

Priporočila



Priporočila 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe

Sprejeta 10. novembra 2020

Kazalo

1. UVOD.....	4
2. POSEGI V TEMELJNE PRAVICE	6
3. EVROPSKA temeljna JAMSTVA.....	8
Jamstvo A – Obdelava mora temeljiti na jasnih, natančnih in dostopnih pravilih	8
Jamstvo B – Nujnost in sorazmernost glede legitimnih ciljev, ki se zasledujejo, je treba dokazati	10
Jamstvo C – Neodvisni nadzorni mehanizem	12
Jamstvo D – Posamezniku morajo biti na voljo učinkovita pravna sredstva	14
4. KONČNE PRIPOMBE	15

Evropski odbor za varstvo podatkov je –

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

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018,²

ob upoštevanju členov 12 in 22 svojega poslovnika,

ob upoštevanju delovnega dokumenta delovne skupine iz člena 29 o utemeljitvi posegov v temeljne pravice do zasebnosti in varstvo podatkov z nadzornimi ukrepi pri prenašanju osebnih podatkov (Evropska temeljna jamstva), WP237 –

SPREJEL NASLEDNJA PRIPOROČILA

1. UVOD

1. Po sodbi v zadevi *Schrems I* si organi EU za varstvo podatkov, zbrani v Delovni skupini iz člena 29, pomagajo s sodno prakso pri prepoznavanju evropskih temeljnih jamstev, ki jih je treba spoštovati, da bi zagotovili, da posegi v pravice do zasebnosti in varstva osebnih podatkov z nadzornimi ukrepi pri prenašanju osebnih podatkov ne presegajo tistega, kar je potrebno in sorazmerno v demokratični družbi.

2. Evropski odbor za varstvo podatkov poudarja, da evropska temeljna jamstva temeljijo na sodni praksi Sodišča Evropske unije, ki se nanaša na člene 7, 8, 47 in 52 Listine EU o temeljnih pravicah, ter odvisno od primera na sodno prakso Evropskega sodišča za človekove pravice, ki se nanaša na člen 8 Evropske konvencije o človekovih pravicah, ki obravnava vprašanja glede splošnega nadzora v državah pogodbenicah Evropske konvencije o človekovih pravicah.³

3. Posodobitev tega dokumenta je mišljena za nadaljnji razvoj evropskih temeljnih jamstev, prvotno zasnovanih v odziv na sodbo v zadevi *Schrems I*,⁴ z odražanjem pojasnil, ki jih podaja Sodišče Evropske unije (in Evropsko sodišče za človekove pravice), odkar je bil prvič objavljen, zlasti v prelomni sodbi v zadevi *Schrems II*.⁵

¹ Ta priporočila ne zajemajo situacij prenosa ali nadaljnje deljenja v okviru Direktive (EU) 2016/680.

² Sklicevanje na „države članice“ v teh priporočilih je treba razumeti kot sklicevanje na „države članice EGP“.

³ V teh priporočilih izraz „temeljne pravice“ izhaja iz Listine EU o temeljnih pravicah EU. Vključuje pa tudi „človekove pravice“, kot so vključene v Evropsko konvencijo o človekovih pravicah.

⁴ Sodba Sodišča Evropske unije z dne 6. oktobra 2015, *Maximillian Schrems proti Data Commissioner*, zadeva C-362/14, EU:C:2015:650 (v nadaljevanju: *Schrems I*).

⁵ Sodba Sodišča Evropske unije z dne 16. julija 2020, *Data Protection Commissioner proti Facebook Ireland Ltd, Maximillian Schrems*, zadeva C-311/18, ECLI:EU:C:2020:559 (v nadaljevanju: *Schrems II*).

4. V sodbi v zadevi *Schrems II* je Sodišče Evropske unije navedlo, da je preučitev Sklepa Komisije 2010/87/EU o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah z vidika členov 7, 8 in 47 Listine EU o temeljnih pravicah razkrila, da ni bil ugotovljen noben element, ki bi lahko vplival na veljavnost tega sklepa, vendar je razveljavila sklep o zasebnostnem ščitju. Sodišče Evropske unije je odločilo, da sklep o zasebnostnem ščitju ni bil v skladu s členom 45(1) Splošne uredbe o varstvu podatkov z vidika členov 7, 8 in 47 Listine. Sodba lahko torej služi kot primer, ko nadzorni ukrepi v tretji državi (v tem primeru ZDA glede člena 702 Zakona o nadzoru tujih obveščevalnih podatkov (FISA) in Odredbe 12 333) niso niti dovolj omejeni niti niso predmet učinkovitega pravnega sredstva, ki je na voljo posamezniku, na katerega se nanašajo osebni podatki, za uveljavljanje njegovih pravic, kot to zahteva pravo EU, da bi se štelo, da je raven varstva v tretji državi „v bistvu enakovredna“ ravni varstva, ki se v Evropski uniji zagotavlja v smislu člena 45(1) Splošne uredbe o varstvu podatkov.

5. Razlogi za razveljavitev zasebnostnega ščitja so imeli posledice tudi za druga orodja za prenos⁶. Čeprav je Sodišče Evropske unije razlagalo člen 46(1) Splošne uredbe o varstvu podatkov v okviru veljavnosti standardnih pogodbenih določil, se njegova razlaga uporablja za vse prenose v tretje države, ki se nanašajo na katero koli orodje iz člena 46 Splošne uredbe o varstvu podatkov.⁷

6. Na koncu mora Sodišče Evropske unije presoditi, ali so posegi v temeljno pravico lahko upravičeni. Vendar, če take sodbe ni in se uporablja stalna sodna praksa, morajo organi za varstvo podatkov oceniti posamezne primere, bodisi po uradni dolžnosti bodisi na podlagi pritožbe, in zadevo bodisi predložiti nacionalnemu sodišču, če sumijo, da prenos ni v skladu s členom 45, kadar gre za sklep o ustreznosti, bodisi prenos začasno odložiti ali ga prepovedati, če ugotovijo, da člena 46 Splošne uredbe o varstvu podatkov ni mogoče izpolniti in varstva prenesenih podatkov, ki ga zahteva pravo EU, ni mogoče zagotoviti z drugimi sredstvi.

