvršitelja obrade o njihovim obvezama i zadaćama te pružanju podrške ispitanicima koji se žele upoznati sa svojim pravima povezanima s osobnim podacima i ostvariti svoja pojedinačna prava na temelju Uredbe Ujedinjene Kraljevine o zaštiti podataka i Zakona o zaštiti podataka iz 2018.

116. **Neovisno o trenutačnoj situaciji EOZP poziva Europsku komisiju da neprekidno prati razinu potpore koju Ured povjerenika za informiranje pruža upravo pojedincima čiji su osobni podaci preneseni u Ujedinjenu Kraljevinu na temelju odluke o primjerenosti kako bi im pomogao u ostvarenju njihovih prava na temelju sustava Ujedinjene Kraljevine za zaštitu podataka.**

[72] Rezolucija Europskog parlamenta od 25. ožujka 2021. o evaluacijskom izvješću Komisije o provedbi Opće uredbe o zaštiti podataka dvije godine nakon njezina stupanja na snagu, stavak 15., https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_HR.html.
[73] Vidjeti WP 254 rev.01, str. 7.

4. PRISTUP JAVNIH TIJELA UJEDINJENE KRALJEVINE OSOBNIM PODACIMA PRENESENIMA IZ EU-A I NJIHOVA UPOTREBA

4.1. Pristup javnih tijela Ujedinjene Kraljevine podacima i njihova upotreba za potrebe izvršavanja zakonodavstva

4.1.1. Pravne osnove i primjenjiva ograničenja / primjenjive zaštitne mjere

117. Kad je riječ o procjeni Europske komisije koja je dokumentirana u uvodnim izjavama 132. i sljedećima nacrta odluke **o pristupu za potrebe izvršavanja zakonodavstva**, Europska komisija iznosi razrađene i detaljne informacije te općenito donosi suvisle zaključke. Stoga EOZP u ovom Mišljenju ne ponavlja većinu činjeničnih nalaza i procjena. Međutim, u određenim slučajevima opis činjenica ili objašnjenje zaključaka nisu dovoljni da bi ih EOZP prihvatio.

4.1.1.1. Upotreba privole

118. EOZP prima na znanje da Europska komisija u bilješci 184. nacrta odluke[74] tvrdi da **privola** nije relevantna u scenariju u kojem se primjenjuje primjerenost jer pri prijenosu tijelo za kaznenog progona Ujedinjene Kraljevine ne prikuplja podatke izravno od ispitanika na temelju privole. Stoga Europska komisija ne procjenjuje upotrebu privole kao pravne osnove u radu policije.

119. U tom pogledu EOZP podsjeća da se člankom 45. stavkom 2. točkom (a) Opće uredbe o zaštiti podataka zahtijeva procjena širokog raspona elemenata koji nisu ograničeni na situaciju prijenosa i uključuju „vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o [...] kaznenom pravu".

120. EOZP napominje, među ostalim na temelju informacija Europske komisije iz uvodne izjave 38. njezina nacrta provedbene odluke na temelju Direktive (EU) 2016/680 Europskog parlamenta i Vijeća o primjerenosti zaštite osobnih podataka u Ujedinjenoj Kraljevini (dalje u tekstu „nacrt odluke o primjerenosti na temelju Direktive LED"), da bi upotreba privole, kako je uređena sustavom Ujedinjene Kraljevine u kontekstu izvršavanja zakonodavstva, uvijek zahtijevala oslanjanje na pravnu osnovu. To znači da čak i ako policija ima zakonske ovlasti za obradu podataka za potrebe istrage, u određenim posebnim okolnostima (na primjer, pri uzimanju uzorka DNK-a) može smatrati primjerenim zatražiti privolu ispitanika.

121. **EOZP poziva Europsku komisiju da u odluku o primjerenosti uključi analizu moguće upotrebe privole u kontekstu izvršavanja zakonodavstva kako je predviđeno u nacrtu odluke o primjerenosti u skladu na temelju Direktive LED.**

4.1.1.2. Nalozi za pretragu i nalozi za dostavljanje

122. Iako EOZP općenito nema primjedbi o prikupljanju dokaza koje policija provodi na temelju naloga za pretragu i naloga za dostavljanje, iz uvodne izjave 136. nacrta odluke proizlazi da je Europska komisija svoja razmatranja o pristupu tijela za izvršavanje zakonodavstva usmjerila na policiju te da je obrada osobnih podataka koju provode druga tijela za izvršavanje zakonodavstva ispitana u manjoj mjeri.

123. Na primjer, na stranici 11. dokumenta *UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement* (Obrazloženje Ujedinjene Kraljevine za rasprave o primjerenosti, odjeljak F:

[74] Vidjeti str. 37. nacrta odluke.

Izvršavanje zakonodavstva)[75] predlaže se da bi **Nacionalna agencija za kriminalitet** (dalje u tekstu „NCA") mogla biti tijelo za izvršavanje zakonodavstva od posebnog interesa, koje, među ostalim , ima širu funkciju prikupljanja obavještajnih podataka o kaznenim djelima. NCA svoju misiju opisuje kao objedinjavanje obavještajnih podataka iz niza izvora kako bi se u najvećoj mogućoj mjeri poboljšale analize, procjene i taktičke mogućnosti, među ostalim iz tehničkog presretanja komunikacija, od partnera u području izvršavanja zakonodavstva u Ujedinjenoj Kraljevini i inozemstvu te od sigurnosnih i obavještajnih agencija[76]. NCA je isto tako jedan od glavnih sugovornika međunarodnih partnera u području izvršavanja zakonodavstva i ima ključnu ulogu u razmjeni obavještajnih podataka o kaznenim djelima[77].

124. EOZP nadalje prima na znanje činjenicu da i Vladin komunikacijski stožer (dalje u tekstu „GCHQ"), čije aktivnosti obično pripadaju području nacionalne sigurnosti kao području primjene dijela 4. Zakona o zaštiti podataka iz 2018., preuzima aktivnu ulogu u smanjenju društvene i financijske štete koju teški i organizirani kriminal nanosi Ujedinjenoj Kraljevini, u bliskoj suradnji s Ministarstvom unutarnjih poslova, NCA-om, Poreznom i carinskom upravom („HMRC") i drugim vladinim ministarstvima[78]. Njegove aktivnosti odnose se na borbu protiv seksualnog zlostavljanja djece, prijevara, drugih vrsta gospodarskog kriminala, uključujući pranje novca, kriminalne upotrebe tehnologije, kiberkriminaliteta, organiziranog imigracijskog kriminala, uključujući trgovinu ljudima, te krijumčarenja droge, vatrenog oružja i drugih nezakonitih aktivnosti krijumčarenja.

125. **EOZP poziva Europsku komisiju da svoju analizu dopuni analizom agencija aktivnih u području izvršavanja zakonodavstva, posebno NCA-a, koje su svoje svakodnevno poslovanje usmjerile na prikupljanje i analizu podataka, uključujući osobne podatke. Osim toga, EOZP poziva Europsku komisiju da pobliže razmotri agencije kao što je GCHQ čije su aktivnosti obuhvaćene područjem**

[75]Vidjeti Vlada Ujedinjene Kraljevine, *Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement* (Obrazloženje za rasprave o primjerenosti, odjeljak F: Izvršavanje zakonodavstva), 13. ožujka 2020., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Vidjeti internetske stranice Nacionalne agencije za kriminalitet, *Intelligence: enhancing the picture of serious organised crime affecting the UK* (Obavještajni podaci: poboljšanje slike teškog organiziranog kriminala koji pogađa Ujedinjenu Kraljevinu), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Iako nisu svi podaci koje NCA obrađuje osobni podaci, oni bi mogli činiti znatan udio, a ovdje opisane aktivnosti razlikuju se od klasičnih policijskih aktivnosti te bi procjena pristupa tijela za izvršavanje zakonodavstva Ujedinjene Kraljevine osobnim podacima bila nepotpuna bez temeljite procjene aktivnosti NCA-a. Čini se razumnim osigurati da sva relevantna tijela za izvršavanje zakonodavstva pridaju isto značenje načelima zaštite podataka te tako pružiti jasniju sliku o agenciji koja se posebno temelji na podacima, kao što je NCA. Osim toga, u odjeljku „Pogled u budućnost" dodatno se pojašnjava da „[n]eprekidno tražimo nove prilike za prikupljanje, razvoj i proširenje tradicionalnih mogućnosti kako bismo povećali količinu i poboljšali kvalitetu obavještajnih podataka dostupnih za iskorištavanje u Ujedinjenoj Kraljevini i inozemstvu". „U tom kontekstu razvijamo novu mogućnost za iskorištavanje nacionalnih podataka u skladu s ovlastima koje su Zakonom o kaznenim djelima i sudovima dodijeljene agenciji kako bismo pristupili podacima u posjedu različitih tijela vlasti te ih povezali i iskoristili." [...] „Svime navedenim poboljšat ćemo agilnost i fleksibilnost u odgovaranju na nove prijetnje i proaktivnom djelovanju te prikupljanju i analizi informacija i obavještajnih podataka o novim prijetnjama, što će nam omogućiti da poduzmemo mjere prije no što se prijetnje ostvare."

[78] Vidjeti internetske stranice GCHQ-a, *Mission, Serious and Organised Crime* (Misija, teški i organizirani kriminal), https://www.gchq.gov.uk/section/mission/serious-crime.

primjene izvršavanja zakonodavstva i nacionalne sigurnosti te pravni okvir koji se na njih primjenjuje kad je riječ o obradi osobnih podataka.

4.1.1.3. Istražne ovlasti za potrebe izvršavanja zakonodavstva

126. U skladu s poglavljem 4. Referentnog dokumenta o primjerenosti „Ključna jamstva u trećim **zemljama za pristup podacima za potrebe izvršavanja zakonodavstva** i nacionalne sigurnosti kako bi se ograničilo zadiranje u temeljna prava" EOZP podsjeća da je „Sud [...] u tom kontekstu ujedno kritizirao prijašnju Odluku o ‚sigurnoj luci' koja ‚ne sadržava nikakvo utvrđenje o postojanju državnih pravila SAD-a za ograničavanje mogućih miješanja u temeljna prava osoba čiji se podaci prenose iz Unije u SAD, **miješanja koja su državna tijela te zemlje ovlaštena provoditi kada slijede legitimne ciljeve** kao što je to nacionalna sigurnost'"[79]. U tom referentnom dokumentu EOZP navodi da **sve treće zemlje trebaju poštovati četiri europska temeljna jamstava**[80] **u pogledu pristupa podacima kako bi ih se smatralo primjerenima, bez obzira na to pristupa li se podacima** za potrebe nacionalne sigurnosti ili **za potrebe izvršavanja zakonodavstva,** a osobito **jamstvo da treba dokazati nužnost i razmjernost u pogledu legitimnih ciljeva.**

127. U tom odjeljku nacrta odluke Europska komisija zaključuje (uvodna izjava 139.) da „budući da su istražne ovlasti predviđene Zakonom o istražnim ovlastima iz 2016. jednake onima koje imaju nacionalne sigurnosne agencije, uvjeti, ograničenja i zaštitne mjere koji se primjenjuju na takve ovlasti detaljno su opisani u odjeljku o pristupu javnih tijela Ujedinjene Kraljevine osobnim podacima i njihovoj upotrebi za potrebe nacionalne sigurnosti". Međutim, kad je riječ o primjeni testa nužnosti i razmjernosti na zakonodavstvo država članica kojim se javnim tijelima omogućuje zadržavanje osobnih podataka i pristup njima, iz sudske prakse Suda EU-a proizlazi da se legitimni ciljevi, kao što su nacionalna sigurnost ili borba protiv teških kaznenih djela, razlikuju i da bi se stoga u jednom određena vrsta zadiranja mogla opravdati, dok u drugom ne bi[81].

