Smernice

Smernice št. 2/2020 o členu 46(2)(a) in (3)(b) Uredbe 2016/679 glede prenosov osebnih podatkov med javnimi organi in telesi v EGP in zunaj EGP

Različica 2.0

Sprejete 15. decembra 2020

Zgodovina različic

Različica 2.0	15. december 2020	Sprejetje smernic po javnem posvetovanju
Različica 1.0	18. februar 2020	Sprejetje smernic za javno posvetovanje

Kazalo

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),

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

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE:

[1] Sklicevanja na „države članice“ v teh smernicah je treba razumeti kot sklicevanja na „države članice EGP“.

1 SPLOŠNO

1.1 Namen

1. Namen tega dokumenta je zagotoviti smernice za uporabo člena 46(2)(a) in (3)(b) Splošne uredbe o varstvu podatkov za prenose osebnih podatkov od javnih organov ali teles (v nadaljevanju: javni organi) v EGP javnim organom v tretjih državah ali mednarodnim organizacijam, če niso zajeti s sklepom o ustreznosti, ki ga je sprejela Evropska komisija.[2] Javni organi se lahko odločijo za uporabo teh mehanizmov, ki se po Splošni uredbi o varstvu podatkov štejejo za primernejše glede na njihov položaj, vendar pa se lahko sklicujejo tudi na druga ustrezna orodja, ki določajo ustrezne zaščitne ukrepe v skladu s členom 46 Splošne uredbe o varstvu podatkov.

2. Smernice ponazarjajo pričakovanja Evropskega odbora za varstvo podatkov glede zaščitnih ukrepov, ki jih morajo v skladu s členom 46(2)(a) Splošne uredbe o varstvu podatkov javni organi sprejeti s pravno zavezujočim in izvršljivim instrumentom ali ki jih je treba z dovoljenjem ustreznega nadzornega organa v skladu s členom 46(3)(b) Splošne uredbe o varstvu podatkov zagotoviti z določbami, ki se vstavijo v upravne dogovore med javnimi organi.[3] Evropski odbor za varstvo podatkov strankam močno priporoča, da smernice uporabljajo kot referenčni dokument v zgodnji fazi, kadar nameravajo skleniti ali spremeniti take instrumente in dogovore.[4]

3. Smernice je treba razumeti v povezavi z drugim prej opravljenim delom Evropskega odbora za varstvo podatkov (vključno s potrjenimi dokumenti njegove predhodnice, tj. Delovne skupine iz člena 29,[5] o osrednjih vprašanjih ozemeljske veljavnosti in prenosov osebnih podatkov v tretje države[6]). Smernice bodo pregledane in po potrebi posodobljene na podlagi praktičnih izkušenj, pridobljenih z uporabo Splošne uredbe o varstvu podatkov.

4. Te smernice zajemajo mednarodne prenose podatkov med javnimi organi za različne namene upravnega sodelovanja, ki spadajo na področje uporabe Splošne uredbe o varstvu podatkov. Posledično in v skladu z njenim členom 2(2) ne zajemajo prenosov na področju javne varnosti, obrambe ali državne varnosti. Poleg tega ne obravnavajo obdelave in prenosov podatkov s strani pristojnih organov za namene kazenskega pregona, saj to ureja ločeni posebni instrument, tj. direktiva o kazenskem pregonu.[7] Nazadnje, smernice obravnavajo le prenose med javnimi organi in ne zajemajo prenosov osebnih podatkov od javnega organa k zasebnemu subjektu ali od zasebnega subjekta k javnemu organu.

---

[2] Na primer japonskim javnim organom, za katere ne velja sklep o ustreznosti za Japonsko, saj ta zajema le organizacije zasebnega sektorja.

[3] V teh smernicah se izraz „mednarodni sporazumi“ uporablja za pravno zavezujoče in izvršljive instrumente v skladu s členom 46(2)(a) ter za upravne dogovore v skladu s členom 46(3)(b) Splošne uredbe o varstvu podatkov.

[4] Člen 96 Splošne uredbe o varstvu podatkov določa, da sporazumi, sklenjeni pred 24. majem 2016, ostanejo veljavni, dokler niso spremenjeni, nadomeščeni ali razveljavljeni.

[5] Delovna skupina organov EU za varstvo podatkov, ustanovljena na podlagi člena 29 Direktive 95/46/ES o varstvu podatkov.

[6] Glej Referenčni dokument Delovne skupine iz člena 29 o ustreznosti (WP 254 rev. 01, ki ga je Evropski odbor za varstvo podatkov potrdil 25. maja 2018), Smernice Evropskega odbora za varstvo podatkov št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679 in Smernice Evropskega odbora za varstvo podatkov št. 3/2018 o ozemeljski veljavnosti Splošne uredbe o varstvu podatkov (člen 3).

[7] Direktiva (EU) 2016/680 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.

1.2 Splošna pravila, ki se uporabljajo za mednarodne prenose

5. V skladu s členom 44 Splošne uredbe o varstvu podatkov mora izvoznik podatkov, ki prenaša osebne podatke v tretje države ali mednarodne organizacije, poleg izpolnjevanja zahtev poglavja V Splošne uredbe o varstvu podatkov izpolnjevati tudi pogoje drugih njenih določb. Natančneje, vsaka obdelava mora biti skladna z načeli varstva podatkov iz člena 5 Splošne uredbe o varstvu podatkov, biti zakonita v skladu z njenim členom 6 in v primeru posebnih vrst podatkov skladna z njenim členom 9. Zato je treba uporabljati dvostopenjski preskus: prvič, za obdelavo podatkov se mora uporabljati pravna podlaga kot taka, skupaj z vsemi ustreznimi določbami Splošne uredbe o varstvu podatkov, in drugič, izpolnjene morajo biti določbe poglavja V Splošne uredbe o varstvu podatkov.

6. Splošna uredba o varstvu podatkov v členu 46 določa, da „[k]adar sklep v skladu s členom 45(3) ni sprejet, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo ali mednarodno organizacijo le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva“. Taki ustrezni zaščitni ukrepi se lahko zagotovijo s pravno zavezujočim in izvršljivim instrumentom, ki ga sprejmejo javni organi (člen 46(2)(a) Splošne uredbe o varstvu podatkov), ali z dovoljenjem ustreznega nadzornega organa z določbami, ki se vstavijo v upravne dogovore med javnimi organi ali telesi in v katere so vključene izvršljive in učinkovite pravice za posameznike, na katere se nanašajo osebni podatki (člen 46(3)(b) Splošne uredbe o varstvu podatkov). Kot je pojasnilo Sodišče EU, morajo ustrezni zaščitni ukrepi zagotavljati, da je osebam, katerih podatki se prenašajo v tretjo državo, zagotovljena raven varstva, ki je v osnovi enakovredna tisti, ki je zagotovljena v EGP.[8]

7. Poleg te rešitve in če te rešitve ni, pa člen 49 Splošne uredbe o varstvu podatkov navaja tudi omejeno število posebnih okoliščin, v katerih lahko mednarodni prenosi podatkov potekajo brez sklepa o ustreznosti, ki ga sprejme Evropska komisija.[9] Natančneje, ena izjema zajema prenose, potrebne zaradi pomembnih razlogov javnega interesa, priznanih v pravu Unije ali pravu države članice, ki velja za upravljavca, vključno v duhu vzajemnosti pri mednarodnem sodelovanju.[10] Vendar je treba, kot je pojasnjeno v prejšnjih smernicah, ki jih je izdal Evropski odbor za varstvo podatkov, odstopanja iz člena 49 Splošne uredbe o varstvu podatkov razlagati ozko in se večinoma nanašajo na obdelave, ki so občasne in se ne ponavljajo.[11]