7. Namen posodobitve evropskih temeljnih jamstev je zagotoviti elemente za preučitev, ali se nadzorni ukrepi, ki omogočajo dostop do osebnih podatkov javnim organom v tretji državi, naj bodo to nacionalne varnostne agencije ali organi kazenskega pregona, lahko štejejo za utemeljen poseg ali ne.

8. Evropska temeljna jamstva so resnično del ocenjevanja, ki ga je treba izvesti, da bi se ugotovilo, ali tretja država zagotavlja raven varstva, ki je v bistvu enakovredna ravni varstva, zagotovljeni v EU, niso pa namenjena temu, da bi sama opredeljevala elemente, potrebne za mnenje, da tretja država zagotavlja tako raven varstva, ki je v skladu s členom 45 Splošne uredbe o varstvu podatkov. Podobno niso namenjena temu, da bi sama opredeljevala vse elemente, ki bi jih bilo treba upoštevati pri ocenjevanju, ali pravna ureditev tretje države izvozniku in uvozniku podatkov preprečuje, da bi zagotovila ustrezne zaščitne ukrepe v skladu s členom 46 Splošne uredbe o varstvu podatkov.

9. Zato je treba elemente, predstavljene v tem dokumentu, razumeti kot temeljna jamstva, ki jih je mogoče najti v tretji državi, ko se ocenjuje poseg, ki ga vključujejo nadzorni ukrepi tretje države, v pravice do zasebnosti in varstva podatkov namesto seznama elementov, ki dokazujejo, da pravna ureditev tretje države kot celota zagotavlja v bistvu enakovredno raven varstva.

⁶ Glej točko 105 sodbe *Schrems II*.

⁷ Glej točko 92 sodbe *Schrems II*.

10. Člen 6(3) Pogodbe o Evropski uniji določa, da temeljne pravice, vsebovane v Evropski konvenciji o človekovih pravicah, pomenijo splošna načela prava EU. Toda, kot opozarja Sodišče Evropske unije v svoji sodni praksi, ta konvencija, dokler Evropska unija ne pristopi k njej, ni pravni instrument, ki bi bil uradno vključen v pravo EU.⁸ Tako mora biti raven varstva temeljnih pravic, ki jo zahteva člen 46(1) Splošne uredbe o varstvu podatkov, določena na podlagi določb navedenega predpisa v povezavi s temeljnimi pravicami, določenimi v Listini EU o temeljnih pravicah. Ob tem velja, da morajo v skladu s členom 52(3) Listine EU o temeljnih pravicah imeti tam vsebovane pravice, ki ustrezajo pravicam, zajamčenim z Evropsko konvencijo o človekovih pravicah, enak pomen in področje uporabe kot tiste, ki jih določa Konvencija, ter da je treba posledično, kot poudarja Sodišče Evropske unije, sodno prakso Evropskega sodišča za človekove pravice v zvezi s pravicami, predvidenimi tudi v Listini EU o temeljnih pravicah, upoštevati kot najnižji prag varstva za razlago ustreznih pravic v Listini⁹. V skladu z zadnjim stavkom člena 52(3) Listine EU o temeljnih pravicah pa „[t]a določba ne preprečuje širšega varstva po pravu Unije“.

11. Zato bo vsebina temeljnih jamstev še naprej deloma temeljila na sodni praksi Evropskega sodišča za človekove pravice do obsega, v katerem Listina EU o temeljnih pravicah, kot jo razlaga Sodišče Evropske unije, ne zagotavlja višje ravni varstva, ki predpisuje druge zahteve poleg sodne prakse Evropskega sodišča za človekove pravice.

12. Ta dokument razlaga ozadje in nadaljnje podrobnosti o štirih evropskih temeljnih jamstvih.

2. POSEGI V TEMELJNE PRAVICE

13. Temeljne pravice do spoštovanja zasebnega in družinskega življenja, vključno s komunikacijami, ter do varstva osebnih podatkov so določene v členih 7 in 8 Listine EU o temeljnih pravicah. Člen 8 dodatno določa pogoje za obdelavo osebnih podatkov, da je zakonita, in priznava pravico do dostopa in popravka ter določa, da so ta pravila pod nadzorom neodvisnega organa.

14. „(D)ejanje, s katerim se osebni podatki iz ene države članice prenesejo v tretjo državo, pomeni obdelavo osebnih podatkov.“¹⁰ Člena 7 in 8 Listine EU o temeljnih pravicah se uporabljata za to posebno dejanje in njuno varstvo se razširja na prenesene podatke, zato je treba posameznikom, na katere se nanašajo osebni podatki, zagotoviti raven varstva, ki je v bistvu enakovredna ravni, zagotovljeni v Evropski uniji.¹¹

15. Po navedbah Sodišča Evropske unije je, če je temeljna pravica do spoštovanja zasebnega življenja iz člena 7 Listine EU o temeljnih pravicah prizadeta z obdelavo posameznikovih osebnih podatkov, prizadeta tudi pravica do varstva podatkov, ker spada taka obdelava na področje uporabe člena 8

⁸ Glej točko 98 sodbe v zadevi *Schrems II*.

⁹ Glej točko 124 sodbe v združenih zadevah C-511/18, C-512/18 in C-520/18, *La Quadrature du Net in drugi* (v nadaljevanju: *La Quadrature du Net in drugi*).

¹⁰ Sodišče Evropske unije, *Schrems II*, točka 83.

¹¹ Sodišče Evropske unije, *Schrems II*, točka 96.

