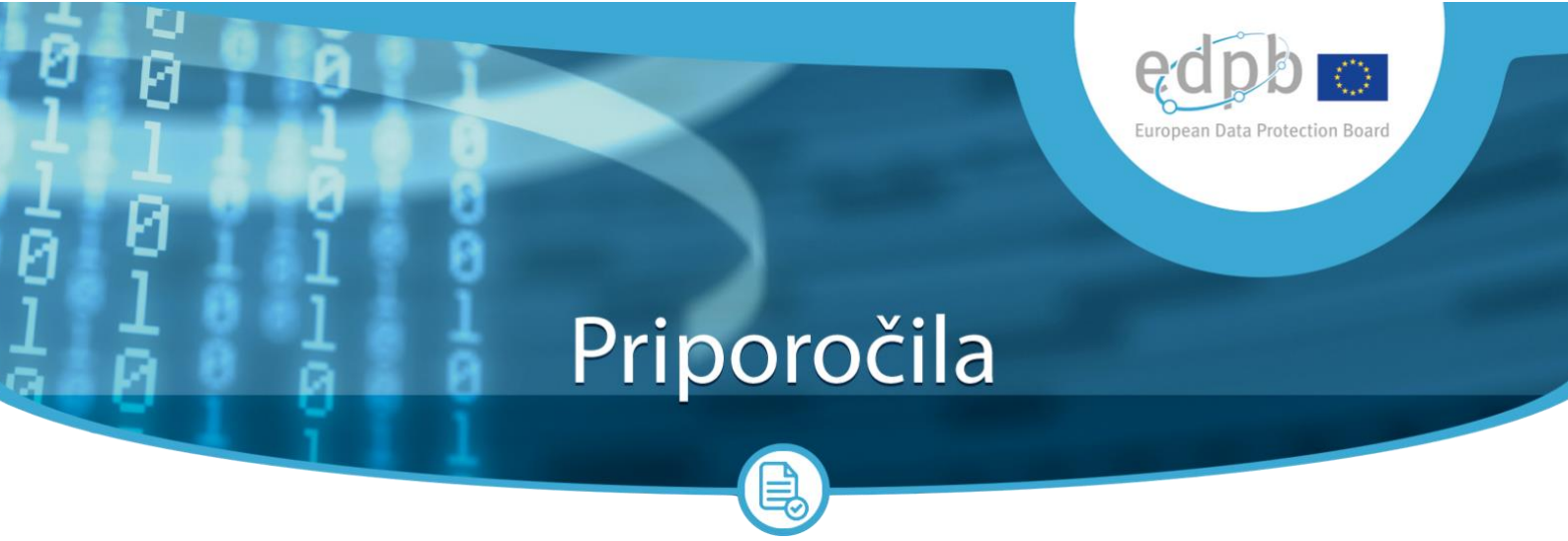

Priporočila št. 1/2021 o referenčnem dokumentu o ustreznosti v skladu z Direktivo o kazenskem pregonu

Sprejeta 2. februarja 2021

Zgodovina različic

Različica 1.1	6. julij 2021	Oblikovne spremembe
Različica 1.0	2. februar 2021	Sprejetje priporočil

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 51(1)(b) Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ[1],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJA PRIPOROČILA:

1. UVOD

1. Delovna skupina iz člena 29 je objavila delovni dokument[2] o referenčnem dokumentu o ustreznosti v skladu s Splošno uredbo o varstvu podatkov[3]. Delovni dokument je Evropski odbor za varstvo podatkov potrdil na prvi plenarni seji.

2. Kot je navedeno v 21. izjavi, priloženi k Lizbonski pogodbi, bi lahko bila zaradi posebne narave pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja na teh področjih potrebna posebna pravila o varstvu osebnih podatkov in o prostem pretoku takih podatkov na podlagi člena 16 Pogodbe o delovanju Evropske unije.

3. Na tej podlagi je zakonodajalec EU sprejel Direktivo (EU) 2016/680 (v nadaljevanju: direktiva o kazenskem pregonu), ki določa posebna pravila glede obdelave osebnih podatkov, ki jih pristojni organi obdelujejo za namene **preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem**.

4. Direktiva o kazenskem pregonu določa podlago za prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo v tem kontekstu. Ena od podlag za tak prenos je sklep Evropske komisije, da zadevna tretja država ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov.

5. Namen delovnega dokumenta WP254.rev01 o referenčnem dokumentu o ustreznosti je zagotoviti smernice Evropski komisiji o ravni varstva podatkov v tretjih državah in mednarodnih organizacijah v skladu s Splošno uredbo o varstvu podatkov, namen tega dokumenta pa je zagotoviti podobne smernice v skladu z Direktivo o kazenskem pregonu. V tem okviru vzpostavlja ključna načela

[1] UL L 119, 4.5.2016, str. 89.
[2] Wp254.rev01, ki ga je Delovna skupina iz člena 29 sprejela 28. novembra 2017, kakor je bil nazadnje revidiran in sprejet 6. februarja 2018. Dokument je posodobitev poglavja 1 delovnega dokumenta z naslovom „Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive“ (Prenosi osebnih podatkov v tretje države: uporaba členov 25 in 26 Direktive EU o varstvu podatkov), WP12, ki ga je Delovna skupina iz člena 29 sprejela 24. julija 1998.
[3] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 26. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

varstva podatkov, ki morajo biti vključena v pravni okvir tretje države ali mednarodne organizacije, da se zagotovi raven varstva, ki je v bistvenem enaka ravni, zagotovljeni v okviru EU znotraj področja uporabe direktive o kazenskem pregonu (tj. za obdelavo osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij). Poleg tega lahko zagotovi smernice za tretje države in mednarodne organizacije, ki želijo zagotoviti ustreznost.

6. Ta dokument se osredotoča izključno na sklepe o ustreznosti. To so izvedbeni akti Evropske komisije v skladu s členom 36(3) Direktive o kazenskem pregonu.

2. POJEM USTREZNOSTI

7. Direktiva o kazenskem pregonu določa pravila o prenosu osebnih podatkov v tretje države in mednarodne organizacije, če taki prenosi spadajo na njeno področje uporabe. Pravila o mednarodnih prenosih osebnih podatkov so določena v poglavju V Direktive o kazenskem pregonu, natančneje v členih 35 do 39.

8. V skladu s členom 36 Direktive o kazenskem pregonu se prenos podatkov v tretjo državo ali mednarodno organizacijo lahko izvede, če tretja država, ozemlje ali eden ali več določenih sektorjev v tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov. Iz sodne prakse Sodišča Evropske unije[4] izhaja, da je treba navedeno določbo razlagati ob upoštevanju člena 35 Direktive o kazenskem pregonu, ki je naslovljen „Splošna načela za prenose osebnih podatkov“ in ki določa, da se „vse določbe [poglavja V direktive o kazenskem pregonu] uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta direktiva“.