1.3 Opredelitev javnega organa ali telesa

8. V Splošni uredbi o varstvu podatkov ni opredeljeno, kaj pomeni „javni organ ali telo“. Evropski odbor za varstvo podatkov meni, da je ta pojem dovolj širok, da zajema tako javne organe v tretjih državah kot tudi mednarodne organizacije.[12] Glede javnih organov v tretjih državah je treba pojem določiti v skladu z notranjim pravom. Skladno s tem javni organi vključujejo vladne organe na različnih ravneh (na primer nacionalni, regionalni in lokalni organi), lahko pa vključujejo tudi druga telesa, ki jih ureja

[8] Sodišče Evropske unije, zadeva C-311/18, *Data Protection Commissioner proti Facebook Ireland in Maximillianu Schremsu (Schrems II)*, točka 96.
[9] Za več informacij o členu 49 in na splošno o njegovi povezanosti s členom 46 glej Smernice Evropskega odbora za varstvo podatkov št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679.
[10] Glej Smernice Evropskega odbora za varstvo podatkov št. 2/2018 o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679, stran 10.
[11] Glej Smernice Evropskega odbora za varstvo podatkov o odstopanjih iz člena 49 v skladu z Uredbo (EU) 2016/679, stran 5.
[12] Glej tudi uvodno izjavo 108 Splošne uredbe o varstvu podatkov.

javno pravo (na primer izvajalske agencije, univerze, bolnišnice itd.).[13] V skladu s členom 4(26) Splošne uredbe o varstvu podatkov se „mednarodna organizacija“ nanaša na organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo ali katero koli drugo telo, ustanovljeno s sporazumom med dvema državama ali na podlagi takega sporazuma.

9. Evropski odbor za varstvo podatkov opozarja, da uporaba Splošne uredbe o varstvu podatkov ne posega v določbe mednarodnega prava, kot so na primer tiste, ki urejajo privilegije in imunitete mednarodnih organizacij. Hkrati je treba spomniti, da mora vsak javni organ v EGP, ki prenaša podatke mednarodnim organizacijam, spoštovati pravila Splošne uredbe o varstvu podatkov o prenosih v tretje države ali mednarodne organizacije.[14]

2 SPLOŠNA PRIPOROČILA ZA USTREZNE ZAŠČITNE UKREPE NA PODLAGI ČLENA 46(2)(A) IN (3)(B) SPLOŠNE UREDBE O VARSTVU PODATKOV

10. Drugače kot člen 26(2) Direktive 95/46/ES člen 46 Splošne uredbe o varstvu podatkov določa dodatne ustrezne zaščitne ukrepe kot orodja za prenos med javnimi organi:

    (i) pravno zavezujoč in izvršljiv instrument (člen 46(2)(a) Splošne uredbe o varstvu podatkov) ali
    (ii) določbe, ki se vstavijo v upravne dogovore (člen 46(3)(b) Splošne uredbe o varstvu podatkov).

    Ti instrumenti in dogovori so lahko dvo- ali večstranski.

11. V naslednjem oddelku je nekaj splošnih priporočil, ki pomagajo zagotavljati, da so pravno zavezujoči instrumenti ali upravni dogovori (v nadaljevanju: mednarodni sporazumi) med javnimi organi skladni s Splošno uredbo o varstvu podatkov.

12. Čeprav člen 46 in uvodna izjava 108 Splošne uredbe o varstvu podatkov ne navajata posebnih jamstev, ki jih je treba vključiti v take mednarodne sporazume, je Evropski odbor za varstvo podatkov ob upoštevanju člena 44 Splošne uredbe o varstvu podatkov[15] in nedavne sodne prakse Sodišča EU[16] izdelal seznam minimalnih zaščitnih ukrepov, ki jih je treba vključiti v mednarodne sporazume med javnimi organi, ki spadajo na področje uporabe člena 46(2)(a) ali (3)(b) Splošne uredbe o varstvu podatkov. Cilj teh zaščitnih ukrepov je zagotoviti, da ni ogrožena raven varstva posameznikov v skladu s Splošno uredbo o varstvu podatkov, kadar se njihovi osebni podatki prenašajo iz EGP, in da je posameznikom, na katere se nanašajo osebni podatki, zagotovljena raven varstva, ki je v bistvu enakovredna tisti, ki jo v EU zagotavlja Splošna uredba o varstvu podatkov.[17]

[13] Glej na primer opredelitvi pojmov „organ javnega sektorja“ in „oseba javnega prava“ v členu 2(1) in (2) Direktive 2003/98/ES Evropskega parlamenta in Sveta z dne 17. novembra 2003 o ponovni uporabi informacij javnega sektorja (UL L 345, 31. 12. 2003, stran 90).
[14] Glej Smernice Evropskega odbora za varstvo podatkov št. 3/2018 o ozemeljski veljavnosti Splošne uredbe o varstvu podatkov, stran 23.
[15] V členu 44 Splošne uredbe o varstvu podatkov je navedeno: „Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba.“
[16] Sodišče EU, sodba z dne 16. julija 2020 v zadevi C-311/18, *Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu (Schrems II)*.
[17] Sodišče EU, sodba z dne 16. julija 2020 v zadevi C-311/18, *Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu (Schrems II)*, točka 105.

13. V skladu z nedavno sodno prakso Sodišča EU[18] mora javni organ v državi članici, ki izvršuje prenos, po potrebi skupaj z javnim organom prejemnikom presoditi, ali se raven varstva, ki jo zahteva pravo EU, spoštuje v tretji državi, da bi določil, ali je mogoče seznam zaščitnih ukrepov, ki jih vsebuje mednarodni sporazum, uporabljati v praksi, ob upoštevanju morebitnih ovir v zakonodaji tretje države za spoštovanje teh zaščitnih ukrepov.

14. Glede tega je treba tudi spomniti, da lahko za zagotavljanje zaščitnih ukrepov, naštetih v teh smernicah, mednarodni sporazumi temeljijo na že obstoječih elementih nacionalnega prava tretje države ali notranjih pravilih oziroma regulativnem okviru mednarodne organizacije.

2.1 Namen in področje uporabe

15. Mednarodni sporazumi bi morali opredeljevati svoje področje uporabe, njihovi nameni pa bi morali biti določeni izrecno in specifično. Poleg tega bi morali jasno navajati vrste zadevnih osebnih podatkov in način obdelave osebnih podatkov, ki se prenašajo in obdelujejo na podlagi sporazuma.

2.2 Opredelitev pojmov

16. Mednarodni sporazumi bi morali vsebovati opredelitev osnovnih pojmov in pravic glede osebnih podatkov v skladu s Splošno uredbo o varstvu podatkov, ki so pomembni za zadevni sporazum. Taki sporazumi bi morali v primeru sklicevanja nanje na primer vsebovati naslednje pomembne opredelitve pojmov: „osebni podatki“, „obdelava osebnih podatkov“, „upravljavec podatkov“, „obdelovalec podatkov“, „uporabnik“ in „občutljivi podatki“.