128. **EOZP bi stoga u okviru odluke pozdravio posebnu procjenu nužnosti i razmjernosti uvjeta, ograničenja i zaštitnih mjera opisanih u odjeljku o mjerama za ostvarenje ciljeva nacionalne sigurnosti koji čine uvodna izjava 174. i sljedeće kad je riječ o primjeni tih uvjeta, ograničenja i zaštitnih mjera u kontekstu mjere za ostvarenje cilja izvršavanja zakonodavstva. Stoga poziva Europsku komisiju da dodatno pojasni jesu li opisano zadržavanje osobnih podataka i pristup tim podacima za potrebe izvršavanja zakonodavstva dovoljno ograničeni kako bi se osigurala razina zaštite koja je u načelu istovjetna onoj koja se jamči u EU-u.**

4.1.2. Daljnja upotreba informacija prikupljenih za potrebe izvršavanja zakonodavstva (uvodne izjave od 140. do 154.)

129. EOZP napominje da su u odnosu na daljnju upotrebu informacija prikupljenih za potrebe izvršavanja zakonodavstva okvirom Ujedinjene Kraljevine za zaštitu podataka predviđene zaštitne mjere i ograničenja slične onima u pravu Unije.

4.1.2.1. Daljnja upotreba za druge potrebe izvršavanja zakonodavstva

130. Zakonom o zaštiti podataka iz 2018. doista se propisuje da se osobni podaci koje je prikupilo nadležno tijelo za potrebe izvršavanja zakonodavstva smiju dalje obrađivati (bez obzira provodi li obradu izvorni ili drugi voditelj obrade) za druge potrebe izvršavanja zakonodavstva, pod uvjetom da je

[79] Vidjeti WP 254 rev.01, str. 9.
[80] Vidjeti Preporuke EOZP-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora.
[81] Vidjeti presudu Suda EU-a u spojenim predmetima C-511/18, C-512/18 i C-520/18, La Quadrature du Net i dr., 6. listopada 2020., ECLI:EU:C:2020:791.

voditelj obrade zakonom ovlašten obrađivati podatke u drugu svrhu te da je obrada nužna i razmjerna toj svrsi. Europska komisija napominje da se sve zaštitne mjere predviđene u dijelu 3. Zakona o zaštiti podataka iz 2018. primjenjuju na obradu koju provodi tijelo primatelj. No EOZP naglašava da se u skladu s dijelom 3. člankom 44. stavkom 4., člankom 45. stavkom 4., člankom 48. stavkom 3. i člankom 68. stavkom 7. Zakona o zaštiti podataka iz 2018. predviđa mogućnost ograničavanja prava ispitanika, a člankom 79. mogućnost izdavanja potvrda da je ograničenje nužna i razmjerna mjera za zaštitu nacionalne sigurnosti. **EOZP stoga preporučuje Europskoj komisiji da dodatno procijeni mogući učinak takvih ograničenja na razinu zaštite osobnih podataka u odnosu na daljnju uporabu prikupljenih informacija. Slično tome, trebalo bi dodatno pojasniti i pravni okvir Ujedinjene Kraljevine kojim se omogućuje takva daljnja razmjena, posebno Zakon o digitalnom gospodarstvu iz 2017. i Zakon o kaznenim djelima i sudovima iz 2013., kojim se omogućuje razmjena informacija s NCA-om.**

4.1.2.2. Daljnja upotreba za druge potrebe osim izvršavanja zakonodavstva u Ujedinjenoj Kraljevini

131. Zakonom o zaštiti podataka iz 2018. propisuje se i da se osobni podaci prikupljeni za potrebe izvršavanja zakonodavstva mogu obrađivati i u druge svrhe ako je obrada odobrena u skladu sa zakonom. U tom je slučaju pravna osnova za takvu razmjenu članak 19. Zakona o borbi protiv terorizma iz 2008. U tom pogledu EOZP napominje da područje primjene i odredbe članka 19. Zakona o borbi protiv terorizma nisu u potpunosti obuhvaćeni procjenom Europske komisije te da mogu podrazumijevati daljnju širu uporabu, posebno u pogledu članka 19. stavka 2., kojim se propisuje da „[o]dređena obavještajna služba informacije koje je dobila u vezi s izvršavanjem neke od svojih funkcija smije upotrijebiti i pri izvršavanju bilo koje svoje druge funkcije”.

132. EOZP napominje i da bi se upućivanje Europske komisije na činjenicu da su nadležna tijela javna tijela koja moraju djelovati u skladu s EKLJP-om, uključujući njegov članak 8., kako bi se osigurala usklađenost cjelokupne razmjene podataka između tijela za izvršavanje zakonodavstva i obavještajnih službi sa zakonodavstvom o zaštiti podataka i EKLJP-om moglo dodatno potkrijepiti utvrđivanjem relevantnih akata i zakona u okviru pravnog poretka Ujedinjene Kraljevine kojima se jasno i precizno utvrđuju takva ograničenja.

4.1.2.3. Daljnja upotreba u kontekstu daljnjih prijenosa izvan Ujedinjene Kraljevine

133. Iako je Europska komisija uputila na činjenicu da Sporazum o zakonu CLOUD između Ujedinjene Kraljevine i SAD-a može utjecati na daljnje prijenose iz pružatelja usluga u oblaku u Ujedinjenoj Kraljevini u SAD, EOZP ističe i da bi stupanje na snagu tog sporazuma moglo utjecati i na daljnju upotrebu informacija prikupljenih daljnjim prijenosima od tijela za izvršavanje zakonodavstva u Ujedinjenoj Kraljevini, posebno u pogledu izdavanja i prijenosa naloga u skladu s člankom 5. Sporazuma o zakonu CLOUD između Ujedinjene Kraljevine i SAD-a.

134. U širem smislu, EOZP smatra da sklapanje budućih bilateralnih sporazuma s trećim zemljama u svrhu suradnje u području izvršavanja zakonodavstva kojima se osigurava pravna osnova za prijenos osobnih podataka u te zemlje može isto tako znatno utjecati na uvjete za daljnju upotrebu prikupljenih informacija jer takvi sporazumi mogu utjecati na procijenjeni okvir Ujedinjene Kraljevine za zaštitu podataka. EOZP stoga preporučuje Europskoj komisiji da dodatno procijeni tu točku, utvrdi postojanje međunarodnih sporazuma i pojasni mogu li odredbe tih sporazuma utjecati na primjenu prava Ujedinjene Kraljevine o zaštiti podataka te može li se tim odredbama predvidjeti dodatno ograničenje ili izuzeće za daljnju upotrebu podataka prikupljenih za potrebe izvršavanja zakonodavstva i njihova otkrivanja u inozemstvu. EOZP smatra da su takve informacije i procjena ključne kako bi se omogućila sveobuhvatna procjena razine zaštite osigurane zakonodavnim okvirom

i praksom Ujedinjene Kraljevine u pogledu otkrivanja informacija u inozemstvu i njihove daljnje upotrebe.

4.1.3. Nadzor

135. EOZP napominje da uz Ured povjerenika za informiranje nadzor nad tijelima za izvršavanje zakonodavstva provodi kombinacija različitih povjerenika. U nacrtu nalaza o primjerenosti spominju se povjerenik za istražne ovlasti, povjerenik za pohranu i upotrebu biometrijskog materijala i povjerenik za nadzorne kamere. U tom kontekstu treba napomenuti da je Sud EU-a u više navrata naglasio potrebu za neovisnim nadzorom. Kad je riječ o pitanjima pristupa osobnim podacima koji se prenose u Ujedinjenu Kraljevinu, posebno je važan povjerenik za istražne ovlasti. EOZP razumije da je povjerenik za istražne ovlasti takozvani „sudski povjerenik" na kojeg se, kao i na druge sudske povjerenike, upućuje u kontekstu poglavlja o nacionalnoj sigurnosti te da ti sudski povjerenici uživaju neovisnost sudaca, čak i kad obavljaju dužnost povjerenika. Kad je riječ o uredu povjerenika za istražne ovlasti, Europska komisija u uvodnoj izjavi 245. nacrta odluke objašnjava da on djeluje neovisno kao nepristrano tijelo, a financira ga Ministarstvo unutarnjih poslova.

136. EOZP u nacrtu odluke nije pronašao daljnje upućivanje na procjenu neovisnosti povjerenika za pohranu i upotrebu biometrijskog materijala i povjerenika za nadzorne kamere.

137. **Poziva se Europska komisija da dodatno procijeni neovisnost sudskih povjerenika, među ostalim i u slučajevima u kojima povjerenik (više) ne obavlja dužnost suca, te da procijeni neovisnost povjerenika za pohranu i upotrebu biometrijskog materijala i povjerenika za nadzorne kamere.**

4.2. Opći pravni okvir za zaštitu podataka u području nacionalne sigurnosti

4.2.1. Potvrde o nacionalnoj sigurnosti

138. U skladu s člankom 111. Zakona o zaštiti podataka iz 2018. voditelji obrade mogu podnijeti zahtjev za potvrde o nacionalnoj sigurnosti koje izdaje ministar, član vlade, javni tužitelj ili nezavisni odvjetnik za Škotsku i kojima se potvrđuje da su izuzeća od obveza i prava utvrđenih u dijelovima od 4. do 6. Zakona o zaštiti podataka iz 2018. nužna i razmjerna mjera za zaštitu nacionalne sigurnosti. Tim se potvrdama voditeljima obrade osigurava veća pravna sigurnost te će one biti nepobitan dokaz da se nacionalna sigurnost primjenjuje pri obradi osobnih podataka. Međutim, trebalo bi napomenuti da te potvrde nisu potrebne za primjenu izuzeća zbog nacionalne sigurnosti, već su mjera transparentnosti[82].

139. EOZP iz članaka 17. i 18. Priloga 20. Zakonu o zaštiti podataka iz 2018. zaključuje da je učinak potvrde o nacionalnoj sigurnosti izdane na temelju Zakona o zaštiti podataka iz 1998. (dalje u tekstu „stara potvrda") bio produljen do 25. svibnja 2019. u pogledu obrade osobnih podataka u skladu sa Zakonom o zaštiti podataka iz 2018. Do tog se datuma sa starim potvrdama, ako nisu bile zamijenjene ili opozvane, postupalo kao da su izdane na temelju Zakona o zaštiti podataka iz 2018.

140. Međutim, ako ne postoji izričiti datum isteka potvrde o nacionalnoj sigurnosti izdane na temelju Zakona o zaštiti podataka iz 1998., EOZP shvaća da će takva potvrda i dalje proizvoditi učinke u odnosu na obradu u skladu sa Zakonom o zaštiti podataka iz 1998., osim ako se potvrda povuče ili

[82] Vidjeti Ministarstvo unutarnjih poslova, *The Data Protection Act 2018, National Security Certificates guidance* (Zakon o zaštiti podataka iz 2018., Smjernice o potvrdama o nacionalnoj sigurnosti), kolovoz 2020., točku 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.

ukine[83]. Iako je zaštita koja je osigurana starim potvrdama ograničena na obradu osobnih podataka u skladu sa Zakonom o zaštiti podataka iz 1998., EOZP primjećuje da se nove potvrde o nacionalnoj sigurnosti mogu izdati na temelju Zakona o zaštiti podataka iz 1998. za osobne podatke koji su obrađeni u skladu sa Zakonom o zaštiti podataka iz 1998.[84]

141. **U svrhu sveobuhvatnosti EOZP poziva Europsku komisiju da u svojem nacrtu odluke pojasni da se potvrde o nacionalnoj sigurnosti i dalje mogu izdavati na temelju Zakona o zaštiti podataka iz 1998. EOZP nadalje poziva Europsku komisiju da u svojem nacrtu odluke opiše mehanizme pravne zaštite i nadzora u pogledu potvrda izdanih na temelju Zakona o zaštiti podataka iz 1998. Naposljetku, EOZP poziva Europsku komisiju da u svoj nacrt odluke uključi broj postojećih potvrda izdanih na temelju Zakona o zaštiti podataka iz 1998. te da pozorno prati taj aspekt.**

4.2.2. Pravo na ispravak i brisanje

142. Kad je riječ o pravu na ispravak i brisanje, EOZP prima na znanje da se u skladu s člancima 100. i 149. Zakona o zaštiti podataka iz 2018. ispitanici mogu obratiti Visokom sudu (u Škotskoj Vrhovnom građanskom sudu) da naloži voditelju obrade ispravak ili brisanje njihovih podatka bez nepotrebne odgode.

