



18/SL

WP 254 rev. 01

Delovna skupina iz člena 29

Referenčni dokument o ustreznosti

Sprejet 28. novembra 2017

Kot je bil nazadnje revidiran in sprejet 6. februarja 2018

Ta delovna skupina je bila ustanovljena v skladu s členom 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Naloge skupine so opredeljene v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES.

Naloge sekretariata opravlja Direktorat C (Temeljne pravice in državljanstvo Unije) Evropske komisije, Generalni direktorat za pravosodje, B-1049 Bruselj, Belgija, pisarna št. MO-59 02/013.

Spletišče: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936.

Uvod

Delovna skupina organov EU za varstvo podatkov ¹ (v nadaljnjem besedilu: Delovna skupina iz člena 29) je predhodno objavila delovni dokument o prenosih osebnih podatkov v tretje države (WP 12)². Po zamenjavi Direktive s Splošno uredbo EU o varstvu podatkov³ Delovna skupina iz člena 29 ponovno proučuje dokument WP 12 oziroma svoje predhodne smernice, da bi ga posodobila na podlagi nove zakonodaje in nedavne sodne prakse Sodišča⁴.

Cilj tega delovnega dokumenta je posodobiti poglavje 1 dokumenta WP 12, ki je povezano z osrednjim vprašanjem ustrezne ravni varstva podatkov v tretji državi, na ozemlju ali v enem ali več določenih sektorjih v tej tretji državi ali v mednarodni organizaciji (v nadaljnjem besedilu: tretje države ali mednarodne organizacije). Ta dokument se bo v prihodnjih letih na podlagi praktičnih izkušenj, pridobljenih z uporabo Splošne uredbe o varstvu podatkov, stalno pregledoval in po potrebi posodabljal. V poznejši fazi bi bilo treba posodobiti poglavje 2 dokumenta WP 12 z naslovom *Applying the approach to countries that have ratified Convention 108* (Uporaba pristopa za države, ki so ratificirale Konvencijo št. 108) in poglavje 3 dokumenta WP 12 z naslovom *Applying the approach to industry self-regulation* (Uporaba pristopa za sektorsko samourejanje).

Ta delovni dokument se v skladu s členom 45 Splošne uredbe o varstvu podatkov osredotoča samo na sklepe o ustreznosti, ki so izvedbeni akti⁵ Evropske komisije. Drugi vidiki prenosov osebnih podatkov v tretje države in mednarodne organizacije bodo proučeni v nadaljnjih delovnih dokumentih, ki bodo objavljeni ločeno (zavezujoča poslovna pravila, odstopanja).

Cilj tega dokumenta je v skladu s Splošno uredbo o varstvu podatkov zagotoviti smernice za Evropsko komisijo in Delovno skupino iz člena 29 za oceno ravni varstva podatkov v tretjih državah in mednarodnih organizacijah z oblikovanjem ključnih načel 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. Poleg tega lahko zagotovi smernice za tretje države in mednarodne organizacije, ki želijo zagotoviti ustreznost. Vendar načela v tem delovnem dokumentu niso namenjena neposredno upravljavcem ali obdelovalcem podatkov.

Ta dokument je sestavljen iz štirih poglavij:

poglavje 1: Nekaterne splošne informacije v zvezi s pojmom ustreznosti;

poglavje 2: Postopkovni vidiki za ugotovitve o ustreznosti v skladu s Splošno uredbo o varstvu podatkov;

poglavje 3: Splošna načela varstva podatkov. V tem poglavju so zajeta ključna splošna načela varstva podatkov, s katerimi se zagotovi, da je raven varstva podatkov v tretji državi ali mednarodni organizaciji v bistvenem enaka ravni, ki je zagotovljena z zakonodajo EU;

poglavje 4: Bistvena jamstva, ki se uporabljajo za dostop za namene kazenskega pregona in nacionalne varnosti, da se omejijo posegi v temeljne pravice. To poglavje vključuje bistvena jamstva v zvezi z dostopom za namene kazenskega pregona in nacionalne varnosti po sodbi Sodišča v zadevi Schrems iz leta 2015 in temelji na delovnem dokumentu o bistvenih jamstvih, ki ga je Delovna skupina iz člena 29 sprejela leta 2016.

¹Kot je določeno v členu 29 Direktive 95/46/ES o varstvu podatkov.

² Delovni dokument WP 12 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), ki ga je Delovna skupina sprejela 24. julija 1998.

³ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Besedilo velja za EGP).

⁴ Vključno s sodbno Sodišča z dne 6. oktobra 2015 v zadevi Maximilian Schrems proti Data Protection Commissioner (C-362/14).

⁵ Za več informacij o izvedbenih aktih glej zadevna člena 45(3) in 93(2) Splošne uredbe o varstvu podatkov.

Poglavje 1: Nekatere splošne informacije v zvezi s pojmom ustreznosti

V členu 45(1) Splošne uredbe o varstvu podatkov je določeno načelo, da se lahko prenosi podatkov v tretjo državo ali mednarodno organizacijo izvedejo samo, če zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavlja ustrežno raven varstva podatkov.

Ta pojem „ustrezne ravni varstva podatkov“, ki je že obstajal v okviru Direktive 95/46/ES, je Sodišče nadalje razvilo. Pri tem je pomembno opozoriti na standard, ki ga je določilo Sodišče v zadevi Schrems, in sicer da mora biti „raven varstva“ v tretji državi „v bistvenem enaka“ ravni, zagotovljeni v EU, „četudi so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj [EU]“⁶. Cilj torej ni v celoti prenesti vseh točk evropske zakonodaje, ampak oblikovati bistvene oziroma ključne zahteve te zakonodaje.

Namen sklepov o ustreznosti Evropske komisije je uradna potrditev z zavezujočim učinkom za države članice⁷, da je raven varstva podatkov v tretji državi ali mednarodni organizaciji v bistvenem enaka ravni varstva podatkov, zagotovljeni v Evropski uniji⁸. 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 samo vsebino predpisov, ki se uporabljajo za osebne podatke, prenesene v tretjo državo ali mednarodno organizacijo, ampak je treba proučiti tudi sistem, ki je vzpostavljen za zagotavljanje učinkovitosti takih predpisov. Učinkoviti mehanizmi izvrševanja so ključnega pomena za učinkovitost predpisov o varstvu podatkov.

V členu 45(2) Splošne uredbe o varstvu podatkov so določeni elementi, ki jih Evropska komisija upošteva pri ocenjevanju ustreznosti ravni varstva v tretji državi ali mednarodni organizaciji.

Komisija na primer upošteva načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno zakonodajo, obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov ter mednarodne zaveze, ki jih je sprejela zadevna tretja država ali mednarodna organizacija.

Zato je jasno, da mora vsaka smiselna analiza ustreznega varstva zajeti dva osnovna elementa: vsebino veljavnih predpisov in sredstva za zagotavljanje njihove učinkovite uporabe. Evropska komisija mora redno preverjati, ali so vzpostavljeni predpisi v praksi učinkoviti.

Jedro vsebinskih načel varstva podatkov in postopkovnih zahtev/zahtev glede izvrševanja, ki se lahko štejejo za minimalno zahtevo za ustreznost varstva, izhaja iz Listine EU o temeljnih pravicah in Splošne uredbe o varstvu podatkov. Poleg tega bi bilo treba upoštevati tudi druge mednarodne sporazume o varstvu podatkov, na primer Konvencijo št. 108⁹.

Pozornost je treba nameniti pravnemu okviru za dostop javnih organov do osebnih podatkov. Nadaljnje smernice o tem so na voljo v delovnem dokumentu št. 237 (tj. dokumentu o bistvenih jamstvih)¹⁰ o zaščitnih ukrepih v okviru nadzora.

Splošne določbe o varstvu podatkov in zasebnosti v tretji državi niso dovolj. Nasprotno je treba v pravni okvir tretje države ali mednarodne organizacije vključiti specifične določbe, ki obravnavajo konkretne potrebe v zvezi s praktičnimi vidiki pravice do varstva podatkov. Te določbe morajo biti izvršljive.

⁶ Sodba Sodišča z dne 6. oktobra 2015 v zadevi Maximillian Schrems proti Data Protection Commissioner (C-362/14) (točki 73 in 74).

⁷ Člen 288(2) PDEU.

⁸ Sodba Sodišča z dne 6. oktobra 2015 v zadevi Maximillian Schrems proti Data Protection Commissioner (C-362/14) (točka 52).

⁹ Uvodna izjava 105 Splošne uredbe o varstvu podatkov.

¹⁰ Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (Delovni dokument št. 01/2016 o utemeljitvi posegov v temeljne pravice do zasebnosti in varstva podatkov na podlagi nadzornih ukrepov ob prenosu osebnih podatkov (evropska bistvena jamstva)), 16/EN WP 237, z dne 13. aprila 2016.