9. Če je Evropska komisija odločila, da je taka ustrezna raven varstva zagotovljena, se lahko prenosi osebnih podatkov v zadevno tretjo državo, ozemlje, sektor ali mednarodno organizacijo izvedejo, ne da bi bilo treba pridobiti posebno dovoljenje, razen če mora druga država članica, iz katere so bili podatki pridobljeni, podati svoje soglasje za prenos, kot je določeno v členih 35 in 36 ter uvodni izjavi 66 Direktive o kazenskem pregonu. To ne posega v zahtevo, da mora biti obdelava podatkov, ki jo izvajajo organi zadevne države članice, skladna z nacionalnimi določbami, sprejetimi v skladu z Direktivo (EU) 2016/680.

10. Ta pojem „ustrezne ravni varstva“, ki je obstajal že v Direktivi 95/46/ES[5] in Okvirnem sklepu Sveta 2008/977/PNZ[6], je Sodišče Evropske unije nadalje razvilo v tem kontekstu in pred kratkim v okviru Splošne uredbe o varstvu podatkov.

11. Kot je poudarilo Sodišče Evropske unije, mora biti raven varstva v tretji državi v bistvenem enaka ravni, ki jo zagotavlja EU, a „so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Unije“, vendar „se morajo ta sredstva

[4] Zadeva C-311/18, Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu, 16. julij 2020, ECLI:EU:C:2020:559, točka 92 (v nadaljnjem besedilu: Schrems II).
[5] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).
[6] Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL L 350, 30.12.2008, str. 60).

vseeno izkazati v praksi kot učinkovita“[7]. Standard ustreznosti torej ne zahteva dobesednega odražanja zakonodaje EU, ampak vzpostavitev bistvenih oziroma ključnih zahtev te zakonodaje.

12. Glede tega je Sodišče tudi pojasnilo, da bi moral sklep Komisije o ustreznosti vsebovati vse ugotovitve o tem, ali v tretji državi obstajajo državni predpisi, katerih namen je omejiti kakršnekoli posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Evropske unije v zadevno tretjo državo, tj. posege, ki naj bi jih državni subjekti v tej državi lahko izvajali, kadar poskušajo doseči legitimne cilje, kot je državna varnost[8].

13. Namen sklepov Evropske komisije o ustreznosti je uradno potrditi, z zavezujočim učinkom za države članice[9], vključno z njihovimi pristojnimi organi za varstvo podatkov[10], da je raven varstva podatkov v tretji državi ali mednarodni organizaciji v bistvenem enaka ravni varstva podatkov v Evropski uniji. Tretja država bi morala nuditi jamstva, ki zagotavljajo ustrezno raven varstva, ki je v bistvenem enakovredna tisti, zagotovljeni v Uniji, zlasti kadar se osebni podatki obdelujejo v enem ali več določenih sektorjih[11].

14. Ustreznost se lahko doseže s kombinacijo pravic za posameznike, na katere se nanašajo osebni podatki, ter obveznosti za tiste, ki obdelujejo osebne podatke ali izvajajo nadzor nad tako obdelavo in nadzorom neodvisnih organov. Vendar so predpisi o varstvu podatkov učinkoviti samo, če so izvršljivi in se izvajajo v praksi. Torej ni dovolj obravnavati le vsebine predpisov, ki se uporabljajo za osebne podatke, prenesene v tretjo državo ali mednarodno organizacijo, ampak je treba proučiti tudi sistem, vzpostavljen za zagotavljanje učinkovitosti takih predpisov. Učinkoviti mehanizmi izvrševanja so izjemnega pomena za učinkovitost predpisov o varstvu podatkov[12].

3. POSTOPKOVNI VIDIKI ZA UGOTOVITVE O USTREZNOSTI V SKLADU Z DIREKTIVO O KAZENSKEM PREGONU

15. Da bi lahko Evropski odbor za varstvo podatkov izpolnil svojo nalogo svetovanja Evropski komisiji v skladu s členom 51(1)(g) Direktive o kazenskem pregonu, mu je treba predložiti vso ustrezno dokumentacijo, vključno z zadevno korespondenco in ugotovitvami Evropske komisije. Nujno je, da se Evropskemu odboru za varstvo podatkov vsi ustrezni dokumenti posredujejo dovolj zgodaj in da so prevedeni v angleščino, da se pred dokončnim sprejetjem sklepov o ustreznosti omogočijo informirane in koristne razprave. V primeru zapletenega pravnega okvira je treba predložiti tudi vsa poročila, pripravljena glede ravni varstva podatkov v tretji državi ali mednarodni organizaciji. Vsekakor bi morale biti informacije, ki jih predloži Evropska komisija, izčrpne, pri čemer Evropskemu odboru za varstvo podatkov omogočijo, da oceni analizo Komisije v zvezi z ravnjo varstva podatkov v tretji državi ali mednarodni organizaciji.

---

[7] Zadeva C−362/14, Maximillian Schrems proti Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650, točki 73 in 74 (v nadaljnjem besedilu: Schrems I).
[8] Schrems I, točka 88.
[9] Člen 288 PDEU.
[10] Schrems I, točka 52.
[11] Uvodna izjava 67 Direktive o kazenskem pregonu.
[12] Schrems I, točke 72 do 74, in Mnenje Sodišča Evropske unije 1/15 o osnutku sporazuma med Kanado in Evropsko unijo, 26. julij 2017, ECLI:EU:C:2017:592 (Mnenje 1/15), točka 134: „Ta pravica do varstva osebnih podatkov zahteva tudi, da se kontinuiteta visoke ravni varstva temeljnih pravic in svoboščin, določena s pravom Unije, zagotavlja v primeru prenosa osebnih podatkov iz Unije v tretje države. Tudi če so lahko sredstva za zagotovitev take ravni varstva drugačna od sredstev, uporabljenih znotraj Unije za zagotovitev spoštovanja zahtev iz prava Unije, se morajo ta sredstva v praksi izkazati kot učinkovita za zagotovitev varstva, ki je v bistvu enakovredno varstvu, zagotovljenemu znotraj Unije.“

16. Evropski odbor za varstvo podatkov bo pravočasno zagotovil mnenje o ugotovitvah Evropske komisije, opredelil pomanjkljivosti v okviru ustreznosti, če obstajajo, in po potrebi predložil možna priporočila.