2.3 Načela varstva podatkov

17. Mednarodni sporazumi bi morali vsebovati posebno besedilo, ki bi zahtevalo, da temeljna načela o varstvu podatkov zagotavljata obe stranki.

2.3.1 Načelo omejitve namena

18. Mednarodni sporazumi morajo podrobno določati namene, za katere se osebni podatki prenašajo in obdelujejo, vključno z združljivimi nameni za nadaljnjo obdelavo, ter tudi zagotavljati, da se podatki ne bodo nadalje obdelovali za nezdružljive namene. Združljivi nameni lahko vključujejo shranjevanje za namene arhiviranja v javnem interesu in tudi obdelavo za namene znanstvenih ali zgodovinskih raziskav ali za statistične namene. Zaradi večje jasnosti je priporočljivo, da so posebni nameni obdelave in prenosa podatkov našteti v samem mednarodnem sporazumu.

19. Da se izogne slehernemu tveganju širitve prvotnega namena, bi taki sporazumi morali podrobno določati tudi prepoved uporabe prenesenih podatkov za kakršne koli druge namene od tistih, ki so izrecno omenjeni v sporazumu, razen kot je določeno v odstavku spodaj.

20. Če želita obe stranki mednarodnega sporazuma javnemu organu prejemniku omogočiti drugo združljivo uporabo prenesenih osebnih podatkov, je nadaljnja uporaba teh s strani javnega organa prejemnika dovoljena le, če je združljiva s prvotno uporabo in predhodno priglašena javnemu organu, ki je izvršil prenos, ki lahko zaradi posebnih razlogov temu nasprotuje.

[18] Prav tam.

2.3.2 Načelo točnosti podatkov in načelo najmanjšega obsega

21. Mednarodni sporazum mora podrobno določati, da morajo biti podatki, ki se prenašajo in nadalje obdelujejo, ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se prenašajo in nadalje obdelujejo.

22. V praksi je načelo najmanjšega obsega podatkov pomembno za preprečevanje prenosa osebnih podatkov, kadar so ti neustrezni ali preobsežni.

23. Poleg tega bi morali biti podatki točni in posodobljeni glede na namene, za katere se obdelujejo. Mednarodni sporazum mora zato določati, da bo stranka, ki izvršuje prenos, zagotovila, da so osebni podatki, preneseni na podlagi sporazuma, točni in po potrebi posodobljeni. Poleg tega bi moral sporazum določati, da mora stranka, če ugotovi, da so bili preneseni ali se obdelujejo netočni ali neposodobljeni podatki, o tem nemudoma obvestiti drugo stranko. Nazadnje, sporazum bi moral zagotavljati, da če je potrjeno, da so podatki, ki so bili preneseni ali se obdelujejo, netočni, vsaka stranka, ki obdeluje podatke, sprejme vse razumne ukrepe, da informacije popravi ali izbriše.

2.3.3 Načelo omejitve hrambe

24. Stranki morata zagotoviti, da mednarodni sporazum vsebuje določbo glede hrambe podatkov. Ta določba bi morala podrobno določati, da se osebni podatki ne hranijo časovno neomejeno, temveč se v obliki, ki dovoljuje identifikacijo posameznikov, na katere se nanašajo osebni podatki, hranijo le tako dolgo, dokler je to potrebno za namen, za katerega so bili podatki preneseni in pozneje obdelani. To lahko vključuje hrambo tako dolgo, dokler je to potrebno za namene arhiviranja v javnem interesu, za namene znanstvenih ali zgodovinskih raziskav ali za statistične namene, če so sprejeti ustrezni tehnični in organizacijski ukrepi za zaščito pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, kot so dodatni tehnični ukrepi (na primer varnostni ukrepi, psevdonimizacija) in omejitve dostopa. Če obdobje najdaljše hrambe ni določeno že v nacionalni zakonodaji ali v notranjih pravilih oziroma regulativnem okviru mednarodne organizacije, bi bilo treba najdaljše obdobje hrambe določiti v besedilu sporazuma.

2.3.4 Varnost in zaupnost podatkov

25. Stranki bi se morali zavezati k zagotavljanju varnosti in zaupnosti obdelave osebnih podatkov in prenosov, ki jih opravljata.
Natančneje, stranki bi se morali zavezati, da imata vzpostavljene ustrezne tehnične in organizacijske ukrepe za varstvo osebnih podatkov pred nenamernim ali nezakonitim dostopom, uničenjem, izgubo, spremembo ali nepooblaščenim razkritjem. Ti ukrepi lahko na primer vključujejo šifriranje, vključno med prenosom, psevdonimizacijo, označevanje informacij kot osebnih podatkov, ki se prenašajo iz EGP, omejevanje dostopa do osebnih podatkov na določene osebe, zagotavljanje varne hrambe osebnih podatkov ali izvajanje politik, namenjenih zagotavljanju varstva in ohranitve zaupnosti osebnih podatkov.
Pri ravni varnosti bi bilo treba upoštevati tveganja, najnovejši tehnološki razvoj in povezane stroške.

26. Poleg tega lahko mednarodni sporazum podrobno določa, da če se ena od strank seznani s kršitvijo varnosti osebnih podatkov, o njej čim prej obvesti drugo(-e) stranko(-e) ter uporabi razumna in ustrezna sredstva za odpravo kršitve varnosti osebnih podatkov ter zmanjšanje morebitnih negativnih posledic, tudi z obvestilom o kršitvi varnosti osebnih podatkov posamezniku, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja, kadar je verjetno, da bo kršitev varnosti osebnih podatkov močno ogrozila pravice in svoboščine posameznika.

Priporočljivo je, da so v mednarodnem sporazumu določeni roki za obveščanje za kršitev varnosti osebnih podatkov in tudi postopki za obveščanje posameznika, na katerega se nanašajo osebni podatki.

2.4 Pravice posameznikov, na katere se nanašajo osebni podatki

27. Mednarodni sporazum mora zagotavljati izvršljive in učinkovite pravice posameznika, na katerega se nanašajo osebni podatki, kot je določeno v členu 46(1) in uvodni izjavi 108 Splošne uredbe o varstvu podatkov.

28. Pravice, ki so na voljo posameznikom, na katere se nanašajo osebni podatki, vključno s posebnimi zavezami, ki jih sprejmeta stranki za zagotavljanje takih pravic, bi morale biti naštete v sporazumu. Da bi bil mednarodni sporazum učinkovit, mora določati mehanizme, ki zagotavljajo njihovo uporabo v praksi. Poleg tega mora biti za vsako kršitev pravic posameznika, na katerega se nanašajo osebni podatki, določen ustrezen način njene odprave.

2.4.1 Pravica do preglednosti

29. Stranki morata zagotoviti, da mednarodni sporazum vsebuje jasno besedilo, ki opisuje obveznosti strank glede preglednosti.

30. Take obveznosti bi morale po eni strani vsebovati splošno informativno obvestilo najmanj z informacijami o tem, kako in zakaj lahko javni organi obdelujejo in prenašajo osebne podatke, ustreznem orodju, ki se uporablja za prenos, subjektih, ki se jim lahko taki podatki prenašajo, pravicah, ki so na voljo posameznikom, na katere se nanašajo osebni podatki, ter veljavnih omejitvah, mehanizmih pravnega varstva, ki so na voljo, in kontaktnih podatkih za predložitev spora ali zahtevka.