143. **EOZP naglašava da je potrebno osigurati učinkovito ostvarivanje prava ispitanika te stoga poziva Europsku komisiju da u svojem nacrtu odluke opiše kako članak 100. Zakona o zaštiti podataka iz 2018. funkcionira u praksi te da pomno prati primjenu tog članka.**

4.2.3. Izuzeća zbog nacionalne sigurnosti

144. EOZP želi skrenuti pozornost na članak 110. Zakona o zaštiti podataka iz 2018., a osobito na njegov Prilog 11., u kojem se utvrđuju posebne svrhe zbog kojih obavještajne službe mogu odstupiti od određenih načela zaštite podataka, među ostalim u pogledu prava ispitanika, te nisu obvezne obavijestiti Ured povjerenika za informiranje o povredama osobnih podataka[85].

145. **EOZP poziva Europsku komisiju da dodatno pojasni područje primjene izuzeća jer se pita jesu li sva izuzeća predviđena u Prilogu 11. Zakonu o zaštiti podataka iz 2018. relevantna za rad obavještajnih službi i osiguravaju li istovjetnost s načelom nužnosti i razmjernosti.** Konkretno, **EOZP poziva Europsku komisiju da pojasni okolnosti u kojima bi se obavještajna služba mogla pozvati na članak 10. Priloga 11. Zakonu o zaštiti podataka iz 2018., u kojem se navodi da se „[n]avedene odredbe ne primjenjuju na osobne podatke koji se sastoje od zapisa o namjerama voditelja obrade u odnosu na bilo koje pregovore s ispitanikom ako bi se primjenom navedenih odredbi mogli ugroziti pregovori".**

---

[83] Vidjeti Ministarstvo unutarnjih poslova, *The Data Protection Act 2018, National Security Certificates guidance* (Zakon o zaštiti podataka iz 2018., Smjernice o potvrdama o nacionalnoj sigurnosti), kolovoz 2020., str. 5.

[84] Vidjeti Ministarstvo unutarnjih poslova, *The Data Protection Act 2018, National Security Certificates guidance* (Zakon o zaštiti podataka iz 2018., Smjernice o potvrdama o nacionalnoj sigurnosti), kolovoz 2020., točku 8., str. 5.

[85] To su sprečavanje i otkrivanje „kaznenih djela", „informacije koje se moraju objaviti u skladu sa zakonom itd. ili u vezi sa sudskim postupcima", „zastupnička nepovredivost", „sudski postupci", „krunska odlikovanja i dostojanstva", „oružane snage", „gospodarska dobrobit", „imunitet pravne profesije", „pregovori", „povjerljiva upućivanja voditelja obrade", „ispitni radovi i ocjene", „istraživački i statistički podaci" i „arhiviranje u javnom interesu".

4.3. Pristup javnih tijela Ujedinjene Kraljevine podacima i njihova upotreba za potrebe nacionalne sigurnosti

146. EOZP općenito prepoznaje da države imaju veliku slobodu prosudbe u pitanjima nacionalne sigurnosti, što priznaje i ESLJP. EOZP podsjeća i na to da je, kako je istaknuto u njegovim ažuriranim preporukama o europskim temeljnim jamstvima za mjere nadzora[86], člankom 6. stavkom 3. Ugovora o Europskoj uniji utvrđeno da temeljna prava sadržana u EKLJP-u čine opća načela prava Unije. Međutim, kako Sud EU-a podsjeća u svojoj sudskoj praksi, navedena konvencija nije pravni instrument koji formalno predstavlja dio pravnog poretka Europske unije jer joj Unija nije pristupila[87]. Stoga se razina zaštite temeljnih prava koja se zahtijeva člankom 45. Opće uredbe o zaštiti podataka mora utvrditi na temelju odredbi te uredbe, tumačenih u kontekstu temeljnih prava koja su zajamčena Poveljom EU-a. S obzirom na to, u skladu s člankom 52. stavkom 3. Povelje EU-a prava koja su u njoj sadržana i koja odgovaraju pravima zajamčenima EKLJP-om imaju isto značenje i opseg primjene kao ona utvrđena EKLJP-om. Stoga se, kako je podsjetio Sud EU-a, radi tumačenja odgovarajućih prava iz Povelje EU-a kao minimalna razina zaštite mora uzeti u obzir sudska praksa ESLJP-a u pogledu prava koja su predviđena i Poveljom EU-a[88]. Međutim, u skladu sa zadnjom rečenicom članka 52. stavka 3. Povelje EU-a „[o]va odredba ne sprječava pravo Unije da pruži širu zaštitu".

147. Stoga je u sljedećoj procjeni EOZP uzeo u obzir sudsku praksu ESLJP-a u mjeri u kojoj se Poveljom EU-a, kako je tumači Sud EU-a, ne predviđa viša razina zaštite kojom se propisuju zahtjevi drukčiji od onih u sudskoj praksi ESLJP-a.

4.3.1. Pravne osnove, ograničenja i zaštitne mjere – istražne ovlasti koje se izvršavaju u kontekstu nacionalne sigurnosti

4.3.1.1. Opće napomene

148. EOZP podsjeća da je Zakon o istražnim ovlastima iz 2016. noviji zakon kojim je izmijenjeno nekoliko odredbi Zakona o obavještajnim službama iz 1994. Njime se utvrđuje u kojoj se mjeri određene istražne ovlasti smiju upotrebljavati za zadiranje u privatnost[89]. Unatoč dvama izvješćima povjerenika za istražne ovlasti koja pružaju korisne informacije o primjeni tog novog pravnog okvira još uvijek nisu preispitani određeni aspekti, posebno u pogledu korištenih čimbenika za odabir i kriterija pretraživanja.

149. Osim toga, kao opću napomenu o Zakonu o istražnim ovlastima iz 2016. i njegovu području primjene EOZP ističe četiri važne točke navedene u nastavku.

150. EOZP želi istaknuti dva aspekta u pogledu **prve važne točke**, koja se odnosi na obilježja prava.

151. Prvo, EOZP napominje da se zakonodavni propis odnosi na opće svrhe primjene postupaka predviđenih Zakonom o istražnim ovlastima iz 2016., a ne na kategorije pojedinaca na koje se može odnositi prikupljanje podataka na temelju dijelova od 2. do 7. Zakona o istražnim ovlastima iz 2016. EOZP u tom pogledu podsjeća da bi trebala postojati veza između kategorija pojedinaca koji mogu

[86] Vidjeti Preporuke EOZP-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora.
[87] Vidjeti presudu u predmetu Schrems II, t. 98.
[88] Vidjeti presudu Suda EU-a u spojenim predmetima C-511/18, C-512/18 i C-520/18, La Quadrature du Net i dr., 6. listopada 2020., ECLI:EU:C:2020:791, t. 124.
[89] Vidjeti članak 1. Zakona o istražnim ovlastima iz 2016.

biti predmet mjera nadzora i svrha koje se žele ostvariti zakonodavstvom kako bi se definiralo osobno područje primjene prava.

152. Nadalje, EOZP naglašava i da su i definicije „telekomunikacijskih operatora", „telekomunikacijske usluge" i „telekomunikacijskog sustava" kojima se utvrđuje područje primjene prava vrlo široke i donekle nejasne. EOZP ističe da se u smislu Zakona o istražnim ovlastima iz 2016. ti pojmovi moraju tumačiti na mnogo općenitiji način nego u zakonodavnim propisima o telekomunikacijama, kako je definirano, na primjer, u Europskom zakoniku elektroničkih komunikacija[90]. EOZP napominje da se smatra da su definicije „telekomunikacijske usluge" i „telekomunikacijskog sustava" u tom zakonu namjerno široke kako bi se mogle primjenjivati na nove tehnologije. Isto tako, definicija telekomunikacijskog operatora vrlo je široka i mogla bi uključivati, na primjer, internetske videoigre s integriranom funkcijom razgovora (*chat*) ili druge internetske stranice koje uključuju samo prozore za razgovor[91].

153. Osim toga, iako su postupci i nadzor koji se odnose na procjenu nužnosti i razmjernosti prikupljanja podataka i pristupa njima općenito predviđeni, kriteriji za provedbu takve procjene nisu definirani u samom zakonu. Dodatni elementi mogu se pronaći u drugim dokumentima, kao što su kodeksi prakse.

154. Međutim, kako se podsjeća u Preporukama EOZP-a 02/2020 o europskim temeljnim jamstvima za mjere nadzora, Sud EU-a naveo je da „zahtjev da svako ograničenje ostvarivanja temeljnih prava mora biti predviđeno zakonom znači da se u samoj pravnoj osnovi kojom se dopušta zadiranje u ta prava mora definirati doseg ograničenja ostvarivanja dotičnog prava"[92]. Točnije, Sud EU-a pojasnio je da propis, „da bi ispunio uvjet proporcionalnosti, [...] mora imati propisana jasna i precizna pravila kojima se uređuje doseg i primjena dotične mjere te propisivati minimalne uvjete, na način da osobe o čijim je osobnim podacima riječ raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu tih podataka od rizika zlouporabe. On mora biti zakonski obvezujuć u unutarnjem pravu i osobito navoditi u kojim se okolnostima i pod kojim uvjetima mjera kojom se predviđa obrada takvih podataka može donijeti, jamčeći time da će njezino zadiranje biti ograničeno na ono što je strogo nužno."[93]

155. ESLJP je isto tako naglasio važnost jasnoće zakona kako bi se pojedincima *„na odgovarajući način naznačilo u kojim okolnostima i pod kojim uvjetima javna tijela imaju ovlast koristiti se takvim mjerama"*[94].

---

[90] Vidjeti članak 2. stavak 5. Europskog zakonika elektroničkih komunikacija, u kojem se utvrđuje, na primjer, da „interpersonalna komunikacijska usluga" znači „usluga koja se uobičajeno pruža uz naknadu, a omogućuje izravnu interpersonalnu i interaktivnu razmjenu informacija putem elektroničkih komunikacijskih mreža između ograničenog broja osoba, pri čemu osobe koje pokreću komunikaciju ili sudjeluju u njoj određuju njezina primatelja ili više njih i ne uključuje usluge koje omogućuju interpersonalnu i interaktivnu komunikaciju samo kao manje bitnu pomoćnu značajku koja je suštinski povezana s drugom uslugom".

[91] Vidjeti Ministarstvo unutarnjih poslova, *Code of practice on the interception of communications* (Kodeks prakse o presretanju komunikacija), ožujak 2018., točka 2.5. i sljedeće, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Vidjeti presudu u predmetu Schrems II, t. 175. i navedenu sudsku praksu, kao i presudu Suda EU-a u predmetu C-623/17, Privacy International protiv Secretary of State for Foreign and Commonwealth Affairs i dr., 6. listopada 2020., ECLI:EU:C:2020:790 (dalje u tekstu „Privacy International"), t. 65.

[93] Vidjeti presudu u predmetu Privacy International, t. 68.

[94] Vidjeti presudu ESLJP-a u predmetu Zakharov protiv Rusije, 4. prosinca 2015., CE:ECHR:2015:1204JUD004714306, t. 229.