Poglavje 2: Postopkovni vidiki za ugotovitve o ustreznosti v skladu s Splošno uredbo o varstvu podatkov

Da lahko Evropski odbor za varstvo podatkov izpolni svojo nalogo svetovanja Evropski komisiji v skladu s členom 70(1)(s) Splošne uredbe o varstvu podatkov, mu je treba predložiti ustrezno dokumentacijo, vključno z zadevno korespondenco in ugotovitvami Evropske komisije. V primeru zapletenega pravnega okvira je treba predložiti tudi vsa poročila, pripravljena v zvezi z ravno varstva podatkov v tretji državi ali mednarodni organizaciji. V vsakem primeru morajo biti informacije, ki jih predloži Evropska komisija, izčrpne, pri čemer morajo Evropskemu odboru za varstvo podatkov omogočiti, da oblikuje svojo oceno o ravni varstva podatkov v tretji državi. Evropski odbor za varstvo podatkov bo pravočasno zagotovil mnenje o ugotovitvah Evropske komisije in po potrebi opredelil pomanjkljivosti v okviru ustreznosti. Prizadeval si bo tudi za predlog popravkov ali sprememb, da se odpravijo morebitne pomanjkljivosti.

V skladu s členom 45(4) Splošne uredbe o varstvu podatkov mora Evropska komisija redno spremljati razvoj dogodkov, ki bi lahko vplival na izvajanje sklepa o ustreznosti.

V členu 45(3) Splošne uredbe o varstvu podatkov 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.

Ker je Evropski odbor za varstvo podatkov pooblaščen, 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 v zvezi s pregledom v tretji državi ali mednarodni organizaciji. Evropski odbor za varstvo podatkov želi biti pozvan k sodelovanju v teh postopkih in misijah v zvezi s pregledom.

Opozoriti je treba tudi, da ima Evropska komisija v skladu s členom 45(5) Splošne uredbe o varstvu podatkov pravico, da razveljavi, spremeni ali začasno odloži izvajanje obstoječih sklepov o ustreznosti. Evropski odbor za varstvo podatkov bi zato moral sodelovati v postopku razveljavitve, spremembe ali začasne odložitve, in sicer bi se moralo od njega zahtevati mnenje na podlagi člena 70(1)(s) Splošne uredbe o varstvu podatkov.

Poleg tega bi morali organi za varstvo podatkov, kot je zdaj priznано v členu 58(5) Splošne uredbe o varstvu podatkov in v skladu s sodbo Sodišča v zadevi Schrems, imeti možnost sodelovati v sodnih postopkih, če ugotovijo, da je zahtevk osebe proti sklepu o ustreznosti utemeljen: „[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“¹¹.

¹¹ Sodba Sodišča z dne 6. oktobra 2015 v zadevi Maximillian Schrems proti Data Protection Commissioner (C-362/14) (točka 65).

Poglavje 3: Splošna načela varstva podatkov za zagotovitev, da je raven varstva podatkov v tretji državi, na ozemlju ali v enem ali več določenih sektorjih v tej tretji državi ali v mednarodni organizaciji v bistvenem enaka ravni, ki je zagotovljena z zakonodajo EU

Sistem tretje države ali mednarodne organizacije mora vsebovati naslednja osnovna vsebinska in postopkovna/izvrševalna načela in mehanizme varstva podatkov:

A. Vsebinska načela:

1) Pojmi

Obstajati bi morali osnovni pojmi in/ali načela varstva podatkov. Ni nujno, da so povsem enaki izrazju Splošne uredbe o varstvu podatkov, vendar morajo odražati pojme, določene v evropski zakonodaji na področju varstva podatkov, in biti skladni z njimi. Splošna uredba o varstvu podatkov na primer vključuje naslednje pomembne pojme: „osebni podatki“, „obdelava osebnih podatkov“, „upravljavec podatkov“, „obdelovalec podatkov“, „uporabnik“ in „občutljivi podatki“.

2) Razlogi za zakonito in pošteno obdelavo za zakonsko utemeljene namene

Obdelava podatkov mora biti zakonita, poštena in zakonsko utemeljena.