31. Vendar je treba spomniti, da za javni organ, ki izvršuje prenos, splošno informativno obvestilo na spletni strani zadevnega javnega organa ne bo zadostovalo. Javni organ, ki izvršuje prenos, bi moral posameznikom, na katere se nanašajo osebni podatki, zagotoviti individualne informacije v skladu z zahtevami glede obveščanja iz členov 13 in 14 Splošne uredbe o varstvu podatkov.[19]
Mednarodni sporazum lahko določa tudi nekatere izjeme za take individualne informacije. Te izjeme so omejene in bi morale biti skladne s tistimi, ki jih določa člen 14(5) Splošne uredbe o varstvu podatkov, na primer če posameznik, na katerega se nanašajo osebni podatki, že ima informacije, ali če se izkaže, da je zagotavljanje takih informacij nemogoče ali bi vključevalo nesorazmeren napor.

32. Stranki se morata zavezati, da bosta mednarodni sporazum na zahtevo dali na voljo posameznikom, na katere se nanašajo osebni podatki, in da bosta na svojih spletiščih omogočili javen dostop do mednarodnega sporazuma ali ustreznih določb, ki določajo ustrezne zaščitne ukrepe. V obsegu, potrebnem za varstvo občutljivih ali drugih zaupnih informacij, se lahko besedilo mednarodnega sporazuma pred zagotovitvijo izvoda ali njegovo javno objavo redigira. Če je to potrebno, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči razumevanje vsebine mednarodnega sporazuma, morata stranki zagotoviti njegov smiseln povzetek.

2.4.2 Pravica do dostopa, popravka, izbrisa, omejitve obdelave in ugovora

33. Mednarodni sporazum bi moral ščititi pravico posameznika, na katerega se nanašajo osebni podatki, da pridobi informacije o vseh osebnih podatkih, ki se nanašajo nanj in se obdelujejo, ter da dostopa do

[19] Glej Smernice Evropskega odbora za varstvo podatkov o preglednosti na podlagi Uredbe (EU) 2016/679, WP 260 rev. 01, strani 13 do 22.

njih, pravico do popravka, izbrisa in omejitve obdelave ter, kadar je to ustrezno, pravico do nasprotovanja obdelavi podatkov iz razlogov, ki se nanašajo na njegov posebni položaj.

34. Glede pravice do dostopa bi moral mednarodni sporazum določati, da imajo posamezniki od javnega organa prejemnika pravico pridobiti potrditev o tem, ali se osebni podatki, ki se nanašajo na njih, obdelujejo ali ne, in če se, dostop do teh podatkov, pa tudi podrobne informacije glede obdelave, vključno z namenom obdelave, vrstami zadevnih osebnih podatkov, prejemniki, ki se jim osebni podatki razkrivajo, predvidenim obdobjem hrambe in možnostmi pravnega varstva.

35. Poleg tega bi moral sporazum določati, kdaj je mogoče te pravice uveljavljati, ter vsebovati načine, kako lahko posamezniki, na katere se nanašajo osebni podatki, izvršujejo te pravice pri obeh strankah in tudi kako se bosta stranki odzvali na take zahteve. Na primer, glede izbrisa bi lahko mednarodni sporazum določal, da je treba podatke izbrisati, če so bile informacije obdelane nezakonito ali če niso več potrebne za namen obdelave. Poleg tega bi moral mednarodni sporazum določati, da se bosta stranki na razumen način in pravočasno odzvali na zahteve posameznikov, na katere se nanašajo osebni podatki. Mednarodni sporazum bi lahko določal tudi, da lahko stranki sprejmeta ustrezne ukrepe, kot je zaračunavanje razumnih pristojbin za pokritje upravnih stroškov, če so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti zaradi njihove ponavljajoče se narave.

36. Prav tako bi moral mednarodni sporazum javnemu organu, ki izvršuje prenos, naložiti, naj posamezniku, na katerega se nanašajo osebni podatki, po prenosu njegovih osebnih podatkov zagotovi informacije o ukrepih, sprejetih v zvezi z njegovo zahtevo na podlagi pravic, ki jih določa mednarodni sporazum, brez nepotrebnega odlašanja z določitvijo ustreznega roka (na primer en mesec). Nazadnje, če stranki ne ukrepata glede zahteve posameznika, na katerega se nanašajo osebni podatki, bi morale biti posamezniku, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja z določitvijo ustreznega roka (na primer en mesec od prejema zahteve) zagotovljene informacije o razlogu za neukrepanje ter o možnosti vložitve pritožbe in uveljavljanja sodnega varstva.

37. Mednarodni sporazum lahko za take pravice določa tudi izjeme. Na primer, lahko bi se zagotovile izjeme za pravici do dostopa in izbrisa, kot jih določata člena 15(4) in 17(3) Splošne uredbe o varstvu podatkov. Podobno bi lahko bile predvidene izjeme za posamezne pravice, če se osebni podatki obdelujejo za namene znanstvenih ali zgodovinskih raziskav, statistične namene ali namene arhiviranja, kolikor bi se izkazalo za verjetno, da bo zaradi takih pravic nemogoče ali zelo težko doseči te posebne namene, in pod pogojem, da so sprejeti ustrezni zaščitni ukrepi (na primer tehnični in organizacijski ukrepi, vključno s psevdonimizacijo). Nazadnje, sporazum lahko določa, da lahko stranki zavrneta odločanje o zahtevi, ki je očitno neutemeljena ali pretirana.

2.4.3 Avtomatizirano sprejemanje posameznih odločitev

38. Če je za zadevni sporazum ustrezno, bi morali mednarodni sporazumi kot splošno načelo vsebovati določbo o tem, da javni organ prejemnik ne bo odločal izključno na podlagi avtomatiziranega sprejemanja posameznih odločitev, vključno z oblikovanjem profilov, ki imajo pravne učinke v zvezi z zadevnim posameznikom, na katerega se nanašajo osebni podatki, ali ki podobno vplivajo na tega posameznika, na katerega se nanašajo osebni podatki. Če namen prenosa vključuje možnost, da javni organ prejemnik sprejema odločitve izključno na podlagi avtomatizirane obdelave v smislu člena 22 Splošne uredbe o varstvu podatkov, lahko to poteka samo pod nekaterimi pogoji, ki so določeni v mednarodnem sporazumu, kot je potreba po pridobitvi izrecnega soglasja posameznika, na katerega se nanašajo osebni podatki. Če odločitev ne izpolnjuje takih pogojev, bi moral imeti posameznik, na katerega se nanašajo osebni podatki, pravico, da zanj ne velja. Če mednarodni

sporazum dopušča avtomatizirano sprejemanje posameznih odločitev, bi moral vsekakor določati potrebne zaščitne ukrepe, vključno s pravico do obveščenosti o posebnih razlogih za odločitev in uporabljeni logiki, do popravka netočnih ali nepopolnih informacij ter do izpodbijanja odločitev in človeškega posredovanja.