Listine EU o temeljnih pravicah in je zato nujno, da se izpolni zahteva glede varstva podatkov iz navedenega člena.¹²

16. Zato se v zvezi z morebitnim posegom v temeljne pravice na podlagi prava EU z obveznostjo, ki nalaga ponudnikom elektronskih komunikacijskih storitev (...), da hranijo podatke o prometu, da se po potrebi pristojnim nacionalnim organom omogoči dostop do teh podatkov, postavljajo vprašanja v zvezi s spoštovanjem členov 7 in 8 Listine EU o temeljnih pravicah.¹³ Enako velja za druge vrste obdelave podatkov, kot je njihov prenos osebam, ki niso uporabniki, ali dostop do teh podatkov za njihovo uporabo¹⁴, ki tako vsebujejo poseg v te temeljne pravice. Še več, v skladu z ustaljeno sodno prakso dostop javnega organa do podatkov pomeni nadaljnji poseg.¹⁵

17. Da pride do posega, ni pomembno, „ali so informacije o zasebnem življenju občutljive in ali so bile zadevne osebe zaradi navedenega posega morda oškodovane“.¹⁶ Sodišče Evropske unije je tudi poudarilo, da ni pomembno, ali so bili shranjeni podatki pozneje uporabljeni ali ne.¹⁷

18. Vendar člena 7 in 8 Listine EU o temeljnih pravicah nista absolutni pravici, ampak ju je treba obravnavati glede na njuno funkcijo v družbi.¹⁸

19. Listina EU o temeljnih pravicah vključuje tudi test nujnosti in sorazmernosti, da se uokvirijo omejitve pravic, ki jih varuje. Njen člen 52(1) določa obseg morebitnih omejitev členov 7 in 8 z navedbo, da „[mora biti] kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina [...] predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.“

20. Sodišče Evropske unije je ponovilo, da mora zakonodaja EU, ki vključuje poseg v temeljne pravice, zajamčene s členoma 7 in 8 Listine EU o temeljnih pravicah, „določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe“, zlasti če se osebni podatki obdelujejo samodejno in „kadar obstaja veliko tveganje nezakonitega dostopa do teh podatkov“.¹⁹

21. Po navedbah Sodišča Evropske unije varstvo pravic zasebnosti zahteva, da se odstopanja od pravice do varstva podatkov in njene omejitve „določijo v mejah tega, kar je nujno potrebno“. Poleg

¹² Sodišče Evropske unije, *Schrems II*, točki 170–171.

¹³ Sodišče Evropske unije, zadeva C-623/17, *Privacy International* (v nadaljevanju: *Privacy International*), točka 60.

¹⁴ Sodišče Evropske unije, *Privacy International*, točka 61.

¹⁵ Evropsko sodišče za človekove pravice, *Leander*, točka 48; Evropsko sodišče za človekove pravice, *Rotaru*, točka 46; Sodišče Evropske unije, *Digital Rights Irska*, točka 35.

¹⁶ Sodišče Evropske unije, *Schrems II*, točka 171, vključno z navedeno sodno prakso.

¹⁷ Sodišče Evropske unije, *Schrems II*, točka 171, vključno z navedeno sodno prakso.

¹⁸ Sodišče Evropske unije, *Privacy International*, točka 63.

¹⁹ Sodišče Evropske unije, *Privacy International*, točka 68 in tam navedena sodna praksa.

tega mora biti cilj splošnega interesa usklajen s temeljnimi pravicami, na katere se nanaša ukrep, s primernim „uravnoveženjem“ cilja in zadevnih pravic.²⁰

22. Posledično dostop, hramba in nadaljnja uporaba osebnih podatkov s strani javnih organov v okviru pristojnosti nadzornih ukrepov ne smejo presegati meja tistega, kar je nujno potrebno po oceni v smislu Listine EU o temeljnih pravicah, sicer tega „ni mogoče šteti za upravičeno v demokratični družbi“.²¹

23. Štiri evropska temeljna jamstva, kot so predstavljena v naslednjem poglavju, so namenjena nadaljnji določitvi, kako oceniti raven posega v temeljne pravice zasebnosti in varstvo podatkov v okviru nadzornih ukrepov javnih organov v tretji državi pri prenašanju osebnih podatkov in katere pravne zahteve se morajo posledično uporabiti, da bi ocenili, ali bi bili taki posegi sprejemljivi na podlagi Listine EU o temeljnih pravicah.

3. EVROPSKA TEMELJNA JAMSTVA

24. Po analizi sodne prakse Evropski odbor za varstvo podatkov meni, da je veljavne pravne zahteve po omejitvah varstva podatkov in pravic do zasebnosti, ki so z Listino EU o temeljnih pravicah priznane kot utemeljene, mogoče povzeti v štirih evropskih temeljnih jamstvih:

- A. obdelava mora temeljiti na jasnih, natančnih in dostopnih pravilih;
- B. nujnost in sorazmernost glede legitimnih ciljev, ki se zasledujejo, je treba dokazati;
- C. obstajati bi moral neodvisni nadzorni mehanizem;
- D. posamezniku morajo biti na voljo učinkovita pravna sredstva.

25. Jamstva temeljijo na temeljnih pravicah do zasebnosti in varstva podatkov, ki veljajo za vsakogar, ne glede na njegovo državljanstvo.

Jamstvo A – Obdelava mora temeljiti na jasnih, natančnih in dostopnih pravilih

26. Na podlagi člena 8(2) Listine EU o temeljnih pravicah se morajo osebni podatki obdelovati med drugim „za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom“,²² kakor je opozorilo Sodišče v sodbi *Schrems II*. Poleg tega mora biti v skladu s členom 52(1) Listine EU o temeljnih pravicah kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih ta priznava, „predpisano z zakonom“. Utemeljen poseg mora biti torej v skladu z zakonom.

27. Ta pravna podlaga mora določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve.²³ Poleg tega je Sodišče Evropske unije opozorilo, da mora biti

²⁰ Sodišče Evropske unije, *Privacy International*, točka 68 in tam navedena sodna praksa.

²¹ Sodišče Evropske unije, *Privacy International*, točka 81.

²² Glej točko 173 *Schrems II*.

²³ Glej točki 175 in 180 *Schrems II* in Mnenje 1/15 (Sporazum EU-Kanada o evidenci podatkov o potnikih) z dne 26. julija 2017, točka 139, in navedeno sodno prakso.