17. V skladu s členom 36(4) Direktive o kazenskem pregonu Evropska komisija redno spremlja razvoj dogodkov, ki bi lahko vplival na izvajanje sklepa o ustreznosti.

18. V členu 36(3) Direktive o kazenskem pregonu je določeno, da je redni pregled treba opraviti vsaj vsaka štiri leta. Vendar je to splošni časovni okvir, ki ga je s sklepom o ustreznosti treba prilagoditi za vsako tretjo državo ali mednarodno organizacijo. Glede na posebne obravnavane okoliščine bo morda potreben krajši cikel pregleda. Razlog za pregled pred predvidenim datumom bi lahko bili tudi incidenti, druge informacije o pravnem okviru zadevne tretje države ali mednarodne organizacije ali spremembe tega okvira. Ustrezno se tudi zdi, da se prvi pregled povsem novega sklepa o ustreznosti opravi precej kmalu, cikel pregleda pa se postopoma prilagodi glede na rezultat.

19. Ker ima Evropski odbor za varstvo podatkov nalogo, da Evropski komisiji zagotovi mnenje o tem, ali tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija ne zagotavlja več ustrezne ravni varstva, mu mora Evropska komisija pravočasno predložiti pomembne informacije o spremljanju ustreznega razvoja dogodkov v tej tretji državi ali mednarodni organizaciji. Zato bi moral biti Evropski odbor za varstvo podatkov obveščen o vseh postopkih in misijah glede pregleda v tretji državi ali mednarodni organizaciji. Evropski odbor za varstvo podatkov predlaga, da se ga pozove k sodelovanju v teh postopkih in misijah glede pregleda, kot je bilo predvideno v sklepu o zasebnostnem ščitu ter je predvideno v sklepu o ustreznosti v zvezi z Japonsko.

20. Opozoriti je treba tudi, da je Evropska komisija v skladu s členom 36(5) Direktive o kazenskem pregonu pooblaščena, da, kadar tretja država ali mednarodna organizacija ne zagotavlja več ustrezne ravni varstva, razveljavi, spremeni ali začasno odloži izvajanje obstoječih sklepov o ustreznosti. Postopek razveljavitve, spremembe ali začasne odložitve izvajanja vključuje Evropski odbor za varstvo podatkov, in sicer se ga zaprosi za mnenje v skladu s členom 51(1)(g) Direktive o kazenskem pregonu.

21. Poleg tega bi morali biti, brez poseganja v pooblastila organov pregona, nadzorni organi prav tako pooblaščeni za opozarjanje pravosodnih organov o kršitvah navedene direktive ali za sodelovanje v sodnih postopkih[13]. Zlasti iz sodbe Sodišča Evropske unije v zadevi Schrems I izhaja, da morajo imeti organi za varstvo podatkov možnost sodelovati v sodnih postopkih pred nacionalnimi sodišči, če menijo, da je zahteva posameznika zoper sklep o ustreznosti utemeljena[14]. Sodba Schrems II je potrdila to oceno[15].

[13] Glej člen 47(5) Direktive o kazenskem pregonu in njeno uvodno izjavo 82.
[14] Glej Schrems I, točka 65: „V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da očitke, ki jih šteje za utemeljene, predloži nacionalnim sodiščem, da bi ta, če bi prav tako kot ta organ dvomila o veljavnosti odločbe Komisije, sprožila postopek predhodnega odločanja za preizkus veljavnosti navedene odločbe.“
[15] Glej Schrems II, točka 120: „Tako mora pristojni nacionalni nadzorni organ, pri katerem oseba vloži pritožbo z namenom varstva njenih pravic in svoboščin pri obdelavi osebnih podatkov, ki se nanjo nanašajo, tudi če obstaja sklep Komisije o ustreznosti, imeti možnost popolnoma neodvisno preučiti, ali se pri prenosu teh podatkov izpolnjujejo zahteve iz Splošne uredbe o varstvu podatkov, in po potrebi na nacionalna sodišča vložiti tožbo zato, da ta sodišča, če se strinjajo s pomisleki tega organa glede veljavnosti sklepa o ustreznosti, sprožijo postopek predhodnega odločanja za preučitev te veljavnosti.“

4. STANDARDI EU ZA USTREZNOST V POLICIJSKEM SODELOVANJU IN PRAVOSODNEM SODELOVANJU V KAZENSKIH ZADEVAH

22. Z vidika vsebine bi se morali sklepi o ustreznosti osredotočati na oceno obstoječe zakonodaje zadevne tretje države kot celote, v teoriji in praksi, ob upoštevanju meril za ocenjevanje iz člena 36 Direktive o kazenskem pregonu. Sistem tretje države ali mednarodne organizacije mora vsebovati naslednja osnovna splošna, postopkovna in izvrševalna načela ter mehanizme varstva podatkov.

23. V členu 36(2) Direktive o kazenskem pregonu so določeni elementi, ki jih Evropska komisija upošteva pri ocenjevanju ustreznosti ravni varstva v tretji državi ali mednarodni organizaciji.

24. Komisija zlasti upošteva načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin[16], ustrezno splošno in področno zakonodajo ter tudi njeno izvajanje, dejanske in izvršljive pravice ter učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo, obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov ter mednarodne zaveze, ki jih je sprejela tretja država ali mednarodna organizacija.

25. Zato je jasno, da mora vsaka smiselna analiza ustreznega varstva vključevati dva osnovna elementa: vsebino veljavnih predpisov in sredstva za zagotavljanje njihovega učinkovitega izvajanja v praksi. Evropska komisija mora redno preverjati, ali so vzpostavljeni predpisi v praksi učinkoviti.

26. Jedro splošnih načel varstva podatkov ter postopkovnih zahtev in zahtev glede izvrševanja, ki lahko štejejo za minimalno zahtevo za ustreznost varstva, izhaja iz Listine EU o temeljnih pravicah in Direktive o kazenskem pregonu. Splošne določbe o varstvu podatkov in zasebnosti v tretji državi ne zadostujejo. Nasprotno, pravni okvir tretje države ali mednarodne organizacije mora vsebovati specifične določbe, ki konkretno obravnavajo pravico do varstva podatkov na področju kazenskega pregona. Tretja država bi morala zagotoviti jamstva, ki zagotavljajo ustrezno raven varstva, ki je v bistvenem enaka tisti, zagotovljeni v Uniji. Te določbe morajo biti izvršljive.

27. Glede načela sorazmernosti[17] je Sodišče Evropske unije v povezavi z zakoni države članice razsodilo, da je treba vprašanje, ali je mogoče upravičiti omejitev pravice do zasebnosti in pravice do varstva podatkov, presojati po eni strani z merjenjem resnosti **posega,** ki ga pomeni taka omejitev[18], in po drugi strani s preverjanjem, da je **pomembnost cilja splošnega interesa**, ki se uresničuje s to omejitvijo, v sorazmerju s to resnostjo[19].