156. **EOZP stoga poziva Europsku komisiju da dodatno procijeni aspekte koji se odnose na preciznost, jasnoću i sveobuhvatnost relevantnog prava te da navede dodatne elemente kako bi dokazala da se tim pravom osigurava razina zaštite koja je u načelu istovjetna onoj koja se jamči u EU-u s obzirom na obilježja prava. EOZP isto tako naglašava da bi široke definicije trebalo ocijeniti i u odnosu na razmjernost mjera presretanja.**

157. Osim toga, iako su u nekoliko internih kodeksa nadležnih tijela obavještajne zajednice djelomično razrađeni neki od tih elemenata, na primjer u odnosu na procjenu nužnosti i razmjernosti prikupljanja podataka, EOZP naglašava da zahtjevi Suda EU-a u pogledu prirode prava podrazumijevaju da temeljni elementi, među ostalim kako bi se pojedinci mogli na njih osloniti u kontekstu pravne zaštite, moraju biti predviđeni zakonodavstvom kojim se propisuju prava na temelju kojih je moguće pokrenuti postupak pred sudom[95]. Doista, u točki 6. Priloga 7. Zakonu o izvršnim ovlastima iz 2016. spominje se činjenica da sudovi (i nadzorna tijela) „uzimaju u obzir propust osobe da pri utvrđivanju pitanja u bilo kojem takvom postupku vodi računa o kodeksu", a da se pritom ne pojašnjava mogu li se pojedinci pred sudovima (ili nadzornim tijelima) pozvati na povredu kodeksa. Osim toga, elementi koji su dosad navedeni u nacrtu odluke odnose se na činjenicu da ESLJP priznaje predvidljivost pravila predviđenih[96] tim kodeksima, a ne njihovu „provedivost" na sudu, kako to zahtijeva Sud EU-a, ili na činjenicu da su sudovi Ujedinjene Kraljevine u nekim predmetima uputili na kodekse, pri čemu se ni u jednom od navedenih predmeta ne spominje mogućnost pojedinaca da pokrenu postupak na temelju prava koja proizlaze iz tih kodeksa. **Ako se zaključi da se u pravu Ujedinjene Kraljevine dostatno ne navode okolnosti i uvjeti pod kojima se mjera može donijeti te da su ti elementi zapravo predviđeni internim kodeksima tijela obavještajne zajednice, EOZP poziva Europsku komisiju da dodatno procijeni mogu li pojedinci pokrenuti postupak pred sudom na temelju ograničenja i zaštitnih mjera predviđenih internim kodeksima tijela obavještajne zajednice te provesti ta ograničenja i zaštitne mjere.**

158. **Druga važna točka** odnosi se na činjenicu da će se odredbe koje se s jedne strane odnose na ciljano pribavljanje i zadržavanje podataka o komunikacijama i s druge strane na masovno prikupljanje, bilo u Zakonu o istražnim ovlastima iz 2016. bilo u drugim zakonodavnim propisima kao što je Zakon o obavještajnim službama iz 1994. ili Zakon o regulaciji istražnih ovlasti iz 2000., primjenjivati i na podatke koji se prenose iz EU-a u Ujedinjenu Kraljevinu. Kad je riječ o masovnom prikupljanju podataka, EOZP ističe da se relevantnim odredbama prava Ujedinjene Kraljevine omogućuje prikupljanje podataka izvan Ujedinjene Kraljevine, što bi moglo uključivati podatke u tranzitu koji se prenose iz EGP-a u Ujedinjenu Kraljevinu na temelju odluke o primjerenosti[97]. Nadalje, EOZP primjećuje da Europska komisija navodi da bi „trebalo napomenuti da se zadržavanje i pribavljanje podataka o komunikacijama obično ne odnosi na osobne podatke ispitanika iz EU-a koji se na temelju ove Odluke prenose u Ujedinjenu Kraljevinu. Obveza zadržavanja ili otkrivanja podataka o komunikacijama u skladu s dijelovima 3. i 4. Zakona o istražnim ovlastima iz 2016. obuhvaća podatke koje telekomunikacijski operatori u Ujedinjenoj Kraljevini prikupljaju izravno od korisnika

[95] Sud EU-a u tom je pogledu smatrao, na primjer, da Predsjednički ukaz br. 28 u SAD-u ne ispunjava uvjete iako su njime predviđena i određena ograničenja u pogledu masovnog prikupljanja podataka, vidjeti presudu u predmetu Schrems II, t. 181.

[96] Vidjeti presudu ESLJP-a Big Brother Watch i drugi protiv Ujedinjene Kraljevine, 13. rujna 2018., ECLI:CE:ECHR:2018:0913JUD00581701 (dalje u tekstu „Big Brother Watch"), t. 325.: „Budući da je Kodeks prakse o presretanju komunikacija javni dokument, pod uvjetom da su ga odobrila oba doma parlamenta, i da ga izvršitelji poslova presretanja i sudovi moraju uzeti u obzir, Sud je izričito prihvatio da se njegove odredbe mogu uzeti u razmatranje pri procjeni predvidljivosti režima Zakona o regulaciji istražnih ovlasti."

[97] Vidjeti t. 183. i sljedeće presude u predmetu Schrems II o procjeni zakonodavstva kojim se predviđa pristup podacima u tranzitu između EU-a i treće zemlje u kontekstu odluke o primjerenosti.

telekomunikacijske usluge."[98] Međutim, EOZP ističe nejasnoću u pogledu činjenice da samo poslovne jedinice tih operatora sa sjedištem u Ujedinjenoj Kraljevini mogu primati zahtjeve nadležnih tijela Ujedinjene Kraljevine jer je definicijom telekomunikacijskog operatora iz članka 261. stavka 10. Zakona o istražnim ovlastima iz 2016. propisano da je „telekomunikacijski operator osoba koja nudi ili pruža telekomunikacijsku uslugu osobama u Ujedinjenoj Kraljevini ili koja kontrolira ili osigurava telekomunikacijski sustav koji se (potpuno ili djelomično) nalazi u Ujedinjenoj Kraljevini ili kontrolira iz nje". Stoga bi osobni podaci ispitanika iz EGP-a doista mogli biti obuhvaćeni, na primjer u slučaju podataka koji su prikupljeni i generirani u poslovnoj jedinici telekomunikacijskog operatora iz Ujedinjene Kraljevine koja se nalazi u EGP-u, preneseni poslovnoj jedinici tog istog operatora koja se nalazi u Ujedinjenoj Kraljevini na temelju odluke o primjerenosti (u komercijalne svrhe) i zatim prikupljeni u nadležnim javnim tijelima u Ujedinjenoj Kraljevini.

159. **EOZP stoga smatra da je procjena tih odredbi relevantna i za procjenu razine primjerenosti pravnog okvira Ujedinjene Kraljevine te poziva Europsku komisiju da pojasni taj aspekt i dodatno procijeni u kojoj je mjeri to slučaj. EOZP posebno poziva Europsku komisiju da pojasni svoje razumijevanje područja primjene tog zakonodavnog propisa, među ostalim što obuhvaća pojam „korisnici telekomunikacijskih usluga", te mogu li se, s obzirom na vrlo široku definiciju telekomunikacijskih operatora, od poslovnih jedinica telekomunikacijskih operatora izvan Ujedinjene Kraljevine zatražiti podaci ako se odnose na ispitanike iz EGP-a.**

160. **Treća važna točka** odnosi se na postupak dvostruke zaštite. EOZP napominje da je u Zakonu o istražnim ovlastima iz 2016. uveden novi postupak dvostruke zaštite. No isto tako shvaća da čak i ako se podaci za potrebe nacionalne sigurnosti ili u obavještajne svrhe mogu prikupljati ili im se može pristupiti samo uz nalog koji je odobrio sudski povjerenik, Zakonom o istražnim ovlastima iz 2016. propisuje se da je „u ograničenom broju posebnih slučajeva zakonito presretanje bez naloga moguće te je potrebno samo prethodno odobrenje nadležnih tijela obavještajne zajednice [vidjeti odjeljak o nadzoru u nastavku], među ostalim za presretanja na temelju međunarodnih zahtjeva (članak 52. Zakona o istražnim ovlastima iz 2016.)". Kako je istaknuto u nastavku, to pridonosi dvojbama EOZP-a u pogledu otkrivanja informacija u inozemstvu. Osim toga, EOZP nadalje napominje i da je za ciljano ili masovno ometanje opreme moguće odstupanje od postupka dvostruke zaštite te da sudski povjerenik ima pravo odobriti samo produljenje naloga za masovno pribavljanje podataka nakon maksimalnog početnog razdoblja od šest mjeseci. **EOZP poziva Europsku komisiju da dodatno procijeni i dokaže da su čak i u slučajevima u kojima se ne primjenjuje postupak dvostruke zaštite pravnim okvirom Ujedinjene Kraljevine predviđene odgovarajuće zaštitne mjere, među ostalim djelotvornim mogućnostima *ex post* nadzora i pravne zaštite koje se nude pojedincima, kako bi se osiguralo da je razina pružene zaštite u načelu istovjetna onoj koja se jamči u EU-u (vidjeti i odjeljak 4.3.3. o nadzoru u nastavku).**

161. Nadalje, iako je Zakonom o istražnim ovlastima iz 2016. doista uveden postupak dvostruke zaštite, EOZP je i dalje zabrinut zbog određenih obilježja novog zakonodavstva. Nakon predstavljanja odgovarajućih odjeljaka nacrta odluke EOZP je analizirao sljedeće vrste prikupljanja podataka i pristupa njima istim redoslijedom kojim ih je predstavila Europska komisija. Redoslijed elemenata koji se procjenjuju u nastavku stoga ne odražava hijerarhiju u smislu razine zabrinutosti EOZP-a.

4.3.1.2. Ciljano pribavljanje i zadržavanje podataka o komunikacijama

162. EOZP napominje da postoje dva službenika koja mogu izdati ciljana odobrenja za pribavljanje podataka o komunikacijama: službenik za odobravanje u Uredu za izdavanje odobrenja za podatke o

[98] Vidjeti uvodnu izjavu 196nacrta odluke.

komunikacijama i nadležni viši službenik (osoba koja obnaša zadanu dužnost ili ima propisani položaj u relevantnom javnom tijelu), uz odobrenje sudskog povjerenika u određenim slučajevima. Međutim, EOZP-u je i dalje nejasno koji službenik, u skladu sa zakonom i relevantnim kodeksom, odobrava koju vrstu ciljanog pribavljanja podataka o komunikacijama i u kojoj bi mjeri nadležni službenik bio dovoljno neovisan[99].

163. **EOZP stoga poziva Europsku komisiju da dodatno procijeni taj aspekt i pojasni te elemente.**

164. Kad je riječ o obavijesti kojom se zahtijeva zadržavanje podataka o komunikacijama, EOZP napominje da se takve obavijesti mogu odnositi i na „opis operatora". Taj pojam znači da se zadržavanje podataka može istodobno zatražiti od više operatora. Pritom se ciljano pribavljanje podataka ne odnosi na broj operatora, već na ime ili opis osoba, organizacija, lokacije ili skupine osoba koje čine „cilj" zadržavanja, opis vrste istrage i opis aktivnosti za koje se oprema upotrebljava. EOZP stoga ističe da, ovisno o broju operatora na koje se odnosi takav „opis operatora", obavijest može biti šira od onoga što bi postupak ciljanog zadržavanja podataka mogao podrazumijevati. **EOZP poziva Europsku komisiju da dodatno procijeni taj aspekt i pruži dodatna jamstva da su obavijesti, čak i kad se odnose na više operatora, i dalje ograničene na ono što je strogo nužno i razmjerno.**

4.3.1.3. Ometanje opreme

165. EOZP napominje da u hitnim situacijama „ometanje opreme" može odstupati od postupka dvostruke zaštite[100]. Stoga upozorava da su svrhe u koje se može zahtijevati takvo ometanje opreme široke, a kriteriji hitnosti (kad sudski povjerenik nije obvezan izdati *ex ante* odobrenje nakon procjene nužnosti i razmjernosti ometanja opreme) i dalje nejasni. Budući da u potonjem slučaju „nalog prestaje važiti i ne može se produljiti" ako sudski povjerenik ne odobri ometanje opreme *ex post*, EOZP shvaća da se podaci prikupljeni u međuvremenu i dalje smatraju zakonito prikupljenima. Za brisanje tih podataka može se izdati poseban nalog sudskog povjerenika[101].