„zakonsko zavezujoča v nacionalnem pravu“.²⁴ Glede tega je Sodišče Evropske unije pojasnilo, da se mora ocenjevanje veljavne zakonodaje tretje države osredotočiti na to, ali se posamezniki lahko nanjo sklicujejo in jo uveljavljajo pred sodiščem.²⁵ Sodišče Evropske unije zato navaja, da morajo biti pravice, dane posameznikom, na katere se nanašajo osebni podatki, iztožljive; kadar posamezniki ne dobijo izvršljivih pravic proti javnim organom, se raven zagotovljenega varstva v nasprotju z zahtevo iz člena 45(2)(a) Splošne uredbe o varstvu podatkov ne more šteti za enakovredno tisti, ki izhaja iz Listine.²⁶

28. Poleg tega Sodišče Evropske unije poudarja, da mora veljavna zakonodaja navajati, v katerih okoliščinah in pod kakšnimi pogoji se lahko sprejme ukrep, ki zagotavlja obdelavo takih podatkov²⁷ (glej spodnje navedbe v točki Jamstvo B za odnos med temi zahtevami ter načeloma nujnosti in sorazmernosti).

29. Sodišče Evropske unije je poleg tega navedlo tudi, da „zahteva, da mora biti kakršno koli omejevanje uresničevanja temeljnih pravic predpisano z zakonom, pomeni, da mora biti že v pravni podlagi, ki omogoča poseg v te pravice, opredeljen obseg omejitve uresničevanja zadevne pravice“.²⁸

30. Končno, Evropsko sodišče za človekove pravice „meni, da ni nobenega razloga, da bi uporabljali različna načela, ki zajemajo dostopnost in jasnost pravil, ki urejajo prestrezanje komunikacij posameznika na eni strani in splošnejše programe nadzora“.²⁹ Evropsko sodišče za človekove pravice je tudi pojasnilo, da bi morala pravna podlaga vključevati vsaj opredelitev kategorij ljudi, ki bi lahko bili podvrženi nadzoru, omejitev trajanja ukrepa, postopek, ki ga je treba upoštevati pri preučevanju, uporabi in shranjevanju pridobljenih podatkov, ter varnostne ukrepe, ki jih je treba sprejeti pri sporočanju podatkov drugim strankam.³⁰

31. Nazadnje, poseg mora biti predvidljiv glede njegovega učinka na posameznika, da bi ga ustrezno in učinkovito zavaroval pred naključnim posegom in tveganjem zlorabe. Posledično mora obdelava temeljiti na natančni, jasni, pa tudi dostopni (tj. javni) pravni podlagi.³¹ Evropsko sodišče za človekove pravice je glede tega vprašanja v zadevi *Zakharov* navedlo, da „sklicevanje na ‚predvidljivost‘ v okviru prestrezanja komunikacij ne more biti enako kot na številnih drugih področjih“. Poročilo navaja, da v okviru ukrepov prikritega nadzora, kot je prestrezanje komunikacij, „zahteva po predvidljivosti ne more pomeniti, da je treba posamezniku omogočiti, da predvidi, ali in kdaj lahko organi prestrezajo njegove komunikacije, da bi lahko skladno s tem prilagodil svoje ravnanje“. Toda ob upoštevanju, da je v takih situacijah tveganje pristranskosti očitno, „so bistvena jasna, podrobna pravila o prestrezanju telefonskih pogovorov, zlasti ker postaja tehnologija, ki je na voljo za uporabo, čedalje bolj

²⁴ Glej točko 68 *Privacy International*. Pojasniti je treba tudi, da Sodišče Evropske unije v francoski različici sodbe uporablja besedo „réglementation“, ki je širša, kot zgolj akti Parlamenta.

²⁵ Glej točko 181 *Schrems II*, v tem odstavku se Sodišče Evropske unije sklicuje na ameriško predsedniško direktivo za določitev politik št. 28.

²⁶ Glej *Schrems II*, točka 181.

²⁷ Glede zakonodaje države članice glej *Privacy International*, točko 68.

²⁸ Glej *Schrems II*, točka 175, in navedeno sodno prakso, ter *Privacy International*, točka 65.

²⁹ Evropsko sodišče za človekove pravice, *Liberty*, točka 63.

³⁰ Evropsko sodišče za človekove pravice, *Weber in Saravia*, točka 95.

³¹ Evropsko sodišče za človekove pravice, *Malone*, točki 65 in 66.

izpopolnjena. Domače pravo mora biti dovolj jasno, da državljanom ustrezno opiše okoliščine in pogoje, v katerih so javni organi pooblaščen za uporabo takih ukrepov.”³²

Jamstvo B – Nujnost in sorazmernost glede legitimnih ciljev, ki se zasledujejo, je treba dokazati

32. V skladu s prvim stavkom člena 52(1) Listine EU o temeljnih pravicah mora kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava Listina EU o temeljnih pravicah, spoštovati bistveno vsebino teh pravic in svoboščin. Na podlagi drugega stavka člena 52(1) Listine EU o temeljnih pravicah so ob upoštevanju načela sorazmernosti omejitve teh pravic in svoboščin dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.³³

33. Glede **načela sorazmernosti** je Sodišče v zvezi z zakonodajo držav članic navedlo, da mora biti vprašanje, ali je omejitev pravic do zasebnosti in varstva podatkov lahko upravičena, po eni strani ocenjeno glede na **resnost posega**, ki ga pomeni taka omejitev,³⁴ in po drugi strani s preverjanjem, ali je **pomembnost cilja javnega interesa**, ki se zasleduje s to omejitvijo, sorazmerna z resnostjo.³⁵

34. V zadevi *La Quadrature du Net in drugi* je mogoče ugotoviti, da je Sodišče Evropske unije razsojalo glede zakonodaje držav članic in ne zakonodaje tretje države, da je s ciljem varovanja državne varnosti zaradi njene pomembnosti mogoče upravičiti ukrepe, ki vključujejo resnejše posege v temeljne pravice, kakor so posegi, ki bi bili lahko upravičeni z drugimi cilji, na primer boj proti kriminalu. Vendar pa je ugotovilo, da to drži v primeru dovolj trdnih dokazov za mnenje, da se zadevna država spopada z resno grožnjo državni varnosti, za katero se izkaže, da je resnična in navzoča ali predvidljiva ter mora izpolniti druge zahteve iz člena 52(1) Listine EU o temeljnih pravicah.³⁶

35. Glede tega se smejo v skladu z ustaljeno sodno prakso Sodišča Evropske unije odstopanja od varstva osebnih podatkov in njegove omejitve uporabljati le v mejah tistega, kar je nujno potrebno.³⁷ Da bi bila izpolnjena ta zahteva, morajo biti v zadevni zakonodaji poleg jasnih in natančnih pravil, ki urejajo obseg in uporabo zadevnega ukrepa, določene minimalne zahteve, tako da imajo osebe,

³² Evropsko sodišče za človekove pravice, *Zakharov*, točka 229.