Pravna podlaga, v skladu s katero se lahko osebni podatki zakonito, pošteno in zakonsko utemeljeno obdelujejo, bi morala biti dovolj jasno določena. Evropski okvir priznava več takih zakonsko utemeljenih razlogov, med drugim na primer določbe v nacionalni zakonodaji, privolitev posameznika, na katerega se nanašajo osebni podatki, izvajanje pogodbe ali zakoniti interes upravljavca podatkov ali tretje osebe, ki ne prevlada nad interesi posameznika.

3) Načelo omejitve namena

Podatki bi se morali obdelovati za določen namen in se nato uporabljati samo, če to ni nezdržljivo z namenom obdelave.

4) Načeli kakovosti podatkov in sorazmernosti

Podatki bi morali biti točni in po potrebi posodobljeni. Morali bi biti ustrezni in relevantni ter ne bi smeli presegati tega, kar je potrebno za name, za katere se obdelujejo.

5) Načelo hrambe podatkov

Osebni podatki se praviloma ne bi smeli hraniti dlje, kot je potrebno za namene, za katere se obdelujejo.

6) Načelo varnosti in zaupnosti

Vsak subjekt, ki obdeluje osebne podatke, bi moral zagotoviti, da se podatki obdelujejo na način, ki zagotavlja varnost osebnih podatkov, vključno z zaščito z ustreznimi tehničnimi ali organizacijskimi ukrepi pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo. Pri ravni varnosti bi bilo treba upoštevati najnovejši tehnološki razvoj in povezane stroške.

7) Načelo preglednosti

Vsak posameznik bi moral biti obveščen o vseh glavnih elementih obdelave njegovih osebnih podatkov na jasn, lahko dostopen, jedrnat, pregleden in razumljiv način. Te informacije bi morale zajemati namen obdelave, identiteta upravljavca podatkov, njegove pravice in druge informacije, če je to potrebno za zagotovitev poštenosti. V zvezi s to pravico do obveščenosti obstajajo pod določenimi pogoji nekatere izjeme, na primer za zaščito kazenskih preiskav, nacionalne varnosti, neodvisnosti sodstva in sodnih postopkov ali drugih pomembnih ciljev v splošnem javnem interesu, kot je določeno v členu 23 Splošne uredbe o varstvu podatkov.

8) Pravica do dostopa, popravka, izbrisa ali ugovora

Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti pravico do pridobitve potrdila o tem, ali se podatki, ki se nanašajo nanj, obdelujejo ali ne, in dostopa do svojih podatkov, vključno s pridobitvijo kopije vseh podatkov, ki se nanašajo nanj in se obdelujejo.

Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti pravico do ustreznega popravka svojih podatkov na podlagi utemeljenega razloga, na primer kadar so netočni ali nepopolni, in do izbrisa svojih osebnih podatkov, na primer kadar obdelava teh podatkov ni več potrebna ali zakonita.

Posameznik, na katerega se nanašajo osebni podatki, bi moral imeti tudi pravico do tega, da na podlagi nujnih legitimnih razlogov, povezanih z njegovim posebnim položajem, kadar koli ugovarja obdelavi svojih podatkov v skladu s posebnimi pogoji, določenimi v pravnem okviru tretje države. V Splošni uredbi o varstvu podatkov taki pogoji na primer vključujejo primere, v katerih je obdelava potrebna za opravljanje naloge, ki se izvaja v javnem interesu, za izvajanje javne oblasti, dodeljene upravljavcu, ali zaradi zakonitih interesov, za katere si prizadeva upravljavec podatkov ali tretja oseba.

Uveljavljanje navedenih pravic za posameznika, na katerega se nanašajo osebni podatki, ne bi smelo biti preveč zapleteno. Obstajajo lahko morebitne omejitve navedenih pravic, na primer za zaščito kazenskih preiskav, nacionalne varnosti, neodvisnosti sodstva in sodnih postopkov ali drugih pomembnih ciljev v splošnem javnem interesu, kot je določeno v členu 23 Splošne uredbe o varstvu podatkov.

9) Omejitve nadaljnjih prenosov podatkov

Prvemu uporabniku prvotnega prenosa osebnih podatkov bi moralo biti dovoljeno nadalje prenesti osebne podatke samo, če tudi za nadaljnjega uporabnika (tj. uporabnika nadaljnjega prenosa podatkov) veljajo predpisi (vključno s pogodbenimi določbami), ki zagotavljajo ustrezno raven varstva in upoštevajo zadevna navodila za obdelavo podatkov v imenu upravljavca podatkov. Nadaljnji prenos ne sme ogroziti ravni varstva fizičnih oseb, na katere se nanašajo podatki, ki se prenašajo. Prvotni uporabnik podatkov, prenesenih iz EU, mora zagotoviti ustrezne zaščitne ukrepe za nadaljnje prenose podatkov, če ne obstaja sklep o ustreznosti. Taki nadaljnji prenosi podatkov bi se lahko izvajali samo, če obstajajo omejeni in posebni nameni ter pravna podlaga za to obdelavo.