166. **EOZP poziva Europsku komisiju da dodatno procijeni uvjete pod kojima se može izdati hitni nalog te da pojasni moguće načine ostvarivanja prava predmetnih ispitanika i mogućnosti pravne zaštite koje im se nude u kontekstu aktivnosti ometanja opreme, posebno u hitnim situacijama koje dovode do odstupanja od postupka dvostruke zaštite.**

4.3.1.4. Masovno presretanje podataka preko nositelja

167. Kako je opisano u izvješću o preispitivanju ovlasti za masovno presretanje[102], „masovno presretanje obično uključuje prikupljanje komunikacija u tranzitu preko određenih nositelja (komunikacijskih poveznica)". U službenom informativnom članku o Zakonu o istražnim ovlastima iz 2016. „masovno presretanje" opisuje se kao „postupak prikupljanja određene količine komunikacija, nakon čega se odabiru konkretne komunikacije koje će se pročitati, pregledati ili preslušati kad je to nužno i razmjerno". EOZP napominje da „masovno presretanje" podataka zapravo podrazumijeva prikupljanje podataka čak i prije njihova filtriranja prema čimbenicima za odabir (jednostavnim u kontekstu praćenja pojedinaca za koje se već zna da predstavljaju prijetnju ili složenim u kontekstu otkrivanja novih prijetnji i nepoznatih osoba od interesa).

[99] Vidjeti i tekst u nastavku o procjeni postupka dvostruke zaštite i neovisnosti sudskog povjerenika.
[100] Vidjeti članak 109. Zakona o istražnim ovlastima iz 2016.
[101] Vidjeti članak 110. stavak 3. točku (b) Zakona o istražnim ovlastima iz 2016.
[102] Vidjeti *Report of the bulk powers review* (Izvješće o pregledu ovlasti za masovno presretanje), koji je izradio neovisni nadzornik zakonodavstva o suzbijanju terorizma, kolovoz 2016.

168. Pribavljanje masovnih podataka o komunikacijama bilo je i jedno od pitanja koja je Sud EU-a razmatrao u predmetu Privacy International, koji je rezultiralo presudom velikog vijeća od 6. listopada 2020. (uz pitanje je li takvo prikupljanje podataka provedeno u okviru prava Unije, čak i za potrebe nacionalne sigurnosti). Zakonom o istražnim ovlastima iz 2016. zamijenjeno je zakonodavstvo na koje se ta presuda odnosila.

169. EOZP napominje da je uvođenjem Zakona o istražnim ovlastima iz 2016. u pravo Ujedinjene Kraljevine nalog sada potreban i za masovno presretanje podataka. Postupak izdavanja tog naloga temelji se na utvrđivanju „operativnih svrha". Popis operativnih svrha utvrđuju čelnici obavještajnih službi, a zatim ga odobrava ministar unutarnjih poslova. Odluku odobrava neovisni sudski povjerenik, koji mora preispitati je li nalog nužan i razmjeran operativnim svrhama. EOZP shvaća da sudski povjerenik nije ovlašten procijeniti operativne svrhe, nego je li nalog nužan i razmjeran operativnim svrhama koje su u njemu navedene. Parlamentarnom odboru za obavještajne poslove i sigurnost svaka se tri mjeseca dostavlja primjerak popisa operativnih svrha, koji predsjednik vlade preispituje najmanje jednom godišnje.

170. No na temelju elemenata koje je Europska komisija navela u nacrtu odluke teško je procijeniti opseg operativnih svrha navedenih u popisu te je li prikupljanje podataka koje se na temelju njih provodi u skladu s pragom koji je utvrdio Sud EU-a (na primjer, zemljopisno područje prikupljanja podataka moglo bi biti ograničeno na svega nekoliko ulica, ali bi moglo uključivati i cijeli EGP).

171. Osim toga, EOZP naglašava da se masovno prikupljeni podaci mogu dugo čuvati (i biti dostupni za daljnji pristup radi pregleda). Napominje da se člankom 150. stavcima 5. i 6. Zakona o istražnim ovlastima iz 2016. predviđa samo uništavanje kopija prikupljenih podataka, i to isključivo ako njihovo zadržavanje nije potrebno ili vjerojatno neće biti potrebno u interesu nacionalne sigurnosti ili na bilo kojoj drugoj osnovi obuhvaćenoj područjem primjene članka 138. stavka 2. Zakona o istražnim ovlastima iz 2016. ili ako zadržavanje nije nužno za neke druge svrhe[103]. EOZP naglašava da se ti razlozi čine vrlo širokima te da se u svakom slučaju spominju samo kopije pribavljenih podataka.

172. Nadalje, EOZP napominje i da se u hitnim situacijama Zakonom o istražnim ovlastima iz 2016. omogućuje i izmjena naloga bez prethodnog odobrenja sudskog povjerenika te da bi u tom slučaju, ako sudski povjerenik od kojega je *ex post* zatraženo mišljenje u roku od tri radna dana nakon izmjene odbije odobriti izmjenu, nalog trebao imati učinak kao da izmjena nije provedena, a podaci prikupljeni u međuvremenu i dalje se smatraju zakonito prikupljenima[104]. Za brisanje tih podataka može se izdati poseban nalog sudskog povjerenika[105].

173. **EOZP stoga poziva Europsku komisiju da dodatno pojasni i procijeni masovna presretanja, posebno u pogledu odabira i primjene čimbenika za odabir u kontekstu postupaka masovnog presretanja kako bi se razjasnilo u kojoj mjeri pristup osobnim podacima zadovoljava prag koji je utvrdio Sud EU-a (vidjeti i odjeljak 4.3.1.7. u nastavku, osobito u odnosu na nadzor nad čimbenicima za odabir) i koje su zaštitne mjere uspostavljene za zaštitu temeljnih prava pojedinaca čiji se podaci presreću u tom kontekstu, među ostalim u pogledu razdoblja zadržavanja podataka. Posebno bi bila korisna neovisna procjena nadležnih nadzornih tijela Ujedinjene Kraljevine.**

174. **EOZP naglašava da se još kritičnijim čini kako „komunikacije povezane s inozemstvom" koje su obuhvaćene praksama masovnog presretanja upućuju na to da bi Ujedinjena Kraljevina mogla izravno presretati i masovno prikupljati podatke u EGP-u, uključujući podatke u tranzitu između**

[103] Vidjeti članak 150. stavke 3. i 6. Zakona o istražnim ovlastima iz 2016.
[104] Vidjeti članak 147. Zakona o istražnim ovlastima iz 2016. (dio 6. poglavlje I.).
[105] Vidjeti članak 181. stavak 3. točku (b) Zakona o istražnim ovlastima iz 2016.

EGP-a i Ujedinjene Kraljevine koji bi bili obuhvaćeni područjem primjene nacrta odluke (vidjeti odjeljak 4.3.2. u nastavku o daljnjoj uporabi informacija prikupljenih za potrebe nacionalne sigurnosti i otkrivanju informacija u inozemstvu).

4.3.1.5. Zaštita i zaštitne mjere za sekundarne podatke

175. Osim toga, EOZP izražava zabrinutost zbog toga što se relevantnim zakonodavstvom Ujedinjene Kraljevine koje se odnosi na masovno presretanje ne predviđa ista razina zaštite za sve podatke o komunikacijama. U skladu s člankom 137. Zakona o istražnim ovlastima iz 2016. sekundarni podaci, koji se mogu prikupljati na temelju naloga za masovno pribavljanje podataka, jesu podaci sustava „koji su sadržani u komunikaciji, uključeni kao njezin dio, koji su joj priloženi ili su s njome logički povezani (od strane pošiljatelja ili na drugi način)" i identifikacijski podaci „koji su sadržani u komunikaciji, uključeni kao njezin dio, koji su joj priloženi ili su s njome logički povezani (od strane pošiljatelja ili na drugi način), mogu se logički odvojiti od ostatka komunikacije te, u slučaju takva odvajanja, ne bi otkrili ništa što bi se razumno moglo smatrati (eventualnim) značenjem komunikacije, pri čemu se ne uzima u obzir značenje koje proizlazi iz činjenice komunikacije ili iz podataka koji se odnose na prijenos komunikacije"[106].

176. EOZP napominje da se na sekundarne podatke, poznate i kao metapodatke[107], koji se prikupljaju masovno ne primjenjuju iste zaštitne mjere kao na podatke prikupljene na temelju ciljanog naloga, ali i na masovno prikupljene podatke o sadržaju. Naime, EOZP primjećuje da se na odabir bilo kojeg od presretanih sadržaja primjenjuje više zaštitnih mjera[108] nego na odabir sekundarnih podataka[109].

177. Nadalje, EOZP naglašava da su ESLJP[110] i Sud EU-a[111] doveli u pitanje činjenicu da su takvi podaci manje osjetljivi od drugih, a posebno od podataka o sadržaju. Doista, u Kodeksu prakse o presretanju navode se primjeri sekundarnih podataka (podataka sustava, kao što su konfiguracije usmjerivača, adrese e-pošte ili identifikacijske oznake korisnika, ali i alternativne identifikacijske oznake računa, i identifikacijskih podataka, kao što su mjesto održavanja sastanka zabilježenog u kalendaru, informacije o fotografijama, na primjer vrijeme, datum i mjesto njihova snimanja). **EOZP stoga**

[106] Podaci sustava i identifikacijski podaci definirani su u članku 263. Zakona o istražnim ovlastima iz 2016.
[107] Vidjeti *Report of the bulk powers review* (Izvješće o pregledu ovlasti za masovno presretanje), koji je izradio neovisni nadzornik zakonodavstva o suzbijanju terorizma, kolovoz 2016.
[108] Vidjeti članak 152. stavak 1. točku (c) i članak 152. stavak 3. i sljedeće Zakona o istražnim ovlastima iz 2016.
[108] Vidjeti članak 152. stavak 1. točku (c) i članak 152. stavak 3. i sljedeće Zakona o istražnim ovlastima iz 2016.
[109] Vidjeti članak 152. stavak 1. točke (a) i (b) Zakona o istražnim ovlastima iz 2016.
[110] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, t. 357., predmet upućen velikom vijeću: „Stoga, iako Sud ne sumnja da su povezani podaci o komunikacijama važan alat obavještajnih službi u borbi protiv terorizma i teških kaznenih djela, ne smatra da su tijela postigla pravednu ravnotežu između suprotstavljenih javnih i privatnih interesa time što su te podatke u cijelosti izuzela od zaštitnih mjera koje se primjenjuju na pretraživanje i pregledavanje sadržaja. Iako Sud ne predlaže da povezani podaci o komunikacijama moraju biti dostupni samo kako bi se utvrdilo nalazi li se pojedinac na britanskim otocima jer bi se time zahtijevala primjena strožih standarda na povezane podatke o komunikacijama od onih koji se primjenjuju na sadržaj, ipak bi trebale postojati dostatne zaštitne mjere kako bi se osiguralo da se izuzeće povezanih podataka o komunikacijama od zahtjeva članka 16. Zakona o regulaciji istražnih ovlasti ograniči na mjeru koja je potrebna kako bi se utvrdilo nalazi li se pojedinac u ovom trenutku na britanskim otocima."
[111] Vidjeti t. 71 presude Suda EU-a u predmetu Privacy International: „Miješanje prijenosa podataka o prometu i lokaciji sigurnosnim i obavještajnim službama u pravo utvrđeno člankom 7. Povelje treba smatrati osobito ozbiljnim, uzimajući u obzir, među ostalim, osjetljivost informacija koje mogu pružiti te podatke, a osobito mogućnost da se na temelju njih utvrdi profil predmetnih osoba, što je jednako osjetljiva informacija kao i sam sadržaj komunikacija. Ono usto može kod predmetnih osoba stvoriti osjećaj da je njihov privatni život predmet trajnog nadzora (vidjeti po analogiji presude od 8. travnja 2014., Digital Rights Ireland i dr., C-293/12 i C-594/12, EU:C:2014:238, t. 27. i 37., i od 21. prosinca 2016., Tele2, C-203/15 i C-698/15, EU:C:2016:970, t. 99. i 100.)."

naglašava dosljednu procjenu ESLJP-a i Suda EU-a te podsjeća na zabrinutost izraženu u vezi sa sekundarnim podacima na koje bi se zbog njihove osjetljivosti trebale primjenjivati posebne zaštitne mjere. Stoga poziva Europsku komisiju da pažljivo procijeni osigurava li se zaštitnim mjerama predviđenima pravom Ujedinjene Kraljevine za takvu kategoriju osobnih podataka razina zaštite koja je u načelu istovjetna onoj koja se jamči u EU-u.