³³ *Schrems II*, točka 174.

³⁴ V tem okviru je sodišče opozorilo na primer na to, da „se zdi poseg, ki ga pomeni zbiranje podatkov, ki omogoča lokalizacijo terminalske opreme v realnem času, posebno resen, ker taki podatki zagotavljajo pristojnim nacionalnim organom sredstvo za natančno in stalno sledenje gibanju uporabnikov mobilnih telefonov [...]“ (*La Quadrature du Net in drugi*, točka 187, vključno z navedeno sodno prakso).

³⁵ *La Quadrature du Net in drugi*, točka 131.

³⁶ Točki 136 in 137. Glej tudi *Privacy International*, kajti Sodišče Evropske unije je pojasnilo, da se lahko take grožnje po svoji naravi in zlasti po resnosti razlikujejo od splošnega tveganja glede pojavljanja napetosti in izgredov, tudi resne narave, ki ogrožajo javno varnost, točka 75. V zadevi *La Quadrature du Net in drugi* je Sodišče Evropske unije na primer opozorilo, da samodejna analiza prometnih in lokacijskih podatkov, ki na splošno in neselektivno zajema podatke oseb, ki uporabljajo elektronske komunikacijske sisteme, pomeni posebno resen poseg, tako da lahko tak ukrep izpolni zahtevo sorazmernosti samo v primerih, ko se zadevna država članica srečuje z resno grožnjo državni varnosti, za katero se izkaže, da je resnična in navzoča ali predvidljiva ter, med drugim, pod pogojem, da je trajanje hrambe omejeno na tisto, kar je nujno potrebno (točke 174–177).

³⁷ *Schrems II*, točka 176, vključno z navedeno sodno prakso.

katerih podatki so bili preneseni, zadostna jamstva za učinkovito varstvo svojih osebnih podatkov pred tveganjem zlorabe. „Zlasti mora biti v tej ureditvi navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno. Nujnost obstoja takih jamstev je toliko pomembnejša, če se osebni podatki obdelujejo samodejno.“³⁸

36. V sodbi v zadevi *Schrems II* je Sodišče Evropske unije poudarilo, da zakonodaja tretje države, ki ne vsebuje omejitev vsebovanega pooblastila za izvajanje programov nadzora za pridobivanje tujih obveščevalnih podatkov, ne more zagotoviti ravni varstva, ki je v bistvu enakovredna ravni varstva, zagotovljeni z Listino EU o temeljnih pravicah. Pravzaprav morajo biti v skladu s sodno prakso, ki je pravna podlaga za poseg v temeljne pravice, zaradi spoštovanja načela sorazmernosti določene omejitve izvrševanja zadevne pravice.³⁹

37. Glede **načela nujnosti** je Sodišče Evropske unije pojasnilo, da zakonodaja, ki „dovoljuje hrambo vseh osebnih podatkov vseh posameznikov, katerih podatki so bili preneseni iz Evropske Unije [...], ne da bi se uporabljalo kakršno koli razlikovanje, omejitev ali izjema glede na cilj, ki se ga poskuša doseči, in ne da bi bilo predvideno objektivno merilo, ki bi omogočalo dostop javnih organov do podatkov in poznejšo uporabo teh podatkov samo v namene, ki so natančno določeni, strogo omejeni in bi lahko utemeljevali poseg, ki ga pomenita dostop in uporaba teh podatkov,“ ne izpolnjuje tega načela.⁴⁰ Predvsem je treba šteti, da ureditev, ki javnim organom omogoča splošen dostop do vsebine elektronskih komunikacij, pomeni poseg v bistvo temeljne pravice do spoštovanja zasebnega življenja, kot je zagotovljena v členu 7 Listine EU o temeljnih pravicah.⁴¹

38. Podobno je tokrat Sodišče Evropske unije pri ocenjevanju zakonodaje države članice in ne zakonodaje tretje države v zadevi *La Quadrature du Net in drugi* odločilo, da „[mora] zakonodaja, ki zahteva hrambo osebnih podatkov, vedno izpolnjevati objektivna merila, ki vzpostavljajo povezavo med podatki, ki se hranijo, in zasledovanim ciljem“.⁴² V enakem okviru je v zadevi *Privacy International*

³⁸ *Schrems II*, točka 175.

³⁹ *Schrems II*, točka 180.

⁴⁰ *Schrems I*, točka 93 z nadaljnjimi sklicevanji. Vendar glej tokrat glede zakonodaje države članice in ne zakonodaje tretje države, *Privacy International*, točka 71, vključno z navedeno sodno prakso. V tem primeru je Sodišče Evropske unije navedlo, da zakonodaja države članice, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da s splošnim in neselektivnim posredovanjem varnostnim in obveščevalnim agencijam razkrijejo prometne in lokacijske podatke, presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva Direktiva o zasebnosti in elektronskih komunikacijah v povezavi z Listino EU o temeljnih pravicah (točka 81).

⁴¹ *Schrems I*, točka 94.