2.4.4 Pravica do pravnega varstva

39. Zaščitene pravice posameznika, na katerega se nanašajo osebni podatki, morajo biti izvršljive in učinkovite. Zato mora imeti posameznik, na katerega se nanašajo osebni podatki, dostop do pravnega varstva. Različni primeri načinov zagotavljanja mehanizmov pravnega varstva so navedeni spodaj v oddelkih 2.7 in 3.

2.4.5 Omejitve pravic posameznikov, na katere se nanašajo osebni podatki

40. Mednarodni sporazum lahko določa tudi omejitve pravic posameznikov, na katere se nanašajo osebni podatki. Te omejitve bi morale biti skladne z omejitvami, predvidenimi v členu 23 Splošne uredbe o varstvu podatkov. Taka omejitev mora biti v demokratični družbi potreben in sorazmeren ukrep za zaščito pomembnih ciljev javnega interesa, v skladu s tistimi, ki so naštete v členu 23(1) Splošne uredbe o varstvu podatkov, vključno s pravicami in svobodo drugih, nacionalno varnostjo, obrambo ali preprečevanjem, preiskovanjem, odkrivanjem ali pregonom kaznivih dejanj. Določena mora biti z zakonom ali v primeru mednarodnih organizacij z veljavnimi notranjimi pravili oziroma regulativnim okvirom, traja pa le tako dolgo, dokler obstaja razlog za omejitev.

2.5 Omejitve nadaljnjih prenosov in izmenjave podatkov (vključno z razkritjem in vladnim dostopom)

41. Nadaljnji prenosi javnega organa prejemnika ali mednarodne organizacije prejemnice prejemnikom, ki jih sporazum ne zavezuje, bi morali biti praviloma iz mednarodnega sporazuma izrecno izključeni. Glede na predmet urejanja in posebne okoliščine se bo morda strankama zdelo nujno omogočiti nadaljnje prenose. V tem primeru bi moral mednarodni sporazum pod pogojem, da se spoštuje načelo omejitve namena,[20] predvidevati, da lahko taki nadaljnji prenosi potekajo le, če je javni organ, ki izvršuje prenos, dal predhodno in izrecno dovoljenje, tretje osebe prejemnice pa se zavežejo k spoštovanju enakih načel o varstvu podatkov in zaščitnih ukrepov, kot so vključeni v mednarodnem sporazumu. To bi moralo vključevati zavezo za zagotavljanje enakih pravic do varstva podatkov in jamstev posameznikom, na katere se nanašajo osebni podatki, kot so določene v mednarodnem sporazumu, za zagotavljanje, da raven varstva ne bo zmanjšana, če se podatki posredujejo naprej.

42. Praviloma bi morali enaki zaščitni ukrepi, kot veljajo za nadaljnje prenose, veljati za izmenjavo osebnih podatkov znotraj iste države, tj. mednarodni sporazum izključuje to nadaljnjo izmenjavo, izjeme pa bi morale biti na splošno dovoljene le, če je javni organ, ki izvršuje prenos, dal predhodno in izrecno dovoljenje, tretje osebe prejemnice pa se zavežejo k spoštovanju enakih načel o varstvu podatkov in zaščitnih ukrepov, kot so vključeni v mednarodnem sporazumu.

43. Priporočljivo je, da preden se od javnega organa, ki izvršuje prenos, zahteva izrecno dovoljenje, javni organ prejemnik ali mednarodna organizacija prejemnica zagotovita zadostne informacije o vrsti osebnih podatkov, ki jih nameravata prenesti/izmenjati, razlogih in namenih, zaradi katerih štejeta prenos/izmenjavo osebnih podatkov za potreben, v primeru nadaljnjih prenosov pa tudi o državah ali mednarodnih organizacijah, v katere nameravata nadalje prenesti osebne podatke, da bi bilo mogoče

[20] Glej zgoraj pod 2.3.1.

oceniti zakonodajo tretje države ali veljavna notranja pravila oziroma veljavni regulativni okvir mednarodne organizacije.

44. V primerih, v katerih je treba dovoliti izmenjavo osebnih podatkov s tretjo osebo v isti državi javnega organa prejemnika ali drugo mednarodno organizacijo, bi bilo izmenjavo mogoče dovoliti v posebnih okoliščinah bodisi s predhodnim in izrecnim dovoljenjem javnega organa, ki izvršuje prenos, ali če je tretja oseba prejemnica zavezana k spoštovanju načel in jamstev, vključenih v mednarodni sporazum.

45. Poleg tega bi lahko mednarodni sporazum določal izjemne okoliščine, v katerih bi lahko potekala nadaljnja izmenjava brez predhodnega dovoljenja ali zgoraj omenjenih zavez v skladu z odstopanji iz člena 49 Splošne uredbe o varstvu podatkov, na primer če bi bila ta posebna izmenjava potrebna za zaščito ključnih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih oseb ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov. Take izjemne okoliščine bi lahko nastale tudi, če je nadaljnja izmenjava potrebna na podlagi zakona stranke prejemnice, kot je to potrebno za neposredno povezane preiskave oziroma sodne postopke.

46. V primerih, omenjenih v zgornjem odstavku, bi moral mednarodni sporazum jasno določati posebne in izjemne okoliščine, v katerih je taka izmenjava podatkov dovoljena. Javni organ prejemnik ali mednarodna organizacija prejemnica bi morala tudi imeti obveznost pred izmenjavo obvestiti javni organ, ki izvršuje prenos, ter vključiti informacije o izmenjanih podatkih, tretji osebi prejemnici in pravni podlagi za izmenjavo. Javni organ, ki izvršuje prenos, bi moral voditi evidenco takih obvestil javnega organa prejemnika ali mednarodne organizacije prejemnice in te informacije zagotoviti svojemu nadzornemu organu na zahtevo. Če bi zagotavljanje takega obvestila pred izmenjavo posegalo v obveznosti glede zaupnosti, določene z zakonom, na primer za ohranjanje zaupnosti preiskave, bi bilo treba posebne informacije zagotoviti čim prej po izmenjavi. V takem primeru bi bilo treba splošne informacije o vrsti zahtev, prejetih v posameznem obdobju, vključno z informacijami o vrstah zahtevanih podatkov, organu, ki jih zahteva, in pravni podlagi za razkritje, redno zagotavljati organu, ki izvršuje prenos.

47. V vseh zgoraj opisanih scenarijih bi moral mednarodni sporazum omogočati le razkritja osebnih podatkov drugim javnim organom v tretji državi javnega organa prejemnika, ki ne presegajo tistega, kar je v demokratični družbi potrebno in sorazmerno za zaščito pomembnih ciljev javnega interesa v skladu s tistimi, ki so našteti v členu 23(1) Splošne uredbe o varstvu podatkov, in s sodno prakso Sodišča EU. Za presojo morebitnega dostopa javnih organov tretjih držav za namene nadzora bi moral javni organ, ki izvršuje prenos, upoštevati elemente, na katere opozarjajo štiri evropska temeljna jamstva.[21] Ta vključujejo razpoložljivost učinkovitega pravnega sredstva posameznikom, na katere se nanašajo osebni podatki, v tretji državi javnega organa prejemnika, če do njihovih osebnih podatkov dostopajo javni organi.[22] V primerih prenosov mednarodnim organizacijam mora biti vsak tak dostop skladen z mednarodnim pravom ter zlasti brez poseganja v privilegije in imunitete mednarodne organizacije.