---

[16] Pri oceni pravnega okvira tretje države bi bilo treba upoštevati možnost, da je mogoče na podlagi podatkov, ki se prenesejo iz EU, izreči smrtno kazen ali kakršno koli obliko krutega in nečlovečnega ravnanja. Če pravo tretje države predvideva tako kazen ali ravnanje, bi bilo treba v pravnem okviru tretje države najti dodatne zaščitne ukrepe, da se zagotovi, da se podatki, preneseni iz EU, ne bodo uporabili pri pozivu k smrtni kazni, njenemu izreku in njeni izvršitvi ali kakršni koli obliki krutega in nečlovečnega ravnanja (na primer mednarodni sporazum, ki pogojuje prenos, zaveza tretje države, da na podlagi podatkov, prenesenih iz EU, ne bo izrekla smrtne kazni ali kakršne koli oblike krutega in nečloveškega ravnanja, ali moratorij na smrtno kazen).

[17] Člen 52(1) Listine EU o temeljnih pravicah.

[18] Sodišče je na primer navedlo, da „je poseg, ki ga pomeni zbiranje podatkov, ki omogočajo lokalizacijo terminalske opreme, v realnem času, še posebej resen, saj pristojni nacionalni organi s temi podatki pridobijo sredstvo za natančno in stalno spremljanje gibanja uporabnikov mobilnih telefonov [...]“ (združene zadeve C-511/18, C-512/18 in C-520/18, La Quadrature du Net in drugi, 6. oktober 2020, ECLI:EU:C:2020:791, točka 187, vključno z navedeno sodno prakso).

[19] La Quadrature du Net in drugi, točka 131.

28. V skladu s sodno prakso Sodišča Evropske unije mora pravna podlaga, ki dovoljuje poseg v temeljne pravice, zaradi spoštovanja zahtev načela sorazmernosti določati omejitve uresničevanja zadevne pravice[20]. Odstopanja in omejitve pri varstvu osebnih podatkov morajo biti strogo omejeni na tisto, kar je nujno[21]. Za spoštovanje te zahteve morajo biti poleg jasnih in natančnih pravil, ki urejajo obseg in uporabo zadevnega ukrepa, z zadevno zakonodajo določene minimalne zahteve, tako da imajo osebe, katerih podatki so bili preneseni, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganjem zlorab. „Zlasti mora biti 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.“[22]

29. Evropski odbor za varstvo podatkov je sprejel priporočila, v katerih so opredeljena temeljna jamstva, ki odražajo sodno prakso Sodišča Evropske unije in Evropskega sodišča za človekove pravice na področju nadzora v pravu tretje države, ko se presojajo posegi takih nadzornih ukrepov tretje države v pravice posameznikov, na katere se nanašajo osebni podatki, ko se podatki v zadevno tretjo državo prenašajo v skladu s Splošno uredbo o varstvu podatkov[23]. Da bi Evropski odbor za varstvo podatkov ocenil, ali so izpolnjeni pogoji iz člena 36(2)(a) Direktive o kazenskem pregonu, meni, da je treba jamstva iz teh priporočil upoštevati pri oceni ustreznosti tretje države v skladu z Direktivo o kazenskem pregonu na področju nadzora, pri čemer je treba upoštevati nadaljnje specifične pogoje na področju nadzora v tem okviru.

30. Glede zahteve iz člena 36(2)(b) bi morala tretja država poleg učinkovitega neodvisnega nadzora varstva podatkov zagotoviti tudi mehanizme sodelovanja z organi za varstvo podatkov držav članic[24].

31. Glede zahteve iz člena 36(2)(c) bi bilo treba poleg mednarodnih zavez, ki jih je sprejela tretja država ali mednarodna organizacija, upoštevati tudi obveznosti, ki izhajajo iz sodelovanja tretje države ali mednarodne organizacije v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov, ter izvajanje takih obveznosti, zlasti pristop tretje države k drugim mednarodnim sporazumom o varstvu podatkov, na primer h Konvenciji Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov in k Dodatnemu protokolu h Konvenciji (Konvencija št. 108[25] in njena posodobljena različica, Konvencija št. 108+). Upoštevati je mogoče tudi skladnost tretje države z načeli iz mednarodnih dokumentov, kot je dokument Sveta Evrope Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime (Praktični vodnik o uporabi osebnih podatkov v policijskem sektorju: kako varovati osebne podatke pri boju proti kriminalu).

32. Sklep o ustreznosti bi moral zagotoviti, da tuj sistem kot celota z vsebino pravice do zasebnosti in pravice do varstva podatkov ter učinkovitim izvajanjem in uveljavljanjem teh pravic in nadzorom nad njima zagotovi potrebno raven varstva, vključno za podatke, ki se prenašajo v tretjo državo. Kot je Sodišče Evropske unije poudarilo v sodbi v zadevi Schrems II, je treba visoko raven varstva zagotoviti tudi v primeru prenosa osebnih podatkov v tretjo državo[26].

[20] Schrems II, točka 180.
[21] Schrems II, točka 176, vključno z navedeno sodno prakso.
[22] Schrems II, točka 176, vključno z navedeno sodno prakso.
[23] Priporočila Evropskega odbora za varstvo podatkov 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe, sprejeta 10. novembra 2020.
[24] Uvodna izjava 67 Direktive o kazenskem pregonu.
[25] Uvodna izjava 68 Direktive o kazenskem pregonu.
[26] Glej točko 93.

33. Evropska komisija bi morala pri sprejetju sklepa o ustreznosti glede ozemlja ali določenega sektorja v tretji državi upoštevati jasna in objektivna merila, kot so posebne dejavnosti obdelave ali področje uporabe veljavnih pravnih standardov in veljavne zakonodaje v tretji državi[27].

A. Splošna načela in zaščitni ukrepi

(a) Pojmi

34. Obstajati bi morali osnovni pojmi varstva podatkov. Ni nujno, da so povsem enaki izrazju Direktive o kazenskem pregonu, morali pa bi odražati pojme iz evropskega prava o varstvu podatkov in biti skladni z njimi. Na primer, direktiva vključuje naslednje pomembne pojme: „osebni podatki“, „obdelava osebnih podatkov“, „pristojni organi“, „upravljavec podatkov“, „obdelovalec podatkov“, „uporabnik“, „občutljivi podatki“, „točnost, „oblikovanje profilov“, „vgrajeno in privzeto varstvo podatkov“, „nadzorni organ“ in „psevdonimizacija“.