⁴² *La Quadrature du Net in drugi*, točka 133. Glede tega je Sodišče potrdilo, da so zakonodajni ukrepi, ki kot preventivni ukrep ponujajo splošno in neselektivno shranjevanje prometnih in lokacijskih podatkov, izključeni z Direktivo o zasebnosti in elektronskih komunikacijah v povezavi z Listino EU o temeljnih pravicah. Nasprotno je Sodišče Evropske unije razsodilo, da lahko zakonodajalec v primeru resne grožnje državni varnosti, za katero se izkaže, da je resnična in navzoča ali predvidljiva, za njeno zavarovanje dovoli navodilo, ki ponudnikom elektronskih komunikacijskih storitev naloži, naj splošno in neselektivno hranijo prometne in lokacijske podatke. Taki ukrepi pa morajo kljub temu izpolnjevati posebne pogoje. Predvsem to, da se lahko navodilo izda samo za omejeno obdobje, ki je nujno potrebno, lahko pa se podaljša, če se grožnja nadaljuje (točka 168).

odločilo, da se [mora] zakonodajalec „pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do zadevnih podatkov, opreti na objektivna merila“.⁴³

Jamstvo C – Neodvisni nadzorni mehanizem

39. Evropski odbor za varstvo podatkov opozarja, da do posega pride v času zbiranja podatkov, pa tudi v času, ko javni organ dostopa do podatkov za nadaljnjo obdelavo. Evropsko sodišče za človekove pravice je že večkrat navedlo, da je treba za vsak poseg v pravico do zasebnosti in varstva podatkov uporabljati učinkovit, neodvisen in nepristranski nadzorni sistem, ki ga mora zagotoviti bodisi sodnik bodisi drug neodvisni organ⁴⁴ (na primer upravni organ ali parlamentarni organ). Neodvisni nadzor nad izvajanjem nadzornih ukrepov je upoštevalo tudi Sodišče Evropske unije v sodbi v zadevi *Schrems II*.⁴⁵

40. Evropsko sodišče za človekove pravice določa, da je ob tem, ko je predhodna (sodna) odobritev nadzornih ukrepov pomembna zaščita pred pristranskostjo, treba upoštevati tudi dejansko delovanje sistema prestrezanja, vključno s preverjanjem in usklajevanjem izvajanja pooblastil in obstoja ali odsotnosti dejanske zlorabe.⁴⁶ V zadevi *Schrems II* je Sodišče Evropske unije upoštevalo tudi obseg nadzorne vloge pri nadzornem mehanizmu, ki ni pokrival posameznih nadzornih ukrepov.⁴⁷

41. Pri zakonodaji držav članic je Sodišče Evropske unije ugotovilo številne ukrepe, ki so skladni z zakonodajo EU samo, če se izvaja učinkovito preverjanje, ki ga izvaja sodišče ali neodvisni upravni organ, katerega odločitev je zavezujoča. Njegov namen je preveriti, ali obstaja stanje, ki upravičuje ukrep, ter ali so upoštevani pogoji in zaščitni ukrepi, ki morajo biti določeni.⁴⁸ Za zbiranje prometnih in lokacijskih podatkov v realnem času mora pregled omogočati predhodno preverjanje, med drugim, ali je odobreno samo v okviru meja nujno potrebnega. V primerih ustrezno utemeljene nujnosti se lahko ukrepi uporabijo brez takega predhodnega pregleda, vendar Sodišče Evropske unije kljub temu zahteva, da se kmalu opravi naknadni pregled.⁴⁹

42. Glede neodvisnosti nadzornega mehanizma v zvezi z nadzorom se lahko upoštevajo ugotovitve Sodišča Evropske unije o neodvisnosti organa v primeru pravnega sredstva (glej spodnje navedbe v točki Jamstvo D). Poleg tega lahko sodna praksa Evropskega sodišča za človekove pravice ponudi dodatne elemente. To sodišče se je zavzelo za to, da je za zagotavljanje nadzora odgovoren sodnik. Vendar ni izključeno, da je lahko odgovoren drug organ, „če je dovolj neodvisen od izvršilne veje oblasti“⁵⁰ in „od organov, ki izvajajo nadzor, in imajo zadostna pooblastila in pristojnosti za izvajanje učinkovitega in stalnega nadzora“.⁵¹ Evropsko sodišče za človekove pravice je dodalo, da je treba pri

⁴³ *Privacy International*, točka 78, vključno z navedeno sodno prakso. V zadevi *Privacy International* je glede dostopa organa do osebnih podatkov, zagotovljenih na podlagi zakonodaje države članice, Sodišče Evropske unije razsodilo, da „ni mogoče šteti, da je splošni dostop do vseh hranjenih podatkov ob neobstoju kakršne koli povezave, tudi posredne, s ciljem, ki se mu sledi, omejen na nujno potrebno“ (točki 77–78).

⁴⁴ Evropsko sodišče za človekove pravice, *Klass*, točki 17 in 51.

⁴⁵ *Schrems II*, točki 179 in 183.

⁴⁶ Evropsko sodišče za človekove pravice, *Big Brother Watch*, vložena pritožba, točki 319–320.

⁴⁷ *Schrems II*, točka 179.

⁴⁸ Sodišče Evropske unije, *La Quadrature du Net in drugi*, točki 168 in 189.

⁴⁹ Sodišče Evropske unije, *La Quadrature du Net in drugi*, točka 189.

⁵⁰ Evropsko sodišče za človekove pravice, *Zakharov*, točka 258; *Iordachi in drugi proti Moldaviji*, točki 40 in 51; ter *Dumitru Popescu proti Romuniji*, točke 70–73.

⁵¹ Evropsko sodišče za človekove pravice, *Klass*, točka 56; in *Big Brother Watch*, vložena pritožba, točka 318.

ocenjevanju neodvisnosti upoštevati „način imenovanja in pravni status članov nadzornega organa“.⁵² To vključuje „osebe, kvalificirane za opravljanje pravosodne funkcije, ki jih imenuje parlament ali predsednik vlade. Nasprotno pa je bilo za ministra za notranje zadeve – ki ni bil zgolj politično imenovan in član izvršilne veje oblasti, temveč je bil tudi neposredno vključen v naročilo posebnih sredstev nadzora – ugotovljeno, da ni dovolj neodvisen.“⁵³ Evropsko sodišče za človekove pravice „ugotavlja [tudi], da je bistveno, da ima nadzorni organ dostop do vseh zadevnih dokumentov, vključno z zaupnim gradivom“.⁵⁴ Končno, Evropsko sodišče za človekove pravice upošteva, „ali so dejavnosti nadzornega organa odprte za javni nadzor“.⁵⁵

⁵² Evropsko sodišče za človekove pravice, *Zakharov*, točka 278.