48. Odvisno od primera je morda koristno zahtevati vključitev priloge k mednarodnemu sporazumu, v kateri so našteti zakoni, ki urejajo nadaljnjo izmenjavo z drugimi javnimi organi, vključno za namene nadzora v namembni državi. Vse spremembe te priloge bi bilo treba v določenem roku sporočiti stranki, ki izvršuje prenos.

2.6 Občutljivi podatki

[21] Glej Priporočila Evropskega odbora za varstvo podatkov 02/2020 glede evropskih temeljnih jamstev za nadzorne ukrepe.
[22] Glej Priporočila Evropskega odbora za varstvo podatkov 02/2020, jamstvo D, str. 13 in naslednje.

49. Če mednarodni sporazum določa prenos občutljivih osebnih podatkov v smislu člena 9(1) Splošne uredbe o varstvu podatkov, bi bilo treba vključiti dodatne zaščitne ukrepe, ki jih mora izvajati javni organ prejemnik ali mednarodna organizacija prejemnica, ki obravnavajo posebna tveganja. Ti bi lahko na primer vključevali omejitve, kot so omejitve dostopa, omejitve namenov, za katere se lahko obdelujejo informacije, omejitve glede nadaljnjih prenosov itd., ali posebne zaščitne ukrepe, na primer dodatne varnostne ukrepe, ki zahtevajo posebno usposabljanje osebja, ki lahko dostopa do informacij.

2.7 Mehanizmi pravnega varstva

50. Za zagotavljanje izvršljivih in učinkovitih pravic posameznikov, na katere se nanašajo osebni podatki, mora mednarodni sporazum zagotavljati sistem, ki posameznikom, na katere se nanašajo osebni podatki, omogoča, da še naprej uporabljajo mehanizme pravnega varstva po tem, ko so bili njihovi podatki preneseni v državo zunaj EGP ali mednarodno organizacijo. Ti mehanizmi pravnega varstva morajo zagotavljati pritožbeni mehanizem za posameznike, na katere vpliva neskladnost z določbami izbranega instrumenta, in torej možnost, da posamezniki, na katere se nanašajo osebni podatki in katerih osebni podatki so bili preneseni iz EGP, vložijo pritožbo v zvezi s tako neskladnostjo in da se njihove pritožbe rešijo. Natančneje, posamezniku, na katerega se nanašajo osebni podatki, je treba zagotoviti učinkovit pritožbeni postopek pri javnih organih, ki so stranke mednarodnega sporazuma, in (bodisi neposredno ali po pritožbi pri ustrezni stranki) dostop do neodvisnega nadzornega mehanizma. Poleg tega bi moralo biti načeloma na voljo sodno varstvo.

51. Prvič, javni organ prejemnik bi se moral zavezati k sprejetju mehanizma za učinkovito in pravočasno obravnavanje in reševanje pritožb posameznikov, na katere se nanašajo osebni podatki, glede skladnosti z dogovorjenimi zaščitnimi ukrepi za varstvo podatkov. Poleg tega bi bilo treba posameznikom, na katere se nanašajo osebni podatki, zagotoviti možnost do učinkovitega upravnega sredstva pri neodvisnem nadzornem organu in, če je na voljo, tudi pri neodvisnem organu za varstvo podatkov.[23]

52. Drugič, sporazum bi moral omogočati sodno varstvo, vključno z odškodnino za materialno in nematerialno škodo, nastalo zaradi nezakonite obdelave osebnih podatkov. Če učinkovitega sodnega varstva ni mogoče zagotoviti, na primer zaradi omejitev v notranjem pravu ali posebnega statusa javnega organa prejemnika, na primer mednarodnih organizacij, mora mednarodni sporazum zagotavljati alternativne zaščitne ukrepe. Ti zaščitni ukrepi morajo posamezniku, na katerega se nanašajo osebni podatki, zagotavljati jamstva, ki so v bistvu enakovredna jamstvom, ki jih zahteva člen 47 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina EU).[24]

53. V tem primeru bi lahko mednarodni sporazum vzpostavil strukturo, ki posamezniku, na katerega se nanašajo osebni podatki, omogoča uveljavljanje njegovih pravic zunaj sodišč, na primer z zavezujočimi mehanizmi, ki so podobni sodnim, kot so arbitraža ali mehanizmi alternativnega reševanja sporov, kot je mediacija, ki bi zagotavljali neodvisen pregled in obvezovali javni organ prejemnik.[25] Poleg tega bi se lahko javni organ, ki prenaša osebne podatke, zavezal k prevzemu odgovornosti za izplačilo odškodnine za škodo, nastalo zaradi nezakonite obdelave osebnih podatkov, ki se dokaže z neodvisnim pregledom.

[23] Glej tudi oddelek 2.8 o nadzornem mehanizmu.
[24] Sodišče EU, sodba z dne 16. julija 2020 v zadevi C-311/18, *Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu (Schrems II)*, točke 96, 186 in naslednje.
[25] Sodišče EU, sodba z dne 6. oktobra 2015 v zadevi C-362/14, *Maximillian Schrems proti Data Protection Commissioner (Schrems)*, točki 41 in 95; Sodišče EU, sodba z dne 16. julija 2020 v zadevi C-311/18, *Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu (Schrems II)*, točke 186, 187, 189, 195 in naslednje.

Izjemoma se lahko s sporazumom sprejmejo drugi, enako neodvisni in učinkoviti mehanizmi pravnega varstva, na primer učinkoviti mehanizmi pravnega varstva, ki jih izvajajo mednarodne organizacije.

54. Za vse zgoraj omenjene mehanizme pravnega varstva bi moral mednarodni sporazum vsebovati obveznost strank, da druga drugo obveščajo o izidu postopka, zlasti če je pritožba posameznika zavrnjena ali ni rešena.

55. Mehanizem pravnega varstva mora biti združen z možnostjo javnega organa, ki izvršuje prenos, da začasno ali dokončno prekine prenos osebnih podatkov na podlagi mednarodnega sporazuma, če stranki spora ne uspeta rešiti sporazumno, dokler ne meni, da je javni organ prejemnik zadevo zadovoljivo uredil. Če pride do take začasne ali dokončne prekinitve, jo mora spremljati zaveza javnega organa prejemnika, da bo osebne podatke vrnil ali izbrisal. Javni organ, ki izvršuje prenos, mora o začasni ali dokončni prekinitvi obvestiti pristojni nacionalni nadzorni organ.

2.8 Nadzorni mehanizmi

56. Za zagotavljanje izpolnitve vseh obveznosti, določenih na podlagi mednarodnega sporazuma, mora ta zagotavljati spremljanje pravilne uporabe sporazuma in poseganja v pravice, ki jih zagotavlja sporazum, s strani neodvisnega nadzornega organa.