4.3.1.6. Automatizirana obrada podataka o komunikacijama

178. EOZP napominje da se tijela obavještajne zajednice pri filtriranju masovno pribavljenih podataka ne služe samo jednostavnim ili složenim čimbenicima za odabir, nego se mogu osloniti i na druge alate za automatiziranu obradu kako bi analizirala „velike količine informacija, što agencijama omogućuje i pronalaženje poveznica, obrazaca, udruženja ili ponašanja koji bi mogli ukazati na ozbiljnu prijetnju koja zahtijeva istragu", kako je navedeno u izvješću Odbora za obavještajne poslove i sigurnost iz 2015[112]. **EOZP je svjestan činjenice da se to javno izvješće odnosi na prakse iz prethodnog pravnog okvira, koji je kasnije zamijenjen Zakonom o istražnim ovlastima iz 2016. Međutim, smatra da postoji potreba za daljnjom neovisnom procjenom i nadzorom upotrebe alata za automatsku obradu u nadležnim nadzornim tijelima Ujedinjene Kraljevine te poziva Europsku komisiju da dodatno procijeni to pitanje i zaštitne mjere koje bi se u tom kontekstu osigurale i/ili mogle osigurati ispitanicima u EGP-u.**

4.3.1.7. Rizici u pogledu usklađenosti i neusklađene prakse nadležnih tijela obavještajne zajednice

179. EOZP prima na znanje da postoje detaljna izvješća o nadzoru. U njima se navode vrijedni elementi koji se ocjenjuju kao pozitivne prakse usklađivanja, kao i oni koji se odnose na utvrđene rizike u pogledu usklađenosti i neusklađene prakse.

180. U tom pogledu povjerenik za istražne ovlasti u svojem izvješću za 2019. naveo je da postoji nekoliko elemenata s obzirom na primjenu pravnog okvira u različitim nadležnim tijelima u kojima su otkriveni rizici od neusklađenosti ili neusklađenosti nadležnih tijela.

181. Prvo, EOZP je primijetio da kriteriji za klasifikaciju skupa podataka kao masovnih osobnih podataka ili kao ciljanih podataka nisu uvijek jasni sigurnosnim službama MI5 i SIS, a posebno službi MI5, što može dovesti do nepostojanja odgovarajućih zaštitnih mjera koje se primjenjuju na podatke[113]. U svojem izvješću za 2019. povjerenik za istražne ovlasti predložio je da bi „rješavanju tog pitanja trebalo dati prioritet"[114]. EOZP o skupovima masovnih osobnih podataka napominje i da je, iako je

---

[112] Vidjeti Parlamentarni odbor za obavještajne poslove i sigurnost, *Privacy and Security: A modern and transparent legal framework* (Privatnost i sigurnost: moderan i transparentan pravni okvir), 2015., točka 18., str. 13., https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), 15. prosinca 2020., točku 8.39., https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: „Primijetili smo pozitivan razvoj [Odbora za nadzor masovnih podataka] i njegov utjecaj na upravljanje unutarnjom usklađenošću. I dalje tražimo da se pojasni postupak koji služba MI5 upotrebljava za provedbu početnih pregleda novih skupova podataka kako bi se bolje razumjele odluke o klasifikaciji skupa podataka kao masovnih osobnih podataka ili, na primjer, kao ciljanih podataka. Bili smo zabrinuti zbog jedne neriješene mjere u zapisniku Odbora za nadzor masovnih podataka koja se odnosila na nepodudarnosti u raspodjeli masovnih osobnih podataka između službi MI5 i SIS. S obzirom na razlike u upotrebi podataka i skupinama podataka koji se čuvaju moguće je da obje agencije mogu imati isti skup podataka ili njegove verzije te da ga jedna agencija može zakonito kategorizirati kao masovne podatke, a druga kao ciljane. Postoji rizik da bi se, ako je jedna od agencija netočno kategorizirala bazu podataka kao ciljanu, podaci mogli čuvati bez odgovarajućeg naloga i možda ne bi podlijegali odgovarajućim zaštitnim mjerama."

[114] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 8.39.

klasifikacija skupova masovnih osobnih podataka zadovoljavajuća (što povjerenik za istražne ovlasti tek treba revidirati), GCHQ izrazio zabrinutost nakon ocjenjivanja unutarnje usklađenosti naloga koje je proveo njegov nadležni tim za usklađenost u ožujku 2019. jer 50 % obrazloženja za naloge za masovno pribavljanje podataka koje je taj tim ocijenio nije ispunilo zahtijevani standard. Prema mišljenju povjerenika za istražne ovlasti tim za usklađenosti počeo je ispitivati problem i provoditi ponovno osposobljavanje osoblja radi poboljšanja tog standarda. Usklađenost GCHQ-a u tom području poboljšala se osposobljavanjem radi obnavljanja znanja o odredbama Zakona o istražnim ovlastima iz 2016. i dodatnim osposobljavanjem koje provode mreže za politiku i usklađenost. Povjerenik za istražne ovlasti ne očekuje da će se u budućim inspekcijama pokazati da se taj standard pogoršao, ali će nastaviti pozorno preispitivati to područje[115]. **EOZP se stoga slaže sa stajalištem da Europska komisija u okviru procjene razine zaštite treba dodatno preispitati i pratiti navedene elemente kako bi se osiguralo poboljšanje tog standarda, kako je istaknuto u izvješću povjerenika za istražne ovlasti, i podsjeća da se pri procjeni bitne ekvivalentnosti treće zemlje uzimaju u obzir provedba i konkretna primjena pravnog okvira, kako je predviđeno člankom 45. Opće uredbe o zaštiti podataka.**

182. U širem smislu EOZP naglašava važne točke koje povjerenik za istražne ovlasti navodi u pogledu „pretraga na temelju zadatka" koje provode službenici službe MI5 i koje istražitelju omogućuju da provede više pretraga dostupnih skupova masovnih osobnih podataka te u pogledu „ozbiljnih rizika usklađenosti povezanih s određenim tehnološkim okruženjima koje upotrebljava služba MI5" koji se odnose na pitanja gdje su podaci bili pohranjeni u okruženju, tko im je imao pristup, u kojoj su se mjeri umnožavali ili dijelili te koji su se postupci brisanja na njih primjenjivali, kao i na razdoblja zadržavanja. Iako povjerenik za istražne ovlasti navodi da su poduzete mjere i uvedene zaštitne mjere, neke od njih i dalje su ručne i provode se na pojedinačnoj, ljudskoj osnovi te se naglašava da je važno da „služba MI5 nastavi održavati te nove postupke i osigura dostatne resurse za njihovo učinkovito funkcioniranje. Ako MI5 utvrdi porast neusklađenih postupanja'"[116]**.** Povjerenik za istražne ovlasti očekuje da će o njima biti obaviješten u najkraćem mogućem roku. **EOZP stoga poziva Europsku komisiju da pomno prati te aspekte u budućnosti**.

183. Kad je riječ o GCHQ-u, EOZP iz izvješća povjerenika za istražne ovlasti zaključuje da se u pogledu operacija provedenih na temelju naloga za masovno prikupljanje podataka „kvaliteta zahtjeva za unutarnje odobrenje razlikovala i primijetili smo da se način na koji se ti zahtjevi sastavljaju može poboljšati"[117] te da su objašnjenja za upotrebu općih deskriptora pri ciljanom ometanju opreme ponekad preopćenita i neprecizna[118]. EOZP je primijetio i da u kontekstu masovnog ometanja opreme povjerenik za istražne ovlasti preporučuje da se „u zahtjevima dosljedno i detaljno evidentira veza između cilja i zakonske svrhe te zahtjeva u pogledu obavještajnih podataka"[119], da se „u svim zahtjevima jasno objasni mogućnost pristupa neciljanim podacima i relevantne mjere ublažavanja pri

[115] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.48.

[116] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 8.52.

[117] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.2.

[118] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točke 10.16 i 10.17.

[119] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.23.

procjeni razmjernosti”[120] te da je povjerenik naglasio da usprkos napretku „još uvijek ima prostora za poboljšanje”[121] i da će i u budućnosti tome trebati posvetiti dodatnu pozornost.

184. Kad je riječ o režimu masovnog presretanja u skladu sa Zakonom o regulaciji istražnih ovlasti iz 2000., koji je u međuvremenu zamijenjen odredbama Zakona o istražnim ovlastima iz 2016., EOZP podsjeća da je nedostatan nadzor odabira internetskih nositelja za presretanje te filtriranja, pretraživanja i odabira presretanih komunikacija radi pregleda bio jedan od ključnih aspekata koje je ESLJP smatrao neusklađenima s člankom 8. EKLJP-a u pogledu prethodnog zakonodavstva o istražnim ovlastima tijela Ujedinjene Kraljevine u kontekstu nacionalne sigurnosti u predmetu Big Brother Watch, koji je sada upućen velikom vijeću. **EOZP poziva Europsku komisiju da provjeri trenutačno stanje postupka, uzme u obzir te elemente i navede ih u odluci o primjerenosti ako je Europska komisija donese.**

185. U tom predmetu ESLJP „nije [bio] uvjeren da su zaštitne mjere za odabir nositelja za presretanje i odabir presretanog materijala radi pregleda dovoljno snažne da pruže odgovarajuća jamstva protiv zlouporabe. No najviše zabrinjava nepostojanje strogog neovisnog nadzora nad čimbenicima za odabir i kriterijima pretraživanja koji se upotrebljavaju za filtriranje presretanih komunikacija.”[122] Kako je istaknuo povjerenik za istražne ovlasti, „taj zaključak sličan je preporuci iz izvješća Odbora za obavještajne poslove i sigurnost *Privacy and Security: A modern and transparent legal framework* (Privatnost i sigurnost: moderan i transparentan pravni okvir) iz ožujka 2015.”[123] **EOZP pozdravlja činjenicu da je zbog toga povjerenik za istražne ovlasti 2019. preispitao svoj pristup inspekcijama masovnog presretanja, „što je uključivalo pažljivo preispitivanje tehnički složenih načina na koje se masovno presretanje zapravo provodi”[124], te se obvezao uključiti „detaljno ispitivanje čimbenika za odabir i kriterija pretraživanja na koje upućuje ESLJP”[125] u inspekcije masovnog presretanja od 2020. nadalje. S obzirom na važnost tog aspekta EOZP je zabrinut jer povjerenik još nije detaljno ispitao čimbenike za odabir i kriterije pretraživanja te poziva Europsku komisiju da pomno prati razvoj događaja u tom pogledu, posebno s obzirom na to da tek treba pojasniti konkretan oblik takva nadzora[126].**

4.3.2. Daljnja upotreba informacija prikupljenih za potrebe nacionalne sigurnosti i otkrivanje informacija u inozemstvu

186. Kad je riječ o daljnjoj upotrebi informacija koje se prikupljaju za potrebe nacionalne sigurnosti, Europska komisija u svojoj procjeni upućuje na članak 87. stavak 1. Zakona o zaštiti podataka iz 2018., u kojem se zaista navodi da se „tako prikupljeni osobni podaci ne smiju obrađivati na način koji nije u skladu sa svrhom u koju su prikupljeni”. Međutim, EOZP ističe da u skladu s člankom 110. Zakona o zaštiti podataka iz 2018. ta odredba može podlijegati izuzećima zbog nacionalne sigurnosti. EOZP

[120] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.23.
[121] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.23.
[122] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, t. 347.
[123] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.28.
[124] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.28.
[125] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.28.
[126] Vidjeti *Annual Report of the Investigatory Powers Commissioner 2019* (Godišnje izvješće povjerenika za istražne ovlasti za 2019.), točku 10.28.: „točan oblik te inspekcije još nije dogovoren”.

nadalje napominje da je zakonodavstvom predviđena mogućnost „otkrivanja informacija u inozemstvu" bez obzira radi li se o ciljanom presretanju i pregledavanju, ciljanom pribavljanju i zadržavanju podataka o komunikacijama, ciljanom ometanju opreme ili masovnom presretanju i masovnom ometanju opreme.