⁵³ Evropsko sodišče za človekove pravice, *Zakharov*, točka 278.

⁵⁴ Evropsko sodišče za človekove pravice, *Zakharov*, točka 281.

⁵⁵ Evropsko sodišče za človekove pravice, *Zakharov*, točka 283.

Jamstvo D – Posamezniku morajo biti na voljo učinkovita pravna sredstva

43. Zadnje evropsko temeljno jamstvo se nanaša na pravice posameznika do pravnega sredstva. Posameznik mora imeti učinkovito pravno sredstvo za izpolnitev svojih pravic, kadar meni, da niso (bile) spoštovane. Sodišče Evropske unije je v sodbi *Schrems I* pojasnilo, da „ureditev, ki ne določa nobene možnosti, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravo ali izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine. Člen 47, prvi odstavek, Listine namreč določa, da ima vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Evropske unije, pravico do učinkovitega pravnega sredstva pred sodiščem v skladu s pogoji, določenimi v tem členu.“⁵⁶

44. Pri ocenjevanju zakonodaje države članice, ki dovoljuje zbiranje prometnih in lokacijskih podatkov v realnem času, je Sodišče Evropske unije menilo, da je nujno obvestilo, ki „omogoči prizadetim osebam, da uveljavljajo svoje pravice na podlagi členov 7 in 8 Listine, da zahtevajo dostop do svojih osebnih podatkov, ki so bili predmet teh ukrepov, in da se ti podatki po potrebi popravijo ali izbrišejo, pa tudi, da v skladu s prvim odstavkom člena 47 Listine izkoristijo učinkovito pravno sredstvo pred sodiščem“.⁵⁷ Kljub temu je priznalo tudi, da se mora obvestilo osebam, katerih podatki so se zbirali ali analizirali, izdati samo do obsega, v katerem in takrat ko obvestilo ne škoduje nalogam, za katere so organi odgovorni.⁵⁸

45. Tudi pri Evropskem sodišču za človekove pravice je vprašanje učinkovitega pravnega sredstva neločljivo povezano z obvestilom o nadzornem ukrepu posamezniku, potem ko je nadzor končan. Sodišče je ugotovilo predvsem, da „je načeloma za zadevnega posameznika malo možnosti za pravno sredstvo pred sodišči, razen če je seznanjen z ukrepi, ki so bili sprejeti brez njegove vednosti, in tako lahko izpodbija njihovo zakonitost za nazaj, ali pa, če lahko vsaka oseba, ki sumi, da so se njene komunikacije prestrezale, zahteva sodno varstvo pred sodišči, tako da sodna pristojnost ni odvisna od sporočila posamezniku, da so bile njegove komunikacije prestrežene“.⁵⁹ Evropsko sodišče za človekove pravice tako priznava, da v nekaterih primerih morda ne bo obvestila, kljub temu pa se mora zagotoviti učinkovito pravno sredstvo. V tem primeru je to sodišče jasno navedlo, na primer v zadevi *Kennedy*, da sodišče ponuja dovolj možnosti za pravno sredstvo, če je izpolnjenih več meril, tj. neodvisni in nepristranski organ, ki je sprejel svoj pravilnik in ga sestavljajo člani, ki imajo ali so imeli visoko pravosodno funkcijo ali so izkušeni odvetniki, ter ni nobenega dokaznega bremena, ki bi ga bilo treba ovreči za vložitev tožbe pri sodišču.⁶⁰ Pri preučitvi pritožb posameznikov mora imeti sodišče dostop do

⁵⁶ Sodišče Evropske unije, *Schrems I*, točka 95.

⁵⁷ Glej *La Quadrature du Net in drugi*, točka 190; in Sodišče Evropske unije, Mnenje 1/15, točka 220.

⁵⁸ Glej *La Quadrature du Net in drugi*, točka 191.

⁵⁹ Evropsko sodišče za človekove pravice, *Zakharov*, točka 234.

⁶⁰ Evropsko sodišče za človekove pravice, *Kennedy*, točka 190.

vseh ustreznih informacij,⁶¹ vključno z zaupnim gradivom. Nazadnje, imeti mora pristojnost za odpravo neskladnosti.⁶²

46. Člen 47 Listine EU o temeljnih pravicah se nanaša na „tribunal“, čeprav jezikovne različice razen angleščine dajejo prednost besedi „sodišče“,⁶³ Evropska konvencija o človekovih pravicah pa obvezuje države članice, naj zagotovijo, da „[ima] vsakdo, čigar pravice in svoboščine so kršene, pravico do učinkovitih pravnih sredstev pred domačimi oblastmi“,⁶⁴ ki niso nujno pravosodni organ.⁶⁵

47. Sodišče Evropske unije je v sodbi v zadevi *Schrems II* pri ocenjevanju ustreznosti ravni varstva tretje države ponovilo, „da morajo imeti posamezniki možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da bi si tako zagotovili dostop do osebnih podatkov, ki se nanje nanašajo, ali dosegli popravilo oziroma izbris takih podatkov“.⁶⁶ V istem okviru Sodišče Evropske unije meni, da lahko učinkovito sodno varstvo pred posegi zagotovi ne le sodišče, temveč tudi organ,⁶⁷ ki zagotavlja jamstva, ki so v bistvu enakovredna tistim, ki se zahtevajo s členom 47 Listine EU o temeljnih pravicah. Sodišče Evropske unije je v sodbi *Schrems II* poudarilo, da je treba zagotoviti neodvisnost sodišča ali organa, zlasti od izvršilne veje oblasti, z vsemi potrebnimi jamstvi, vključno s pogoji za odpoklic ali razveljavitev imenovanja,⁶⁸ in da morajo biti pooblastila, ki jih je treba dodeliti sodišču, v skladu z zahtevami iz člena 47 Listine EU o temeljnih pravicah. V tem pogledu mora biti organu⁶⁹ dodeljena pristojnost za sprejemanje odločitev, ki so zavezujoče za obveščevalne službe, v skladu s pravnimi zaščitnimi ukrepi, na katere se posamezniki, na katere se nanašajo osebni podatki, lahko zanesejo.⁷⁰

4. KONČNE PRIPOMBE

48. Štiri evropska temeljna jamstva je treba razumeti kot glavne elemente, ki jih je mogoče najti pri ocenjevanju ravni posega v temeljne pravice do zasebnosti in varstva podatkov. Ni jih dopustno ocenjevati neodvisno, ker so tesno medsebojno povezana, ampak skupaj s pregledovanjem ustrezne zakonodaje glede nadzornih ukrepov, minimalne ravni zaščitnih ukrepov za varstvo pravic posameznikov, na katere se nanašajo osebni podatki, in pravna sredstva, ki jih zagotavlja nacionalno pravo tretje države.