57. Prvič, sporazum bi moral zagotavljati notranji nadzor za zagotavljanje skladnosti s sporazumom. Vsaka stranka sporazuma bi morala izvajati redne notranje kontrole vzpostavljenih postopkov in učinkovite uporabe zaščitnih ukrepov, določenih v sporazumu. Pri rednih notranjih kontrolah bi bilo treba preverjati tudi morebitne spremembe zakonodaje, ki bi stranki(-am) preprečevale spoštovanje načel o varstvu podatkov in zaščitnih ukrepov, vključenih v mednarodnem sporazumu. Poleg tega bi lahko bilo določeno, da lahko stranka sporazuma od druge stranke sporazuma zahteva izvedbo takega pregleda. Mednarodni sporazum mora vsebovati zahtevo, da se morata stranki odzvati na poizvedbe druge stranke glede učinkovitega izvajanja zaščitnih ukrepov iz sporazuma. Vsaka stranka, ki izvaja pregled, bi morala rezultate kontrol sporočiti drugi(-m) stranki(-am) sporazuma. Načeloma bi se tako sporočilo moralo poslati tudi neodvisnemu nadzornemu mehanizmu za sporazum.

58. Poleg tega mora mednarodni sporazum vsebovati obveznost, da stranka drugo stranko brez nepotrebnega odlašanja obvesti o svoji nezmožnosti učinkovitega izvajanja zaščitnih ukrepov iz sporazuma iz katerega koli razloga. Za tak primer mora mednarodni sporazum predvidevati možnost, da javni organ, ki izvršuje prenos, začasno ali dokončno prekine prenos osebnih podatkov na podlagi mednarodnega sporazuma javnemu organu prejemniku, dokler javni organ prejemnik javnega organa, ki izvršuje prenos, ne obvesti, da lahko spet deluje v skladu z zaščitnimi ukrepi. Organ, ki izvršuje prenos, mora pristojni nadzorni organ obvestiti o spremembi položaja, pa tudi o začasni prekinitvi prenosov ali odpovedi sporazuma.

59. Drugič, v sporazumu mora biti določen neodvisen nadzor, s katerim se zagotavlja, da stranki spoštujeta določbe iz sporazuma. To izhaja neposredno iz Listine EU[26] in Evropske konvencije o človekovih pravicah (EKČP)[27] v skladu s sodno prakso Evropskega sodišča za človekove pravice (ESČP) ter pogojev, določenih v primarnem pravu,[28] in tudi ustrezne sodne prakse.

60. Sodišče EU od leta 2015[29] vedno znova poudarja potrebo po neodvisnem pravnem varstvu in nadzornem mehanizmu.[30] Podobno je ESČP v svojih sodbah že večkrat poudarilo, da se mora za vsak

[26] Členi 7, 8 in 47 Listine EU.
[27] Člen 8 EKČP.
[28] Člen 6 Lizbonske pogodbe:
„1. Unija priznava pravice, svoboščine in načela iz Listine Evropske unije o temeljnih pravicah z dne 7. decembra 2000, prilagojene 12. decembra 2007 v Strasbourgu, ki ima enako pravno veljavnost kot Pogodbi. Z določbami Listine se na nikakršen način ne širijo pristojnosti Unije, opredeljene v Pogodbah.
Pravice, svoboščine in načela Listine se razlagajo v skladu s splošnimi določbami naslova VII Listine o njeni razlagi in uporabi ter ob ustreznem upoštevanju pojasnil iz Listine, ki navajajo vire teh določb.
2. Unija pristopi k Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin. Ta pristop ne spreminja pristojnosti Unije, opredeljene v Pogodbah.
3. Temeljne pravice, kakor jih zagotavlja Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin in kakor izhajajo iz ustavnega izročila, skupnega državam članicam, so kot splošna načela del prava Unije.“
[29] Sodišče EU, sodba z dne 6. oktobra 2015 v zadevi C-362/14, *Maximillian Schrems proti Data Protection Commissioner (Schrems)*, točki 41 in 95.
[30] Sodišče EU, 27. julij 2017, mnenje 1/15 z dne 26. julija 2017 o predvidenem sporazumu med Evropsko unijo in Kanado o prenosu podatkov iz evidence podatkov o potnikih, točka 228 in naslednje; Sodišče EU, mnenje 1/17 z dne 30. aprila 2019 o Celovitem gospodarskem in trgovinskem sporazumu med Kanado in Evropsko unijo, točka 190 in naslednje.

poseg v pravico do spoštovanja zasebnega življenja iz člena 8 EKČP uporabljati učinkovit, neodvisen in nepristranski nadzorni sistem.[31]

61. Sporazum bi se lahko na primer skliceval na nadzor s strani pristojnega nadzornega organa, če ta obstaja v državi javnega organa, ki prejema osebne podatke iz EGP, čeprav Splošna uredba o varstvu podatkov specifično ne določa, da mora biti pristojni nadzorni organ zunanje nadzorno telo. Poleg tega bi lahko sporazum vključeval prostovoljno zavezo stranke prejemnice k sodelovanju z nadzornimi organi iz EGP.

62. Če ne obstaja nadzorni organ, ki je posebej odgovoren za nadzorovanje izvajanja zakona o varstvu podatkov v tretji državi ali mednarodni organizaciji, mora biti potreba po neodvisnem, učinkovitem in nepristranskem nadzornem mehanizmu izpolnjena drugače. Vrsta vzpostavljenega neodvisnega nadzornega mehanizma je lahko odvisna od konkretnega primera.

63. Sporazum bi lahko na primer napotoval na obstoječe nadzorne organe v tretji državi, ki niso nadzorni organ na področju varstva podatkov. Poleg tega bi se lahko, če zunanjega neodvisnega nadzora s strukturnega ali institucionalnega vidika ni mogoče zagotoviti zaradi na primer privilegijev in imunitet nekaterih mednarodnih organizacij, nadzor zagotavljal s samostojno delujočimi mehanizmi. Slednji morajo biti organi, ki čeprav niso zunanji, izvajajo svoje naloge neodvisno, tj. brez navodil, z zadostnimi človeškimi, tehničnimi in finančnimi viri itd. Odločitve nadzornega organa so za stranko prejemnico zavezujoče.

2.9 Klavzula o odpovedi

64. Mednarodni sporazum bi moral predvidevati, da se vsi osebni podatki, ki so bili iz EGP preneseni v skladu z mednarodnim sporazumom pred njegovo dejansko odpovedjo, še naprej obdelujejo v skladu z določbami mednarodnega sporazuma.

[31] ESČP, 6. september 1978, *Klass in drugi proti Nemčiji*, točki 55 in 56. Zahteva ESČP se od takrat uporablja tudi za vsak poseg v člena 7 in 8 Listine EU, saj sta v skladu s členom 52(3) Listine EU pomen in področje uporabe teh temeljnih pravic enaka tistima iz člena 8 EKČP.

3 POSEBNE INFORMACIJE O ČLENU 46 SPLOŠNE UREDBE O VARSTVU PODATKOV

3.1 Posebne informacije o pravno zavezujočih in izvršljivih instrumentih – člen 46(2)(a) Splošne uredbe o varstvu podatkov

65. Člen 46(2)(a) Splošne uredbe o varstvu podatkov javnim organom v EGP omogoča, da prenose javnim organom v tretji državi ali mednarodni organizaciji oprejo na instrumente, sklenjene med njimi, brez pridobitve predhodnega dovoljenja nadzornega organa. Taki instrumenti morajo biti pravno zavezujoči in izvršljivi. Zato se lahko na podlagi te določbe uporabljajo mednarodne pogodbe, pogodbe javnega prava ali samoizvršujoči upravni sporazumi.