B. Primeri dodatnih vsebinskih načel, ki se uporabljajo za posebne vrste obdelave:

1) Posebne vrste podatkov

Za posebne vrste podatkov bi morali obstajati posebni zaščitni ukrepi¹². Posebne vrste podatkov bi morale odražati te, ki so določene v členih 9 in 10 Splošne uredbe o varstvu podatkov. Ti zaščitni ukrepi bi se morali vzpostaviti s strožjimi zahtevami za obdelavo podatkov, na primer z izrecno privolitvijo posameznika, na katerega se nanašajo osebni podatki, v obdelavo ali dodatnimi varnostnimi ukrepi.

¹² Take posebne vrste podatkov se v uvodni izjavi 10 Splošne uredbe o varstvu podatkov imenujejo tudi „občutljivi podatki“.

2) Neposredno trženje

Kadar se podatki obdelujejo za namene neposrednega trženja, mora imeti posameznik, na katerega se nanašajo osebni podatki, možnost, da kadar koli brezplačno ugovarja obdelavi svojih osebnih podatkov za take namene.

3) Avtomatizirano sprejemanje odločitev in oblikovanje profilov

Odločitve, ki temeljijo samo na avtomatizirani obdelavi (avtomatizirano sprejemanje posameznih odločitev), vključno z oblikovanjem profilov, ki ima pravne učinke na posameznika, na katerega se nanašajo osebni podatki, ali nanj znatno vpliva, se lahko sprejemajo samo pod nekaterimi pogoji, določenimi v pravnem okviru tretje države. V evropskem okviru taki pogoji na primer vključujejo potrebo po pridobitvi izrecnega dovoljenja posameznika, na katerega se nanašajo osebni podatki, ali potrebo po taki odločitvi za sklenitev pogodbe. Če odločitev ni v skladu s pogoji, ki so določeni v pravnem okviru tretje države, bi moral imeti posameznik, na katerega se nanašajo osebni podatki, pravico, da ta odločitev zanj ne velja. V vsakem primeru bi morali biti z zakonodajo tretje države zagotovljeni potrebni zaščitni ukrepi, vključno s pravico do obveščenosti o posebnih razlogih za odločitev in s tem povezani logiki, do popravka netočnih ali nepopolnih podatkov in do izpodbijanja odločitve, če je bila sprejeta na podlagi napačnih dejstev.

C. Postopkovni in izvrševalni mehanizmi:

Čeprav so sredstva, ki jih tretja država uporabi za zagotovitev ustrezne ravni varstva, lahko drugačna od sredstev, uporabljenih znotraj Evropske unije¹³, morajo biti v sistemu, skladnem z evropskim, vključeni naslednji elementi:

1) Pristojni neodvisni nadzorni organ

Obstajati mora eden ali več neodvisnih nadzornih organov, ki spremljajo, zagotavljajo in izvršujejo skladnost z določbami varstva podatkov in zasebnosti v tretji državi. Nadzorni organ pri izvajanju svojih dolžnosti in pooblastil ravna popolnoma neodvisno in nepristransko ter pri tem ne prosi za navodila niti jih ne sprejema. V zvezi s tem bi moral imeti nadzorni organ vsa potrebna in razpoložljiva pooblastila in pristojnosti, da zagotovi skladnost s pravicami glede varstva podatkov in spodbuja ozaveščenost. Obravnavati bi bilo treba tudi osebje in proračun nadzornega organa. Nadzorni organ ima tudi možnost, da na lastno pobudo izvaja preiskave.

2) Sistem varstva podatkov mora zagotoviti ustrezno raven skladnosti

Sistem tretje države bi moral zagotoviti visoko stopnjo odgovornosti in 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 uveljavljanje teh pravic. Obstoj učinkovitih in odvračilnih sankcij ter nedvomno tudi sistemi neposrednega preverjanja s strani organov, revizorjev ali neodvisnih pooblaščenih oseb za varstvo osebnih podatkov imajo lahko pomembno vlogo pri zagotavljanju upoštevanja pravil.