4.3.2.1. Daljnja upotreba, otkrivanje informacija u inozemstvu i primjenjivi pravni okvir u Ujedinjenoj Kraljevini

187. Europska komisija utvrdila je da dio 4. Zakona o zaštiti podataka iz 2018., a posebno njegov članak 109., čini relevantne odredbe u kojima se utvrđuju posebni zahtjevi za daljnju uporabu prikupljenih informacija, u prvom redu za međunarodni prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama koji provode obavještajne službe. No EOZP napominje da je člankom 110. Zakona o zaštiti podataka iz 2018. predviđeno izuzeće zbog nacionalne sigurnosti i utvrđeno da se određene odredbe Zakona o zaštiti podataka iz 2018. ne primjenjuju ako je potrebno izuzeće od tih odredbi u svrhu zaštite nacionalne sigurnosti. Odredbe koje se možda ne primjenjuju uključuju dio 4. poglavlje 2. Zakona o zaštiti podataka iz 2018. o načelima zaštite podataka, među ostalim o ograničenju svrhe, te dio 4. poglavlje 3. Zakona o zaštiti podataka iz 2018. o pravima ispitanika. Članak 109. Zakona o zaštiti podataka iz 2018. u vezi s člankom 110. istog zakona i uvjetima pod kojima se primjenjuje može dovesti do slučajeva u kojima obavještajne službe prenose osobne podatke u inozemstvo trećim zemljama bez primjene odredbi o načelima zaštite podataka i pravima ispitanika.

188. Kako je utvrdila Europska komisija, takvo izuzeće mora se procijeniti u svakom pojedinom slučaju i na njega se može pozvati samo ako bi primjena određene odredbe imala negativne posljedice za nacionalnu sigurnost. Naime, izdavanjem nacionalne potvrde obavještajnim službama Ujedinjene Kraljevine nastoji se potvrditi da je izuzeće potrebno za određene osobne podatke koji se obrađuju u svrhu zaštite nacionalne sigurnosti. No EOZP napominje da u svojim smjernicama o potvrdama o nacionalnoj sigurnosti u skladu sa Zakonom o zaštiti podataka iz 2018. Ministarstvo unutarnjih poslova Ujedinjene Kraljevine pojašnjava da je „[v]ažno [...] od samog početka napomenuti da potvrda nije potrebna za primjenu izuzeća zbog nacionalne sigurnosti, već će u većini slučajeva voditelji obrade sami utvrditi primjenjuje li se izuzeće zbog nacionalne sigurnosti". [127] Osim toga, u smjernicama Ministarstva unutarnjih poslova Ujedinjene Kraljevine navodi se da se „[p]otvrde o nacionalnoj sigurnosti mogu [...] primjenjivati na osobne podatke koji se mogu konkretno utvrditi ili koji obuhvaćaju širu kategoriju osobnih podataka. Potvrde mogu biti preventivne ili retroaktivne." [128] Izuzeće zbog nacionalne sigurnosti stoga se može primijeniti u odnosu na međunarodni prijenos osobnih podataka trećim zemljama koji provode obavještajne službe u slučaju nepostojanja potvrde o nacionalnoj sigurnosti.

189. EOZP nadalje napominje da se, na primjer, u potvrdi o nacionalnoj sigurnosti DPA/S27/Security Service[129] predviđa da su osobni podaci koji se obrađuju „za Sigurnosnu službu, u njezino ime, na njezin zahtjev ili uz njezinu pomoć ili" i „ako je takva obrada potrebna kako bi se olakšalo pravilno

[127] Vidjeti Ministarstvo unutarnjih poslova, *The Data Protection Act 2018, National Security Certificates guidance* (Zakon o zaštiti podataka iz 2018., Smjernice o potvrdama o nacionalnoj sigurnosti), kolovoz 2020., točku 3., str. 3.

[128] Vidjeti Ministarstvo unutarnjih poslova, *The Data Protection Act 2018, National Security Certificates guidance* (Zakon o zaštiti podataka iz 2018., Smjernice o potvrdama o nacionalnoj sigurnosti), kolovoz 2020., točku 5., str. 4.

[129] Vidjeti DPA/S27/Security Service, članak 27. Zakona o zaštiti podataka iz 2018, potvrda ministra unutarnjih poslova, 24. srpnja 2019., https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

obavljanje funkcija Sigurnosne službe opisanih u članku 1. Zakona o Sigurnosnoj službi iz 1989." do 24. srpnja 2024. izuzeti od odredbi prava Ujedinjene Kraljevine koje odgovaraju poglavlju V. Opće uredbe o zaštiti podataka o prijenosima osobnih podataka trećim zemljama ili međunarodnim organizacijama. Iako se drugim javno dostupnim potvrdama o nacionalnoj sigurnosti ne predviđa izuzeće od odredbi članka 109. Zakona o zaštiti podataka iz 2018., valja podsjetiti da se dio teksta ili cijeli tekst potvrde o nacionalnoj sigurnosti može izostaviti ako bi njegova objava bila protivna interesima nacionalne sigurnosti ili javnom interesu ili bi mogla ugroziti sigurnost bilo koje osobe.

190. Pri procjeni nacrta odluke u odnosu na te odredbe EOZP općenito primjećuje da zaštitne mjere za takvo otkrivanje obuhvaćaju samo zahtjev da primatelj podataka poštuje zahtjeve koji se odnose na sigurnost podataka, ograničavanje opsega otkrivanja na ono što je nužno, zadržavanje podataka i ograničavanje pristupa podacima na određeni broj osoba. Stoga **EOZP naglašava da, kad je riječ o otkrivanju informacija u inozemstvu, primjena izuzeća zbog nacionalne sigurnosti predviđenog pravom Ujedinjene Kraljevine može dovesti do situacija u kojima se u trećoj zemlji odredišta ne bi u potpunosti osigurale ili poštovale zaštitne mjere kojima se jamče poštovanje načela ograničenja svrhe, nužnosti i razmjernosti te prava pojedinaca, nadzor i pravna zaštita. EOZP stoga preporučuje Europskoj komisiji da dodatno ispita opće zaštitne mjere predviđene pravom Ujedinjene Kraljevine kad je riječ o otkrivanju informacija u inozemstvu, posebno s obzirom na primjenu izuzeća zbog nacionalne sigurnosti.**

4.3.2.2. Otkrivanje informacija u inozemstvu i dijeljenje obavještajnih podataka u okviru međunarodne suradnje

191. EOZP napominje i da Europska komisija u svojoj procjeni primjerenosti nije uzela u obzir postojeće međunarodne sporazume sklopljene između Ujedinjene Kraljevine i trećih zemalja ili međunarodnih organizacija u kojima bi mogle biti predviđene posebne odredbe o međunarodnom prijenosu osobnih podataka trećim zemljama koji provode obavještajne službe.

192. EOZP naglašava i da se procjena Europske komisije uglavnom temelji na procjeni dijela 4. Zakona o zaštiti podataka iz 2018., a posebno je zabrinut zbog toga što je Zakon o istražnim ovlastima iz 2016. u prvom redu usmjeren na „zahtjeve" za razmjenu obavještajnih podataka sa stranim partnerima te se ne bavi drugim oblicima dijeljenja obavještajnih podataka. EOZP u tom pogledu napominje da se u nacrtu odluke Europske komisije ne upućuje na povezanost zakonodavnog okvira Ujedinjene Kraljevine sa Sporazumom Ujedinjene Kraljevine i SAD-a o obavještajnim podacima o komunikacijama niti se ona procjenjuje. U nedavnoj izjavi povodom 75. obljetnice tog sporazuma američka Agencija za nacionalnu sigurnost (dalje u tekstu „NSA") navela je da to partnerstvo omogućuje „dvjema agencijama da u što većoj mjeri dijele informacije uz minimalna ograničenja" i da su „tim povijesnom dokumentom uspostavljeni politike i postupci za dijeljenje informacija o komunikacijama, prijevodima, analizama i dešifriranju kodova između obavještajnih stručnjaka iz Ujedinjene Kraljevine i SAD-a"[130]. Taj je sporazum postao i temelj za druga partnerstva u području obavještajnog rada s Australijom, Kanadom i Novim Zelandom.

193. Tajnost tog sporazuma i njegovih posebnih odredbi ozbiljno ugrožava jasnoću i predvidljivost prava s obzirom na daljnju upotrebu informacija koje tijela Ujedinjene Kraljevine prikupljaju za potrebe nacionalne sigurnosti i njihovo otkrivanje u inozemstvu. U tom kontekstu EOZP podsjeća da je u pogledu razine zaštite zajamčene u EU-u Sud EU-a naglasio da zakonodavstvo koje uključuje zadiranje u temeljno pravo na zaštitu osobnih podataka mora „predvidjeti jasna i precizna pravila koja uređuju

[130] Vidjeti priopćenje NSA-a za medije, *GCHQ and NSA Celebrate 75 Years of Partnership* (NSA i GCHQ obilježavaju 75 godina partnerstva), 5. veljače 2021., https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

doseg i primjenu mjere te propisati minimalne uvjete na način da osobe čiji se osobni podaci obrađuju raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih podataka od rizika zloporabe kao i od svih nezakonitih pristupa i uporabe tih podataka. Nužnost raspolaganja takvim jamstvima još je i značajnija kada su osobni podaci podvrgnuti automatskoj obradi te postoji značajan rizik od nezakonitog pristupa tim podacima"[131]. EOZP stoga smatra da bi Europska komisija u okviru svoje procjene primjerenosti trebala razmotriti učinak Sporazuma Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama.

194. ESLJP je u svojoj presudi Prvog odjela od 13. rujna 2018. u predmetu Big Brother Watch ocijenio režim dijeljenja obavještajnih podataka Ujedinjene Kraljevine, a posebno Sporazum Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama. Naveo je da „[z]akonski okvir kojim se obavještajnim službama Ujedinjene Kraljevine dopušta da zatraže presretani materijal od stranih obavještajnih agencija nije sadržan u Zakonu o regulaciji istražnih ovlasti. Sporazumom Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama od 5. ožujka 1946. izričito se dopušta razmjena materijala između Sjedinjenih Američkih Država i Ujedinjene Kraljevine"[132] te je taj sud smatrao da postoji „osnova u pravu za traženje obavještajnih podataka od stranih obavještajnih agencija i da je to pravo dovoljno dostupno"[133]. Iako je ESLJP zaključio da nije došlo do povrede članka 8.[134] EKLJP-a u pogledu režima dijeljenja obavještajnih podataka, EOZP napominje da je ta presuda sada upućena velikom vijeću, koje je još nije donijelo odluku. Nadalje navodi da je sutkinja Koskelo u svojem djelomično izdvojenom, a djelomično suglasnom mišljenju kojem se pridružila sutkinja Turković[135] zaključila da je došlo do povrede članka 8. EKLJP-a u odnosu na režim dijeljenja obavještajnih podataka, navodeći da je„[l]ako [...] složiti se s načelom da nijedan aranžman za pribavljanje obavještajnih podataka iz presretanih komunikacija od stranih obavještajnih službi, na temelju zahtjeva za provedbu takvog presretanja ili za prenošenje njegovih rezultata, ne bi smio uključivati izbjegavanje zaštitnih mjera koje moraju biti uspostavljene za svaki nadzor koji provode nacionalna tijela (vidjeti točke 216., 423. i 447.). Naime, svaki drugi pristup bio bi neprihvatljiv."

195. Kako je istaknuto u nekoliko izvješća medija i nevladinih organizacija[136][137], zadnja verzija Sporazuma Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama objavljena je 1956., otkad su se komunikacijska tehnologija i priroda obavještajnih podataka prikupljenih elektroničkim izviđanjem znatno promijenile. Izvješća medija otkrila su, na primjer, da GCHQ presreće i stavlja NSA-u na raspolaganje podatke koji se prenose podmorskim kabelima do Ujedinjene Kraljevine[138].