66. Vsak pravno zavezujoč in izvršljiv instrument bi moral vsebovati temeljni sklop načel o varstvu podatkov in pravic posameznika, na katerega se nanašajo osebni podatki, kot to zahteva Splošna uredba o varstvu podatkov.

67. Stranki se morata za prenos podatkov zavezati k sprejetju zadostnih zaščitnih ukrepov za varstvo podatkov. Posledično bi moral sporazum določati tudi način, kako bo javni organ prejemnik uporabljal temeljni sklop osnovnih načel o varstvu podatkov in pravic posameznika, na katerega se nanašajo osebni podatki, za vse prenesene osebne podatke za zagotovitev, da ni ogrožena raven varstva posameznikov v skladu s Splošno uredbo o varstvu podatkov.

68. Če v pravno zavezujočih in izvršljivih instrumentih ni mogoče zagotoviti učinkovitega sodnega varstva in se je zato treba dogovoriti o alternativnem mehanizmu pravnega varstva, bi se morali javni organi v EGP pred sklenitvijo teh instrumentov posvetovati s pristojnim nadzornim organom.

69. Čeprav oblika instrumenta ni odločilna, dokler je ta pravno zavezujoč in izvršljiv, Evropski odbor za varstvo podatkov meni, da bi bilo najbolje podrobne določbe o varstvu podatkov vključiti neposredno v instrument. Če ta rešitev zaradi posebnih okoliščin ni izvedljiva, pa Evropski odbor za varstvo podatkov močno priporoča, da se neposredno v besedilo instrumenta vključi vsaj splošna določba, ki opredeljuje načela o varstvu podatkov, podrobnejše določbe in zaščitni ukrepi pa se vstavijo v prilogo k instrumentu.

3.2 Posebne informacije o upravnih dogovorih – člen 46(3)(b) Splošne uredbe o varstvu podatkov

70. Splošna uredba o varstvu podatkov v členu 46(3)(b) določa tudi alternativne instrumente v obliki upravnih dogovorov, na primer memorandumov o soglasju, ki zagotavljajo varstvo z zavezami, ki jih sprejmeta obe stranki za uveljavitev njunega skupnega dogovora.

71. Glede tega člen 46(1) in uvodna izjava 108 Splošne uredbe o varstvu podatkov določata, da morajo ti dogovori zagotavljati izvršljive pravice posameznika, na katerega se nanašajo osebni podatki, in učinkovita pravna sredstva. Če so v upravnih dogovorih predvideni zaščitni ukrepi, ki niso pravno zavezujoči, je treba pridobiti dovoljenje pristojnega nadzornega organa.

72. Glede na obravnavani namen obdelave in naravo podatkov bi bilo treba skrbno oceniti uporabo ali neuporabo pravno nezavezujočih upravnih dogovorov za zagotavljanje zaščitnih ukrepov v javnem sektorju. Če notranje pravo tretje države ali notranja pravila oziroma regulativni okvir mednarodne organizacije posameznikom iz EGP ne zagotavljajo pravic glede varstva podatkov in pravnega varstva, bi bilo treba dati prednost sklenitvi pravno zavezujočega dogovora. Ne glede na vrsto sprejetega

instrumenta morajo biti veljavni ukrepi učinkoviti pri zagotavljanju ustreznega izvajanja, izvrševanja in nadzora.

73. V upravnih dogovorih je treba sprejeti posebne ukrepe za zagotavljanje učinkovitih pravic posameznikov, pravnega varstva in nadzora. Natančneje, za zagotavljanje učinkovitih in izvršljivih pravic bi moral nezavezujoč instrument vsebovati zagotovila javnega organa, ki prejema osebne podatke iz EGP, da so pravice posameznikov v celoti zagotovljene z notranjim pravom ter jih lahko posamezniki iz EGP uveljavljajo pod enakimi pogoji kot državljani in prebivalci zadevne tretje države. Enako velja, če je posameznikom iz EGP na voljo upravno in sodno varstvo v okviru notranjega prava javnega organa prejemnika. Podobno bi morale mednarodne organizacije zagotoviti jamstva o pravicah posameznikov, ki jih zagotavljajo njihova notranja pravila, in tudi razpoložljivih mehanizmih pravnega varstva.

74. V nasprotnem primeru bi morale biti pravice posameznikov zajamčene s posebnimi zavezami strank, ki bi jih morali spremljati postopkovni mehanizmi za zagotavljanje njihove učinkovitosti in pravnega varstva posamezniku. Te posebne zaveze in postopkovni mehanizmi morajo v praksi omogočati zagotavljanje skladnosti z ravnjo varstva, ki je v bistvu enakovredna tisti, ki jo v EU zagotavlja Splošna uredba o varstvu podatkov.
Taki postopkovni mehanizmi lahko na primer vključujejo zaveze strank k medsebojnemu obveščanju o zahtevah posameznikov iz EGP in k pravočasnemu reševanju sporov ali zahtevkov.

75. Poleg tega je treba v primerih, kadar takih sporov ali zahtevkov stranki sami ne moreta rešiti sporazumno, posamezniku zagotoviti neodvisno in učinkovito pravno varstvo z alternativnimi mehanizmi, na primer tako, da ima posameznik na voljo mehanizem za alternativno reševanje sporov, kot sta arbitraža ali mediacija. Tak mehanizem za alternativno reševanje sporov mora biti zavezujoč.[32]

76. Odvisno od primera bi bilo treba za zagotavljanje učinkovitega pravnega varstva v upravnem dogovoru določiti kombinacijo vseh ali nekaterih zgoraj navedenih ukrepov. Sprejemljivi bi bili lahko tudi drugi ukrepi, ki jih te smernice ne vključujejo, če zagotavljajo neodvisno in učinkovito pravno varstvo.

77. Vsak upravni dogovor, pripravljen v skladu s členom 46(3)(b) Splošne uredbe o varstvu podatkov, bo pristojni nadzorni organ preučil za vsak primer posebej, temu pa bo po potrebi sledil ustrezen postopek Evropskega odbora za varstvo podatkov. Pristojni nadzorni organ bo svoj pregled oprl na splošna priporočila, določena v teh smernicah, vendar lahko glede na zadevni primer zahteva tudi dodatna jamstva.

[32] Sodišče EU, sodba z dne 16. julija 2020 v zadevi C-311/18, *Data Protection Commissioner proti Facebook Ireland Ltd in Maximillianu Schremsu (Schrems II)*, točke 189, 196 in naslednje.

4 POSTOPKOVNA VPRAŠANJA

78. Upravni dogovori, sklenjeni na podlagi člena 46(3)(b) Splošne uredbe o varstvu podatkov, se bodo preučevali za vsak primer posebej zaradi zahtev za dovoljenje pristojnega nadzornega organa, ki v skladu s členom 46(4) Splošne uredbe o varstvu podatkov uporablja mehanizem za skladnost iz njenega člena 64(2). Pri vključevanju alternativnih mehanizmov pravnega varstva v zavezujoče in izvršljive instrumente v skladu s členom 46(2)(a) Splošne uredbe o varstvu podatkov Evropskemu odboru za varstvo podatkov priporoča tudi posvetovanje s pristojnim nadzornim organom. Evropski odbor za varstvo podatkov posvetovanje s pristojnim nadzornim organom močno priporoča v zgodnji fazi.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)