3) Odgovornost

Okvir za varstvo podatkov v tretji državi bi moral upravljavce podatkov in/ali tiste, ki v njihovem imenu obdelujejo osebne podatke, zavezati k temu, da upoštevajo ta okvir in da lahko dokažejo tako skladnost,

¹³ Sodba Sodišča z dne 6. oktobra 2015 v zadevi Maximillian Schrems proti Data Protection Commissioner (C-362/14) (točka 74).

zlasti pristojnemu nadzornemu organu. Taki ukrepi lahko na primer vključujejo ocene učinka v zvezi z varstvom podatkov, vodenje evidenc ali dnevnikov o dejavnostih obdelave podatkov v ustreznem obdobju, imenovanje pooblaščenih oseb za varstvo podatkov ter vgrajeno in privzeto varstvo podatkov.

4) S sistemom varstva podatkov je treba zagotoviti podporo in pomoč posameznikom, na katere se nanašajo osebni podatki, pri uveljavljanju njihovih pravic ter ustrezne mehanizme sodnega varstva

Posamezniki bi morali imeti možnost, da za uveljavljanje svojih pravic in zagotovitev skladnosti uporabijo pravna sredstva hitro in učinkovito ter brez previsokih stroškov. 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.

Kadar se predpisi ne upoštevajo, bi se moralo posamezniku, na katerega se nanašajo osebni podatki, zagotoviti tudi učinkovito upravno in sodno varstvo, 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.

Poglavje 4: Bistvena jamstva v tretjih državah, ki se uporabljajo za dostop za namene kazenskega pregona in nacionalne varnosti, da se omejijo posegi v temeljne pravice

Komisija mora pri ocenjevanju ustreznosti ravni varstva v skladu s členom 45(2)(a) Splošne uredbe o varstvu podatkov upoštevati „ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje [...]“.

Sodišče je v zadevi Schrems navedlo, da je treba „izraz ‚ustrezna raven varstva‘ razumeti tako, da se z njim zahteva, da ta tretja država zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti dejansko zagotavlja raven varstva temeljnih svoboščin in pravic, ki je v bistvenem enaka ravni, zagotovljeni v Uniji na podlagi Direktive 95/46, razlagani ob upoštevanju Listine“. Čeprav so sredstva, ki jih ta tretja država uporabi za zagotovitev take ravni varstva, lahko drugačna od sredstev, uporabljenih v Evropski uniji, se morajo ta sredstva v praksi vseeno izkazati kot učinkovita¹⁴.

V zvezi s tem je Sodišče kritično ugotovilo, da prejšnja odločba o varnem pristanu „ne vsebuje nobene ugotovitve glede tega, ali v Združenih državah obstajajo državni predpisi, katerih namen bi bil omejiti morebitne posege v temeljne pravice posameznikov, katerih podatki se prenašajo iz Unije v Združene države, posege, ki naj bi jih državni subjekti v tej državi lahko izvajali, kadar poskušajo doseči legitimne cilje, kot je nacionalna varnost“.

Delovna skupina iz člena 29 je v mnenju WP 237, sprejetem 13. aprila 2016, opredelila bistvena jamstva, ki odražajo sodno prakso Sodišča in Evropskega sodišča za človekove pravice na področju nadzora. Priporočila, podrobno opisana v mnenju WP 237, so še vedno veljavna in bi jih bilo treba upoštevati pri ocenjevanju ustreznosti sistema tretje države na področju nadzora, uporaba teh jamstev pa se lahko na področju dostopa do podatkov za namene kazenskega pregona in nacionalne varnosti razlikuje. Da bi se raven varstva tretjih držav štela za ustrezno, pa morajo pri dostopu do podatkov tako za namene nacionalne varnosti kot za namene kazenskega pregona vseeno upoštevati naslednja štiri jamstva:

- 1) obdelava bi morala temeljiti na jasnih, natančnih in dostopnih predpisih (pravna podlaga);**
- 2) dokazati je treba nujnost in sorazmernost v zvezi z opredeljenimi zakonsko utemeljenimi cilji;**
- 3) obdelavo podatkov je treba neodvisno nadzirati;**
- 4) posameznikom morajo biti na voljo učinkovita pravna sredstva.**

¹⁴ Glej sodbo Sodišča z dne 6. oktobra 2015 v zadevi Maximillian Schrems proti Data Protection Commissioner (C-362/14) (točka 74).