---

[131] Vidjeti presudu u predmetu Schrems I, t. 91.
[132] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, t. 425.
[133] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, t. 427.
[134] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, t. 448.
[135] Vidjeti presudu ESLJP-a u predmetu Big Brother Watch, djelomično suglasno i djelomično izdvojeno mišljenje sutkinje Koskelo, kojoj se pridružila sutkinja Turković.
[136] Vidjeti BBC, *Diary reveals birth of secret UK-US spy pact that grew into Five Eyes* (Dnevnik otkriva nastanak tajnog britansko-američkog špijunskog pakta koji je prerastao u dogovor „Pet očiju"), 5. ožujka 2021., https://www.bbc.com/news/uk-56284453.
[137] Vidjeti Privacy International, *Policy Briefing – UK Intelligence Sharing Arrangements* (Kratki prikaz politike – Aranžmani Ujedinjene Kraljevine za dijeljenje obavještajnih podataka), travanj 2018., https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Vidjeti The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications* (GCHQ tajno pristupa svjetskim komunikacijama služeći se optičkim kabelima), 21. lipnja 2013., https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

196. Kad je riječ o dijeljenju obavještajnih podataka, EOZP ključnim smatra pitanje jesu li članak 109. Zakona o zaštiti podataka iz 2018. i odredbe Zakona o istražnim ovlastima iz 2016. i dalje primjenjivi ka obavještajne službe Ujedinjene Kraljevine postupaju u skladu sa Sporazumom Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama. Drugi ključni element koji treba procijeniti jest utječu li odredbe ili učinkovita primjena tog sporazuma na razinu zaštite osobnih podataka u tranzitu iz EGP-a u Ujedinjenu Kraljevinu te omogućuju li obavještajnim službama drugih trećih zemalja izravan pristup osobnim podacima i njihovo pribavljanje.

197. Slijedom toga, osim zadrški izraženih u pogledu „otkrivanja informacija u inozemstvu" na temelju dijela 4. Zakona o zaštiti podataka iz 2018. i povezanog izuzeća zbog nacionalne sigurnosti, kao i zahtjeva u okviru Zakona o istražnim ovlastima iz 2016., **EOZP izražava zabrinutost zbog drugih oblika dijeljenja i otkrivanja informacija na temelju drugih instrumenata, posebno različitih međunarodnih sporazuma koje je Ujedinjena Kraljevina sklopila s drugim trećim zemljama, osobito ako ti instrumenti i dalje nisu dostupni javnosti, kao što je Sporazum Ujedinjene Kraljevine i SAD-a o razmjeni obavještajnih podataka o komunikacijama. Učinak takvog sporazuma mogao bi dovesti do izbjegavanja zaštitnih mjera utvrđenih u pogledu pristupa osobnim podacima i njihove upotrebe za potrebe nacionalne sigurnosti.**

198. Naime, EOZP dijeli stajalište posebnog izvjestitelja Ujedinjenih naroda Joea Cannataccija da „[d]ijeljenje obavještajnih podataka ne smije rezultirati skrivenim pokušajem da se drugima omogući ili olakša pribavljanje obavještajnih podataka bez nacionalnih zaštitnih mjera, kao ni rupom u zakonu na temelju koje strane vlade s nižim standardima zaštite privatnosti (ili drugih ljudskih prava) od obavještajnih službi Ujedinjene Kraljevine pribavljaju obavještajne podatke koji bi mogli dovesti do povreda ljudskih prava"[139].

199. Osim toga, **EOZP smatra da sklapanje bilateralnih ili multilateralnih sporazuma s trećim zemljama u svrhu suradnje u području obavještajnog rada kojima se osigurava pravna osnova za izravno presretanje ili pribavljanje osobnih podataka ili njihov prijenos tim zemljama može isto tako znatno utjecati na uvjete za daljnju upotrebu prikupljenih informacija jer takvi sporazumi mogu utjecati na pravni okvir Ujedinjene Kraljevine za zaštitu podataka koji se ocjenjuje.**

4.3.3. Nadzor

200. EOZP naglašava važnost sveobuhvatnog nadzora koji provode neovisna nadzorna tijela za primjerenost razine zaštite podataka. Cilj je jamstva neovisnosti nadzornih tijela u smislu članka 8. stavka 3. Povelje EU-a osigurati učinkovito i pouzdano praćenje usklađenosti s pravilima o zaštiti pojedinaca u vezi s obradom osobnih podataka.

201. Kad se osobnim podacima pristupa i kad se oni upotrebljavaju za potrebe nacionalne sigurnosti, funkciju nadzora uglavnom imaju povjerenik za istražne ovlasti i sudski povjerenici (dalje u tekstu „sudski povjerenici").

202. **EOZP općenito prepoznaje uvođenje sudskih povjerenika u Zakon o istražnim ovlastima iz 2016. kao znatno poboljšanje.** U skladu s navedenim zahtjevom Europska komisija poziva se da detaljnije procijeni neovisnost **sudskih povjerenika, a posebno u kojoj je mjeri pravno osigurana neovisnost**

[139] Vidjeti *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* (Izjava o završetku misije posebnog izvjestitelja za pravo na privatnost na kraju njegove misije u Ujedinjenoj Kraljevini Velike Britanije i Sjeverne Irske), London, 29. lipnja 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.

povjerenika za istražne ovlasti i Ureda povjerenika za istražne ovlasti s obzirom na to da se ona ne spominje u Zakonu o istražnim ovlastima iz 2016. To je još važnije jer povjerenik za istražne ovlasti odlučuje o žalbama vlade u slučaju da je sudski povjerenik odbio zahtjev za **mjeru** nadzora.

203. Povjerenik za istražne ovlasti ima funkcije *ex ante* i *ex post* nadzora. Kad je riječ o *ex ante* nadzoru, EOZP shvaća da je funkcija sudskih povjerenika da u pojedinačnim slučajevima odobravaju različite mjere nadzora, uključujući ciljano presretanje i masovno pribavljanje podataka o komunikacijama. EOZP nadalje napominje da se prethodno odobrenje mjera nadzora ne može izvesti iz sudske prakse Suda EU-a kao apsolutni zahtjev za razmjernost mjera nadzora[140].

204. Kako bi se procijenila učinkovitost te razine nadzora, EOZP ipak smatra da je potrebno dodatno pojasniti scenarije u kojima je moguće zakonito presretanje bez prethodnog odobrenja sudskih povjerenika.

205. U svojem nacrtu odluke Europska komisija u pogledu ciljanih presretanja u bilješkama 201. i 266. navodi „ograničen broj posebnih slučajeva" predviđenih u člancima od 44. do 52. Zakona o istražnim ovlastima iz 2016. EOZP napominje da su članci od 45. do 51. Zakona o istražnim postupcima iz 2016. izuzeća za koja se tvrdi da ih obavještajne službe ne upotrebljavaju redovito. Nadalje, **EOZP shvaća** da se **u slučajevima u kojima se primjenjuju izuzeća** (npr. pružatelji telekomunikacijskih i poštanskih usluga) prethodno odobrenje koje daju sudski povjerenici treba provesti ako tijela za izvršavanje zakonodavstva ili obavještajne službe **zatraže** pristup tim podacima **te poziva Europsku komisiju da u svojoj odluci potvrdi da je to točno.**

206. EOZP prepoznaje da se člankom 44. stavkom 2. Zakona o istražnim ovlastima iz 2016. dopušta presretanje komunikacija ako je jedna od stranaka (pošiljatelj ili primatelj) dala suglasnost i ako postoji odobrenje u skladu sa Zakonom o regulaciji istražnih ovlasti iz 2000. ili Zakonom o regulaciji istražnih ovlasti (Škotska) iz 2000. (2000 asp 11), odnosno prethodna pravna situacija prije uspostave sudskih povjerenika. EOZP **poziva** Europsku komisiju da pojasni znači li to da se u slučajevima u kojima postoji jednostrana suglasnost postupak prethodnog odobrenja uopće ne bi primjenjivao.

207. Kad je riječ o *ex post* nadzoru, važno je provjeriti i je li osiguran učinkovit neovisan nadzor bez nedostataka, posebno ako nije predviđen *ex ante* nadzor.

208. EOZP napominje da za članke od 48. do 52. Zakona o istražnim ovlastima iz 2016. sudski povjerenici provode *ex post* preispitivanje te **poziva Europsku komisiju da pojasni u skladu s kojim se zahtjevima i na čiju inicijativu ono provodi.**

209. U skladu s člankom 229. stavkom 4. Zakona o istražnim ovlastima iz 2016. povjerenik za istražne ovlasti ne mora preispitivati obavljanje određenih funkcija. U tom pogledu EOZP poziva Europsku komisiju da pojasni odredbe članka 229. stavka 4. točaka (d) i (e) Zakona o istražnim ovlastima iz 2016. s obzirom na njegov praktični učinak na nadležnost povjerenika za istražne ovlasti u pogledu preispitivanja. **EOZP smatra da je Ured povjerenika za informiranje nadležno nadzorno tijelo kad se primjenjuju izuzeća iz članka 229. stavka 4. Zakona o istražnim ovlastima iz 2016. te poziva Europsku komisiju da u svojoj odluci potvrdi da je to točno.**

210. **Pri provedbi** *ex post* nadzora uloga **povjerenika za istražne ovlasti ograničena je** na davanje preporuka u slučajevima neusklađenosti i obavješćivanje ispitanika ako je pogreška ozbiljna i u

[140] Međutim, napominje i da je Sud EU-a, kad je poništio sustav zaštite privatnosti u presudi u predmetu Schrems II, primio na znanje činjenicu da u skladu s pravom SAD-a takozvani Sud FISA-e „ne odobrava pojedinačne mjere nadzora, već odobrava programe nadzora (npr. PRISM, UPSTREAM) na temelju godišnjih certifikacija" (t. 179.).

javnom je interesu da se osoba obavijesti. **EOZP poziva Europsku komisiju da pojasni kako Ured povjerenika za istražne ovlasti može učinkovito osigurati usklađenost sa zakonom.**

211. **Naposljetku, EOZP razumije da se pogođeni pojedinci ne mogu izravno obratiti Uredu povjerenika za istražne ovlasti, već moraju podnijeti pritužbu Uredu povjerenika za informiranje, čije su nadležnosti u području nacionalne sigurnosti ograničene. EOZP stoga poziva Europsku komisiju da dodatno pojasni kako je zakonom osigurano da Ured povjerenika za istražne ovlasti rješava pritužbe u tim slučajevima.**

4.3.4. Pravna zaštita

212. S obzirom na presude Suda EU-a u predmetima Schrems I i Schrems II jasno je da je djelotvorna sudska zaštita u smislu članka 47. Povelje EU-a od temeljne važnosti za pretpostavku primjerenosti prava treće zemlje. Te su presude pokazale i da se u tom pogledu posebna pozornost mora posvetiti djelotvornoj sudskoj zaštiti u području pristupa osobnim podacima za potrebe nacionalne sigurnosti.

213. **EOZP prepoznaje da je Ujedinjena Kraljevina uspostavila Sud za istražne ovlasti. Sud za istražne ovlasti nadležan je za predmete koji proističu iz toga kako se tijela za izvršavanje zakonodavstva, ali i obavještajne službe, koriste svojim istražnim ovlastima. Prema shvaćanju EOZP-a Sud za istražne ovlasti djeluje kao pravi sud u smislu članka 47. Povelje EU-a. Kad je riječ o njegovim ovlastima, Europska komisija poziva se da potvrdi da taj sud ima sve ovlasti navedene u uvodnoj izjavi 262. nacrta odluke, bez obzira na pravnu osnovu na temelju koje je podnesena pritužba.**

214. Tajni nadzor koji provode obavještajne agencije često znači da predmet nadzora, odnosno ispitanik, nije i neće biti svjestan nadzora. U tom kontekstu, kad je morao analizirati pravo SAD-a, EOZP je više puta izrazio zabrinutost u pogledu zahtjeva „osnovanosti" u slučajevima nadzora kako se tumači u pravu SAD-a. EOZP u tom kontekstu napominje da pritužba podnesena Sudu za istražne ovlasti zahtijeva samo test „vjerodostojnosti", prema kojem podnositelj pritužbe mora dokazati da bi mogao biti podvrgnut mjeri.

215. Pri analizi Suda za istražne ovlasti EOZP obraća posebnu pozornost i na činjenicu da je u više navrata utvrđeno da je funkcioniranje tog suda u skladu s EKLJP-om, kako ga tumači ESLJP.