(b) Zakonitost in poštenost obdelave osebnih podatkov (člen 4, uvodna izjava 26)

35. V skladu s členom 8(2) Listine EU o temeljnih pravicah se morajo osebni podatki med drugim obdelovati „za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom“[28]. Vendar je treba v kontekstu kazenskega pregona opozoriti, da lahko pristojni organi za opravljanje nalog preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, ki je institucionalno preneseno nanje z zakonom, od posameznikov zahtevajo ali jim odredijo, da izvršijo dane zahteve. V takem primeru soglasje posameznika, na katerega se nanašajo osebni podatki, ne bi smelo zagotavljati pravne podlage za obdelavo osebnih podatkov s strani pristojnih organov[29].

36. Ta pravna podlaga bi morala določati jasna in natančna pravila, ki urejajo obseg in uporabo ustreznih dejavnosti obdelave podatkov ter določajo minimalne zahteve[30]. Poleg tega je Sodišče Evropske unije opozorilo, da „ureditev mora biti zakonsko zavezujoča v nacionalnem pravu“[31].

37. Da bi bila obdelava podatkov[32] zakonita, bi morala biti nujna za opravljanje nalog, ki jih pristojni organi opravljajo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali za izvrševanje kazenskih sankcij, vključno z zaščitnimi ukrepi za varovanje pred grožnjami javni varnosti in z njihovim preprečevanjem[33]. Ti nameni bi morali biti določeni v nacionalnem pravu.

---

[27] Uvodna izjava 67 Direktive o kazenskem pregonu.
[28] Glej Schrems II, točka 173.
[29] V uvodni izjavi 35 Direktive o kazenskem pregonu je navedeno tudi, da „[k]adar mora posameznik, na katerega se nanašajo osebni podatki, ravnati v skladu z zakonsko obvezo, ne more dejansko in svobodno izbirati, zato odziva tega posameznika ne bi smeli obravnavati kot prostovoljni izraz njegove volje. To državam članicam ne bi smelo preprečevati, da z zakonom določijo, da lahko posameznik, na katerega se nanašajo osebni podatki, izrazi soglasje za obdelavo svojih osebnih podatkov za namene te direktive, kot je test DNK v kazenskih preiskavah ali spremljanje njegove lokacije z elektronskimi zapestnicami pri izvrševanju kazenskih sankcij.“
[30] Glej Schrems II, točki 175 in 180, Mnenje 1/15, točko 139, in navedeno sodno prakso.
[31] Glej zadevo C-623/17, Privacy International proti Secretary of State for Foreign and Commonwealth Affairs in drugim, 6. oktober 2020, ECLI:EU:C:2020:790, točka 68. Pojasniti je treba, da Sodišče Evropske unije v francoski različici sodbe uporablja besedo „*réglementation*“, ki zajema več kot le akte parlamenta.
[32] Obdelava osebnih podatkov v celoti ali delno z avtomatiziranimi sredstvi in drugačna obdelava kakor z avtomatiziranimi sredstvi za osebne podatke, ki so del zbirke ali so namenjeni oblikovanju dela zbirke.
[33] Pristojni organi so vsi javni organi, pristojni za take namene, ali kateri koli drug organ ali subjekt, ki je z zakonom pooblaščen za izvajanje javne oblasti in javnih pooblastil za take namene.

38. Osebni podatki se obdelujejo pošteno. Načelo poštene obdelave v okviru varstva podatkov je pojem, ki je jasno ločen od pravice do poštenega sojenja, ki je opredeljena v členu 47 Listine EU o temeljnih pravicah ter v členu 6 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin[34].

(c) Načelo omejitve namena (člen 4)

39. Posebni nameni, za katere se osebni podatki obdelujejo, bi morali biti izrecni, zakoniti in določeni v času zbiranja osebnih podatkov[35].

40. Podatki bi se morali obdelovati za določen, izrecen in zakonit namen v okviru namenov preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij[36], vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem v tretji državi, ter posledično uporabljeni za katerega koli od teh namenov, če to ni nezdružljivo s prvotnim namenom obdelave (na primer za izvršilne postopke, ki potekajo hkrati, ali arhiviranje v javnem interesu, znanstveno, statistično ali zgodovinsko uporabo za take namene) in če je zagotovljena ustrezna zaščita pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki. Če osebne podatke obdeluje isti ali drugi upravljavec (pristojni organ[37]) za namen preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, ki ni namen, za katerega so bili zbrani, bi morala biti taka obdelava dovoljena, če je ta obdelava v skladu z veljavnimi pravnimi določbami ter je za zadevni drugi namen nujna in z njim sorazmerna[38]. Upoštevati bi bilo treba tudi obstoj mehanizma za obveščanje pristojnih organov zadevne države članice o taki nadaljnji obdelavi podatkov[39]. Poleg tega v nobenem primeru ne bi smela biti ogrožena raven varstva posameznikov, ki jo v Uniji zagotavlja Direktiva o kazenskem pregonu, tudi v tistih primerih, ko se osebni podatki iz tretje države prenašajo upravljavcem ali obdelovalcem v isti tretji državi[40].

(d) Posebni pogoji za nadaljnjo obdelavo za druge namene (člen 9)

41. Tudi nadaljnja obdelava ali razkritje podatkov, ki se iz EU prenašajo za namene, ki niso nameni kazenskega pregona, na primer nameni državne varnosti, bi morali biti določeni z zakonom, nujni in sorazmerni. Upoštevati bi bilo treba tudi obstoj mehanizma za obveščanje pristojnih organov zadevne države članice o taki nadaljnji obdelavi podatkov[41]. Tudi tukaj bi morala za nadalje obdelane ali razkrite podatke veljati enaka raven varstva, kot je veljala, ko jih je prvotno obdeloval pristojni organ, ki jih je prejel.

---

[34] Uvodna izjava 26 Direktive o kazenskem pregonu.
[35] Uvodna izjava 26 Direktive o kazenskem pregonu.
[36] Vključuje „policijske dejavnosti v primerih, ko še ni jasno, ali gre za kaznivo dejanje ali ne. Takšne dejavnosti lahko vključujejo izvajanje pristojnosti s prisilnimi ukrepi, kot so policijske dejavnosti ob demonstracijah, na velikih športnih dogodkih in ob izgredih. Vključujejo tudi vzdrževanje javnega reda in miru, nalogo, za katero je pristojna policija ali drug organ preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kadar je to potrebno za varovanje pred grožnjami javni varnosti in pravno zaščitenim temeljnim interesom družbe ter preprečevanje teh groženj, ki bi lahko vodile v kazniva dejanja“ (uvodna izjava 12 Direktive o kazenskem pregonu). Treba je razlikovati od namena varnosti države ali dejavnosti, ki spadajo v področje uporabe poglavja 2 naslova V Pogodbe o Evropski uniji (PEU) (uvodna izjava 14 Direktive o kazenskem pregonu).
[37] Glej opombo 33.
[38] Uvodna izjava 29 Direktive o kazenskem pregonu.
[39] Taki mehanizmi bi lahko bili na primer vzajemno dogovorjene kodeksi ravnanja s podatki, obveznost obveščanja v skladu z mednarodnim instrumentom, vključno z morebitnimi samodejnimi obvestili, ali drugi podobni ukrepi za preglednost.
[40] Uvodna izjava 64 Direktive o kazenskem pregonu.
[41] Glej opombo 39.