⁶¹ Evropski odbor za varstvo podatkov ugotavlja, da komisar Sveta Evrope za človekove pravice meni, da se tako imenovano pravilo tretjih strani – po katerem lahko obveščevalne agencije v eni državi, ki zagotavljajo podatke obveščevalnim agencijam v drugi državi, naložijo agencijam prejemnicam obveznost, da prenesenih podatkov ne razkrijejo nobeni tretji strani – ne bi smelo uporabljati za nadzorne organe, da se ne bi ogrozila možnost za učinkovito pravno sredstvo (dokument o vprašanju demokratičnega in učinkovitega nadzora nacionalnih varnostnih služb).

⁶² Evropsko sodišče za človekove pravice, *Kennedy*, točka 167.

⁶³ Beseda tribunal se na primer prevaja „Gericht“ v nemščino in „gerecht“ v nizozemščino.

⁶⁴ Člen 13 Evropske konvencije o človekovih pravicah.

⁶⁵ Evropsko sodišče za človekove pravice, *Klass*, točka 67.

⁶⁶ Glej točko 194 *Schrems II*.

⁶⁷ Glej točko 197 *Schrems II*, v kateri je Sodišče izrecno uporabilo to besedo.

⁶⁸ Glej točko 195 *Schrems II*.

⁶⁹ Glej točko 197 *Schrems II*, v kateri je Sodišče izrecno uporabilo to besedo.

⁷⁰ Glej točko 196 *Schrems II*.

49. Ta jamstva zahtevajo določeno stopnjo razlage, zlasti ker zakonodaja tretje države ni nujno enaka pravnemu okviru EU.

50. Kot je Evropsko sodišče za človekove pravice navedlo v zadevi *Kennedy*, je „ocena“ odvisna od vseh okoliščin primera, kot so narava, obseg in trajanje morebitnih ukrepov, razlogi, ki se zahtevajo za njihovo odreditev, organi, pristojni za njihovo odobritev, izvajanje in nadzorovanje ter vrsta pravnega sredstva, ki ga zagotavlja nacionalno pravo⁷¹.

51. Posledično lahko ocena nadzornih ukrepov tretje države glede na evropska temeljna jamstva vodi do dveh sklepnih ugotovitev:

- J zadevna zakonodaja tretje države ne zagotavlja zahtev evropskih temeljnih jamstev: v tem primeru zakonodaja tretje države ne ponuja ravni varstva, ki je v bistvu enakovredna ravni v EU;
- J zadevna zakonodaja tretje države ustreza evropskim temeljnim jamstvom.

52. Pri ocenjevanju ustreznosti ravni varstva na podlagi člena 45 Splošne uredbe o varstvu podatkov bo Komisija morala oceniti, ali se spoštujejo evropska temeljna jamstva glede elementov, ki jih je treba upoštevati za jamstvo, da zakonodaja tretje države kot celota ponuja raven varstva, ki je v bistvu enakovredna ravni, ki je zajamčena v EU.

53. Kadar se izvozniki podatkov skupaj z uvozniki podatkov zanašajo na ustrezne zaščitne ukrepe na podlagi člena 46 Splošne uredbe o varstvu podatkov glede na zahteve zakonodaje tretje države, ki se uporablja predvsem za prenesene podatke, morajo zagotoviti, da se dejansko doseže v bistvu enakovredna raven varstva. Zlasti kadar zakonodaja tretje države ne izpolnjuje zahtev evropskih temeljnih jamstev, to pomeni, da je treba zagotoviti, da zadevna zakonodaja ne bo vplivala na jamstva in zaščitne ukrepe, ki spremljajo prenos, da bi lahko zagotovili raven varstva, v bistvu enakovredno ravni, zajamčeni v EU.

54. Evropski odbor za varstvo podatkov je izdal nadaljnja navodila in priporočila, ki jih je treba upoštevati pri nadaljnjem ocenjevanju, odvisno od orodja prenosa, ki se bo uporabljalo, in nujnosti, da se zagotovijo ustrezni zaščitni ukrepi, vključno, če je treba, z dopolnilnimi ukrepi.⁷²

55. Poleg tega je treba opozoriti, da evropska temeljna jamstva temeljijo na tem, kar zahteva zakon. Evropski odbor za varstvo podatkov poudarja, da evropska temeljna jamstva temeljijo na temeljnih pravicah, ki veljajo za vsakogar, ne glede na posameznikovo državljanstvo.

56. Evropski odbor za varstvo podatkov ponavlja, da so evropska temeljna jamstva referenčni standard za ocenjevanje posega, ki ga vključujejo nadzorni ukrepi tretje države, v okviru mednarodnih prenosov podatkov. Ti standardi izvirajo iz zakonodaje EU ter sodne prakse Sodišča Evropske unije in Evropskega sodišča za človekove pravice, ki zavezuje države članice.

⁷¹ Evropsko sodišče za človekove pravice, *Kennedy*, točka 153.

⁷² Referenčni dokument o ustreznosti, WP 254 rev. 01, revidiran in sprejet 6. februarja 2018; Priporočila Evropskega odbora za varstvo podatkov 01/2020 o ukrepih, ki dopolnjujejo orodje za prenos, da bi se zagotovila skladnost z ravno varstva osebnih podatkov v EU, 10. novembra 2020.