(e) Načelo najmanjšega obsega podatkov

42. Podatki bi morali biti ustrezni, relevantni in ne prekomerni glede na namene, za katere se obdelujejo. Zlasti bi bilo treba upoštevati uporabo zahtev za vgrajeno in privzeto varstvo podatkov, kot so omejena podatkovna polja (strukturirana sporočila) ali avtomatizirano ali neavtomatizirano preverjanje kakovosti.

(f) Načelo točnosti podatkov

43. Podatki bi morali biti točni in po potrebi posodobljeni. Kljub temu bi bilo treba uporabiti načelo točnosti podatkov, hkrati pa upoštevati naravo in namen zadevne obdelave. Zlasti izjave, podane v sodnih postopkih, ki vsebujejo osebne podatke, temeljijo na subjektivnem dojemanju posameznikov in niso vedno preverljive. Zato se zahteva po točnosti ne bi smela nanašati na točnost izjave, ampak zgolj na dejstvo, da je bila določena izjava podana[42].

44. Zagotoviti bi bilo treba, da se osebni podatki, ki so netočni, nepopolni ali neposodobljeni, ne posredujejo ali dajo na voljo[43] in da so predvideni postopki za popravo ali izbris netočnih podatkov. Zlasti bi bilo treba upoštevati vsakršne sisteme razvrščanja obdelanih informacij glede na zanesljivost vira in raven preverjanja dejstev[44].

(g) Načelo hrambe podatkov

45. Podatki bi se morali hraniti le toliko časa, kot je potrebno za zamene, za katere se obdelujejo. Vzpostaviti bi bilo treba ustrezne mehanizme za izbris osebnih podatkov; osebni podatki se izbrišejo po določenem času ali pa se potreba po shranjevanju osebnih podatkov redno preverja (ali pa kombinacija obojega: fiksno najdaljše obdobje in redni pregledi v določenih časovnih presledkih)[45]. Za osebne podatke, ki se zaradi arhiviranja v javnem interesu ali v znanstvene, statistične ali zgodovinske namene shranjujejo za daljše obdobje, bi morali veljati ustrezni zaščitni ukrepi (na primer glede dostopa)[46].

(h) Načelo varnosti in zaupnosti (člen 29, uvodni izjavi 28 in 71)

46. Vsak subjekt, ki obdeluje osebne podatke, bi moral zagotoviti, da se podatki obdelujejo na način, ki zagotavlja varnost osebnih podatkov, vključno s preprečevanjem nepooblaščenega dostopa do osebnih podatkov ali njihove uporabe in do opreme, ki se uporablja za obdelavo. To vključuje zaščito pred nezakonito obdelavo in ustrezne ukrepe za obravnavo take obdelave ter tudi zaščito pred nenamerno izgubo, uničenjem ali poškodbo, in sicer z ustreznimi tehničnimi ali organizacijskimi ukrepi. Pri določanju ravni varnosti bi bilo treba upoštevati najsodobnejše tehnologije, stroške izvajanja, naravo, obseg, okoliščine in namene obdelave ter tudi tveganje za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti.

47. Zagotoviti bi bilo treba varne načine komuniciranja med organi držav članic, ki prenašajo osebne podatke, in organi tretjih držav, ki jih prejmejo.

(i) Načelo preglednosti (člen 13, uvodne izjave 26, 39, 42, 43, 44, 46)

[42] Uvodna izjava 30 Direktive o kazenskem pregonu.
[43] Uvodna izjava 32 Direktive o kazenskem pregonu.
[44] Na primer mreže 4 x 4 za ocene zanesljivosti in kode za ravnanje s podatki.
[45] Člen 5 Direktive o kazenskem pregonu.
[46] Uvodna izjava 26 Direktive o kazenskem pregonu.

48. Posameznike bi bilo treba opozoriti na tveganja, pravila, zaščitne ukrepe in pravice glede obdelave njihovih osebnih podatkov ter na to, kako lahko uresničujejo svoje pravice glede take obdelave[47].

49. Informacije o vseh glavnih elementih obdelave njihovih osebnih podatkov bi morale biti posameznikom na voljo. Take informacije bi morale biti lahko dostopne ter z uporabo jasnega in preprostega jezika enostavno razumljive. Vključevati bi morale namen obdelave, identiteto upravljavca podatkov, pravice, ki so jim na voljo[48], in druge informacije, če je to potrebno za zagotavljanje poštenosti.

50. Glede te pravice do obveščenosti lahko obstajajo nekatere izjeme. Vendar bi morala biti taka omejitev dovoljena z zakonodajnim ukrepom ter biti nujna in sorazmerna, da se prepreči oviranje uradnih ali zakonitih preiskav, poizvedb ali postopkov, prepreči vplivanje na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, zaščiti javna varnost ali varnost države ali zaščitijo pravice in svoboščine drugih, če je taka delna ali popolna omejitev nujen in sorazmeren ukrep v demokratični družbi, ki ustrezno spoštuje temeljne pravice in zakonite interese zadevnega posameznika. Take omejitve bi bilo treba tudi proučiti in oceniti ob upoštevanju možnosti za vložitev pritožbe pri nadzornem organu ali za uveljavitev pravnega sredstva. V vsakem primeru bi morala biti vsaka morebitna omejitev začasna in ne splošna ter povezana s podobnimi pogoji, zaščitnimi ukrepi in omejitvami, kot jih zahtevata Listina EU o temeljnih pravicah in Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin in kakor jih razlagata sodna praksa Sodišča Evropske unije oziroma Evropsko sodišče za človekove pravice, zlasti pa spoštovati bistvo zadevnih pravic in svoboščin.

(j) Pravica do dostopa, popravka in izbrisa (člena 14 in 16)

51. Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti pravico, da pridobi potrditev, da se v zvezi z njim obdelujejo podatki in da se mu v tem primeru zagotovi dostop do njegovih podatkov. Ta pravica bi morala vključevati vsaj določene informacije o obdelavi, kot so nameni obdelave in pravna podlaga zanjo, pravica do vložitve pritožbe pri nadzornem organu ali vrste zadevnih osebnih podatkov[49]. To je še zlasti pomembno, če se preglednost uresničuje s splošnim obvestilom (na primer informacije na spletnem mestu organa).

52. Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti pravico do popravka podatkov v zvezi z njim, če za to obstajajo določeni razlogi, na primer, kadar se izkaže, da so netočni ali nepopolni. Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti tudi pravico do izbrisa podatkov v zvezi z njim, kadar na primer njihova obdelava ni več potrebna ali je nezakonita.

53. Uresničevanje teh pravic za posameznika, na katerega se nanašajo osebni podatki, ne bi smelo biti prekomerno zapleteno.

(k) Omejitve pravic posameznika, na katerega se nanašajo osebni podatki

54. Morebitne omejitve takih pravic bi lahko obstajale, da se prepreči oviranje uradnih ali zakonitih preiskav, poizvedb ali postopkov, prepreči vplivanje na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, zaščiti javna varnost ali varnost države ali zaščitijo pravice in svoboščine drugih, če je taka delna ali popolna omejitev nujen in sorazmeren ukrep v demokratični družbi, ki ustrezno spoštuje temeljne pravice in zakonite

[47] Uvodna izjava 26 Direktive o kazenskem pregonu.
[48] Materialne pravice (pravica do dostopa, do popravka itd.) in pravica do sodnega varstva.
[49] Člen 14 Direktive o kazenskem pregonu.

interese zadevnega posameznika. Take omejitve bi bilo treba tudi proučiti in oceniti ob upoštevanju možnosti za vložitev pritožbe pri nadzornem organu ali za uveljavitev pravnega sredstva.

(l) Omejitve za nadaljnje prenose (člen 35, uvodni izjavi 64 in 65)

55. Nadaljnji prenos osebnih podatkov, ki ga prvotni uporabnik izvede v drugo tretjo državo ali mednarodno organizacijo, ne sme ogroziti ravni varstva, ki ga Unija zagotavlja za posameznike, katerih podatki se prenašajo. Zato se lahko taki nadaljnji prenosi dovolijo le, če je zagotovljena neprekinjenost ravni varstva, ki ga zagotavlja pravo EU[50]. Zlasti bi moral biti nadaljnji uporabnik (tj. uporabnik nadaljnjega prenosa) pristojni organ za namene kazenskega pregona[51], taki nadaljnji prenosi podatkov pa se lahko izvedejo le za omejene in točno določene namene ter če za to obdelavo obstaja pravna podlaga.

56. Upoštevati je treba tudi obstoj mehanizma, s katerim se obveščajo pristojni organi zadevne države članice in dovoljuje tak nadaljnji prenos podatkov. Prvotni uporabnik podatkov, prenesenih iz EU, bi moral biti odgovoren in zmožen dokazati, da je zadevni pristojni organ države članice dovolil nadaljnji prenos[52] ter da so v odsotnosti sklepa o ustreznosti v zvezi s tretjo državo, v katero se bodo podatki nadalje prenesli[53], zagotovljeni ustrezni zaščitni ukrepi za nadaljnji prenos podatkov.

(m) Načelo odgovornosti (člen 4(4))

57. Upravljavec bi moral biti odgovoren za načela varstva podatkov iz člena 4 Direktive o kazenskem pregonu in biti zmožen dokazati skladnost z njimi.

[50] Glej tudi Mnenje 1/15.
[51] Glej opombo 33.
[52] Glede tega bi bilo treba upoštevati obstoj obveznosti ali zaveze za izvajanje ustreznih kodeksov ravnanja s podatki, ki jih opredelijo organi držav članic, ki prenašajo podatke.
[53] Te zahteve ne posegajo v posebne pogoje za nadaljnje prenose v ustrezno državo, določene v Direktivi o kazenskem pregonu (člen 35(1)(c) in (e)).

B. Primeri dodatnih načel, ki se uporabijo za posebne vrste obdelave

(a) Posebne vrste osebnih podatkov (člen 10 in uvodna izjava 37)

58. Za „posebne vrste podatkov“[54] bi morali obstajati posebni zaščitni ukrepi za obravnavo posebnih tveganj[55]. Te vrste bi morale izražati tiste iz člena 10 Direktive o kazenskem pregonu. Za obdelavo posebnih vrst podatkov bi torej morali veljati posebni zaščitni ukrepi, dovoljena pa bi morala biti le takrat, kadar je nujno potrebna pod določenimi pogoji, na primer za zaščito življenjskih interesov posameznika.

(b) Avtomatizirano sprejemanje odločitev in oblikovanje profilov (člen 11 in uvodna izjava 38)

59. Odločitve, ki temeljijo izključno na avtomatizirani obdelavi (avtomatizirano sprejemanje posameznih odločitev), vključno z oblikovanjem profilov, ki imajo škodljive pravne učinke za posameznika, na katerega se nanašajo osebni podatki, ali močno vplivajo nanj, bi se morale sprejemati le pod določenimi pogoji pravnega okvira tretje države[56].

60. V okviru Evropske unije taki pogoji vključujejo na primer konkretno seznanitev posameznika, na katerega se nanašajo osebni podatki, in pravico do osebnega posredovanja s strani upravljavca, kar bi mu zlasti omogočilo, da izrazi svoje stališče, dobi pojasnilo o odločitvi po takem ocenjevanju ali da izpodbija odločitev.

61. Pravo tretje države bi v vsakem primeru moralo zagotavljati potrebne zaščitne ukrepe za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki. Glede tega bi bilo treba upoštevati tudi obstoj mehanizma za obveščanje pristojnih organov zadevne države članice o vsaki nadaljnji obdelavi, kot je uporaba prenesenih podatkov za obsežno oblikovanje profilov.

(c) Vgrajeno in privzeto varstvo podatkov (člen 20)

62. Pri oceni ustreznosti bi bilo treba pozornost nameniti obstoju obveznosti za upravljavca, da sprejme notranje politike in izvede ukrepe, ki spoštujejo načeli vgrajenega in privzetega varstva podatkov, ob upoštevanju najsodobnejših tehnologij, stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave in tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, ki jih pomeni obdelava, tako v času določanja sredstev obdelave kot tudi v času same obdelave, da sprejme ustrezne tehnične in organizacijske ukrepe, kot je psevdonimizacija, ki so oblikovani za učinkovito izvajanje načel varstva podatkov, kot je načelo najmanjšega obsega podatkov, ter v obdelavo vključi potrebne zaščitne ukrepe.

[54] Take posebne vrste so v uvodni izjavi 37 Direktive o kazenskem pregonu znane tudi kot „občutljivi podatki“.
[55] Taki dodatni zaščitni ukrepi bi bili lahko na primer posebni varnostni ukrepi, omejene pravice osebja do dostopa, omejitve v zvezi z nadaljnjo obdelavo, avtomatizirano sprejemanje odločitev, nadaljnja izmenjava ali nadaljnji prenosi.
[56] Mnenje 1/15, točka 173.

C. Postopkovni mehanizmi in mehanizmi izvrševanja

63. Čeprav so lahko sredstva, ki jih lahko tretja država uporabi za zagotovitev ustrezne ravni varstva, drugačna od tistih, ki se uporabljajo v Evropski uniji[57], morajo biti za sistem, ki je skladen z evropskim, značilni naslednji elementi:

(a) Pristojni neodvisni nadzorni organ (člen 36(2)b, člen 36(3) in uvodna izjava 67)

64. V tretji državi bi moral obstajati eden ali več neodvisnih nadzornih organov, ki zagotavljajo in izvršujejo skladnost s predpisi o varstvu podatkov in zasebnosti. Nadzorni organ pri izvajanju svojih dolžnosti in pooblastil ravna popolnoma neodvisno in nepristransko ter pri tem ne prosi za navodila niti jih ne sprejema. Glede tega bi moral imeti nadzorni organ vsa ustrezna izvršilna pooblastila za učinkovito zagotavljanje skladnosti s pravicami do varstva podatkov in za spodbujanje ozaveščenosti. Upoštevati bi bilo treba tudi osebje in proračun nadzornega organa. Nadzorni organ bi moral tudi imeti možnost, da na lastno pobudo izvaja preiskave. Zadolžen bi moral biti tudi za svetovanje in pomoč posameznikom, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic (glej tudi točko (c) v nadaljevanju). Sklepi o ustreznosti bi morali, kjer je ustrezno, opredeliti nadzorni organ ali organe in mehanizme sodelovanja z nadzornimi organi držav članic za izvrševanje predpisov o varstvu podatkov.

(b) Učinkovito izvajanje predpisov o varstvu podatkov

65. Sistem tretje države bi moral zagotoviti visoko stopnjo ozaveščenosti upravljavcev podatkov in tistih, ki v njihovem imenu obdelujejo osebne podatke, o njihovih obveznostih, nalogah in odgovornostih, ter posameznikov, na katere se nanašajo osebni podatki, o njihovih pravicah in sredstvih za uresničevanje teh pravic. Pri zagotavljanju spoštovanja pravil imajo lahko pomembno vlogo obstoj učinkovitih in odvračilnih sankcij ter sistemi neposrednega preverjanja s strani organov, revizorjev ali neodvisnih pooblaščenih oseb za varstvo osebnih podatkov.

66. Okvir za varstvo podatkov v tretji državi bi moral upravljavce podatkov ali tiste, ki v njihovem imenu obdelujejo osebne podatke, zavezati k temu, da upoštevajo ta okvir in da lahko dokažejo tako skladnost, zlasti pristojnemu nadzornemu organu. Taki ukrepi bi morali vključevati vodenje evidenc ali dnevnikov dejavnosti obdelave podatkov za ustrezno časovno obdobje. To lahko vključuje na primer tudi oceno učinka glede varstva podatkov, imenovanje pooblaščene osebe za varstvo podatkov ali vgrajeno in privzeto varstvo podatkov.

(c) Sistem za varstvo podatkov olajšuje uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki (členi 12, 17 in 46 direktive o kazenskem pregonu)

67. Okvir za varstvo podatkov v tretji državi bi moral upravljavce podatkov zavezati k temu, da olajšujejo uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, navedenih v oddelku A (j) zgoraj, ter določati, da nadzorni organ tretje države na zahtevo obvesti posameznike, na katere se nanašajo osebni podatki, o uresničevanju njihovih pravic[58].

(d) Sistem za varstvo podatkov zagotavlja ustrezne mehanizme sodnega varstva

[57] Schrems I, točka 74.
[58] Uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, je lahko bodisi neposredno bodisi posredno.

68. Čeprav trenutno ni sodne prakse v zvezi z ustreznostjo pravnega sistema tretje države glede na Direktivo o kazenskem pregonu, je Sodišče Evropske unije temeljno pravico do učinkovitega sodnega varstva razložilo, kot je določena v členu 47 Listine EU o temeljnih pravicah. Prvi odstavek člena 47 Listine EU o temeljnih pravicah določa, da ima vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Evropske unije, pravico do učinkovitega pravnega sredstva pred sodiščem[59] v skladu s pogoji, določenimi v členu 47 Listine EU o temeljnih pravicah.

69. V skladu z ustaljeno sodno prakso Sodišča Evropske unije je sam obstoj učinkovitega sodnega nadzora, namenjenega zagotovitvi spoštovanja določb prava Unije, neločljivo povezan z obstojem pravne države. Tako 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 oziroma izbris takih podatkov, posega v bistvo temeljne pravice do učinkovitega sodnega varstva, določene v členu 47 Listine EU o temeljnih pravicah[60].

70. Posameznik bi moral imeti možnost, da za uveljavljanje svojih pravic in zagotovitev skladnosti uporabi pravna sredstva hitro in učinkovito ter brez previsokih stroškov.

71. Zato morajo biti vzpostavljeni nadzorni mehanizmi, ki omogočajo neodvisno preiskovanje pritožb, opredeljevanje kakršnih koli kršitev pravice do varstva podatkov in spoštovanja zasebnega življenja ter kaznovanje takih kršitev v praksi.

72. Kadar se predpisi ne upoštevajo, bi se moralo posamezniku, na katerega se nanašajo osebni podatki in čigar osebni podatki se prenašajo v tretjo državo, zagotoviti tudi učinkovito upravno in sodno varstvo v tretji državi, vključno z odškodnino za škodo, ki nastane zaradi nezakonite obdelave njegovih osebnih podatkov. To je ključen element, ki mora vključevati sistem za neodvisno odločanje ali arbitražo, ki po potrebi omogoča plačilo odškodnine in izrek sankcij.

[59] Sodišče Evropske unije meni, da lahko učinkovito sodno varstvo poleg sodišča zagotovi tudi organ, ki zagotavlja jamstva, ki so v bistvenem enakovredna tistim, ki se zahtevajo s členom 47 Listine EU o temeljnih pravicah (glej Schrems II, točka 197). To je lahko pomembno zlasti za mednarodne organizacije.
[60] Schrems II, točki 187 in 194, vključno z navedeno sodno prakso.